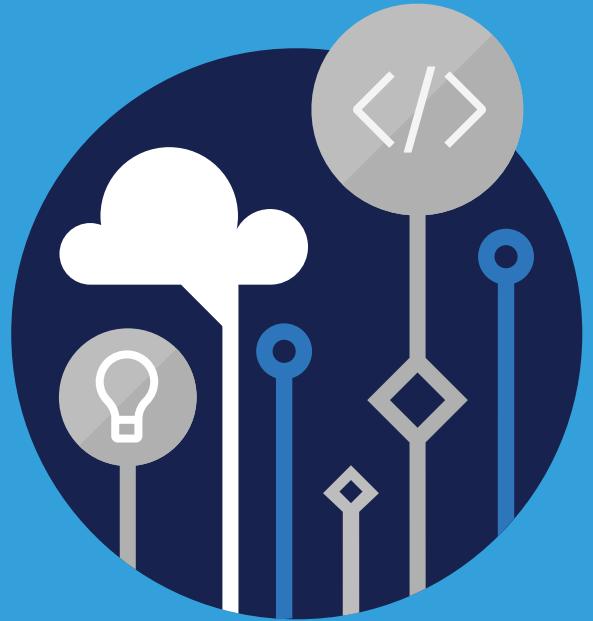


Microsoft  
Official  
Course



**AZ-303T00**

Microsoft Azure Architect  
Technologies

**AZ-303T00**  
**Microsoft Azure Architect  
Technologies**

---

## 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><sup>1</sup> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

---

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

## MICROSOFT LICENSE TERMS

### MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

#### 1. DEFINITIONS.

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

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

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

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

**2. If you are a Microsoft Learning Competency Member:**

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

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

**3. If you are a MPN Member:**

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

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

**4. If you are an End User:**

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

**5. If you are a Trainer.**

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

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

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

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

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

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

This limitation applies to

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

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

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

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

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

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

Cette limitation concerne:

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

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

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

Revised April 2019



# Contents

■	<b>Module 0 Welcome</b>	1
	Start Here	1
■	<b>Module 1 Implement Azure Active Directory</b>	11
	Overview of Azure Active Directory	11
	Create Management Groups, Subscriptions, and Resource Groups	15
	Users and Groups	21
	Domains and Custom Domains	31
	Azure AD Identity Protection	37
	Implement Conditional Access	38
	Configure Multi-Factor Authentication	45
	Configure Trusted IPs	55
	Configure Guest Users in Azure AD	59
	Module 1 Review Questions	68
■	<b>Module 2 Implement and Manage Hybrid Identities</b>	71
	Hybrid Identity	71
	Install and Configure Azure AD Connect	77
	Configure Password Sync and Password Writeback	85
	Configure Azure AD Connect Health	91
	Module 2 Review Questions	95
■	<b>Module 3 Implement Virtual Networking</b>	97
	Virtual Networking	97
	Virtual Network Peering	102
	Implement VNet Peering	106
	Module 3 Review Questions	112
■	<b>Module 4 Implement VMs for Windows and Linux</b>	115
	Overview - Running Linux and Windows Virtual Machines on Azure	115
	Configure High Availability	123
	Deploy and Configure Scale Sets	126
	Implement Azure Dedicated Hosts	133
	Configure Azure Disk Encryption	137
	Module 4 Review Questions	139
■	<b>Module 5 Implement Load Balancing and Network Security</b>	145
	Implement Azure Load Balancer	145

Implement an Application Gateway .....	160
Web Application Firewall .....	165
Implement Azure Front Door .....	173
Implementing Azure Traffic Manager .....	177
Implement Azure Firewall .....	182
Implement Network Security Groups and Application Security Groups .....	187
Implement Azure Bastion .....	191
Module 5 Review Questions .....	196
Lab .....	198
<b>Module 6 Implement Storage Accounts .....</b>	<b>203</b>
Storage Accounts .....	203
Blob Storage .....	211
Storage Security .....	217
Accessing Blobs and Queues using AAD .....	225
Configure Azure Storage Firewalls and Virtual Networks .....	228
Managing Storage .....	235
Lab .....	240
Module 6 Review Questions .....	243
<b>Module 7 Implement NoSQL Databases .....</b>	<b>251</b>
Configure Storage Account Tables .....	251
Select Appropriate CosmosDB APIs .....	255
Module 7 Review Questions .....	266
<b>Module 8 Implement Azure SQL Databases .....</b>	<b>269</b>
Configure Azure SQL Database Settings .....	269
Implement Azure SQL Database Managed Instances .....	278
High-Availability and Azure SQL Database .....	286
Module 8 Review Questions .....	289
<b>Module 9 Automate Deployment and Configuration of Resources .....</b>	<b>293</b>
Azure Resource Manager Templates .....	293
Save a Template for a VM .....	300
Configure a Virtual Hard Disk Template .....	301
Deploy from a Template .....	312
Create and Execute an Automation Runbook .....	319
Module 9 Review Questions .....	332
<b>Module 10 Implement and Manage Azure Governance Solutions .....</b>	<b>335</b>
Overview of Role-Based Access Control (RBAC) .....	335
Role-Based Access Control (RBAC) Roles .....	340
Azure AD Access Reviews .....	349
Implement and Configure an Azure Policy .....	352
Azure Blueprints .....	358
Lab .....	363
Module 10 Review Questions .....	365
<b>Module 11 Manage Security for Applications .....</b>	<b>369</b>
Azure Managed Identity .....	369
Azure Key Vault .....	372
Module 11 Review Questions .....	381
<b>Module 12 Manage Workloads in Azure .....</b>	<b>385</b>
Migrate Workloads using Azure Migrate .....	385

VMware - Agentless Migration .....	390
VMware - Agent-Based Migration .....	406
Implement Azure Backup .....	421
Azure to Azure Site Recovery .....	427
Lab .....	437
Module 12 Review Questions .....	439
<b>Module 13 Implement Container-Based Applications</b> .....	443
Configure Azure Kubernetes Service .....	443
Azure Container Instances .....	448
Module 13 Review Questions .....	453
<b>Module 14 Implement an Application Infrastructure</b> .....	457
Create and Configure Azure App Service .....	457
Create an App Service Web App for Containers .....	467
Create and Configure an App Service Plan .....	473
Configure Networking for an App Service .....	478
Create and Manage Deployment Slots .....	483
Implement Azure Functions .....	486
Implement Logic Apps .....	493
Labs .....	505
Module 14 Review Questions .....	509
<b>Module 15 Implement Cloud Infrastructure Monitoring</b> .....	513
Azure Infrastructure Security Monitoring .....	513
Azure Monitor .....	529
Azure Alerts .....	535
Log Analytics .....	540
Network Watcher .....	546
Azure Service Health .....	555
Azure Workbooks .....	565
Azure Application Insights .....	571
Unified Monitoring in Azure .....	577
Monitor Azure Costs .....	593
Module 15 Review Questions .....	596



# Module 0 Welcome

## Start Here

### About this Course

#### AZ-303: Microsoft Azure Architect Technologies

This course teaches Solutions Architects how to translate business requirements into secure, scalable, and reliable solutions. Lessons include virtualization, automation, networking, storage, identity, security, data platform, and application infrastructure. This course outlines how decisions in each these areas affects an overall solution.

**Level:** Advanced

### Audience

This course is for IT Professionals with expertise in designing and implementing solutions running on Microsoft Azure. They should have broad knowledge of IT operations, including networking, virtualization, identity, security, business continuity, disaster recovery, data platform, budgeting, and governance. Azure Solution Architects use the Azure Portal and as they become more adept they use the Command Line Interface.

Candidates must have expert-level skills in Azure administration and have experience with Azure development processes and DevOps processes.

### Prerequisites

Successful Azure Architect students have prior experience with operating systems, virtualization, cloud infrastructure, storage structures, and networking:

- Understanding of on-premises virtualization technologies, including VMs and virtual networking
- 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, and domain controllers

If you are new to Azure and cloud computing, consider one of the following resources:

- Free online: Azure Fundamentals (<https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals/>)

## Expected learning

- Secure identities with Azure Active Directory and users and groups.
- Implement identity solutions spanning on-premises and cloud-based capabilities
- Apply monitoring solutions for collecting, combining, and analyzing data from different sources.
- Manage subscriptions, accounts, Azure policies, and Role-Based Access Control.
- Deploy globally distributed elastic database solutions with Azure Cosmos DB.
- Administer Azure using the Resource Manager, Azure portal, Cloud Shell, Azure PowerShell, CLI, and ARM templates.
- Configure intersite connectivity solutions like VNet Peering, virtual network gateways, and Site-to-Site VPN connections.
- Manage network traffic using network routing and service endpoints, Azure load balancer, and Azure Application Gateway.
- Implement, manage and secure Azure storage accounts and blob storage.
- Administer Azure App Service, Azure Container Instances, and Kubernetes.

## Syllabus

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

### Module 1: Implement Azure Active Directory

- Lesson 1: Overview of Azure Active Directory
- Lesson 2: Create Management Groups, Subscriptions, and Resource Groups
- Lesson 3: Users and Groups
- Lesson 4: Configure Fraud Alerts for MFA
- Lesson 5: Domains and Custom Domains
- Lesson 6: Azure AD Identity Protection
- Lesson 7: Implement Conditional Access
- Lesson 8: Configure Trusted IPs
- Lesson 9: Configure Guest Users in Azure AD
- Lesson 10: Module 1 Review Questions

### Module 2: Implement and Manage Hybrid Identities

- Lesson 1: Install and Configure Azure AD Connect
- Lesson 2: Configure Password Sync and Password Writeback
- Lesson 3: Configure Azure AD Connect Health

- 
- Lesson 4: Module 2 Review Questions

### **Module 3: Implement Virtual Networking**

- Lesson 1: Virtual Networking
- Lesson 2: Virtual Network Peering
- Lesson 3: Implement VNet Peering
- Lesson 4: Module 3 Review Questions

### **Module 4: Implement VMs for Windows and Linux**

- Lesson 1: Overview Running Linux and Windows Virtual Machines on Azure
- Lesson 2: Select Virtual Machine Size
- Lesson 3: Configure High Availability
- Lesson 4: Implement Azure Dedicated Hosts
- Lesson 5: Deploy and Configure Scale Sets
- Lesson 6: Configure Azure Disk Encryption
- Lesson 7: Module 4 Review Questions

### **Module 5: Implement Load Balancing and Network Security**

- Lesson 1: Implement Azure Load Balancer
- Lesson 2: Implement an Application Gateway
- Lesson 3: Web Application Firewall
- Lesson 4: Implement Azure Firewall
- Lesson 5: Implement Azure Front Door
- Lesson 6: Implementing Azure Traffic Manager
- Lesson 7: Implement Network Security Groups and Application Security Groups
- Lesson 8: Implement Azure Bastion
- Lesson 9: Module 5 Review Questions

### **Module 6: Implement Storage Accounts**

- Lesson 1: Storage Accounts
- Lesson 2: Blob Storage
- Lesson 3: Storage Security
- Lesson 4: Managing Storage
- Lesson 5: Accessing Blobs and Queues using AAD
- Lesson 6: Configure Azure Storage Firewalls and Virtual Networks
- Lesson 7: Module 6 Review Questions

### **Module 7: Implement NoSQL Databases**

- Lesson 1: Configure Storage Account Tables
- Lesson 2: Select Appropriate CosmosDB APIs
- Lesson 3: Module 7 Review Questions

**Module 8: Implement Azure SQL Databases**

- Lesson 1: Configure Azure SQL Database Settings
- Lesson 2: Implement Azure SQL Database Managed Instances
- Lesson 3: High-Availability and Azure SQL Database
- Lesson 4: Module 8 Review Questions

**Module 9: Automate Deployment and Configuration of Resources**

- Lesson 1: Azure Resource Manager Templates
- Lesson 2: Save a Template for a VM
- Lesson 3: Evaluate Location of New Resources
- Lesson 4: Configure a Virtual Hard Disk Template
- Lesson 5: Deploy from a Template
- Lesson 6: Create and Execute an Automation Runbook
- Lesson 7: Module 9 Review Questions

**Module 10: Implement and Manage Azure Governance Solutions**

- Lesson 1: Overview of Role-Based Access Control (RBAC)
- Lesson 2: Role-Based Access Control (RBAC) Roles
- Lesson 3: Azure AD Access Reviews
- Lesson 4: Implement and Configure an Azure Policy
- Lesson 5: Azure Blueprints
- Lesson 6: Lab
- Lesson 7: Module 10 Review Questions

**Module 11: Manage Security for Applications**

- Lesson 1: Azure Key Vault
- Lesson 2: Azure Managed Identity
- Lesson 3: Module 11 Review Questions

**Module 12: Manage Workloads in Azure**

- Lesson 1: Migrate Workloads using Azure Migrate
- Lesson 2: VMware Agentless Migration
- Lesson 3: VMware Agent-Based Migration
- Lesson 4: Implement Azure Backup
- Lesson 5: Azure to Azure Site Recovery
- Lesson 6: Implement Azure Update Management
- Lesson 7: Lab
- Lesson 8: Module 12 Review Questions

**Module 13: Implement Container-Based Applications**

- Lesson 1: Azure Container Instances

- Lesson 2: Configure Azure Kubernetes Service
- Lesson 3: Module 13 Review Questions

#### **Module 14: Implement an Application Infrastructure**

- Lesson 1: Create and Configure Azure App Service
- Lesson 2: Create an App Service Web App for Containers
- Lesson 3: Create and Configure an App Service Plan
- Lesson 4: Configure Networking for an App Service
- Lesson 5: Create and Manage Deployment Slots
- Lesson 6: Implement Logic Apps
- Lesson 7: Implement Azure Functions
- Lesson 8: Labs
- Lesson 9: Module 14 Review Questions

#### **Module 15: Implement Cloud Infrastructure Monitoring**

- Lesson 1: Azure Infrastructure Security Monitoring
- Lesson 2: Azure Monitor
- Lesson 3: Azure Workbooks
- Lesson 4: Azure Alerts
- Lesson 5: Log Analytics
- Lesson 6: Network Watcher
- Lesson 7: Azure Service Health
- Lesson 8: Monitor Azure Costs
- Lesson 9: Azure Application Insights
- Lesson 10: Unified Monitoring in Azure
- Lesson 11: Module 15 Review Questions

## **AZ-303 Certification Exam**

The AZ-303, **Microsoft Azure Architect Technologies<sup>1</sup>**, certification exam is geared towards Azure Solutions Architect candidates who advise stakeholders and translate business requirements into secure, scalable, and reliable solutions.

Candidates should have advanced experience and knowledge of IT operations, including networking, virtualization, identity, security, business continuity, disaster recovery, data platform, budgeting, and governance. This role requires managing how decisions in each area affects an overall solution.

The exam includes four 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.

<b>AZ-303 Study Areas</b>	<b>Weights</b>
Implement and Monitor an Azure Infrastructure	50-55%

<sup>1</sup> <https://docs.microsoft.com/en-us/learn/certifications/exams/az-303>

AZ-303 Study Areas	Weights
Implement Management and Security Solutions	25-30%
Implement Solutions for Apps	10-15%
Implement and Manage Data Platforms	10-15%

## Microsoft Learn

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

### Module 01 - Identity

- **Create Azure users and groups in Azure Active Directory<sup>2</sup>**
- **Manage users and groups in Azure Active Directory<sup>3</sup>**
- **Secure your Azure resources with role-based access control<sup>4</sup>**
- **Secure Azure Active Directory users with Multi-Factor Authentication<sup>5</sup>**
- **Allow users to reset their password with Azure Active Directory self-service password reset<sup>6</sup>**
- **Secure your application by using OpenID Connect and Azure AD<sup>7</sup>**

### Module 02 - Governance and Compliance

- **Analyze costs and create budgets with Azure Cost Management<sup>8</sup>**
- **Predict costs and optimize spending for Azure<sup>9</sup>**
- **Control and organize Azure resources with Azure Resource Manager<sup>10</sup>**
- **Apply and monitor infrastructure standards with Azure Policy<sup>11</sup>**
- **Create custom roles for Azure resources with role-based access control<sup>12</sup>**
- **Manage access to an Azure subscription by using Azure role-based access control<sup>13</sup>**
- **Secure your Azure resources with role-based access control<sup>14</sup>**

### Module 03 - Azure Administration

- **Core Cloud Services - Manage services with the Azure portal<sup>15</sup>**
- **Control and organize Azure resources with Azure Resource Manager<sup>16</sup>**

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Build Azure Resource Manager templates<sup>17</sup>
- Automate Azure tasks using scripts with PowerShell<sup>18</sup>
- Manage virtual machines with the Azure CLI<sup>19</sup>

## Module 04 - Virtual Networking

- Networking Fundamentals - Principals<sup>20</sup>
- Design an IP addressing schema for your Azure deployment<sup>21</sup>
- Secure and isolate access to Azure resources by using network security groups and service endpoints<sup>22</sup>

## Module 05 - Intersite Connectivity

- Distribute your services across Azure virtual networks and integrate them by using virtual network peering<sup>23</sup>
- Connect your on-premises network to Azure with VPN Gateway<sup>24</sup>
- Connect your on-premises network to the Microsoft global network by using ExpressRoute<sup>25</sup>

## Module 06 - Network Traffic Management

- Manage and control traffic flow in your Azure deployment with routes<sup>26</sup>
- Improve application scalability and resiliency by using Azure Load Balancer<sup>27</sup>
- Load balance your web service traffic with Application Gateway<sup>28</sup>
- Enhance your service availability and data locality by using Azure Traffic Manager<sup>29</sup>

## Module 07 - Azure Storage

- Create an Azure Storage account<sup>30</sup>
- Secure your Azure Storage<sup>31</sup>
- Optimize storage performance and costs using Blob storage tiers<sup>32</sup>
- Make your application storage highly available with read-access geo-redundant storage<sup>33</sup>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Copy and move blobs from one container or storage account to another from the command line and in code<sup>34</sup>**
- **Move large amounts of data to the cloud by using Azure Data Box family<sup>35</sup>**
- **Monitor, diagnose, and troubleshoot your Azure storage<sup>36</sup>**

## Module 08 - Azure Virtual Machines

- **Build a scalable application with virtual machine scale sets<sup>37</sup>**
- **Deploy Azure virtual machines from VHD templates<sup>38</sup>**
- **Choose the right disk storage for your virtual machine workload<sup>39</sup>**
- **Add and size disks in Azure virtual machines<sup>40</sup>**
- **Protect your virtual machine settings with Azure Automation State Configuration<sup>41</sup>**

## Module 09 - Serverless Computing

- **Host a web application with Azure App service<sup>42</sup>**
- **Stage a web app deployment for testing and rollback by using App Service deployment slots<sup>43</sup>**
- **Scale an App Service web app to efficiently meet demand with App Service scale up and scale out<sup>44</sup>**
- **Dynamically meet changing web app performance requirements with autoscale rules<sup>45</sup>**
- **Capture and view page load times in your Azure web app with Application Insights<sup>46</sup>**
- **Run Docker containers with Azure Container Instances<sup>47</sup>**
- **Introduction to the Azure Kubernetes Service<sup>48</sup>**

## Module 10 - Data Protection

- **Protect your virtual machines by using Azure Backup<sup>49</sup>**
- **Back up and restore your Azure SQL database<sup>50</sup>**
- **Protect your Azure infrastructure with Azure Site Recovery<sup>51</sup>**

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Protect your on-premises infrastructure from disasters with Azure Site Recovery<sup>52</sup>

## Module 11 - Monitoring

- Analyze your Azure infrastructure by using Azure Monitor logs<sup>53</sup>
- Improve incident response with alerting on Azure<sup>54</sup>
- Monitor the health of your Azure virtual machine by collecting and analyzing diagnostic data<sup>55</sup>
- Monitor, diagnose, and troubleshoot your Azure storage<sup>56</sup>

## Additional Study Resources

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

- **Azure forums**<sup>57</sup>. 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 Blog**<sup>58</sup>. Get the latest information about the certification tests and exam study groups.
- **Channel 9**<sup>59</sup>. Channel 9 provides a wealth of informational videos, shows, and events.
- **Azure Tuesdays with Corey**<sup>60</sup>. Corey Sanders answers your questions about Microsoft Azure - Virtual Machines, Web Sites, Mobile Services, Dev/Test etc.
- **Azure Fridays**<sup>61</sup>. Join Scott Hanselman as he engages one-on-one with the engineers who build the services that power Microsoft Azure, as they demo capabilities, answer Scott's questions, and share their insights.
- **Microsoft Azure Blog**<sup>62</sup>. Keep current on what's happening in Azure, including what's now in preview, generally available, news & updates, and more.
- **Azure Documentation**<sup>63</sup>. Stay informed on the latest products, tools, and features. Get information on pricing, partners, support, and solutions.
- **Azure Architecture Center**<sup>64</sup>. The Azure Architecture Center provides best practices for running your workloads on Azure.
  - **Azure Reference Architectures**<sup>65</sup>. Architecture diagrams, reference architectures, example scenarios, and solutions for common workloads on Azure.

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

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

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

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

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

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

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

<sup>59</sup> <https://channel9.msdn.com/>

<sup>60</sup> <https://channel9.msdn.com/Shows/Tuesdays-With-Corey/>

<sup>61</sup> <https://channel9.msdn.com/Shows/Azure-Friday>

<sup>62</sup> <https://azure.microsoft.com/en-us/blog/>

<sup>63</sup> <https://docs.microsoft.com/en-us/azure/>

<sup>64</sup> <https://docs.microsoft.com/en-us/azure/architecture/>

<sup>65</sup> <https://docs.microsoft.com/en-us/azure/architecture/browse/>

- **Cloud Design Patterns<sup>66</sup>**. Cloud design patterns for building reliable, scalable, secure applications in the cloud.
- **Tailwind Traders<sup>67</sup>**. A three-tier legacy app re-written for modern cloud app ARM Solution]

---

<sup>66</sup> <https://docs.microsoft.com/en-us/azure/architecture/patterns/>

<sup>67</sup> <https://github.com/microsoft/ignite-learning-paths-training-ops>

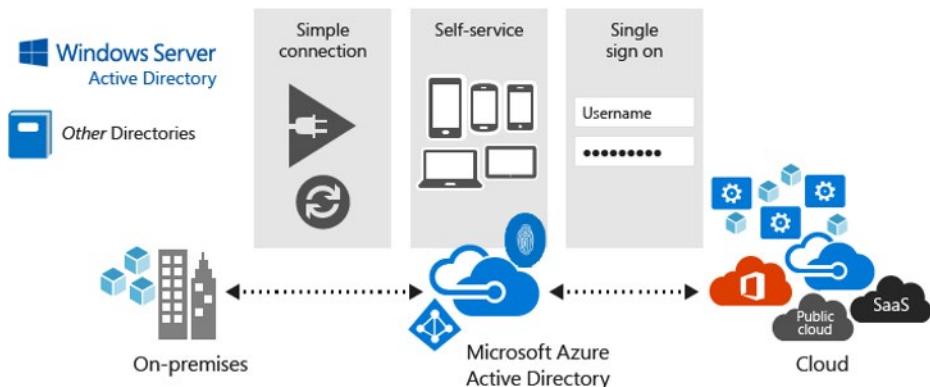
# Module 1 Implement Azure Active Directory

## Overview of Azure Active Directory

### Azure Active Directory (Azure AD)

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

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



### Benefits and features

- Single sign-on to any cloud or on-premises web app.** Azure Active Directory provides secure single sign-on to cloud and on-premises applications including Microsoft Office 365 and thousands of SaaS applications such as Salesforce, Workday, DocuSign, ServiceNow, and Box.
- Works with iOS, Mac OS X, Android, and Windows devices.** Users can launch applications from a personalized web-based access panel, mobile app, Office 365, or custom company portals using their

existing work credentials—and have the same experience whether they're working on iOS, Mac OS X, Android, and Windows devices.

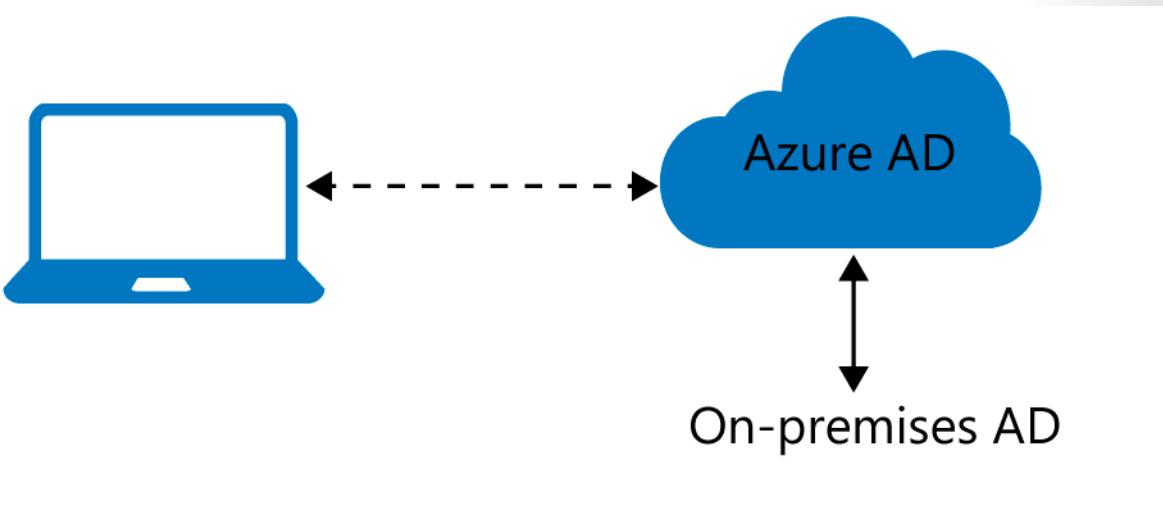
- **Protect on-premises web applications with secure remote access.** Access your on-premises web applications from everywhere and protect with multi-factor authentication, conditional access policies, and group-based access management. Users can access SaaS and on-premises web apps from the same portal.
  - **Easily extend Active Directory to the cloud.** Connect Active Directory and other on-premises directories to Azure Active Directory in just a few clicks and maintain a consistent set of users, groups, passwords, and devices across both environments.
  - **Protect sensitive data and applications.** Enhance application access security with unique identity protection capabilities that provide a consolidated view into suspicious sign-in activities and potential vulnerabilities. Take advantage of advanced security reports, notifications, remediation recommendations and risk-based policies to protect your business from current and future threats.
  - **Reduce costs and enhance security with self-service capabilities.** Delegate important tasks such as resetting passwords and the creation and management of groups to your employees. Providing self-service application access and password management through verification steps can reduce helpdesk calls and enhance security.
- ✓ If you are an Office365, Azure or Dynamics CRM Online customer, you might not realize that you are already using Azure AD. Every Office365, Azure and Dynamics CRM tenant is already an Azure AD tenant. Whenever you want you can start using that tenant to manage access to thousands of other cloud applications Azure AD integrates with.

## Azure AD Concepts

- **Identity.** A thing that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates.
- **Account.** An identity that has data associated with it. You cannot have an account without an identity.
- **Azure AD Account.** An identity created through Azure AD or another Microsoft cloud service, such as Office 365. Identities are stored in Azure AD and accessible to your organization's cloud service subscriptions. This account is also sometimes called a Work or school account.
- **Azure subscription.** Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.
- **Azure tenant.** A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription, such as Microsoft Azure, Microsoft Intune, or Office 365. An Azure tenant represents a single organization.
- **Azure AD directory.** Each Azure tenant has a dedicated and trusted Azure AD directory. The Azure AD directory includes the tenant's users, groups, and apps and is used to perform identity and access management functions for tenant resources.

## Azure AD Join

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



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

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

## Connection options

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

- **Registering** a device to Azure AD enables you to manage a device's identity. When a device is registered, Azure AD device registration provides the device with an identity that is used to authenticate the device when a user signs-in to Azure AD. You can use the identity to enable or disable a device.
  - **Joining** a device is an extension to registering a device. This means, it provides you with all the benefits of registering a device and in addition to this, it also changes the local state of a device. Changing the local state enables your users to sign-in to a device using an organizational work or school account instead of a personal account.
- ✓ Registration combined with a mobile device management (MDM) solution such as Microsoft Intune, provides additional device attributes in Azure AD. This allows you to create conditional access rules that enforce access from devices to meet your standards for security and compliance.
- ✓ Although AD Join is intended for organizations that do not have on-premises Windows Server Active Directory infrastructure it can be used for other scenarios like branch offices.

# Devices in Azure AD

Below are the following options for devices in Azure AD:

## Azure AD registered

Devices that are Azure AD registered are typically personally owned or mobile devices and are signed in with a personal Microsoft account or another local account.

- Windows 10
- iOS
- Android
- MacOS

## Azure AD joined

Devices that are Azure AD joined are owned by an organization, and are signed in with an Azure AD account belonging to that organization. They exist only in the cloud.

- Windows 10
- **Windows Server 2019 Virtual Machines running in Azure<sup>1</sup>** (Server core is not supported)

## Hybrid Azure AD joined

Devices that are hybrid Azure AD joined are owned by an organization and are signed in with an Active Directory Domain Services account belonging to that organization. They exist in the cloud and on-premises.

- Windows 7, 8.1, or 10
- Windows Server 2008 or newer

NAME	ENABLED	OS	VERSION	JOIN TYPE	OWNER	MGR
Server01	Yes	Windows Server 2016 ...	10.0 (14393)	Hybrid Azure AD joined	N/A	None
Server02	Yes	Windows Server 2019 ...	10.0 (17763)	Hybrid Azure AD joined	N/A	None
AndroidPhone	Yes	Android	6.0.1	Azure AD registered	Bala Sandhu	None
DESKTOP-F5V53FT	Yes	Windows	10.0.18362.145	Azure AD joined	Alain Charon	None

**Note:** A hybrid state refers to more than just the state of a device. For a hybrid state to be valid, a valid Azure AD user also is required.

<sup>1</sup> <https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows>

# Create Management Groups, Subscriptions, and Resource Groups

## Resource Groups

Resource groups are a fundamental element of the Azure platform. A resource group is a logical container for resources deployed on Azure. These resources are anything you create in an Azure subscription like virtual machines, Application Gateways, and CosmosDB instances.

All resources must be in a resource group and a resource can only be a member of a single resource group. Many resources can be moved between resource groups with some services having specific limitations or requirements to move.

Resource groups can't be nested. Before any resource can be provisioned, you need a resource group for it to be placed in.

### Logical grouping

Resource groups exist to help manage and organize your Azure resources. By placing resources of similar usage, type, or location, you can provide some order and organization to resources you create in Azure.



### Life cycle

If you delete a resource group, all resources contained within are also deleted.

Organizing resources by life cycle can be useful in non-production environments, where you might try an experiment, but then dispose of it when done. Resource groups make it easy to remove a set of resources at once.

## Resource Group Organization

Below are best practices for resource groups within your organization.

### Consistent naming convention

Earlier in this lesson, you named a resource group *msftlearn-core-infrastructure-rg*. The name indicates it's used for (msftlearn), the types of resources contained within (core-infrastructure), and the type of resource it is itself (rg). This descriptive name gives us a better idea of what it is.

If you had named the *group my-resource-group* or *rg1*, you have no idea on a glance of what the usage may be. In this case, you can deduce that there are probably core pieces of infrastructure contained within. If you created additional virtual networks, storage accounts, or other resources the company may consider core infrastructure, you could place them here as well, to improve the organization of our resources.

## Organizing principles

You might put all resources that are core infrastructure into this resource group. But you could also organize them strictly by resource type. For example, put all virtual networks in one resource group, all virtual machines in another resource group, and all Azure Cosmos DB instances in yet another resource group.



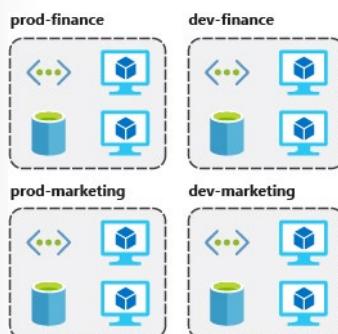
You could organize them by environment (prod, qa, dev). In this case, all production resources are in one resource group, all test resources are in another resource group, and so on.



You could organize them by department (marketing, finance, human resources). Marketing resources go in one resource group, finance in another resource group, and HR in a third resource group.



You could even use a combination of these strategies and organize by environment and department. Put production finance resources in one resource group, dev finance resources in another, and the same for the marketing resources.



## Organizing for authorization

Since resource groups are a scope of RBAC, you can organize resources by who needs to administer them. If a database administration team is responsible for managing all of your Azure SQL Database instances, putting them in the same resource group would simplify administration. You could give them the proper permissions at the resource group level to administer the databases within the resource group.

## Organizing for life cycle

If you delete a resource group, you delete all the resources in it. Use this where resources are more disposable, like non-production environments. If you deploy 10 servers for a project that you know will only last a couple of months, you might put them all in a single resource group. One resource group is easier to clean up than 10 or more resource groups.

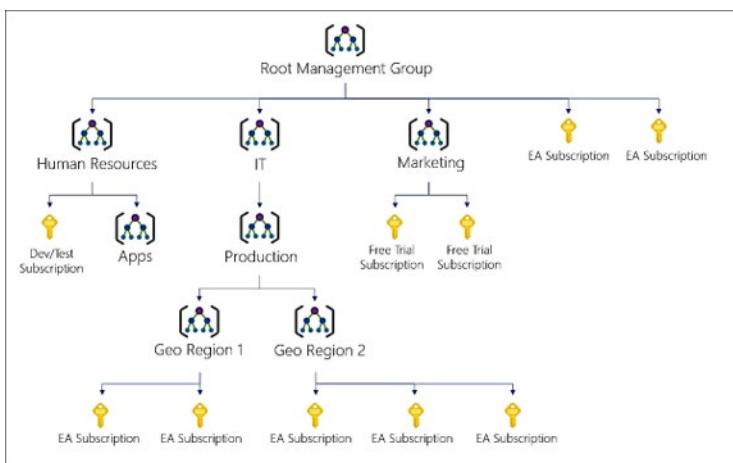
## Organizing for billing

Placing resources in the same resource group is a way to group them for usage in billing reports. If you're trying to understand how your costs are distributed in your Azure environment, grouping them by resource group is one way to filter and sort the data to better understand where costs are allocated.

## Management Groups

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

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



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

## Creating management groups

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

The screenshot shows the Azure Management Groups blade. At the top, there's a red box around the '+ New management group' button and the 'Refresh' button. Below that, the breadcrumb navigation shows 'Root Management G... > Contoso Redmond'. A search bar with the placeholder 'Search by name or ID' is followed by a magnifying glass icon and a 'X' button. To the right of the search bar is a blue tree icon representing management groups. A callout text says: 'Using management groups helps you manage access, policy, and compliance by grouping multiple subscriptions together. [Learn more.](#)' Below the search bar is a table with three rows:

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

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

For more information, [Organize your resources with Azure management groups<sup>2</sup>](#)

## Azure Subscription and Service Limits

This topic lists some of the most common Microsoft Azure limits, which are also sometimes called quotas.

### Managing limits

#### ✓ Note:

Some services have adjustable limits.

When a service doesn't have adjustable limits, the following tables use the header Limit. In those cases, the default and the maximum limits are the same.

When the limit can be adjusted, the tables include Default limit and Maximum limit headers. The limit can be raised above the default limit but not above the maximum limit.

If you want to raise the limit or quota above the default limit, [open an online customer support request at no charge<sup>3</sup>](#).

Some limits are managed at a regional level.

For example, to request a quota increase with support for vCPUs, you must decide how many vCPUs you want to use in which regions. You then make a specific request for Azure resource group vCPU quotas for the amounts and regions that you want. If you need to use 30 vCPUs in West Europe to run your application there, you specifically request 30 vCPUs in West Europe. Your vCPU quota isn't increased in any other region—only West Europe has the 30-vCPU quota.

As a result, decide what your Azure resource group quotas must be for your workload in any one region. Then request that amount in each region into which you want to deploy.

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management-groups-overview>

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/error-resource-quota>

# Subscription and Service General Limits

For limits on resource names, see [Naming rules and restrictions for Azure resources<sup>4</sup>](#).

## Management group limits

The following limits apply to management groups.

Resource	Limit
Management groups per directory	10,000
Subscriptions per management group	Unlimited.
Levels of management group hierarchy	Root level plus 6 levels <sup>1</sup>
Direct parent management group per management group	One
Management group level deployments per location	800 <sup>2</sup>

<sup>1</sup>The 6 levels don't include the subscription level.

<sup>2</sup>If you reach the limit of 800 deployments, delete deployments from the history that are no longer needed. To delete management group level deployments, use **Remove-AzManagementGroupDeployment<sup>5</sup>** or **az deployment mg delete<sup>6</sup>**.

## Subscription limits

The following limits apply when you use Azure Resource Manager and Azure resource groups.

Resource	Limit
Subscriptions per Azure Active Directory tenant	Unlimited.
Coadministrators per subscription	Unlimited.
Resource groups per subscription	980
Azure Resource Manager API request size	4,194,304 bytes.
Tags per subscription <sup>1</sup>	50
Unique tag calculations per subscription <sup>1</sup>	10,000
Subscription-level deployments per location	800 <sup>2</sup>

<sup>1</sup>You can apply up to 50 tags directly to a subscription. However, the subscription can contain an unlimited number of tags that are applied to resource groups and resources within the subscription. The number of tags per resource or resource group is limited to 50. Resource Manager returns a **list of unique tag name and values<sup>7</sup>** in the subscription only when the number of tags is 10,000 or less. You still can find a resource by tag when the number exceeds 10,000.

<sup>2</sup>If you reach the limit of 800 deployments, delete deployments from the history that are no longer needed. To delete subscription level deployments, use **Remove-AzDeployment<sup>8</sup>** or **az deployment sub delete<sup>9</sup>**.

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules>

<sup>5</sup> <https://docs.microsoft.com/en-us/powershell/module/az.resources/Remove-AzManagementGroupDeployment>

<sup>6</sup> <https://docs.microsoft.com/en-us/cli/azure/deployment/mg?view=azure-cli-latest>

<sup>7</sup> <https://docs.microsoft.com/en-us/rest/api/resources/tags>

<sup>8</sup> <https://docs.microsoft.com/en-us/powershell/module/az.resources/Remove-AzDeployment>

<sup>9</sup> <https://docs.microsoft.com/en-us/cli/azure/deployment/sub?view=azure-cli-latest>

## Resource group limits

Resource	Limit
Resources per resource group	Resources aren't limited by resource group. Instead, they're limited by resource type in a resource group. See next row.
Resources per resource group, per resource type	800 - Some resource types can exceed the 800 limit. See Resources not limited to 800 instances per resource group.
Deployments per resource group in the deployment history	800 <sup>1</sup>
Resources per deployment	800
Management locks per unique scope	20
Number of tags per resource or resource group	50
Tag key length	512
Tag value length	256

<sup>1</sup>If you reach the limit of 800 deployments per resource group, delete deployments from the history that are no longer needed. Deleting an entry from the deployment history doesn't affect the deployed resources.

## Template limits

Value	Limit
Parameters	256
Variables	256
Resources (including copy count)	800
Outputs	64
Template expression	24,576 chars
Resources in exported templates	200
Template size	4 MB
Parameter file size	64 KB

You can exceed some template limits by using a nested template.

# Users and Groups

## User accounts

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

Name	User name	User type
		Guest
	CB	Member

Typically, Azure AD defines users in three ways:

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

✓ Have you given any thought as to the type of users you will need?

## Create and Manage Users

Every user who needs access to Azure resources needs an Azure user account. A user account contains all the information needed to authenticate the user during the sign-on process. Once authenticated, Azure AD builds an access token to authorize the user and determine what resources they can access and what they can do with those resources.

You use the **Azure Active Directory** dashboard in the Azure portal to work with user objects. Keep in mind that you can only work with a single directory at a time - but you can use the **Directory + Subscription** panel to switch directories. The dashboard also has a button in the toolbar which makes it easy to switch to another available directory.

## Adding users

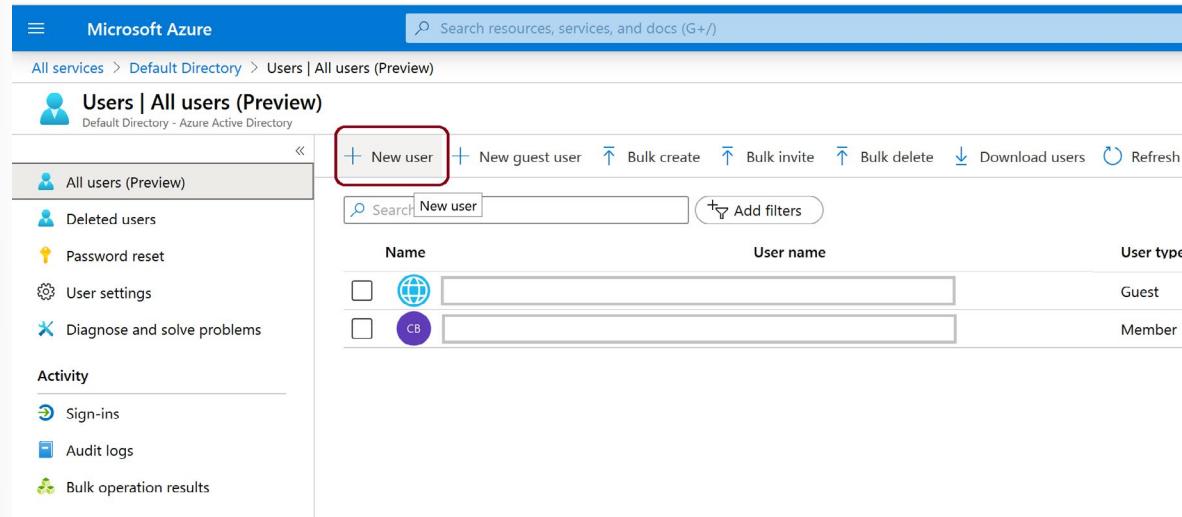
You can add users to Azure AD in multiple ways:

**Syncing an on-premises Windows Server Active Directory**

Azure AD Connect is a separate service that allows you to synchronize a traditional Active Directory with your Azure AD instance. This is how most enterprise customers add users to the directory. The advantage to this approach is users can use single-sign-on (SSO) to access local and cloud-based resources.

You can manually add new users through the Azure portal. This is the easiest way to add a small set of users. You need to be in the **User Administrator** role to perform this function.

1. To add a new user with the Azure portal, select the the **+ New user** button in the toolbar.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar. Below the header, the URL shows 'All services > Default Directory > Users | All users (Preview)'. The main area has a title 'Users | All users (Preview)' with a subtitle 'Default Directory - Azure Active Directory'. On the left, there's a sidebar with links like 'All users (Preview)', 'Deleted users', 'Password reset', 'User settings', and 'Diagnose and solve problems'. In the center, there's a toolbar with buttons for '+ New user', '+ New guest user', 'Bulk create', 'Bulk invite', 'Bulk delete', 'Download users', and 'Refresh'. Below the toolbar is a search bar with 'Search' and 'New user' placeholder text, and a 'Add filters' button. The main table lists users with columns for 'Name', 'User name', and 'User type'. Two rows are shown: one for a guest user named 'CB' and another for a member user named 'CB'. Both rows have a checkbox and a profile icon.

Name	User name	User type
<input type="checkbox"/>  CB		Guest
<input type="checkbox"/>  CB		Member

2. In addition to **Name** and **User name**, you can add profile information, like **Job Title** and **Department**.

**New user**  
Default Directory

Got feedback?

**Create user**

Create a new user in your organization.  
This user will have a user name like  
`alice@callumbrightoutlook.onmicrosoft.com`.  
[I want to create users in bulk](#)

**Invite user**

Invite a new guest user to collaborate with  
your organization. The user will be emailed  
an invitation they can accept in order to  
begin collaborating.  
[I want to invite guest users in bulk](#)

[Help me decide](#)

---

**Identity**

User name *	<input type="text" value="Example: chris"/> @ <input type="text"/> <small>The domain name I need isn't shown here</small>
Name *	<input type="text" value="Example: 'Chris Green'"/>
First name	<input type="text"/>
Last name	<input type="text"/>

---

**Groups and roles**

Groups	0 groups selected
Roles	User

---

**Settings**

Block sign in	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Usage location	<input type="text"/>

---

**Job info**

Job title	<input type="text"/>
Department	<input type="text"/>

---

[Create](#)

The default behavior is to create a new user in the organization. The user will have a username with the default domain name assigned to the directory such as alice@staracoustics.onmicrosoft.com.

3. can also *invite* a user into the directory. In this case, an email is sent to a known email address and an account is created and associated with that email address if they accept the invitation.

**New user**  
Default Directory

Got feedback?

**Create user**

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

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

**Invite user**

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

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

[Help me decide](#)

### Identity

Name	<input type="text" value="Example: 'Chris Green'"/>
Email address  *	<input type="text" value="Example: chris@contoso.com"/>
First name	<input type="text"/>
Last name	<input type="text"/>

### Personal message

### Groups and roles

Groups	0 groups selected
Roles	User

### Settings

Block sign in	<input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
Usage location	<input type="text"/>

---

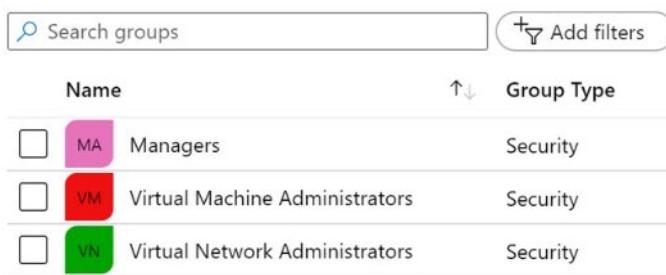
[Invite](#)

The invited user will need to create an associated Microsoft account (MSA) if that specific email address isn't associated with one and the account will be added to the Azure AD as a guest user.

## Group Accounts

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

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



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

## Adding Members to Groups

There are different ways you can assign access rights:

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

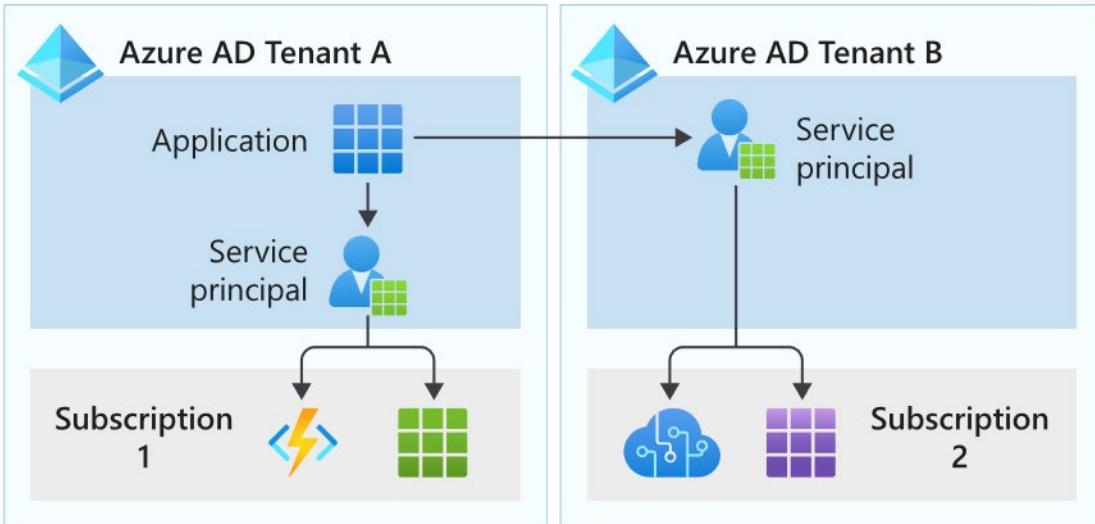
## Azure Service Principals

Think of an Azure service principal as a proxy account, or identity, that represents your app or service. This account is managed by Azure Active Directory (Azure AD). You grant the service principal access to the Azure resources that you need. Use the service principal instead of embedding credentials or creating a dummy account for your app.

Service principals exist at the tenant level in Azure. They're used to grant access to resources in that tenant.

In the Azure portal, you create an Azure AD application to represent your app. You then associate this application object with a service principal.

If all of the resources are in the same tenant, then you need to associate only one service principal. If your app needs access to Azure resources in a different tenant, then you need a service principal for each tenant.

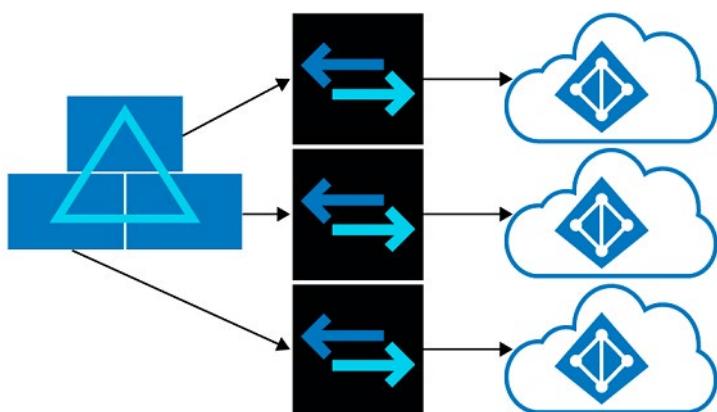


You create your service principal:

- Through the portal
- By using PowerShell
- Through CLI commands
- By using API calls

## Managing Multiple Directories

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



### Resource independence

- If you create or delete a resource in one tenant, it has no impact on any resource in another tenant, with the partial exception of external users.

- If you use one of your domain names with one tenant, it cannot be used with any other tenant.

### Administrative independence

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

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

### Synchronization independence

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

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

### Add an Azure AD tenant

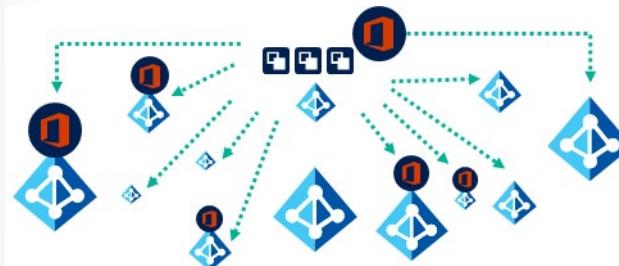
To add an Azure AD tenant in the Azure portal, sign in to the Azure portal with an account that is an Azure AD global administrator, and, on the left, select New.

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

## Azure B2B and B2C

### Azure AD B2B

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



With Azure AD B2B:

- There is no external administrative overhead for your organization.
- The partner uses their own identities and credentials; Azure AD is not required.
- You don't need to manage external accounts or passwords.
- You don't need to sync accounts or manage account lifecycles.

## Azure AD B2C

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



## With Azure AD B2C:

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

## Demonstration - Users and Groups

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

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

### Determine domain information

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

### Explore user accounts

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

### Explore group accounts

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

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

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

### Explore PowerShell for group management

1. Create a new group called Developers.

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

2. Retrieve the Developers group ObjectId.

```
Get-AzADGroup
```

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

```
Get-AzADUser
```

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

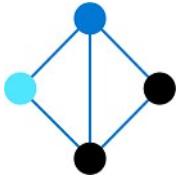
```
Add-AzADGroupMember -MemberUserPrincipalName ""myemail@domain.com"" -TargetGroupDisplayName ""MyGroupDisplayName""
```

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

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

# Domains and Custom Domains

## 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.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, a breadcrumb trail says 'All services > Default Directory | Custom domain names'. On the left, there's a sidebar with 'Overview', 'Getting started', 'Diagnose and solve problems', and a 'Manage' section containing 'Users', 'Groups', 'External Identities', 'Roles and administrators', 'Administrative units (Preview)', and 'Enterprise applications'. In the main content area, there's a 'Search (Ctrl+ /)' input, a 'Refresh' button, and a 'Troubleshoot' link. A red box highlights the 'Add custom domain' button. Below that is a 'Search domains' input and a 'Name' section. A modal window is open in the bottom right, titled 'Custom domain name' under 'Default Directory'. It has a 'Custom domain name \*' field containing 'contoso.com', which is also highlighted with a blue border.

## 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.

## Add a Custom Domain Name to Azure AD

After you create your directory, you can add your custom domain name.

1. Sign in to the **Azure portal**<sup>10</sup> using a *Global administrator* account for the directory.
2. Search for and select **Azure Active Directory** from any page. Then select **Custom domain names > Add custom domain**.

<sup>10</sup> <https://portal.azure.com/>

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the breadcrumb navigation shows "All services > Default Directory | Overview". The main title is "Default Directory | Overview" under "Azure Active Directory". On the left, a sidebar menu lists several options: "Overview", "Getting started", "Diagnose and solve problems", "Manage" (with sub-options like "Users", "Groups", "External Identities", "Roles and administrators", "Administrative units (Preview)", "Enterprise applications", "Devices", "App registrations", "Identity Governance", "Application proxy", "Licenses", "Azure AD Connect", and "Custom domain names"), and "Mobility (MDM and MAM)". The "Custom domain names" option is highlighted with a red box. The main content area has a heading "Azure Active Directory can help you enable remote work for your organization". Below it, there's a section titled "Default Directory" with a sub-section titled "Azure AD Connect" showing "Status Not enabled" and "Last sync Sync has never run".

3. In Custom domain name, enter your organization's new name, in this example, *contoso.com*. Select **Add domain**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the URL "All services > Default Directory | Custom domain names" is visible. On the left, there's a sidebar with a "Default Directory" icon and the text "Azure Active Directory". The main content area has a "Search (Ctrl+ /)" input field and a toolbar with "Add custom domain" (which is highlighted with a red box), "Refresh", and "Troubleshoot". On the left, under the "Manage" section, there are links for Overview, Getting started, Diagnose and solve problems, and several management categories: Users, Groups, External Identities, Roles and administrators, Administrative units (Preview), and Enterprise applications. In the center, there's a "Search domains" input field and a "Name" section. A modal window titled "Custom domain name" is open, showing "Default Directory" above a form field labeled "Custom domain name \*". The value "contoso.com" is entered into this field. The entire screenshot is framed by a thick black border.

**✓ Important:**

You must include .com, .net, or any other top-level extension for this to work properly.

The unverified domain is added. The contoso.com page appears showing your DNS information.

The screenshot shows the Azure portal interface for managing custom domain names. At the top, the navigation path is "All services > Default Directory | Custom domain names > az303.contoso.com". The main title is "az303.contoso.com" with the subtitle "Custom domain name". Below this are two buttons: "Delete" and "Got feedback?". A callout box contains the text: "To use az303.contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below." Under "Record type", the "TXT" option is selected. The "Alias or host name" field contains "@". The "Destination or points to address" field contains "MS=ms77751575". The "TTL" field contains "3600". A link "Share these settings via email" is present, along with a note: "Verification will not succeed until you have configured your domain with your registrar as described above."

## 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.

All services > Default Directory | Custom domain names > az303.contoso.com

## az303.contoso.com

Custom domain name

 Delete |  Got feedback?

**i** To use az303.contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

**Record type**

**TXT** **MX**

**Alias or host name**

@ 

**Destination or points to address**

MS=ms77751575 

**TTL**

3600 

[Share these settings via email](#)

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

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

## Azure AD Identity Protection

### Azure Active Directory Identity Protection

Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

#### Risk detection and remediation

Identity Protection identifies risks in the following classifications:

Risk detection type	Description
<b>Atypical travel</b>	Sign in from an atypical location based on the user's recent sign-ins.
<b>Anonymous IP address</b>	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).
<b>Unfamiliar sign-in properties</b>	Sign in with properties we've not seen recently for the given user.
<b>Malware linked IP address</b>	Sign in from a malware linked IP address
<b>Leaked Credentials</b>	This risk detection indicates that the user's valid credentials have been leaked
<b>Azure AD threat intelligence</b>	Microsoft's internal and external threat intelligence sources have identified a known attack pattern

The risk signals can trigger remediation efforts such as requiring users to: perform Azure Multi-Factor Authentication, reset their password using self-service password reset, or blocking until an administrator takes action.

#### Risk investigation

Administrators can review detections and take manual action on them if needed. There are three key reports that administrators use for investigations in Identity Protection:

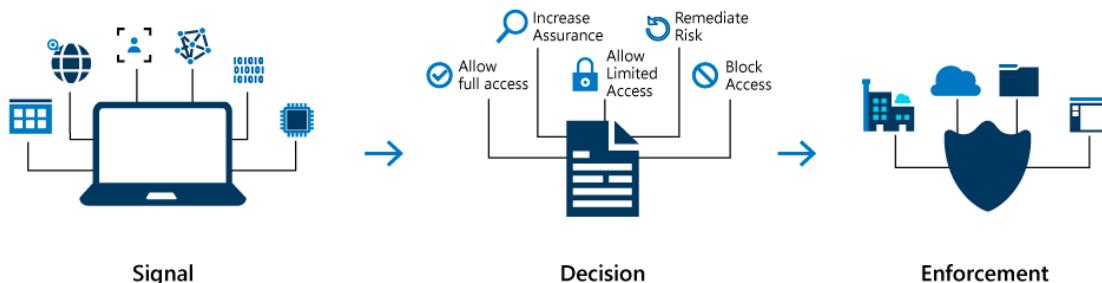
- Risky users
- Risky sign-ins
- Risk detections

# Implement Conditional Access

## Overview of Conditional Access

The modern security perimeter now extends beyond an organization's network to include user and device identity. Organizations can utilize these identity signals as part of their access control decisions.

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.



Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

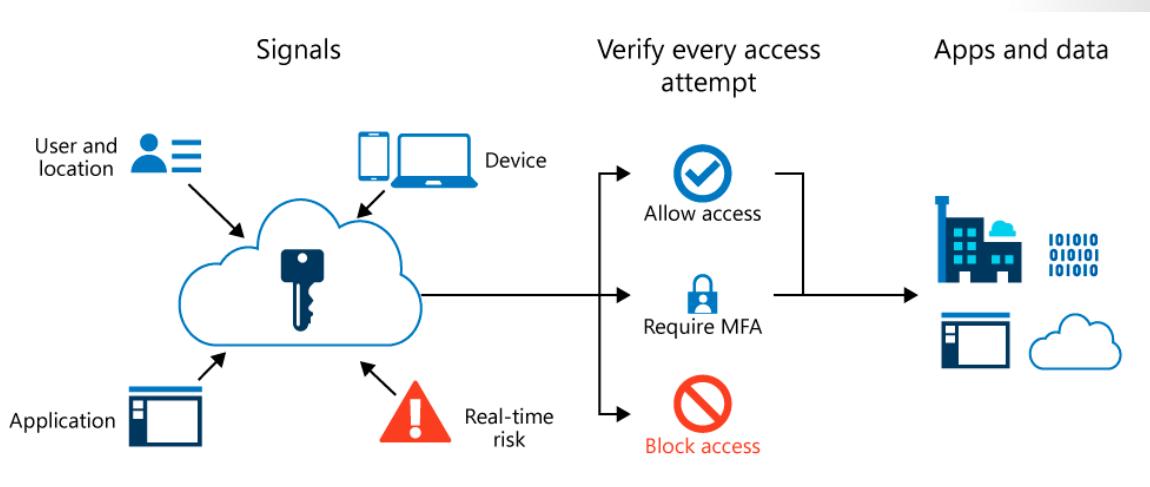
By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.

Conditional Access policies are enforced after the first-factor authentication has been completed. Conditional Access is not intended as an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but can use signals from these events to determine access.

## Conditional Access and Azure Multi-Factor Authentication

Users and groups can be enabled for Azure Multi-Factor Authentication to prompt for additional verification during the sign-in event. Security defaults are available for all Azure AD tenants to quickly enable the use of the Microsoft Authenticator app for all users.

For more granular controls, Conditional Access policies can be used to define events or applications that require MFA. These policies can allow regular sign-in events when the user is on the corporate network or a registered device, but prompt for additional verification factors when remote or on a personal device.



## Conditional Access - Signals and Decisions

Common signals that Conditional Access can take in to account when making a policy decision include the following signals:

### User or group membership

- Policies can be targeted to specific users and groups giving administrators fine-grained control over access.

### IP Location information

- Organizations can create trusted IP address ranges that can be used when making policy decisions.
- Administrators can specify entire countries IP ranges to block or allow traffic from.

### Device

- Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

### Application

- Users attempting to access specific applications can trigger different Conditional Access policies.

### Real-time and calculated risk detection

- Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to perform password changes or multi-factor authentication to reduce their risk level or be blocked from access until an administrator takes manual action.

### Microsoft Cloud App Security (MCAS)

- Enables user application access and sessions to be monitored and controlled in real time, increasing visibility and control over access to and activities performed within your cloud environment.

## Common Decisions

### Block access

- Most restrictive decision

### Grant access

Least restrictive decision, can still require one or more of the following options:

- Require multi-factor authentication
- Require device to be marked as compliant
- Require Hybrid Azure AD joined device
- Require approved client app
- Require app protection policy (preview)

## Common Applied Policies

Many organizations have common access concerns that Conditional Access policies can help with such as:

- Requiring multi-factor authentication for users with administrative roles
- Requiring multi-factor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Requiring trusted locations for Azure Multi-Factor Authentication registration
- Blocking or granting access from specific locations
- Blocking risky sign-in behaviors
- Requiring organization-managed devices for specific applications

## Demonstration - Secure user sign-in events with Azure Multi-Factor Authentication

Multi-factor authentication (MFA) is a process where a user is prompted during a sign-in event for additional forms of identification. This prompt could be to enter a code on their cellphone or to provide a fingerprint scan. When you require a second form of authentication, security is increased as this additional factor isn't something that's easy for an attacker to obtain or duplicate.

Azure Multi-Factor Authentication and Conditional Access policies give the flexibility to enable MFA for users during specific sign-in events.

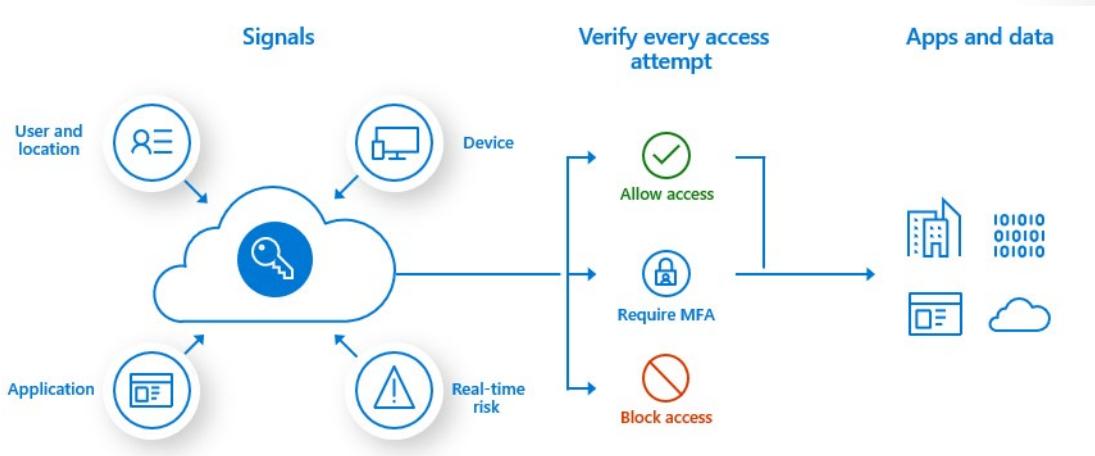
### Prerequisites

To perform this demonstration you need the following resources and privileges:

- A working Azure AD tenant with Azure AD Premium or trial license enabled.
- An account with global administrator privileges.
- A non-administrator user with a password you know, such as *testuser*. You test the end-user Azure Multi-Factor Authentication experience using this account in this demonstration.
- A group that the non-administrator user is a member of, such as MFA-Test-Group. You enable Azure Multi-Factor Authentication for this group in this demonstration.

## Create a Conditional Access Policy

The recommended way to enable and use Azure Multi-Factor Authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

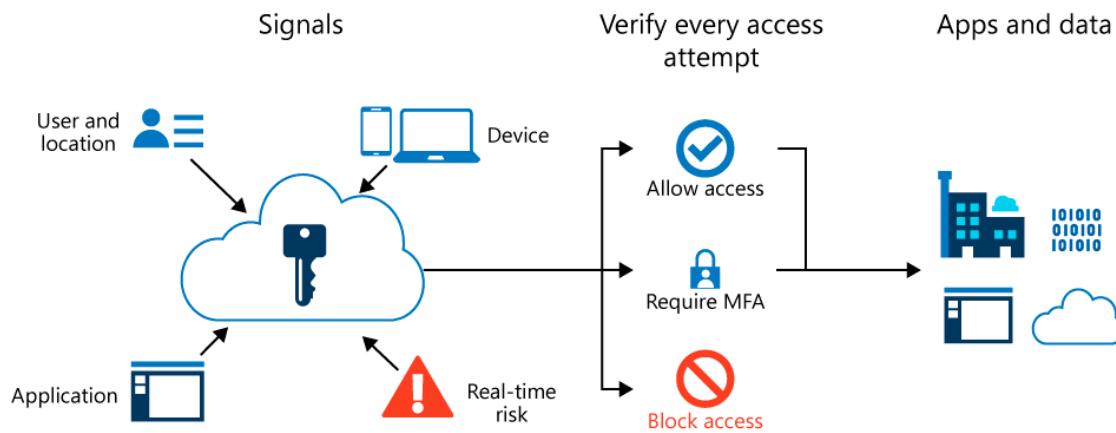


In this demonstration you will create a basic Conditional Access policy to prompt for MFA when a user signs in to the Azure portal.

First, create a Conditional Access policy and assign your test group of users as follows:

1. Sign in to the [Azure portal<sup>11</sup>](https://portal.azure.com/) using an account with global administrator permissions.
2. Search for and select **Azure Active Directory**, then choose **Security**.
3. Select **Conditional Access**, then choose **+ New policy**.
4. Enter a name for the policy, such as *MFA Pilot*.
5. Under **Assignments**, choose **Users and groups**, then **Select users and groups**.
6. Check the box for **Users and groups**, then **Select**.
7. Browse for and select your Azure AD group, such as *MFA-Test-Group*, then choose **Select**.

<sup>11</sup> <https://portal.azure.com/>



8. To apply the Conditional Access policy for the group, select **Done**.

## Configure the conditions for Multi-Factor Authentication

With the Conditional Access policy created and a test group of users assigned, now define the cloud apps or actions that trigger the policy. These cloud apps or actions are the scenarios you decide require additional processing, such as to prompt for MFA.

Configure the Conditional Access policy to require MFA when a user signs in to the Azure portal.

1. Select **Cloud apps or actions**. You can choose to apply the Conditional Access policy to *All cloud apps* or *Select apps*.

On the Include page, choose Select apps.

2. Choose **Select**, then browse the list of available sign-in events that can be used.

Choose **Microsoft Azure Management** so the policy applies to sign-in events to the Azure portal.

3. To apply the select apps, choose **Select**, then **Done**.

The screenshot shows the 'New' blade for creating a Conditional Access policy. In the center, under 'Cloud apps or actions', it says 'Select what this policy applies to' with options for 'Cloud apps' (selected) and 'User actions'. Below that are 'Include' and 'Exclude' buttons, and radio buttons for 'None', 'All cloud apps', and 'Select apps', with 'Select apps' selected. A 'Select' button leads to a modal dialog on the right. This dialog lists 'Applications' with checkboxes: GE (Graph explorer), Microsoft Azure Information Protec..., MA (Microsoft Azure Linux Virtual Mach...), MA (Microsoft Azure Management) which is checked, Microsoft Cloud App Security, Microsoft Intune, Microsoft Intune Enrollment, and Microsoft OneDrive. At the bottom of the list is 'Selected Microsoft Azure Management' with a 'Select' button.

Access controls let you define the requirements for a user to be granted access, such as needing an approved client app or using a device that's Hybrid Azure AD joined. Configure the access controls to require MFA during a sign-in event to the Azure portal.

1. Under **Access controls**, choose **Grant**, then make sure that **Grant access** is selected.
2. Check the box for **Require multi-factor authentication**, then choose **Select**.

Conditional Access policies can be set to Report-only if you want to see how the configuration would impact users, or Off if you don't want to use the policy right now. As a test group of users was targeted for this demonstration, let's enable the policy and then test Azure Multi-Factor Authentication.

1. Set the *Enable policy* to **On**.
2. To apply the *Conditional Access policy*, select **Create**.

## Test Azure Multi-Factor Authentication

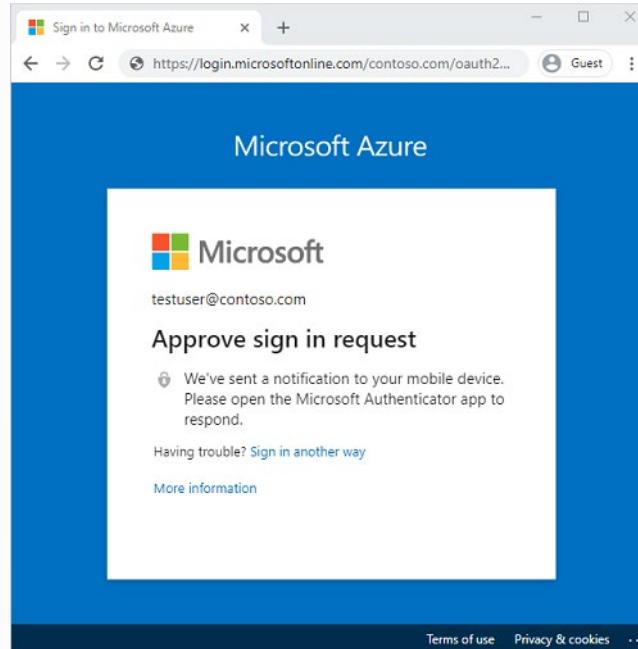
To view the Conditional Access policy and Azure Multi-Factor Authentication sign in to a resource that doesn't require MFA as follows:

1. Open a new browser window in InPrivate or incognito mode and browse to <https://account.activedirectory.windowsazure.com><sup>12</sup>
2. Sign in with your non-administrator test user, such as testuser. There's no prompt for you to complete MFA.
3. Close the browser window.

<sup>12</sup> <https://account.activedirectory.windowsazure.com/>

Now sign in to the Azure portal. As the Azure portal was configured in the Conditional Access policy to require additional verification, you get an Azure Multi-Factor Authentication prompt.

1. Open a new browser window in InPrivate or incognito mode and browse to <https://portal.azure.com><sup>13</sup>.
2. Sign in with your non-administrator test user, such as testuser. You're required to register for and use Azure Multi-Factor Authentication. Follow the prompts to complete the process and verify you successfully sign in to the Azure portal.



---

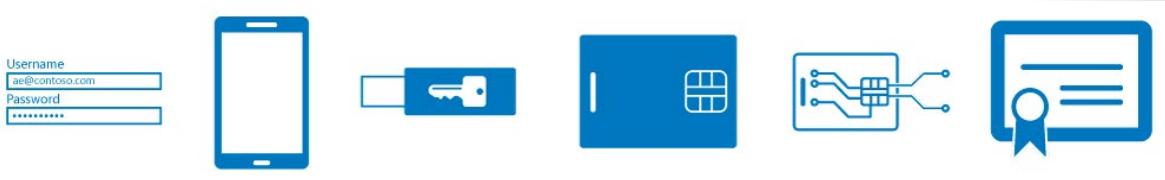
<sup>13</sup> <https://portal.azure.com/>

# Configure Multi-Factor Authentication

## Azure Multi-Factor Authentication

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

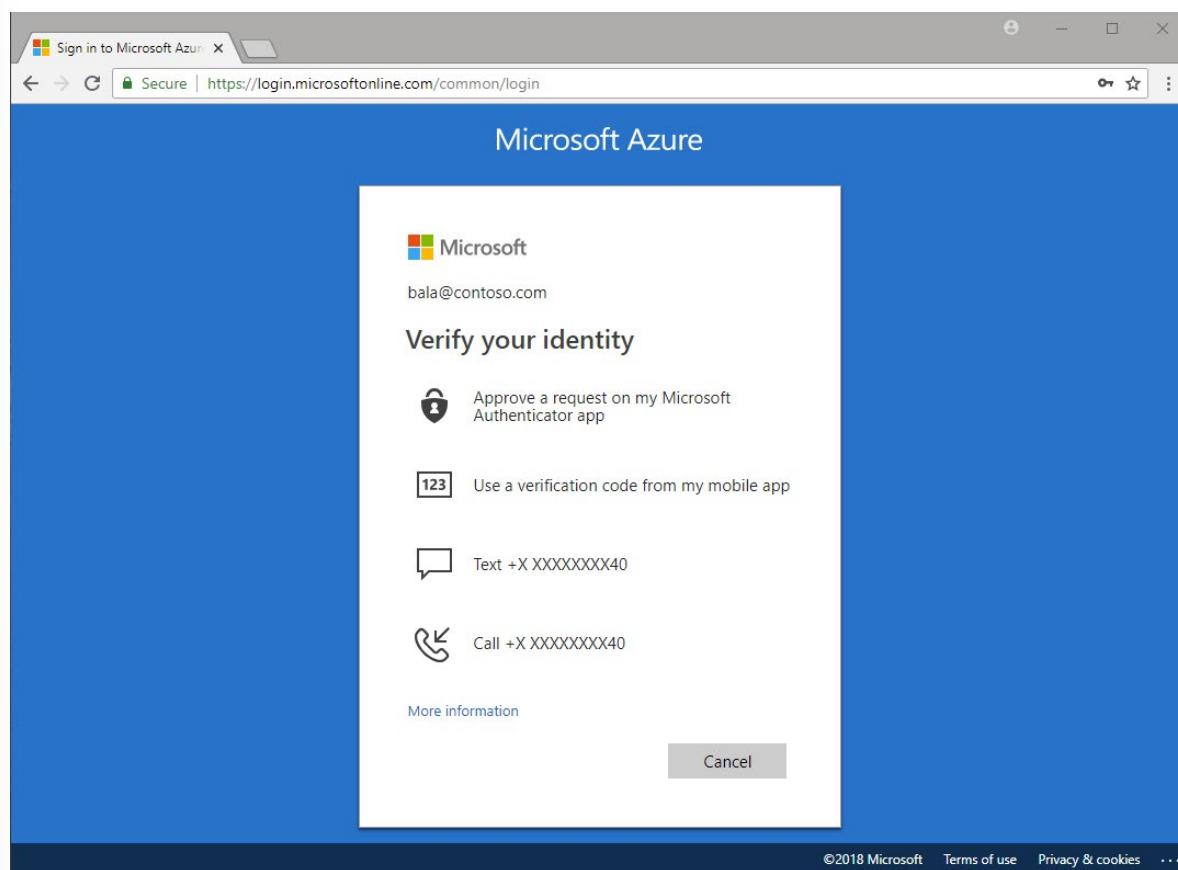
If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or has been exposed elsewhere, is it really the user signing in with the username and password, or is it an attacker? When you require a second form of authentication, security is increased as this additional factor isn't something that's easy for an attacker to obtain or duplicate.



Azure Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password.
- Something you have, such as a trusted device that is not easily duplicated, like a phone or hardware key.
- Something you are - biometrics like a fingerprint or face scan.

Users can register themselves for both self-service password reset and Azure Multi-Factor Authentication in one step to simplify the on-boarding experience. Administrators can define what forms of secondary authentication can be used. Azure Multi-Factor Authentication can also be required when users perform a self-service password reset to further secure that process.



Azure Multi-Factor Authentication provides additional security by requiring a second form of authentication and delivers strong authentication using a range of use authentication methods.

Users may or may not be challenged for MFA based on configuration decisions that an administrator makes.

Applications or services don't need to make any changes to use Azure Multi-Factor Authentication. The verification prompts are part of the Azure AD sign-in event, which automatically requests and processes the MFA challenge when required.

## Available verification methods

When a user signs in to an application or service and receive an MFA prompt, they can choose from one of their registered forms of additional verification. An administrator could require registration of these Azure Multi-Factor Authentication verification methods, or the user can access their own My Profile to edit or add verification methods.

The following additional forms of verification can be used with Azure Multi-Factor Authentication:

- Microsoft Authenticator app
- OATH Hardware token
- SMS

## Authentication Methods

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

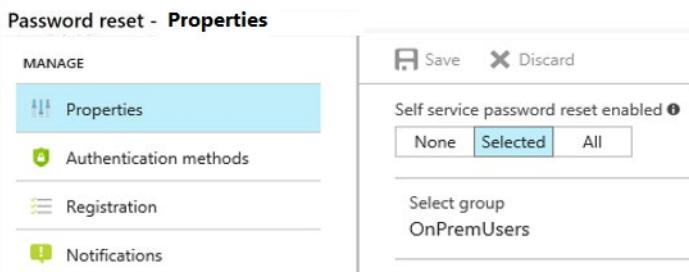
- ✓ There is also a selection to cache passwords so that users do not have to authenticate on trusted devices. The number of days before a user must re-authenticate on trusted devices can also be configured with the value from 1 to 60 days. The default is 14 days.

## 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**.



## 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' configuration page. On the left, there's a sidebar with various management options like 'Properties', 'Authentication methods', 'Registration', etc. The 'Authentication methods' tab is currently active. In the main pane, it says 'Number of methods required to reset' is set to 1. Below that, under 'Methods available to users', several options are listed with checkboxes: 'Mobile app notification' (unchecked), 'Mobile app code' (unchecked), 'Email' (checked), 'Mobile phone' (checked), 'Office phone' (unchecked), and 'Security questions' (checked). Further down, there are two more sliders for 'Number of questions required to register' (set to 5) and 'Number of questions required to reset' (set to 5). At the bottom, a box highlights 'Select security questions' and '5 security questions selected'.

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

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

## Configure Azure MFA Settings

This topic describes where to manage Multi-Factor Authentication settings in the Azure portal.

You access to Azure Multi-Factor Authentication settings by browsing to **Azure Active Directory**, and Select **Security**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G)". Below the header, the breadcrumb navigation shows "Home > Default Directory | Overview". The main title is "Default Directory | Overview" with a blue info icon. A sub-header "Azure Active Directory" is visible. On the left, a sidebar menu has several items: "Overview" (selected), "Getting started", "Diagnose and solve problems", "Manage" (selected), "Users", "Groups", "Organizational relationships", "Roles and administrators (Pr...)", "Administrative units (Preview)", "Enterprise applications", "Devices", "App registrations", "Identity Governance", "Application proxy", "Licenses", "Azure AD Connect", "Custom domain names", "Mobility (MDM and MAM)", "Password reset", "Company branding", "User settings", "Properties", and "Security". The "Security" item is highlighted with a red rounded rectangle. The main content area has a "Switch directory", "Delete directory", and "Create" buttons at the top right. A message box says "Azure Active Directory can help you enable remote". Below it, the "Overview" section is titled "Default Directory". It shows a "Tenant ID" section with a "Not enabled" status for "Azure AD Connect". The "Sign-ins" section shows a single entry for "Mar 29". At the bottom, there are "Create" and "User" buttons, and "Other capabilities" like "Identity Protection".

**Select MFA.**

The screenshot shows the Microsoft Azure portal's "Security | Getting started" page. On the left, there's a sidebar with various navigation links. One link, "MFA", is highlighted with a red box. The main content area discusses security features like Conditional Access, Identity Protection, and Security Center. It also lists several items under "Documentation", including "Azure AD Conditional Access", "Azure AD Identity Protection", "Azure Security Center", "Identity Secure Score", "Named locations", "Authentication methods", and "Multi Factor Authentication (MFA)". Below this, there's a section titled "Security guidance" with a blue info icon, which recommends steps for a strong security posture.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Default Directory > Security | Getting started

Security | Getting started

Search (Ctrl+ /) <<

Getting started

Protect

- Conditional Access
- Identity Protection
- Security Center

Manage

- Identity Secure Score
- Named locations
- Authentication methods

MFA

Report

- Risky users
- Risky sign-ins

Troubleshooting + Support

- New support request

Got feedback?

- Documentation

Azure Active Directory offers a range of security features to protect your organization.

- Azure AD Conditional Access
- Azure AD Identity Protection
- Azure Security Center
- Identity Secure Score
- Named locations
- Authentication methods
- Multi Factor Authentication (MFA)

i Security guidance

For a strong security posture, we recommend the following:

- 5 steps to secure your identity infrastructure
- Azure AD Password Guidance
- Azure AD Data Security Whitepaper
- How Password Hash Sync (PHS) works

Configure **Settings**.

## Settings

The following settings apply to MFA Server, Azure MFA, or both.

Feature	Description
Account lockout	Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate. (MFA Server)
Block/unblock users	Used to block specific users from being able to receive Multi-Factor Authentication requests. Any authentication attempts for blocked users are automatically denied. Users remain blocked for 90 days from the time that they are blocked.
Fraud alert	Configure settings related to users ability to report fraudulent verification requests
Notifications	Enable notifications of events from MFA Server.

Feature	Description
OATH tokens	Used in cloud-based Azure MFA environments to manage OATH tokens for users.
Phone call settings	Configure settings related to phone calls and greetings for cloud and on-premises environments.
Providers	This will show any existing authentication providers that you may have associated with your account.

## Reports for Azure Multi-Factor Authentication

Azure Multi-Factor Authentication provides reports available in the Azure portal.

The reports are summarized in the following table:

Report	Location	Description
<b>Blocked User History</b>	Azure AD > Security > MFA > Block/unblock users	Shows the history of requests to block or unblock users.
<b>Usage and fraud alerts</b>	Azure AD > Sign-ins	Provides information on overall usage, user summary, and user details; as well as a history of fraud alerts submitted during the date range specified.
<b>Usage for on-premises components</b>	Azure AD > Security > MFA > Activity Report	Provides information on overall usage for MFA through the NPS extension, ADFS, and MFA server.
<b>Bypassed User History</b>	Azure AD > Security > MFA > One-time bypass	Provides a history of requests to bypass Multi-Factor Authentication for a user.
<b>Server status</b>	Azure AD > Security > MFA > Server status	Displays the status of Multi-Factor Authentication Servers associated with your account.

## View the MFA Reports

1. Sign in to the [Azure portal<sup>14</sup>](https://portal.azure.com/).
2. Select **Azure Active Directory > Security > MFA**.
3. See **Reports**.

<sup>14</sup> <https://portal.azure.com/>

The screenshot shows the Microsoft Azure Multi-Factor Authentication Activity report interface. On the left, there's a sidebar with links like 'Getting started', 'Diagnose and solve problems', 'Settings' (with sub-links for 'Account lockout', 'Block/unblock users', 'Fraud alert', 'Notifications', 'OATH tokens', 'Phone call settings', and 'Providers'), 'Manage MFA Server' (with sub-links for 'Server settings', 'One-time bypass', 'Caching rules', and 'Server status'), and 'Reports' (with 'Activity report' highlighted by a red box). The main area has filters for 'Time interval' (set to 'Last 24 hours') and 'Authentication mode' (set to 'All'). It displays a table with columns 'Date/Time' and 'Username', showing 'No results'.

## Azure AD Sign-ins Report

The Azure Sign-ins report provides information on managed applications and user sign-in activities, which includes information about MFA usage.

The MFA data provides insights into how MFA is working in your organization and answer questions like:

- Was the sign-in challenged with MFA?
- How did the user complete MFA?
- Why was the user unable to complete MFA?
- How many users are challenged for MFA?
- How many users are unable to complete the MFA challenge?
- What are the common MFA issues end users are running into?

This data is available through the Azure portal and the reporting API.

Microsoft Azure

Contoso - Sign-ins

Search resources, services, and docs

User Application Sign-in status

Conditional Access All

Date Show dates as: Local UTC

Last 7 days

Apply Reset

DATE	USER	APPLICATION	SIGN-IN STATUS	CONDITIONAL ACC...	MFA REQUIRED
7/29/2018, 11:26:37 PM	Bala Sandhu	Azure Portal	Success	Not Applied	Yes
7/26/2018, 5:21:00 PM	Bala Sandhu	Azure Portal	Success	Not Applied	Yes
7/26/2018, 3:54:00 PM	Tommy Weber	Microsoft App Acces...	Success	Not Applied	Yes
7/26/2018, 3:53:46 PM	Tommy Weber	Microsoft App Acces...	Success	Not Applied	No

ACTIVITY

Sign-ins

Audit logs

TROUBLESHOOTING + SUPPORT

Troubleshoot

Sign-In Info Device Info MFA Conditional Access

Request Id	IP address
3cab366a-5abc-4d2f-acf8-xxxxxx5d0200	192.168.160.79

Correlation Id	Location
xxxxxc8-c2xd-4f21-a606-c8fec4072061	Sammamish, Washington, US

User	Date
Tommy Weber	7/26/2018, 3:54:00 PM

Username	Sign-in status
tommy@contoso.com	Success

User ID	Client App	Browser
xxxxxe2-66xd-4fd2-a3a0-e1f9d828e07c		

Application	
Microsoft App Access Panel	

Application ID
0000000c-0000-0000-c000-000000000000

# Configure Trusted IPs

## Azure AD Conditional Access Location Condition

With Azure Active Directory (Azure AD) Conditional Access, you can control how authorized users can access your cloud apps. The location condition of a Conditional Access policy enables you to tie access controls settings to the network locations of your users.

This lesson provides you with the information you need to configure the location condition.

### Locations

Azure AD enables single sign-on to devices, apps, and services from anywhere on the public internet. With the location condition, you can control access to your cloud apps based on the network location of a user. Common use cases for the location condition are:

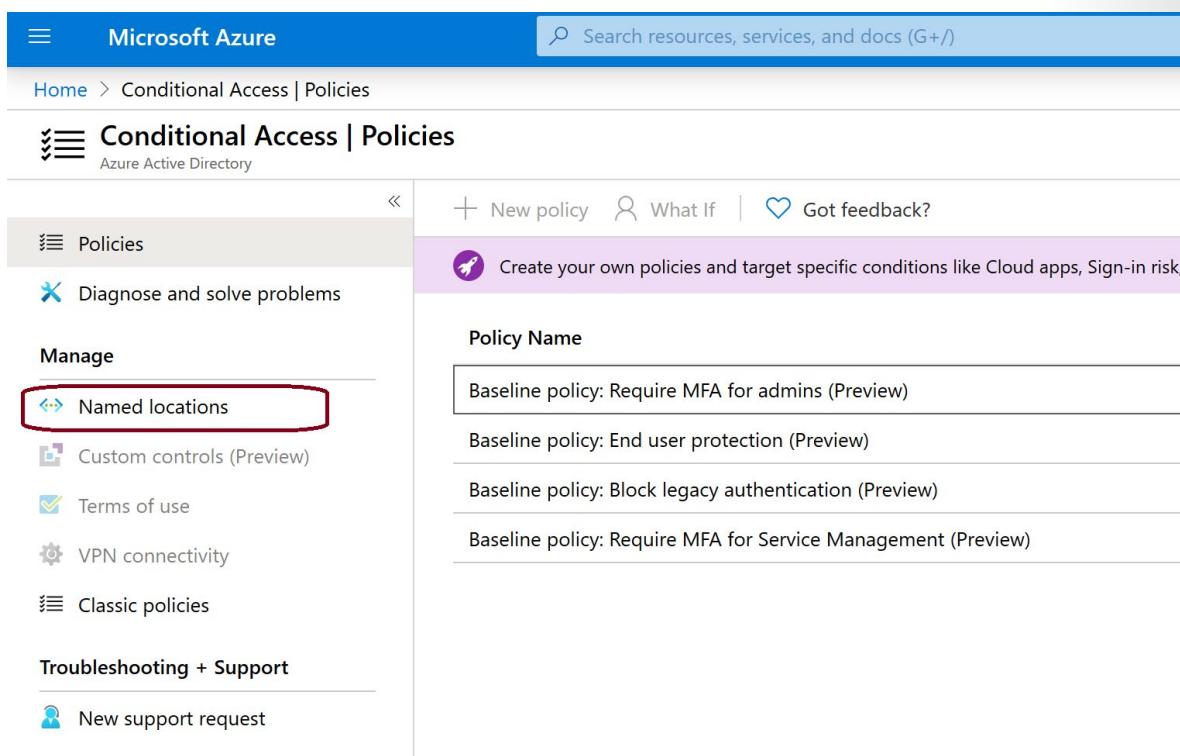
- Requiring multi-factor authentication for users accessing a service when they are off the corporate network.
- Blocking access for users accessing a service from specific countries or regions.

A location is a label for a network location that either represents a named location or multi-factor authentication Trusted IPs.

### Named locations

With named locations, you can create logical groupings of IP address ranges or countries and regions.

You can access your named locations in the Manage section of the Conditional Access page.



The screenshot shows the Microsoft Azure Conditional Access Policies page. The left sidebar has a 'Manage' section with 'Named locations' highlighted with a red box. The main area shows a list of policies:

- Baseline policy: Require MFA for admins (Preview)
- Baseline policy: End user protection (Preview)
- Baseline policy: Block legacy authentication (Preview)
- Baseline policy: Require MFA for Service Management (Preview)

At the top right, there are buttons for 'New policy', 'What If', and 'Got feedback?'. A purple banner says 'Create your own policies and target specific conditions like Cloud apps, Sign-in risk'.

A named location has the following components:

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the navigation path is "Home > Conditional Access | Named locations > New named location". The main title is "New named location". There are two buttons at the top left: "Upload" with an upward arrow icon and "Download" with a downward arrow icon. The first section is labeled "Name \*". A text input field contains the placeholder "Example: 'Redmond office'". Below this, the instruction "Define the location using:" is followed by two radio button options: "IP ranges" (which is selected) and "Countries/Regions". There's also a checkbox labeled "Mark as trusted location" with a help icon. The next section is titled "IP ranges" and contains a text input field with the placeholder "Add a new IP range (ex: 40.77.182.32/27)" and a three-dot ellipsis button. Below this is a link "No IP ranges".

- **Name** - The display name of a named location.
- **IP ranges** - One or more IPv4 address ranges in CIDR format. Specifying an IPv6 address range is not supported.

✓ **Note:**

IPv6 address ranges cannot currently be included in a named location. This means IPv6 ranges cannot be excluded from a Conditional Access policy. IPv6 ranges are only supported in the Named location (preview) interface.

- **Mark as trusted location** - A flag you can set for a named location to indicate a trusted location. Typically, trusted locations are network areas that are controlled by your IT department. In addition to Conditional Access, trusted named locations are also used by Azure Identity Protection and Azure AD security reports to reduce **false positives**<sup>15</sup>.
- **Countries/Regions** - This option enables you to select one or more country or region to define a named location.
- **Include unknown areas** - Some IP addresses are not mapped to a specific country or region. This option allows you to choose if these IP addresses should be included in the named location. Use this setting when the policy using the named location should apply to unknown locations.

The number of named locations you can configure is constrained by the size of the related object in Azure AD. You can configure locations based on the following limitations:

- One named location with up to 1200 IP ranges.
- A maximum of 90 named locations with one IP range assigned to each of them.

<sup>15</sup> <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events>

Conditional Access policy applies to IPv4 and IPv6 traffic. Currently named locations do not allow IPv6 ranges to be configured. This limitation causes the following situations:

- Conditional Access policy cannot be targeted to specific IPv6 ranges
- Conditional Access policy cannot exclude specific IPv6 ranges (NOTE: IPv6 ranges are only supported in the Named location (preview) interface.)

## Trusted IPs

You can also configure IP address ranges representing your organization's local intranet in the multi-factor authentication service settings. This feature enables you to configure up to 50 IP address ranges. The IP address ranges are in CIDR format.

If you have Trusted IPs configured, they show up as MFA Trusted IPs in the list of locations for the location condition.

## Skipping multi-factor authentication

On the multi-factor authentication service settings page, you can identify corporate intranet users by selecting Skip multi-factor authentication for requests from federated users on my intranet. This setting indicates that the inside corporate network claim, which is issued by AD FS, should be trusted and used to identify the user as being on the corporate network.

After checking this option, including the named location MFA Trusted IPs will apply to any policies with this option selected.

For mobile and desktop applications, which have long lived session lifetimes, Conditional Access is periodically reevaluated. The default is once an hour. When the inside corporate network claim is only issued at the time of the initial authentication, Azure AD may not have a list of trusted IP ranges. In this case, it is more difficult to determine if the user is still on the corporate network:

1. Check if the user's IP address is in one of the trusted IP ranges.
2. Check whether the first three octets of the user's IP address match the first three octets of the IP address of the initial authentication. The IP address is compared with the initial authentication when the inside corporate network claim was originally issued and the user location was validated.

If both steps fail, a user is no longer on a trusted IP.

## Location Condition Configuration

When you configure the location condition, you have the option to distinguish between:

- Any location
- All trusted locations
- Selected locations

The screenshot shows the Microsoft Azure Conditional Access Policies blade. The URL is https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/ConditionalAccessBlade/Policies. The page title is 'Conditional Access | Policies > New > Conditions > Locations'. The 'Locations' section is highlighted with a red border. It contains the following configuration:

- Configure:** Yes (selected)
- Include:** Any location (radio button selected)
- Select:** None

The 'Conditions' section lists several conditions that are not configured:

- Sign-in risk
- Device platforms
- Locations
- Client apps (Preview)
- Device state (Preview)

The 'New' section shows the configuration for the policy:

- Name:** Example: 'Device compliance app poli'
- Assignments:**
  - Users and groups: 0 users and groups selected
  - Cloud apps or actions: No cloud apps or actions sele...
  - Conditions: 0 conditions selected

## Any location

By default, selecting Any location causes a policy to be applied to all IP addresses, which means any address on the Internet. This setting is not limited to IP addresses you have configured as named location. When you select Any location, you can still exclude specific locations from a policy. For example, you can apply a policy to all locations except trusted locations to set the scope to all locations, except the corporate network.

## All trusted locations

This option applies to:

- All locations that have been marked as trusted location
- MFA Trusted IPs (if configured)

## Selected locations

With this option, you can select one or more named locations. For a policy with this setting to apply, a user needs to connect from any of the selected locations. When you click Select the named network selection control that shows the list of named networks opens. The list also shows if the network location has been marked as trusted. The named location called MFA Trusted IPs is used to include the IP settings that can be configured in the multi-factor authentication service setting page.

# Configure Guest Users in Azure AD

## Add Guest users to Azure AD in the Azure Portal

You can invite anyone to collaborate with your organization by adding them to your directory as a guest user. Then you can either send an invitation email that contains a redemption link or send a direct link to an app you want to share.

Guest users can sign in with their own work, school, or social identities.

In this demonstration, you'll add a new guest user to Azure AD and send an invitation.

### Prerequisites

To complete the scenario in this demonstration, you need:

- A role that allows you to create users in your tenant directory, like the Global Administrator role or any of the limited administrator directory roles.
- A valid email account that you can add to your tenant directory, and that you can use to receive the test invitation email.

## Add Guest Users to Azure AD

1. Sign in to the **Azure portal<sup>16</sup>** as an Azure AD administrator.
2. In the left pane, select **Azure Active Directory**.
3. Under **Manage**, select **Users**.

<sup>16</sup> <https://portal.azure.com/>

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and d...". Below the header, the breadcrumb navigation shows "Home > Default Directory | Overview". The main title is "Default Directory | Overview" with a blue info icon. To the right of the title are "Switch directory" and "Delete directory" buttons. A search bar with "Search (Ctrl+ /)" placeholder text is also present. On the left, there's a sidebar with sections like "Overview", "Getting started", and "Diagnose and solve problems". Under "Manage", the "Users" option is highlighted with a red oval, while other options like "Groups", "Organizational relationships", and "Roles and administrators" are shown below it. The main content area has a heading "Default Directory" and a sub-section "Overview". A callout box on the right says "Azure Active Directory can help you enable".

4. Select **New guest user**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+)". Below the header, the navigation path is "Home > Default Directory > Users | All users (Preview)". The main title is "Users | All users (Preview)" under "Default Directory - Azure Active Directory". On the left, there's a sidebar with links like "All users (Preview)", "Deleted users", "Password reset", "User settings", and "Diagnose and solve problems". Below that is a section for "Activity" with "Sign-ins", "Audit logs", and "Bulk operation results". At the bottom of the sidebar is a "Troubleshooting + Support" section with "New support request". On the right, there's a "Name" search bar and three buttons at the top: "New user", "New guest user" (which is highlighted with a red box), and "Bulk create". A "Search users" input field is also present.

5. On the **New user** page, select **Invite user** and add the guest user's information.

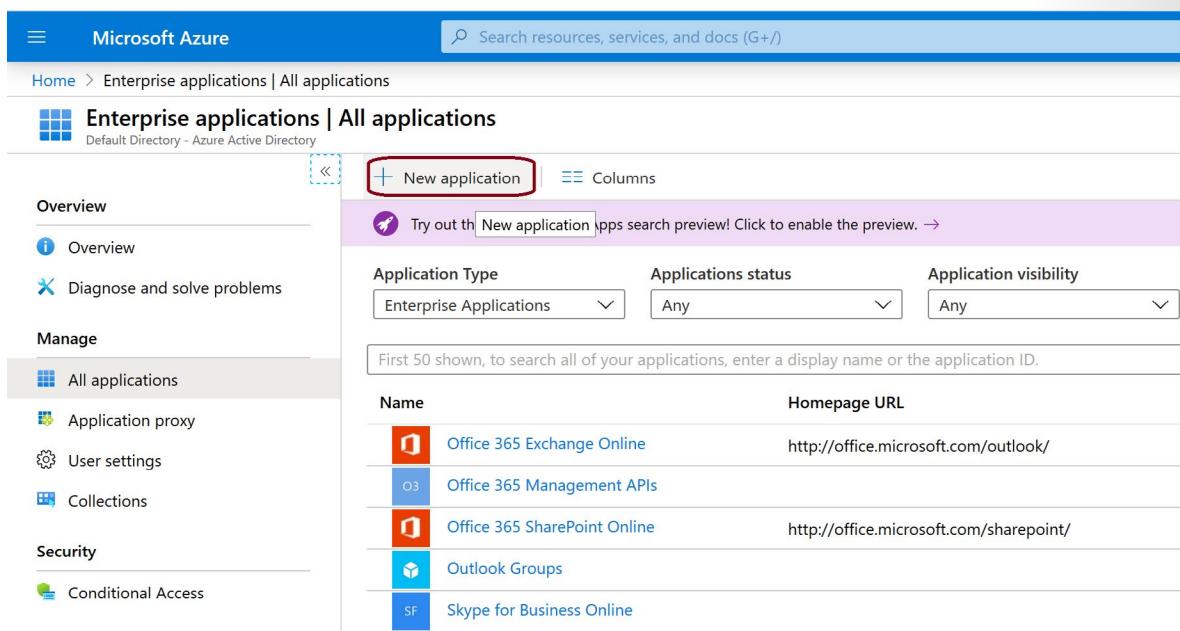
The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/UsersBlade/~/NewUserBlade](#). The page title is "New user". The "Identity" section is visible, containing fields for Name, Email address, First name, and Last name.

- **Name** The first and last name of the guest user.
  - **Email address (required)** The email address of the guest user.
  - **Personal message (optional)** Include a personal welcome message to the guest user.
  - **Groups** You can add the guest user to one or more existing groups, or you can do it later.
  - **Directory role** If you require Azure AD administrative permissions for the user, you can add them to an Azure AD role.
6. Select **Invite** to automatically send the invitation to the guest user. A notification appears in the upper right with the message Successfully invited user.
7. After you send the invitation, the user account is automatically added to the directory as a guest.

## Assign an App to a Guest User

Add the *Active Directory for GitHub Enterprise* app to your test tenant and assign the test guest user to the app.

1. Sign in to the Azure portal as an Azure AD administrator.
2. In the left pane, select **Enterprise applications**.
3. Select **New application**.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the URL "Home > Enterprise applications | All applications" is visible. The main title is "Enterprise applications | All applications" with a subtitle "Default Directory - Azure Active Directory". On the left, there's a sidebar with sections: Overview (with "Overview" and "Diagnose and solve problems" buttons), Manage (with "All applications" selected, showing a list of applications like Office 365 Exchange Online, Office 365 Management APIs, etc.), User settings, Collections, Security, and Conditional Access. At the top right, there's a "New application" button with a plus sign, which is highlighted with a red box. Below it are filter options for "Application Type" (set to "Enterprise Applications"), "Applications status" (set to "Any"), and "Application visibility" (set to "Any"). A note says "First 50 shown, to search all of your applications, enter a display name or the application ID." The main area displays a table of applications:

Name	Homepage URL
Office 365 Exchange Online	http://office.microsoft.com/outlook/
Office 365 Management APIs	
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/
Outlook Groups	
Skype for Business Online	

4. Under **Add from the gallery**, search for **GitHub**, and then select **Active Directory for GitHub Enterprise**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/-)". Below the header, the breadcrumb navigation shows "Home > Enterprise applications | All applications > Add an application". The main title is "Add an application". A callout box with an info icon suggests trying the new app gallery.

**Add your own app**

- Application you're developing**: Register an app you're working on to integrate it with Azure AD.
- On-premises application**: Configure Azure AD Application Proxy to enable secure remote access.
- Non-gallery application**: Integrate any other application that you don't find in the gallery.

**Add from the gallery**

**Category**:  
All (3418) ▾  
github ▾

2 applications matched "github".

Name	Category
 Active Directory for GitHub Enterprise	Developer services
 GitHub.com	All

5. Select **Add**.
6. Under Manage, select Single **sign-on**, and under **Single Sign-on Mode**, select **Password-based Sign-on**, and click **Add**.

The screenshot shows the Microsoft Azure portal interface. At the top, there are icons for file operations, notifications, settings, help, and a user profile. The text "DEFAULT DIRECTORY" is displayed next to a user icon. Below the header, the title "Active Directory for GitHub Enterprise" is shown, along with a "Add app" button and a close button ("X"). A blue banner at the top says "Integration by Microsoft". The main content area contains the following information:

- Name** (i)
- Publisher** (i)
- Single Sign-On Mode** (i)
- URL** (i)
- Logo** (i) A purple square containing the white GitHub logo, which is a stylized octocat.

At the bottom of the configuration pane, there is a blue "Add" button.

7. Under **Manage**, select **Users and groups > Add user > Users and groups**, click **Select**.

Users and groups X

Search

CB Test User - Demo

**Selected items**

No items selected

Select

8. Select **Assign**.

## Accept the Guest User Invite

Now sign in to the guest user email account to view the invitation.

1. Sign in to your test guest user's email account.
2. In the inbox, find the "You're invited" email.
3. In the email body, select Get Started. A Review permissions page opens in the browser.
4. Select **Accept Invitation**. The Access Panel opens, which lists the applications the guest user can access.

Default Directory invited you to access applications within their organization



Microsoft Invitations on behalf of Default Directory <invites@microsoft.com>

If there are problems with how this message is displayed, click here to view it in a web browser.

Please only act on this email if you trust the organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Organization: Default Directory  
Domain:

This message was provided by the sender and is not from Microsoft Corporation.

CB

Message from  
Default Directory:

“

Test message for guest user invite.

”

If you accept this invitation, you'll be sent to <https://myapps.microsoft.com/>

Accept invitation

## Module 1 Review Questions

### Module 1 Review Questions



#### Review Question 1

*An organization that you are advising has MFA enabled for all users.*

- They have MFA configured to send verification codes to their user's cell phones.
- You are asked to recommend how they should configure an additional MFA verification option for their users.
- They have an Azure AD tenant.

*What should you advise?*

- From the Security blade of Azure AD configure the Authentication settings
- From the Security blade of Azure AD configure the phone call settings
- From Multi-Factor Authentication, configure in the service settings
- Azure Policy

#### Review Question 2

*You are advising a company that has enabled MFA for all its users.*

- The company's support desk is seeing an increase in support tickets from users who are receiving MFA requests while working within the company's main campus.
- You are asked to provide a recommendation that prevents the users from receiving MFA requests while on the main campus. The company has an Azure subscription.

*What do you advise?*

- From the MFA service settings, create a trusted IP range.
- From the conditional access in Azure AD, create a named location.
- From the conditional access in Azure AD, create a custom control.
- From the conditional access in Azure AD, configure organizational relationships.

# Answers

## Review Question 1

An organization that you are advising has MFA enabled for all users.

What should you advise?

- From the Security blade of Azure AD configure the Authentication settings
- From the Security blade of Azure AD configure the phone call settings
- From Multi-Factor Authentication, configure in the service settings
- Azure Policy

*Explanation*

*Correct Answer: From Multi-Factor Authentication, configure in the service settings. You configure verification options that are used for MFA authentication in Multi-factor authentication portal, by configuring verification options on service settings tab. These settings are global and are used for all users who are authenticated by using MFA.*

## Review Question 2

You are advising a company that has enabled MFA for all its users.

What do you advise?

- From the MFA service settings, create a trusted IP range.
- From the conditional access in Azure AD, create a named location.
- From the conditional access in Azure AD, create a custom control.
- From the conditional access in Azure AD, configure organizational relationships.

*Explanation*

*Correct Answer: From the MFA service settings, create a trusted IP range. By creating a trusted IP range in the MFA service settings you provide users with the ability to avoid MFA requests while on company sites.*



## Module 2 Implement and Manage Hybrid Identities

### Hybrid Identity

#### Hybrid Identity with Azure Active Directory

Organizations are a mixture of on-premises and cloud applications. Users require access to those applications both on-premises and in the cloud.

Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.

With hybrid identity to Azure AD and hybrid identity management these scenarios become possible.

To achieve hybrid identity with Azure AD, one of three authentication methods can be used, depending on your scenarios. The three methods are:

- **Password hash synchronization (PHS)**<sup>1</sup>
- **Pass-through authentication (PTA)**<sup>2</sup>
- **Federation (AD FS)**<sup>3</sup>

These authentication methods also provide single-sign on capabilities. Single-sign on automatically signs your users in when they are on their corporate devices, connected to your corporate network.

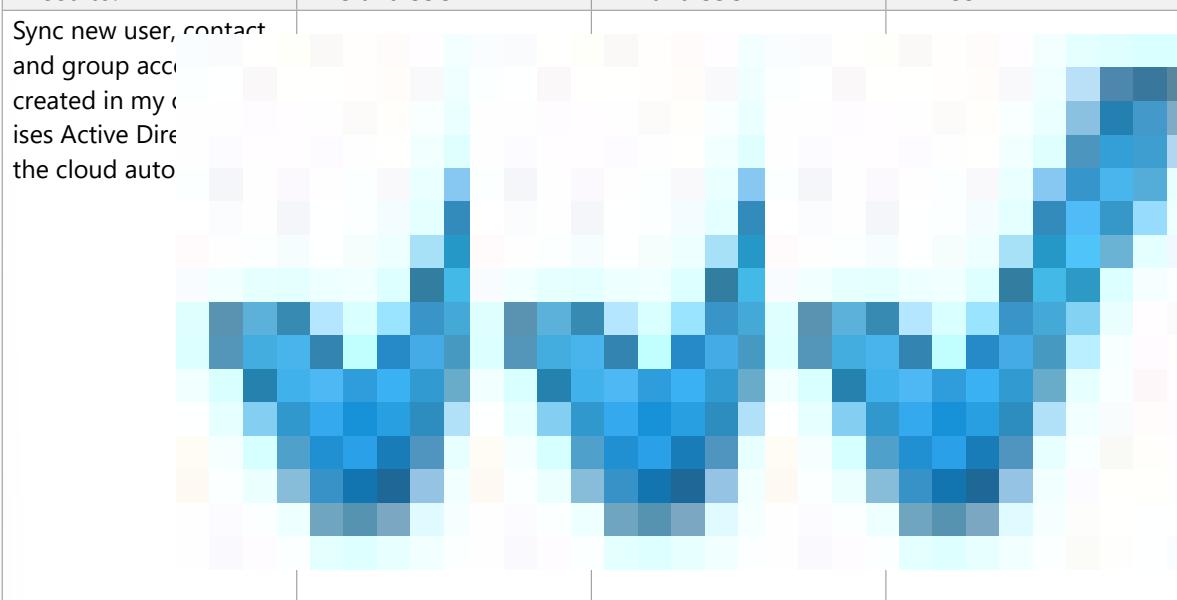
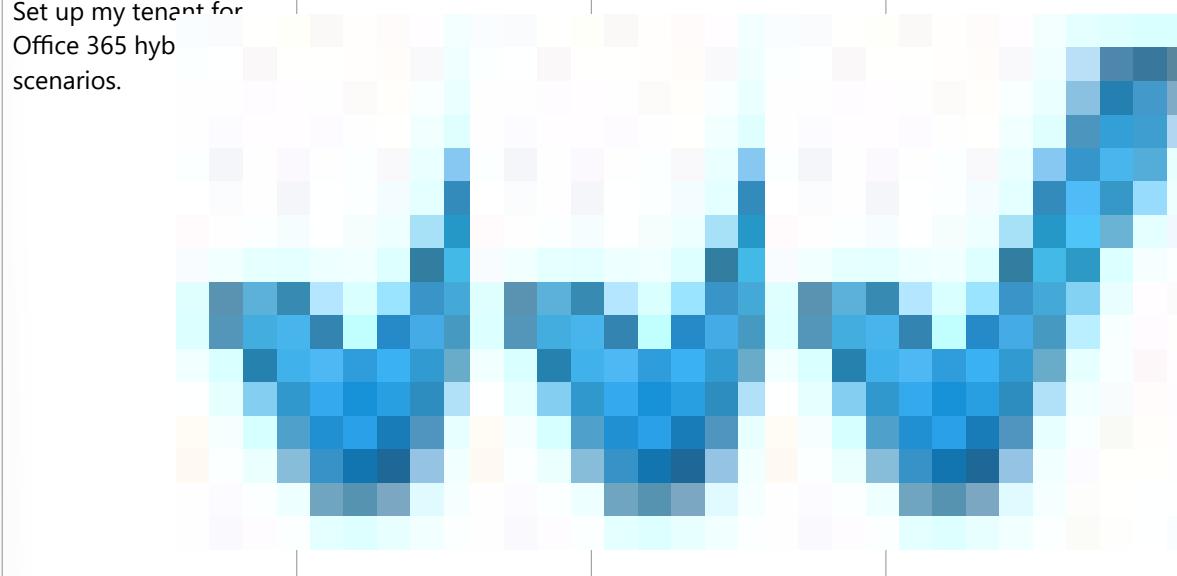
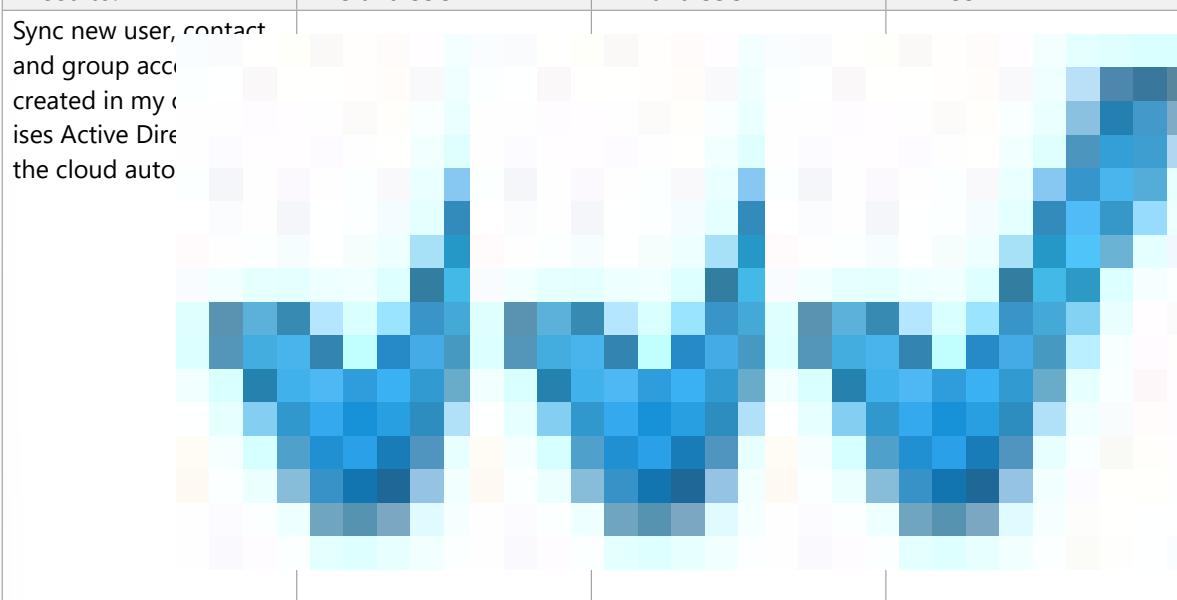
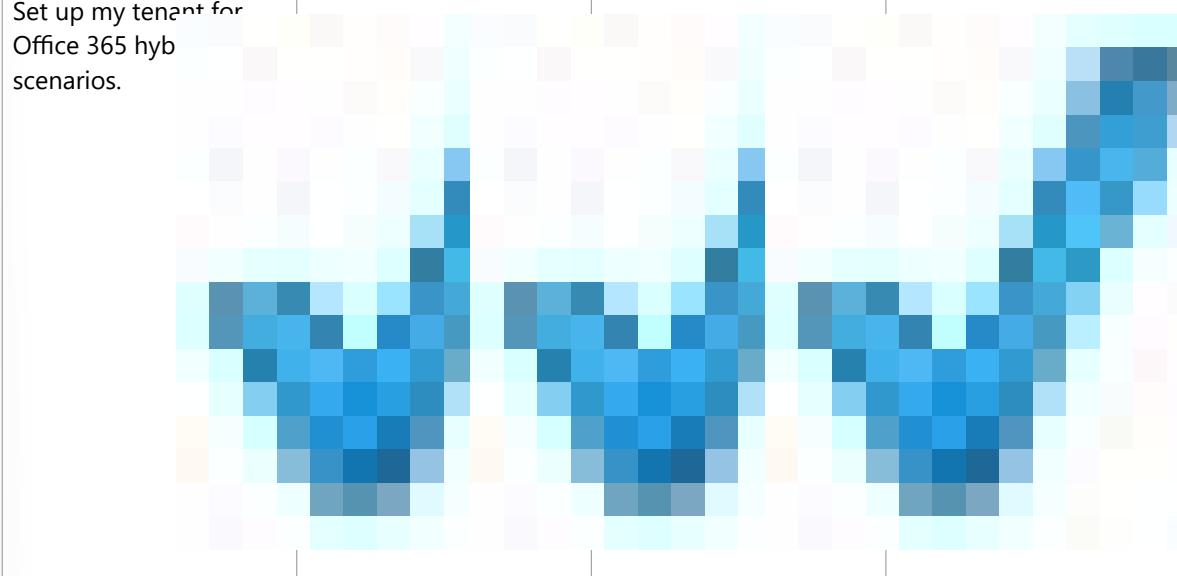
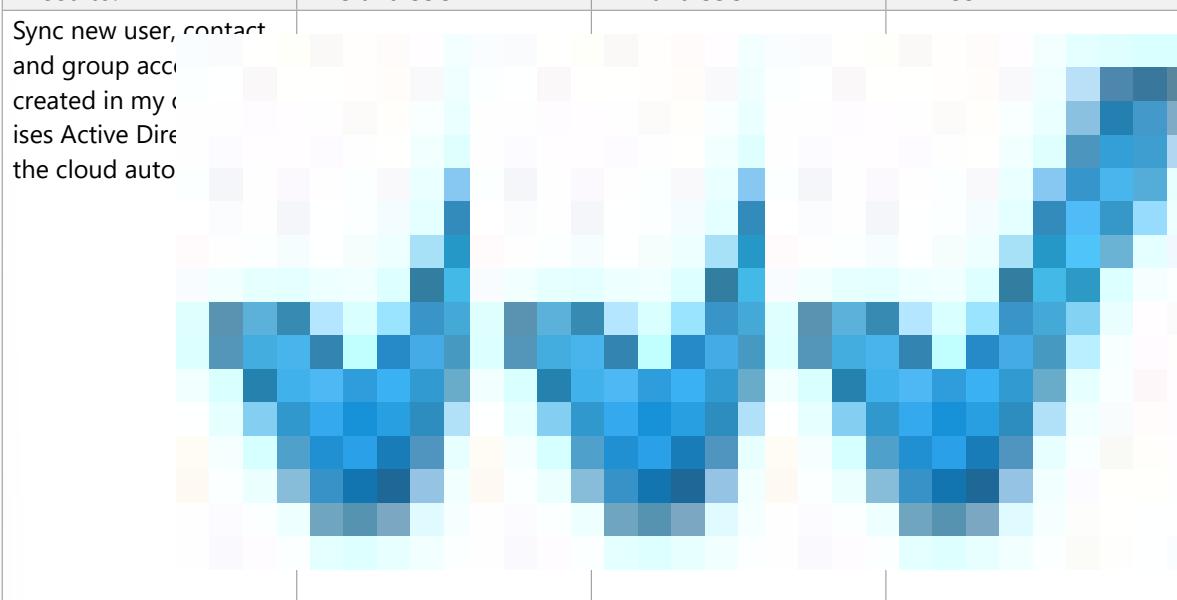
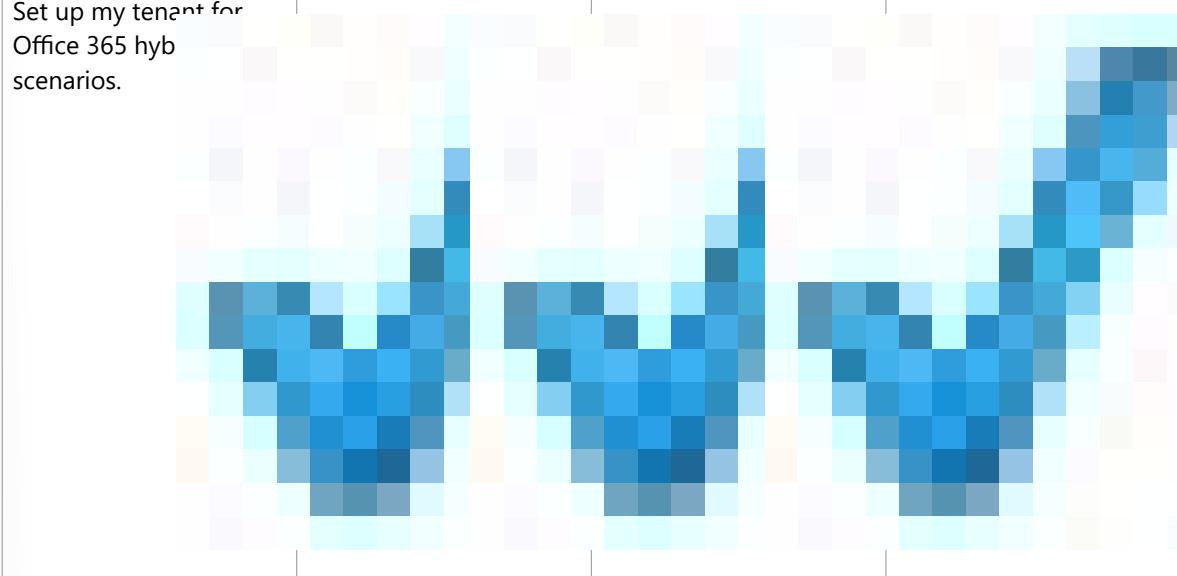
### Common scenarios and recommendations

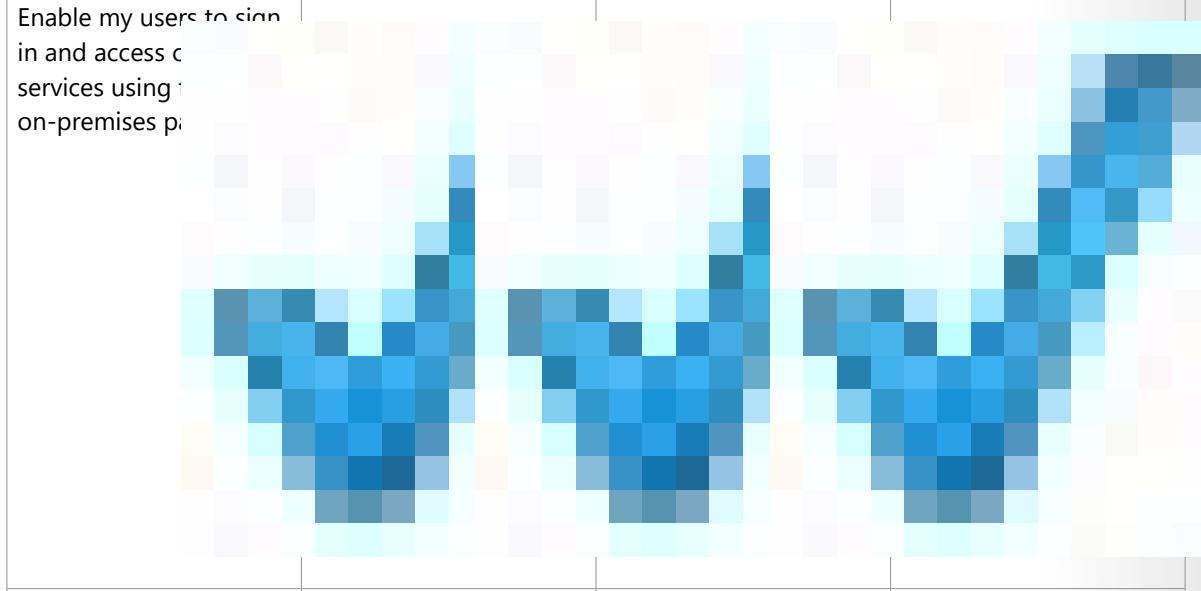
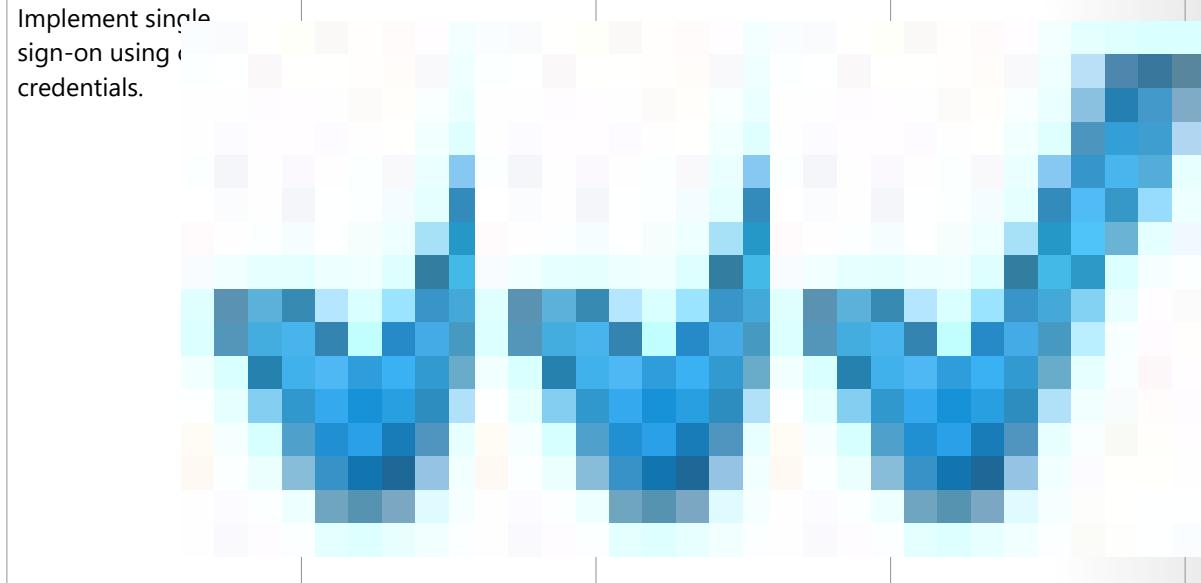
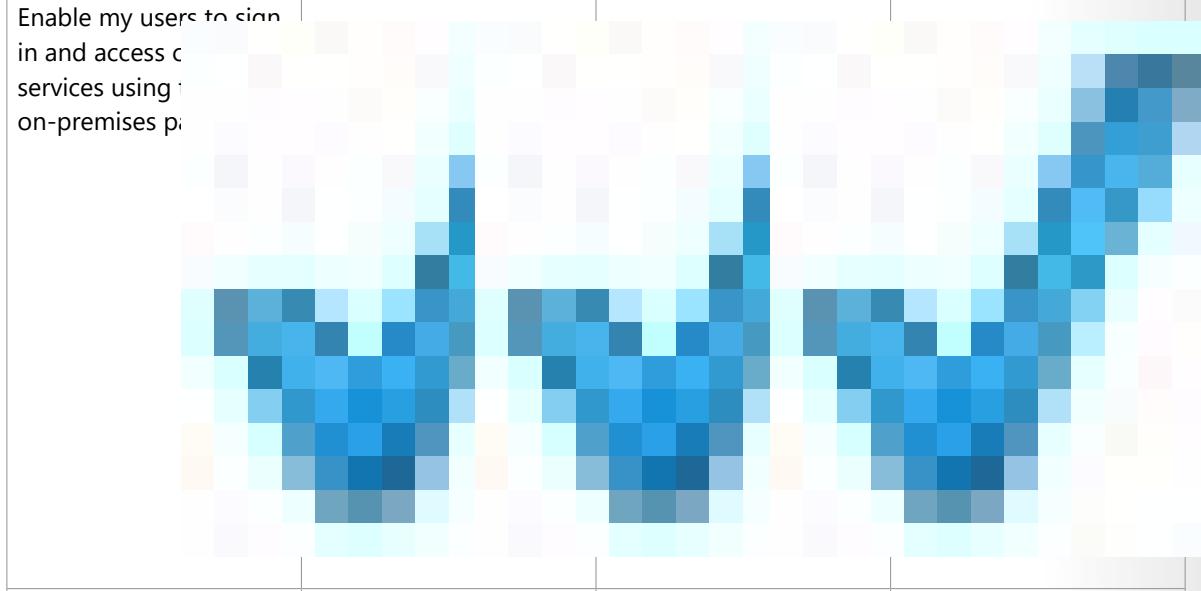
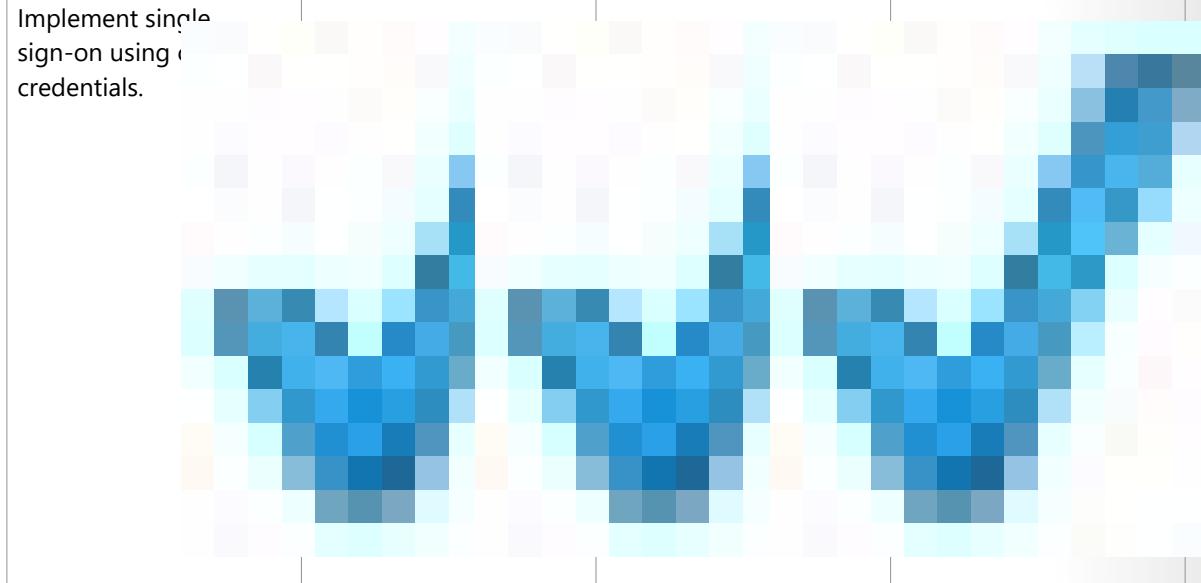
Below are common hybrid identity and access management scenarios with recommendations as to which hybrid identity option (or options) might be appropriate for each.

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

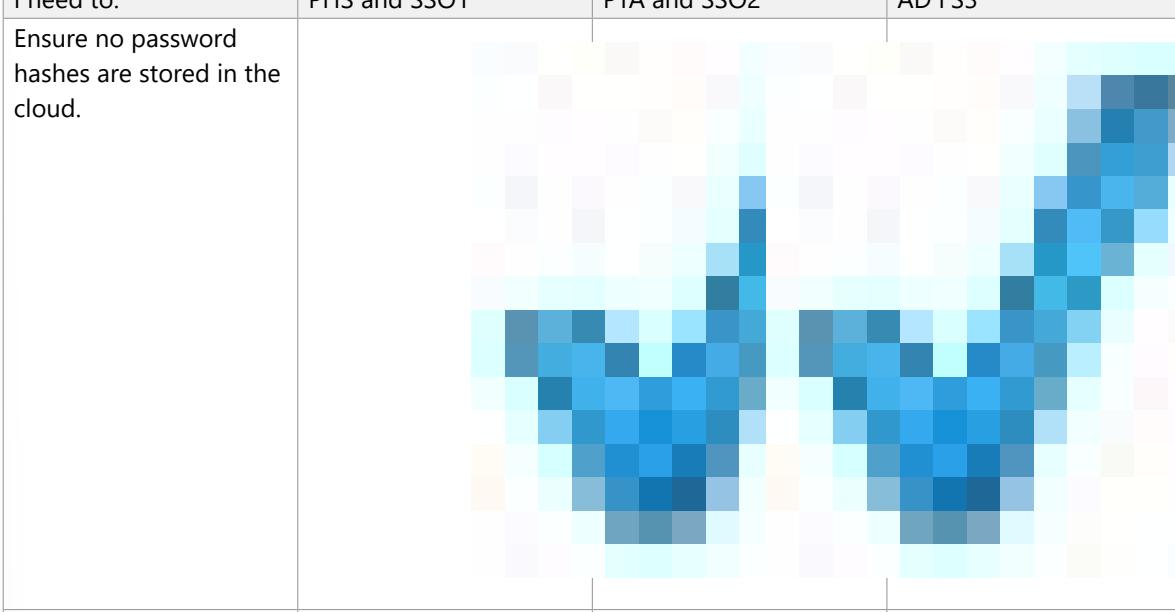
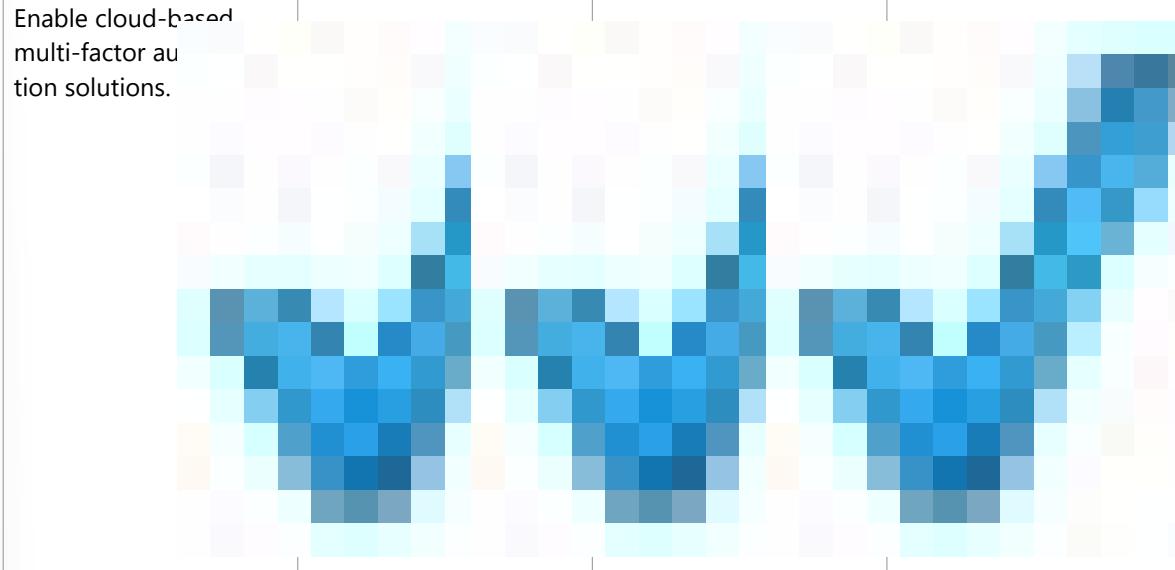
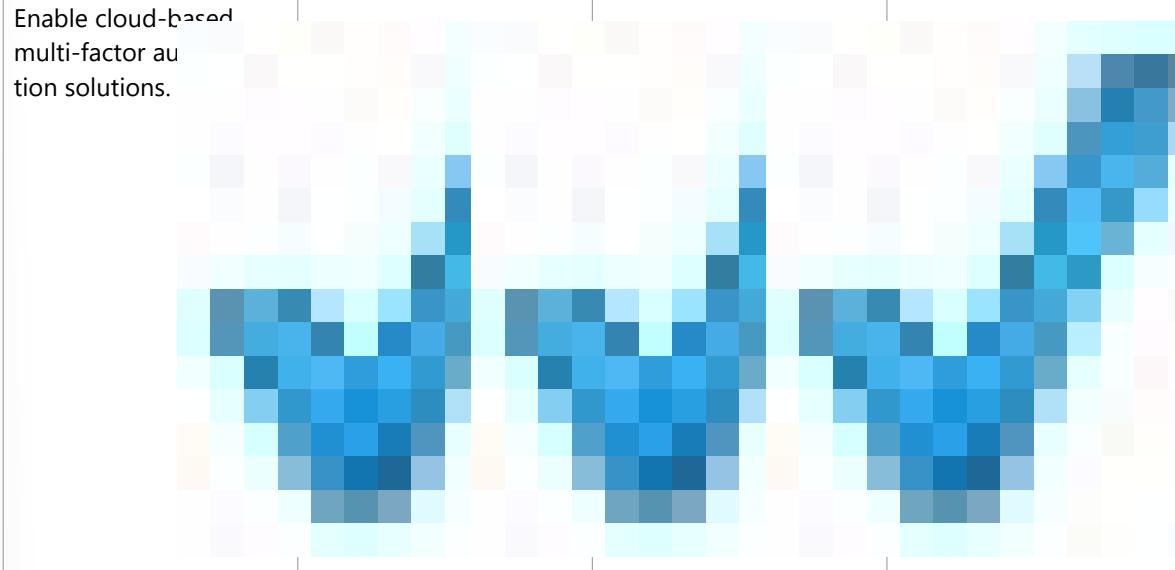
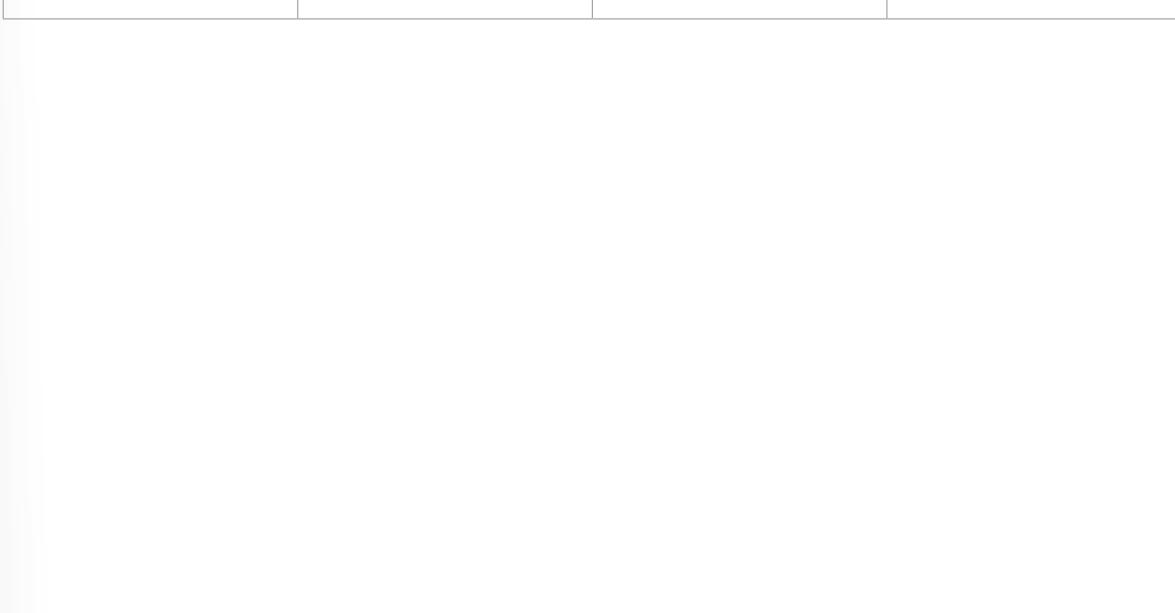
<sup>2</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

I need to:	PHS and SSO1 <sup>1</sup>	PTA and SSO2 <sup>2</sup>	AD FS3 <sup>3</sup>
Sync new user, contact and group accounts created in my cloud account. This uses Active Directory Federation Services (AD FS) to sync the cloud automatically.			
Set up my tenant for Office 365 hybrid scenarios.			

I need to:	PHS and SSO1 <sup>1</sup>	PTA and SSO2 <sup>2</sup>	AD FS3 <sup>3</sup>
Enable my users to sign in and access cloud services using on-premises protocols.			
Implement single sign-on using cloud credentials.			

AUTHORIZED TRAINING USE ONLY. STUDENT USE PROHIBITED

I need to:	PHS and SSO1 <sup>1</sup>	PTA and SSO2 <sup>2</sup>	AD FS3 <sup>3</sup>
Ensure no password hashes are stored in the cloud.			
Enable cloud-based multi-factor authentication solutions.			

I need to:	PHS and SSO1 <sup>1</sup>	PTA and SSO2 <sup>2</sup>	AD FS3 <sup>3</sup>
Enable on-premises multi-factor authentication solutions.			
Support smartcard authentication for my users. <sup>4</sup>			

AUTHORIZED TRAINING USE ONLY. STUDENT USE PROHIBITED

I need to:	PHS and SSO <sup>1</sup>	PTA and SSO <sup>2</sup>	AD FS <sup>3</sup>
Display password expiry notifications in the Office Portal and on the Windows 10 desktop.			

<sup>1</sup> Password hash synchronization with single sign-on.

<sup>2</sup> Pass-through authentication and single sign-on.

<sup>3</sup> Federated single sign-on with AD FS.

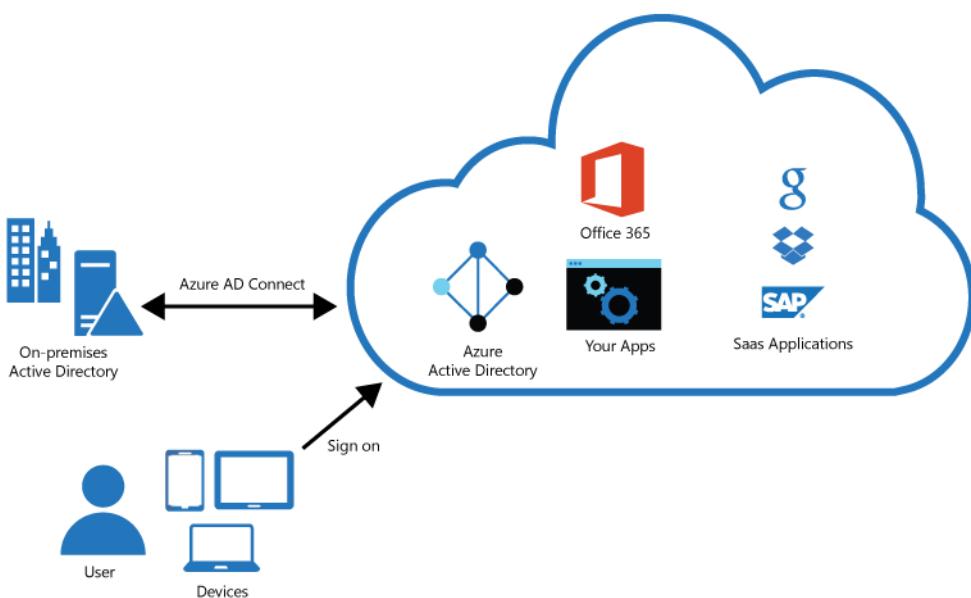
<sup>4</sup> AD FS can be integrated with your enterprise PKI to allow sign-in using certificates. These certificates can be soft-certificates deployed via trusted provisioning channels such as MDM or GPO or smartcard certificates (including PIV/CAC cards) or Hello for Business (cert-trust).

# Install and Configure Azure AD Connect

## Azure AD Connect

Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals. It provides the following features:

- **Password hash synchronization<sup>4</sup>** - A sign-in method that synchronizes a hash of a user's on-premises AD password with Azure AD.
- **Pass-through authentication<sup>5</sup>** - 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<sup>6</sup>** - 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<sup>7</sup>** - 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<sup>8</sup>** - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.



<sup>4</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs>

<sup>5</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

<sup>6</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-whatis>

<sup>7</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis>

<sup>8</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity-health>

## Why use Azure AD Connect?

Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. Users and organizations can take advantage of:

- Users can use a single identity to access on-premises applications and cloud services such as Office 365.
- Single tool to provide an easy deployment experience for synchronization and sign-in.
- Provides the newest capabilities for your scenarios. Azure AD Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync.

## Azure AD Connect Installation

**Azure AD Connect Express Settings** is used when you have a single-forest topology and password hash synchronization for authentication. Express Settings is the default option and is used for the most commonly deployed scenario.

**Azure AD Connect Custom** settings is used when you want more options for the installation. It is used if you have multiple forests or if you want to configure optional features not covered in the express installation. It is used in all cases where the express installation option does not satisfy your deployment or topology.

## Install Azure AD Connect

### ✓ Important

Microsoft doesn't support modifying or operating Azure AD Connect sync outside of the actions that are formally documented. Any of these actions might result in an inconsistent or unsupported state of Azure AD Connect sync. As a result, Microsoft can't provide technical support for such deployments.

Solution	Scenario
<b>Express settings</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express</a> )	If you have a single forest AD then this is the recommended option to use. User sign in with the same password using password synchronization.
<b>Customized settings</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom</a> )	Used when you have multiple forests. Supports many on-premises topologies. Customize your sign-in option, such as pass-through authentication, ADFS for federation or use a 3rd party identity provider. Customize synchronization features, such as filtering and writeback.
<b>Upgrade from DirSync</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-dirsync-upgrade-get-started">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-dirsync-upgrade-get-started</a> )	Used when you have an existing DirSync server already running.
<b>Upgrade from Azure AD Sync or Azure AD Connect</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-upgrade-previous-version">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-upgrade-previous-version</a> )	There are several different methods depending on your preference.

## Next steps to Install Azure AD Connect

Topic	Link
Download Azure AD Connect	<b>Download Azure AD Connect</b> ( <a href="https://go.microsoft.com/fwlink/?LinkId=615771">https://go.microsoft.com/fwlink/?LinkId=615771</a> )
Install using Express settings	<b>Express installation of Azure AD Connect</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express</a> )
Install using Customized settings	<b>Custom installation of Azure AD Connect</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom</a> )
Upgrade from DirSync	<b>Upgrade from Azure AD sync tool (DirSync)</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-dirsync-upgrade-get-started">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-dirsync-upgrade-get-started</a> )
After installation	<b>Verify the installation and assign licenses</b> ( <a href="https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-post-installation">https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-post-installation</a> )

## Configure sync features

Azure AD Connect comes with several features you can optionally turn on or are enabled by default. Some features might sometimes require more configuration in certain scenarios and topologies.

- **Filtering** is used when you want to limit which objects are synchronized to Azure AD. By default all users, contacts, groups, and Windows 10 computers are synchronized. You can change the filtering based on domains, OUs, or attributes.
- **Password hash synchronization** synchronizes the password hash in Active Directory to Azure AD. The end-user can use the same password on-premises and in the cloud but only manage it in one location. Since it uses your on-premises Active Directory as the authority, you can also use your own password policy.
- **Password writeback** allows your users to change and reset their passwords in the cloud and have your on-premises password policy applied.
- **Device writeback** allows a device registered in Azure AD to be written back to on-premises Active Directory so it can be used for Conditional Access.
- The **prevent accidental deletes** feature is turned on by default and protects your cloud directory from numerous deletes at the same time. By default it allows 500 deletes per run. You can change this setting depending on your organization size.
- **Automatic upgrade** is enabled by default for express settings installations and ensures your Azure AD Connect is always up to date with the latest release.

## Single Sign-On

Single sign-on (SSO) adds security and convenience when users sign-on to applications in Azure Active Directory (Azure AD). This article describes the single sign-on methods, and helps you choose the most appropriate SSO method when configuring your applications.

- **With single sign-on**, users sign in once with one account to access domain-joined devices, company resources, software as a service (SaaS) applications, and web applications. After signing in, the user can launch applications from the Office 365 portal or the Azure AD MyApps access panel. Administra-

tors can centralize user account management, and automatically add or remove user access to applications based on group membership.

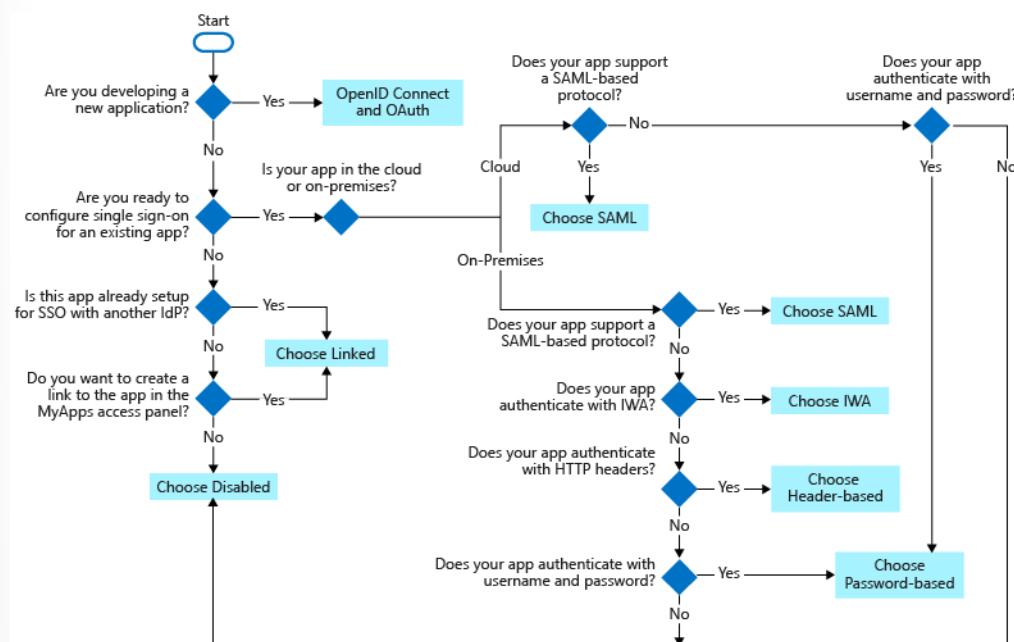
- Without **single sign-on**, users must remember application-specific passwords and sign in to each application. IT staff needs to create and update user accounts for each application such as Office 365, Box, and Salesforce. Users need to remember their passwords, plus spend the time to sign in to each application.

## Choosing a single sign-on method

There are several ways to configure an application for single sign-on. Choosing a single sign-on method depends on how the application is configured for authentication.

- Cloud applications can use OpenID Connect, OAuth, SAML, password-based, linked, or disabled methods for single sign-on.
- On-premises applications can use password-based, Integrated Windows Authentication, header-based, linked, or disabled methods for single sign-on. The on-premises choices work when applications are configured for Application Proxy.

This flowchart helps you decide which single sign-on method is best for your situation.



The following table summarizes the single sign-on methods, and links to more details.

Single sign-on method	Application types	When to use
<b>OpenID Connect and OAuth</b>	cloud only	Use OpenID Connect and OAuth when developing a new application. This protocol simplifies application configuration, has easy-to-use SDKs, and enables your application to use MS Graph.

<b>Single sign-on method</b>	<b>Application types</b>	<b>When to use</b>
<b>SAML</b>	cloud and on-premises	Choose SAML whenever possible for existing applications that do not use OpenID Connect or OAuth. SAML works for applications that authenticate using one of the SAML protocols.
<b>Password-based</b>	cloud and on-premises	Choose password-based when the application authenticates with username and password. Password-based single sign-on enables secure application password storage and replay using a web browser extension or mobile app. This method uses the existing sign-in process provided by the application, but enables an administrator to manage the passwords.
<b>Linked</b>	cloud and on-premises	Choose linked sign-on when the application is configured for single sign-on in another identity provider service. This option doesn't add single sign-on to the application. However, the application might already have single sign-on implemented using another service such as Active Directory Federation Services.
<b>Disabled</b>	cloud and on-premises	Choose disabled single sign-on when the app isn't ready to be configured for single sign-on. This mode is the default when you create the app.
<b>Integrated Windows Authentication (IWA)</b>	on-premises only	Choose IWA single sign-on for applications that use Integrated Windows Authentication (IWA), or claims-aware applications. For IWA, the Application Proxy connectors use Kerberos Constrained Delegation (KCD) to authenticate users to the application.

Single sign-on method	Application types	When to use
<b>Header-based</b>	on-premises only	Use header-based single sign-on when the application uses headers for authentication. Header-based single sign-on requires PingAccess for Azure AD. Application Proxy uses Azure AD to authenticate the user and then passes traffic through the connector

## Demonstration - Azure AD Seamless Single Sign-On

Azure Active Directory (Azure AD) Seamless Single Sign-On (Seamless SSO) automatically signs in users when they are on their corporate desktops that are connected to your corporate network. Seamless SSO provides your users with easy access to your cloud-based applications without needing any additional on-premises components.

### Prerequisites

Ensure that the following prerequisites are in place prior to this demonstration:

- **Set up your Azure AD Connect server:** If you use Pass-through Authentication as your sign-in method, no additional prerequisite check is required. If you use password hash synchronization as your sign-in method, and if there is a firewall between Azure AD Connect and Azure AD, ensure that:
  - You use version 1.1.644.0 or later of Azure AD Connect.
  - If your firewall or proxy allows DNS whitelisting, whitelist the connections to the \*.msappproxy.net URLs over port 443.
- **Set up domain administrator credentials:** You need to have enterprise administrator credentials for each Active Directory forest that:
  - You synchronize to Azure AD through Azure AD Connect.
  - Contains users you want to enable for Seamless SSO.

### Enable Azure AD Connect.

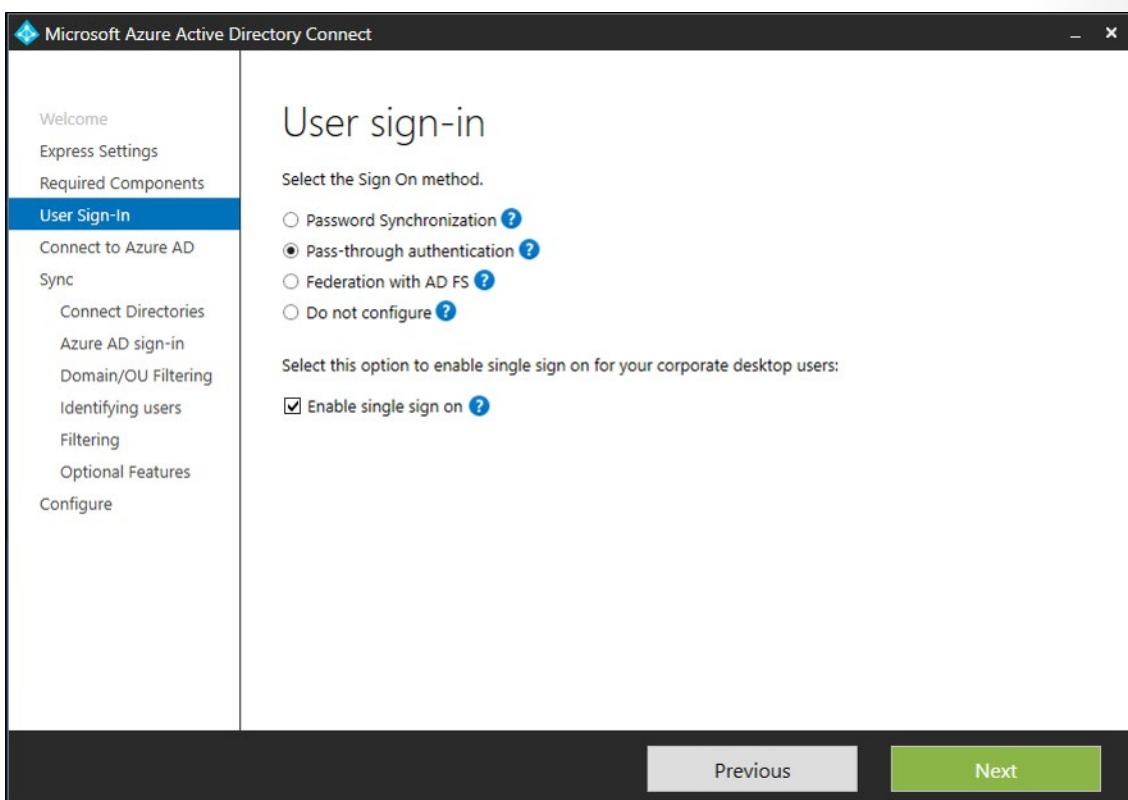
Enable Seamless SSO through **Azure AD Connect**<sup>9</sup>.

If you're doing a fresh installation of Azure AD Connect, choose the **custom installation path**<sup>10</sup>. At the User sign-in page, select the Enable single sign on option.

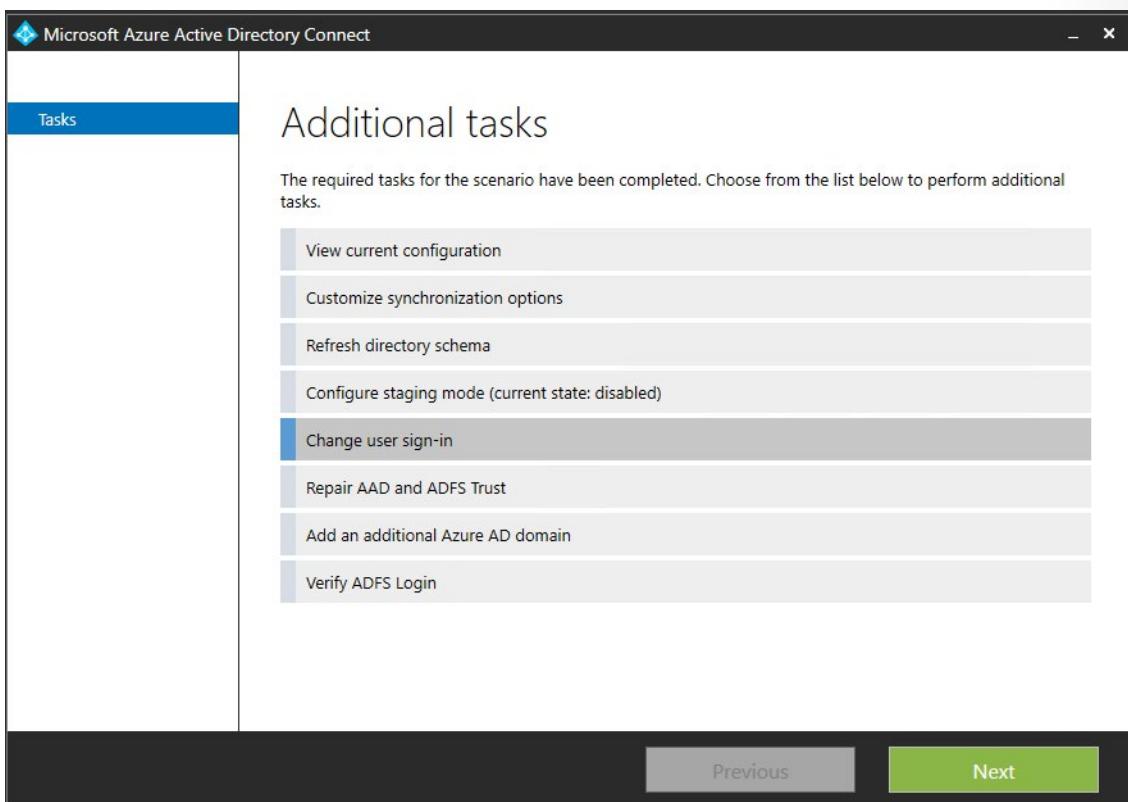
---

<sup>9</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity>

<sup>10</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>



If you already have an installation of Azure AD Connect, select the Change user sign-in page in Azure AD Connect, and then select Next.



Continue through the wizard until you get to the Enable single sign on page. Provide domain administrator credentials for each Active Directory forest that:

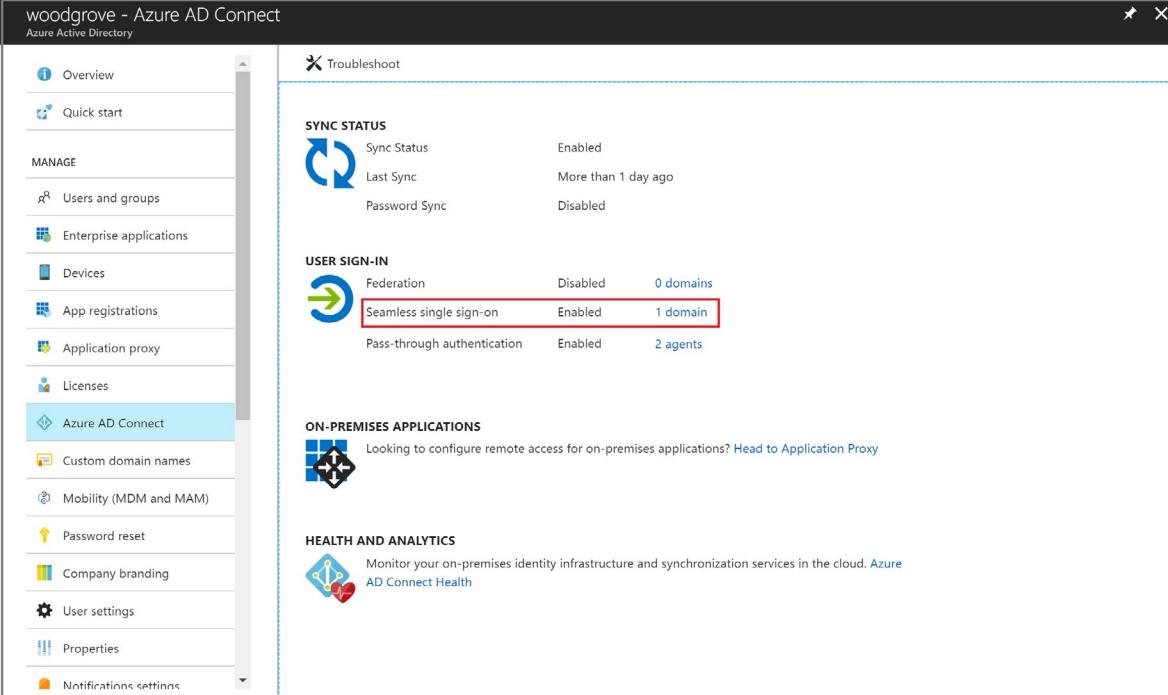
- You synchronize to Azure AD through Azure AD Connect.
- Contains users you want to enable for Seamless SSO.

After completion of the wizard, Seamless SSO is enabled on your tenant.

## Verify Seamless SSO is enabled

Follow procedure below to verify that you have enabled Seamless SSO correctly:

1. Sign in to the **Azure Active Directory administrative center<sup>11</sup>** with the global administrator credentials for your tenant.
2. Select **Azure Active Directory** in the left pane.
3. Select **Azure AD Connect**.
4. Verify that the Seamless single sign-on feature appears as *Enabled*.



The screenshot shows the Azure Active Directory administrative center interface. On the left, there's a navigation menu with various options like Overview, Quick start, and Azure AD Connect (which is selected). The main content area is titled 'Troubleshoot'. It has sections for 'SYNC STATUS' and 'USER SIGN-IN'. In the 'USER SIGN-IN' section, there's a table with three rows: 'Federation' (Disabled, 0 domains), 'Seamless single sign-on' (Enabled, 1 domain, highlighted with a red box), and 'Pass-through authentication' (Enabled, 2 agents). Below these sections are 'ON-PREMISES APPLICATIONS' and 'HEALTH AND ANALYTICS' sections.

### Important

Seamless SSO creates a computer account named AZUREADSSOACC in your on-premises Active Directory (AD) in each AD forest. The AZUREADSSOACC computer account needs to be strongly protected for security reasons. Only Domain Admins should be able to manage the computer account. Ensure that Kerberos delegation on the computer account is disabled, and that no other account in Active Directory has delegation permissions on the AZUREADSSOACC computer account. Store the computer account in an Organization Unit (OU) where they are safe from accidental deletions and where only Domain Admins have access.

<sup>11</sup> <https://aad.portal.azure.com/>

# Configure Password Sync and Password Write-back

## Enable Azure AD Self-Service Password

Azure Active Directory (Azure AD) self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unlock themselves and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.

This topic demonstrates how to enable self-service password reset.

- Enable self-service password reset for a group of Azure AD users
- Configure authentication methods and registration options
- Test the SSPR process as a user

### Prerequisites

To complete this demonstration, you need the following resources and privileges:

- A working Azure AD tenant with at least a trial license enabled.
- An account with Global Administrator privileges.
- A non-administrator user with a password you know, such as testuser. You test the end-user SSPR experience using this account in this demonstration.
- A group that the non-administrator user is a member of, such as SSPR-Test-Group. You enable SSPR for this group in this demonstration.

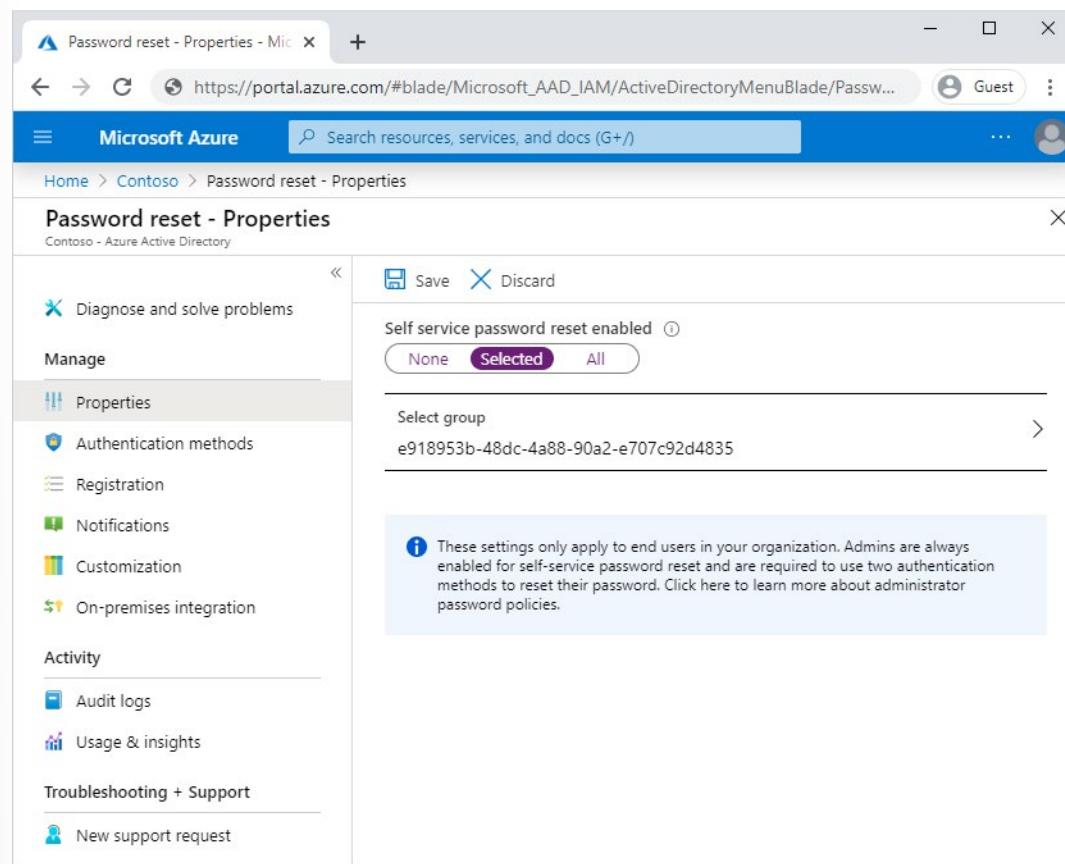
### Enable self-service password reset

Azure AD lets you enable SSPR for None, Selected, or All users. This granular ability lets you choose a subset of users to test the SSPR registration process and workflow. When you're comfortable with the process and can communicate the requirements with a broader set of users, you can select additional groups of users to enable for SSPR. Or, you can enable SSPR for everyone in the Azure AD tenant.

In this demonstration, configure SSPR for a set of users in a test group. In the following example, the group SSPR-Test-Group is used. Provide your own Azure AD group as needed:

1. Sign in to the **Azure portal**<sup>12</sup> using an account with global administrator permissions.
2. Search for and select **Azure Active Directory**, then choose **Password reset** from the menu on the left-hand side.
3. From the **Properties** page, under the option Self service password reset enabled, choose **Select group**.
4. Browse for and select your Azure AD group, such as *SSPR-Test-Group*, then choose **Select**.

<sup>12</sup> <https://portal.azure.com/>



The screenshot shows the Microsoft Azure portal with the URL [https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/ActiveDirectoryMenuBlade/PasswordResetProperties](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/PasswordResetProperties). The page title is "Password reset - Properties" for the "Contoso - Azure Active Directory". On the left, there's a navigation menu with sections like "Diagnose and solve problems", "Manage", "Properties" (which is selected), "Authentication methods", "Registration", "Notifications", "Customization", "On-premises integration", "Activity", "Audit logs", "Usage & insights", "Troubleshooting + Support", and "New support request". The main content area has a "Save" and "Discard" button at the top. Under "Properties", it says "Self service password reset enabled" and shows "Selected" under the "None" tab. Below that, there's a "Select group" dropdown with the value "e918953b-48dc-4a88-90a2-e707c92d4835". A note in a callout box says: "These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies." There are also "Save" and "Discard" buttons at the top right.

As part of a wider deployment of SSPR, nested groups are supported. Make sure that the users in the group(s) you choose have the appropriate licenses assigned. There's currently no validation process of these licensing requirements.

5. To enable SSPR for the select users, select **Save**.

## Select authentication methods and registration options

When users need to unlock their account or reset their password, they're prompted for an additional confirmation method. This additional authentication factor makes sure that only approved SSPR events are completed. You can choose which authentication methods to allow, based on the registration information the user provides.

1. On the **Authentication methods** page from the menu in the left-hand side, set the **Number of methods required to reset** to 1.

To improve security, you can increase the number of authentication methods required for SSPR.

2. Choose the **Methods available to users** that your organization wants to allow. For this demonstration, check the boxes to enable the following methods:

- *Mobile app notification*
- *Mobile app code*
- *Email*

- *Mobile phone*
  - *Office phone*
3. To apply the authentication methods, select **Save**.

Before users can unlock their account or reset a password, they must register their contact information. This contact information is used for the different authentication methods configured in the previous steps.

An administrator can manually provide this contact information, or users can go to a registration portal to provide the information themselves. In this demonstration, configure the users to be prompted for registration when they next sign in.

1. On the **Registration** page from the menu in the left-hand side, select Yes for **Require users to register when signing in**.
2. It's important that contact information is kept up to date. If the contact information is outdated when an SSPR event is started, the user may not be able to unlock their account or reset their password.

Set **Number of days before users are asked to reconfirm their authentication information** to **180**.

3. To apply the registration settings, select **Save**.

## Configure notifications and customizations

To keep users informed about account activity, you can configure e-mail notifications to be sent when an SSPR event happens. These notifications can cover both regular user accounts and admin accounts. For admin accounts, this notification provides an additional layer of awareness when a privileged administrator account password is reset using SSPR.

1. On the **Notifications** page from the menu in the left-hand side, configure the following options:
  - Set **Notify users on password resets option** to Yes.
  - Set **Notify all admins when other admins reset their password** to Yes.
2. To apply the notification preferences, select **Save**.

## Test Self-Service Password Reset

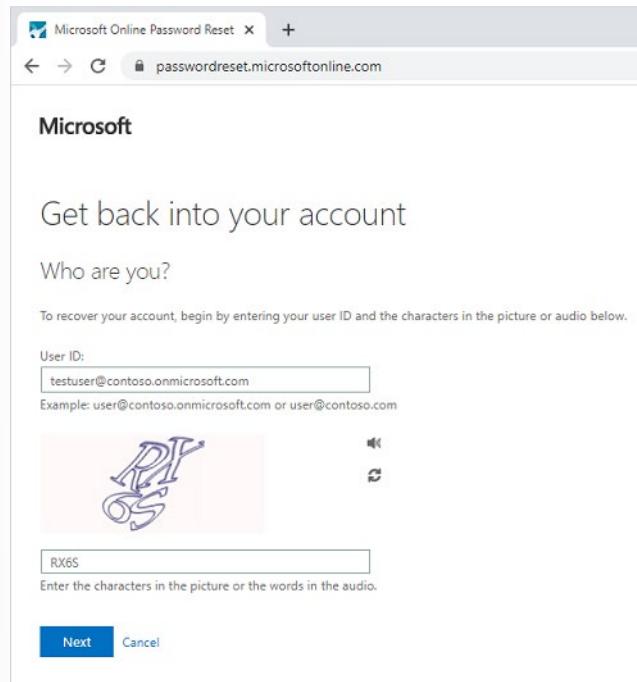
With SSPR enabled and configured, test the SSPR process with a user that's part of the group you selected in the previous section, such as Test-SSPR-Group. In the following example, the testuser account is used. Provide your own user account that's part of the group you enabled for SSPR in the first section of this demonstration.

### ✓ Note

When you test the self-service password reset, use a non-administrator account. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password.

1. To see the manual registration process, open a new browser window in InPrivate or incognito mode, and browse to <https://aka.ms/ssprsetup>. Users should be directed to this registration portal when they next sign-in.
2. Sign in with a non-administrator test user, such as testuser, and register your authentication methods contact information.
3. Once complete, select the button marked **Looks good** and close the browser window.
4. Open a new browser window in InPrivate or incognito mode, and browse to <https://aka.ms/sspr>.

5. Enter your non-administrator test users' account information, such as testuser, the characters from the CAPTCHA, and then select **Next**.



6. Follow the verification steps to reset your password. When complete, you should receive an e-mail notification that your password was reset.

## Self-Service Password Reset (SSPR) Writeback

Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment where their users exist. 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. In this configuration, as users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.

Password writeback is supported in environments that use the following hybrid identity models:

- Password hash synchronization
- Pass-through authentication
- Active Directory Federation Services

Password writeback provides the following features:

- **Enforcement of on-premises Active Directory Domain Services (AD DS) password policies:** When a user resets their password, it's checked to ensure it meets your on-premises AD DS policy before committing it to that directory. This review includes checking the history, complexity, age, password filters, and any other password restrictions that you define in AD DS.
- **Zero-delay feedback:** Password writeback is a synchronous operation. Users are notified immediately if their password doesn't meet the policy or can't 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 AD DS.
- **Supports password writeback when an admin resets them from the Azure portal:** When 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.

## How password writeback works

When a federated or password hash synchronized user attempts to reset or change their password in the cloud, the following actions occur:

1. A check is performed to see what type of password the user has. If the password is managed on-premises:
  - A check is performed to see if the writeback service is up and running. If it is, the user can proceed.
  - If the writeback service is down, the user is informed that their password can't be reset right now.
2. Next, the user passes the appropriate authentication gates and reaches the **Reset password** page.
3. The user selects a new password and confirms it.
4. When the user selects **Submit**, the plaintext password is encrypted with a symmetric key created during the writeback setup process.
5. The encrypted password is included in a payload that gets sent over an HTTPS channel to your tenant-specific service bus relay (that is set up for you during the writeback setup process). This relay is protected by a randomly generated password that only your on-premises installation knows.
6. After the message reaches the service bus, the password-reset endpoint automatically wakes up and sees that it has a reset request pending.
7. The service then looks for the user by using the cloud anchor attribute. For this lookup to succeed, the following conditions must be met:
  - The user object must exist in the Active Directory connector space.
  - The user object must be linked to the corresponding metaverse (MV) object.
  - The user object must be linked to the corresponding Azure Active Directory connector object.
  - The link from the Active Directory connector object to the MV must have the synchronization rule Microsoft.InfromADUserAccountEnabled.xxx on the link.

When the call comes in from the cloud, the synchronization engine uses the **cloudAnchor** attribute to look up the Azure Active Directory connector space object. It then follows the link back to the MV object, and then follows the link back to the Active Directory object. Because there can be multiple Active Directory objects (multi-forest) for the same user, the sync engine relies on the Microsoft.InfromADUserAccountEnabled.link to pick the correct one.

8. After the user account is found, an attempt to reset the password directly in the appropriate Active Directory forest is made.
9. If the password set operation is successful, the user is told their password has been changed.

10. If the password set operation fails, an error prompts the user to try again. The operation might fail because of the following reasons:

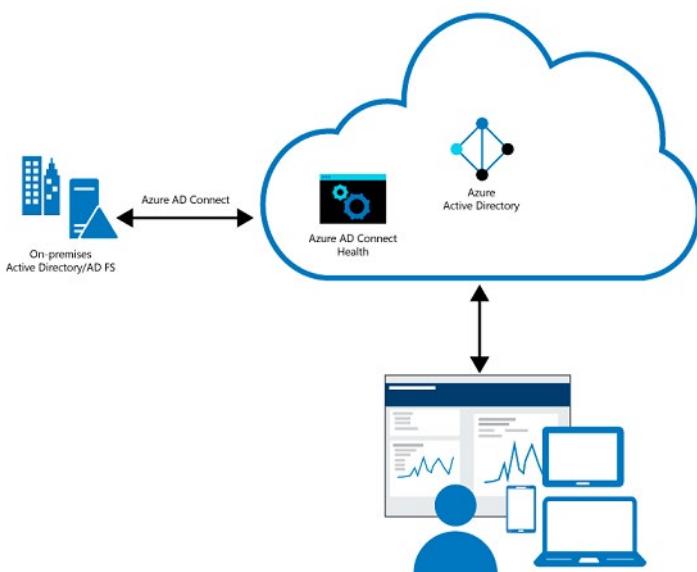
- The service was down.
- The password they selected doesn't meet the organization's policies.
- Unable to find the user in local Active Directory.

The error messages provide guidance to users so they can attempt to resolve without administrator intervention.

# Configure Azure AD Connect Health

## Azure AD Health Overview

Azure Active Directory (Azure AD) Connect Health provides monitoring of 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.



## Why use Azure AD Connect Health?

When using Azure AD, users are more productive because there's a common identity to access both cloud and on-premises resources. Ensuring the environment is reliable, so that users can access these resources, becomes a challenge. Azure AD Connect Health helps monitor and gain insights into your on-premises identity infrastructure thus ensuring the reliability of this environment. It is enabled by installing an agent on each on-premises identity server.

Azure AD Connect Health for AD FS supports AD FS 2.0 on Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016. It also supports monitoring the AD FS proxy or web application proxy servers that provide authentication support for extranet access. With an easy and quick installation of the Health Agent, Azure AD Connect Health for AD FS provides you a set of key capabilities.

Key benefits and best practices:

Key Benefits	Best Practices
<b>Enhanced security</b>	Extranet lockout trends Failed sign-ins report In privacy compliant
<b>Get alerted on all critical ADFS system issues</b>	Server configuration and availability Performance and connectivity Regular maintenance

Key Benefits	Best Practices
<b>Easy to deploy and manage</b>	Quick agent installation Agent auto upgrade to the latest Data available in portal within minutes
<b>Rich usage metrics</b>	Top applications usage Network locations and TCP connection Token requests per server
<b>Great user experience</b>	Dashboard fashion from Azure portal Alerts through emails

## Implement Azure AD Connect Health

To install the Azure AD Connect Health agent, do the following:

- Make sure that you **satisfy the requirements**<sup>13</sup> for Azure AD Connect Health.
- Install the Azure AD Connect Health agent
  - **Download Azure AD Connect Health Agent for AD FS.**<sup>14</sup>
  - **See the installation instructions**<sup>15</sup>.
- Get started using Azure AD Connect Health for sync
  - **Download and install the latest version of Azure AD Connect**<sup>16</sup>. The Health Agent for sync will be installed as part of the Azure AD Connect installation (version 1.0.9125.0 or higher).

## Azure AD Connect Health portal

The Azure AD Connect Health portal shows views of alerts, performance monitoring, and usage analytics. The <https://aka.ms/aadconnecthealth> URL takes you to the main blade of Azure AD Connect Health. You can think of a blade as a window. On The main blade, you see Quick Start, services within Azure AD Connect Health, and additional configuration options. See the following screenshot and brief explanations that follow the screenshot. After you deploy the agents, the health service automatically identifies the services that Azure AD Connect Health is monitoring.

---

<sup>13</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install>

<sup>14</sup> <https://go.microsoft.com/fwlink/?LinkID=518973>

<sup>15</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-agent-install>

<sup>16</sup> <https://go.microsoft.com/fwlink/?linkid=615771>

**Quick start**

**Azure Active Directory Connect (Sync)**

- Sync errors
- Sync services

**Active Directory Federation Services**

- AD FS services

**Active Directory Domain Services**

- AD DS services

**Configure**

- Settings
- Role based access control (IAM)

**TROUBLESHOOTING + SUPPORT**

- Troubleshoot
- New support request

**What's New**

Get a free Azure AD Premium trial to help you monitor on-premises identity infrastructure and sync services.

Azure AD Connect Health for Sync - Diagnose and remediate duplicated attribute sync errors from the portal is now generally available!

[Learn more about release history](#)

**Get tools**

Download and install Azure AD Connect Health Agents to get health and usage information of your on-premise services.

- Download Azure AD Connect Health Agent for AD FS
- Download Azure AD Connect (configures Azure AD Connect Health agent for sync)
- Download Azure AD Connect Health Agent for AD DS

**Provide feedback**

Report an issue, ask a question or provide feedback on the Azure Active Directory Connect Health Service

**Learn more**

Documentation and FAQs for using Azure AD Connect Health

- **Quick Start:** When you select this option, the Quick Start blade opens. You can download the Azure AD Connect Health Agent by selecting Get Tools.
- **Azure Active Directory Connect (sync):** This option shows your Azure AD Connect servers that Azure AD Connect Health is currently monitoring. Sync errors entry will show basic sync errors of your first onboarded sync service by categories. When you select the Sync services entry, the blade that opens shows information about your Azure AD Connect servers.
- **Active Directory Federation Services:** This option shows all the AD FS services that Azure AD Connect Health is currently monitoring. When you select an instance, the blade that opens shows information about that service instance. This information includes an overview, properties, alerts, monitoring, and usage analytics.
- **Active Directory Domain Services:** This option shows all the AD DS forests that Azure AD Connect Health is currently monitoring. When you select a forest, the blade that opens shows information about that forest.
- **Configure:** This section includes options to turn the following on or off:
  - The automatic update of the Azure AD Connect Health agent to the latest version: the Azure AD Connect Health agent is automatically updated whenever new versions are available.
  - Access to data from the Azure AD directory integrity by Microsoft only for troubleshooting purposes: if this option is enabled, Microsoft can access the same data viewed by the user. This information can be useful for troubleshooting and to provide the necessary assistance.

- **Role based access control (IAM)** is the section to manage the access to Connect Health data in role base.

## Module 2 Review Questions

### Module 2 Review Question



#### Review Question 1

An organization you advise has an Azure Directory forest named Tailwind.com.

- They have installed and configured Azure AD Connect to use password hash synchronization as the single sign-on (SSO) approach. Note: Staging mode is enabled.
- They have reviewed the synchronization results and noticed that the Synchronization Service Manager doesn't display any previous sync jobs.
- You are asked to find a way to ensure that the synchronization completes successfully.

What do you advise?

- From Synchronization Service Manager, run a full import
- Run AD Connect and disable staging mode.
- Run AD Connect and set the SSO method to Pass-Through authentication.
- Run from Azure PowerShell, Start-AdSyncSyncCycle -policyType Initial.

# Answers

## Review Question 1

An organization you advise has an Azure Directory forest named Tailwind.com.

What do you advise?

- From Synchronization Service Manager, run a full import
- Run AD Connect and disable staging mode.
- Run AD Connect and set the SSO method to Pass-Through authentication.
- Run from Azure PowerShell, Start-AdSyncSyncCycle -policyType Initial.

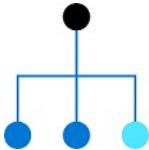
*Explanation*

*Correct Answer: Run AD Connect and disable staging mode. AD Connect needs to be taken out of staging mode so that objects are synced.*

## Module 3 Implement Virtual Networking

### Virtual Networking

#### Azure Virtual Networking



The first thing you should think about isn't the virtual machine - it's 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.

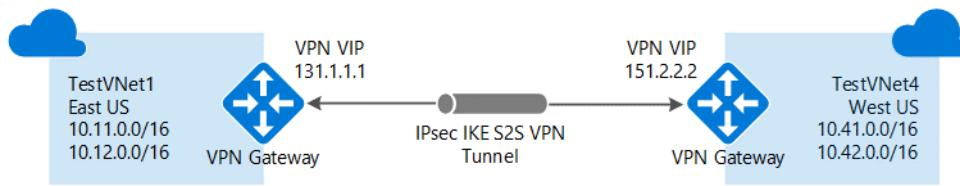
Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

#### VNet concepts

- **Address space:** When creating a VNet, you must specify a custom private IP address space using public and private (RFC 1918) addresses. Azure assigns resources in a virtual network a private IP

address from the address space that you assign. For example, if you deploy a VM in a VNet with address space, 10.0.0.0/16, the VM will be assigned a private IP like 10.0.0.4.

- **Subnets:** Subnets enable you to segment the virtual network into one or more sub-networks and allocate a portion of the virtual network's address space to each subnet. You can then deploy Azure resources in a specific subnet. Just like in a traditional network, subnets allow you to segment your VNet address space into segments that are appropriate for the organization's internal network. This also improves address allocation efficiency. You can secure resources within subnets using Network Security Groups.
- **Regions:** VNet is scoped to a single region/location; however, multiple virtual networks from different regions can be connected together using Virtual Network Peering. You can also use a VPN gateway to send traffic between VNets.



- **Subscription:** VNet is scoped to a subscription. You can implement multiple virtual networks within each Azure subscription and Azure region.

## Best practices

As you build your network in Azure, it is important to keep in mind the following universal design principles:

- Ensure non-overlapping address spaces. Make sure your VNet address space (CIDR block) does not overlap with your organization's other network ranges.
- Your subnets should not cover the entire address space of the VNet. Plan ahead and reserve some address space for the future.
- It is recommended you have fewer large VNets than multiple small VNets. This will prevent management overhead.
- Secure your VNet's by assigning Network Security Groups (NSGs) to the subnets beneath them.

## Communicate with the internet

All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use public IP or public Load Balancer to manage your outbound connections.

- ✓ **Note:** When using only an internal Standard Load Balancer, outbound connectivity is not available until you define how you want outbound connections to work with an instance-level public IP or a public Load Balancer.

## Communicate between Azure resources

Azure resources communicate securely with each other in one of the following ways:

- **Through a virtual network:** You can deploy VMs, and several other types of Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets.
- **Through a virtual network service endpoint:** Extend your virtual network private address space and the identity of your virtual network to Azure service resources, such as Azure Storage accounts and Azure SQL databases, over a direct connection. Service endpoints allow you to secure your critical Azure service resources to only a virtual network.
- **Through VNet Peering:** You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions.
- **Through Private Link:** You can access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in a virtual network.

## Communicate with on-premises resources

You can connect your on-premises computers and networks to a virtual network using any combination of the following options:

- **Point-to-site virtual private network (P2S VPN):** Established between a virtual network and a single computer in your network. Each computer that wants to establish connectivity with a virtual network must configure its connection. This connection type is great if you're just getting started with Azure, or for developers, because it requires little or no changes to your existing network. The communication between your computer and a virtual network is sent through an encrypted tunnel over the internet.
- **Site-to-site VPN (S2S VPN):** Established between your on-premises VPN device and an Azure VPN Gateway that is deployed in a virtual network. This connection type enables any on-premises resource that you authorize to access a virtual network. The communication between your on-premises VPN device and an Azure VPN gateway is sent through an encrypted tunnel over the internet.
- **Azure ExpressRoute:** Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not go over the internet.

## Filter network traffic

You can filter network traffic between subnets using either or both of the following options:

- **Network Security groups (NSGs):** Network security groups and application security groups can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.
- **Network virtual appliances (NVA):** A network virtual appliance (NVA) is a VM that performs a network function, such as a firewall, WAN optimization, or other network function.

## Route network traffic

Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

- **Route tables:** You can create custom route tables with routes that control where traffic is routed to for each subnet.
- **Border gateway protocol (BGP) routes:** If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate your on-premises BGP routes to your virtual networks.

## Virtual network integration for Azure services

Integrating Azure services to an Azure virtual network enables private access to the service from virtual machines or compute resources in the virtual network. You can integrate Azure services in your virtual network with the following options:

- Deploying **dedicated instances of the service** into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.
- Using **Private Link** to access privately a specific instance of the service from your virtual network and from on-premises networks.
- You can also access the service using public endpoints by extending a virtual network to the service, through **service endpoints**. Service endpoints allow service resources to be secured to the virtual network.

## Comparison of Virtual Network Peering and VPN Gateway

Virtual network peering and VPN gateways both support the following connection types:

- Virtual networks in different regions.
- Virtual networks in different Azure Active Directory tenants.
- Virtual networks in different Azure subscriptions.
- Virtual networks that use a mix of Azure deployment models (Resource Manager and classic).

Item	Virtual network peering	VPN Gateway
<b>Limits</b>	Up to 500 virtual network peerings per virtual network (see Networking limits).	One VPN gateway per virtual network. The maximum number of tunnels per gateway depends on the gateway SKU.
<b>Pricing model</b>	Ingress/Egress	Hourly + Egress
<b>Encryption</b>	Software-level encryption is recommended.	Custom IPsec/IKE policy can be applied to new or existing connections. See About cryptographic requirements and Azure VPN gateways.

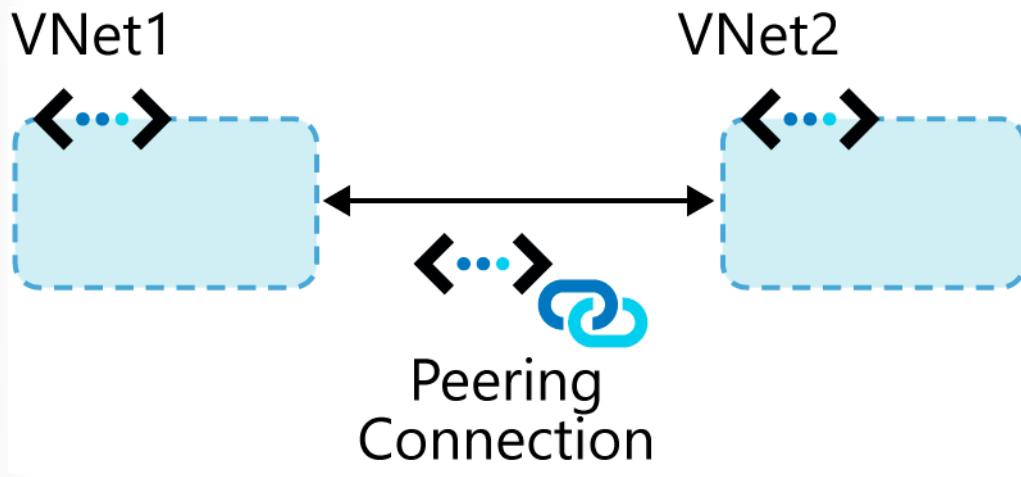
<b>Item</b>	<b>Virtual network peering</b>	<b>VPN Gateway</b>
<b>Bandwidth limitations</b>	No bandwidth limitations.	Varies based on SKU. See Gateway SKUs by tunnel, connection, and throughput.
<b>Private?</b>	Yes. Routed through Microsoft backbone and private. No public internet involved.	Public IP involved.
<b>Transitive relationship</b>	Peering connections are non-transitive. Transitive networking can be achieved using NVAs or gateways in the hub virtual network. See Hub-spoke network topology for an example.	If virtual networks are connected via VPN gateways and BGP is enabled in the virtual network connections, transitivity works.
<b>Initial setup time</b>	Fast	~30 minutes
<b>Typical scenarios</b>	Data replication, database failover, and other scenarios needing frequent backups of large data.	Encryption-specific scenarios that are not latency sensitive and do not need high throughout.

# Virtual Network Peering

## Connect Services with Virtual Network Peering

You can use virtual network peering to directly connect Azure virtual networks. When you use peering to connect virtual networks, virtual machines (VMs) in these networks can communicate with each other as if they were in the same network.

In peered virtual networks, traffic between virtual machines is routed through the Azure network. The traffic uses only private IP addresses. It doesn't rely on internet connectivity, gateways, or encrypted connections. The traffic is always private, and it takes advantage of the high bandwidth and low latency of the Azure backbone network.



The two types of peering connections are created in the same way:

- **Virtual network peering** connects virtual networks in the same Azure region, such as two virtual networks in North Europe.
- **Global virtual network peering** connects virtual networks that are in different Azure regions, such as a virtual network in North Europe and a virtual network in West Europe.

Virtual network peering doesn't affect or disrupt any resources that you've already deployed to the virtual networks. But when you use virtual network peering, consider the key features that the following sections define.

### Reciprocal connections

When you create a virtual network peering connection in only one virtual network to connect to a peer in another network, you're not connecting the networks together. To connect the networks by using virtual network peering, you have to create connections in each virtual network.

Think of how you connect two network switches together. You connect a cable to each switch and maybe configure some settings so that the switches can communicate. Virtual network peering requires similar connections in each virtual network. Reciprocal connections provide this functionality.

### Cross-subscription virtual network peering

You can use virtual network peering even when both virtual networks are in different subscriptions. This might be necessary for mergers and acquisitions or to connect virtual networks in subscriptions that different departments manage. Virtual networks can be in different subscriptions, and the subscriptions can use the same or different Azure Active Directory tenants.

When you use virtual network peering across subscriptions, you might find that an administrator of one subscription doesn't administer the peer network's subscription. The administrator might not be able to configure both ends of the connection. To peer the virtual networks when both subscriptions are in different Azure Active Directory tenants, the administrators of each subscription must grant the peer subscription's administrator the Network Contributor role on their virtual network.

## Transitivity and Gateway Transit

Virtual network peering is nontransitive. Only virtual networks that are directly peered can communicate with each other. The virtual networks can't communicate with the peers of their peers.

Suppose, for example, that your three virtual networks (A, B, C) are peered like this: A <-> B <-> C. Resources in A can't communicate with resources in C because that traffic can't transit through virtual network B. If you need communication between virtual network A and virtual network C, you must explicitly peer these two virtual networks.

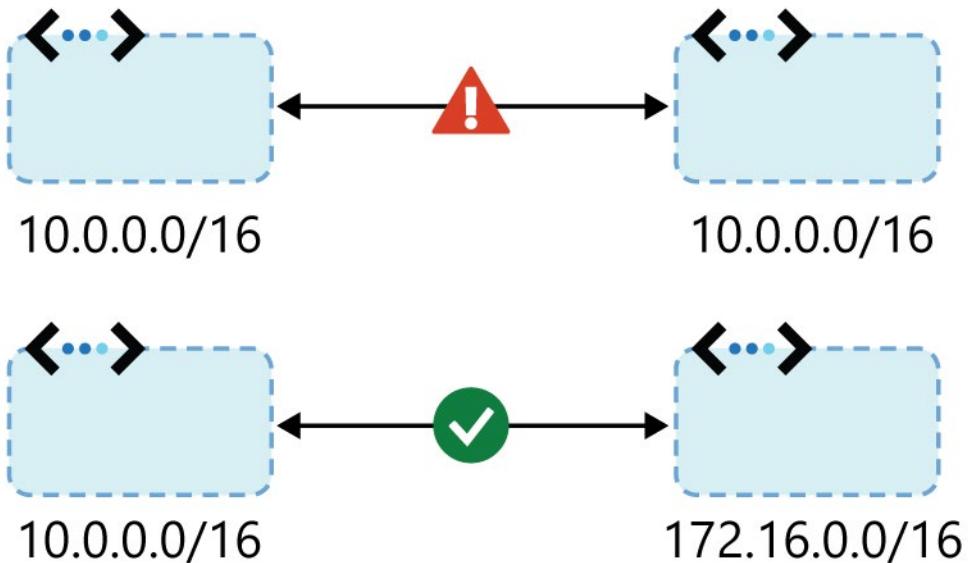
### Gateway Transit

You can configure transitive connections on-premises if you use virtual network gateways as transit points. Using gateway transit, you can enable on-premises connectivity without deploying virtual network gateways to all your virtual networks. This method might reduce cost and complexity. By using gateway peering, you can configure a single virtual network as a hub network. Connect this hub network to your on-premises datacenter and share its virtual network gateway with peers.

To enable gateway transit, configure the **Allow gateway transit** option in the hub virtual network where you deployed the gateway connection to your on-premises network. Also configure the Use remote gateways option in any spoke virtual networks.

### Overlapping address spaces

IP address spaces of connected networks within Azure and between Azure and your on-premises system can't overlap. This is also true for peered virtual networks. Keep this rule in mind when you're planning your network design. In any networks you connect through virtual network peering, VPN, or ExpressRoute, assign different address spaces that don't overlap.



### When to choose virtual network peering

Virtual network peering can be the best way to enable network connectivity between services that are in different virtual networks. Because it's easy to implement and deploy, and it works well across regions and subscriptions, virtual network peering should be your first choice when you need to integrate Azure virtual networks.

Peering might not be your best option if you have existing VPN or ExpressRoute connections or services behind Azure Basic Load Balancers that would be accessed from a peered virtual network. In these cases, you should research alternatives.

## Choose Between Virtual Network Peering and VPN Gateways in Azure

This section compares two ways to connect virtual networks in Azure: virtual network peering and VPN gateways.

A virtual network is a virtual, isolated portion of the Azure public network. By default, traffic cannot be routed between two virtual networks. However, it's possible to connect virtual networks, either within a single region or across two regions, so that traffic can be routed between them.

### Overview

**Virtual network peering.** Virtual network peering connects two Azure virtual networks. Once peered, the virtual networks appear as one for connectivity purposes. Traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, through private IP addresses only. No public internet is involved. You can also peer virtual networks across Azure regions (global peering).

**VPN gateways.** A VPN gateway is a specific type of virtual network gateway that is used to send traffic between an Azure virtual network and an on-premises location over the public internet. You can also use a VPN gateway to send traffic between Azure virtual networks. Each virtual network can have at most one VPN gateway.

Virtual network peering provides a low-latency, high-bandwidth connection. There is no gateway in the path, so there are no extra hops, ensuring low latency connections. It's useful in scenarios such as cross-region data replication and database failover. Because traffic is private and remains on the Microsoft backbone, also consider virtual network peering if you have strict data policies and want to avoid sending any traffic over the internet.

VPN gateways provide a limited bandwidth connection and are useful in scenarios where you need encryption but can tolerate bandwidth restrictions. In these scenarios, customers are also not as latency-sensitive.

### Gateway transit

Virtual network peering and VPN Gateways can also coexist via gateway transit

Gateway transit enables you to use a peered virtual network's gateway for connecting to on-premises, instead of creating a new gateway for connectivity. As you increase your workloads in Azure, you need to scale your networks across regions and virtual networks to keep up with the growth. Gateway transit allows you to share an ExpressRoute or VPN gateway with all peered virtual networks and lets you manage the connectivity in one place. Sharing enables cost-savings and reduction in management overhead.

With gateway transit enabled on virtual network peering, you can create a transit virtual network that contains your VPN gateway, Network Virtual Appliance, and other shared services. As your organization grows with new applications or business units and as you spin up new virtual networks, you can connect to your transit virtual network using peering. This prevents adding complexity to your network and reduces management overhead of managing multiple gateways and other appliances.

# Implement VNet Peering

## Configure VNet Peering

Here are the steps to configure VNet peering. Notice you will need two virtual networks. To test the peering, you will need a virtual machine in each network. Initially, the VMs will not be able to communicate, but after configuration the communication will work. The step that is new is configuring the peering of the virtual networks.

1. Create two virtual networks.
2. **Peer the virtual networks.**
3. Create virtual machines in each virtual network.
4. Test the communication between the virtual machines.

To configure the peering use the **Add peering** page. There are only a few optional configuration parameters to consider.

### Configuration

#### Configure virtual network access settings

Allow virtual network access from vnet1 to vnet2 (i)

Disabled  Enabled

#### Configure forwarded traffic settings

Allow forwarded traffic from vnet2 to vnet1 (i)

Disabled  Enabled

#### Configure gateway transit settings

Allow gateway transit (i)

#### Configure Remote Gateways settings

Use remote gateways (i)

**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

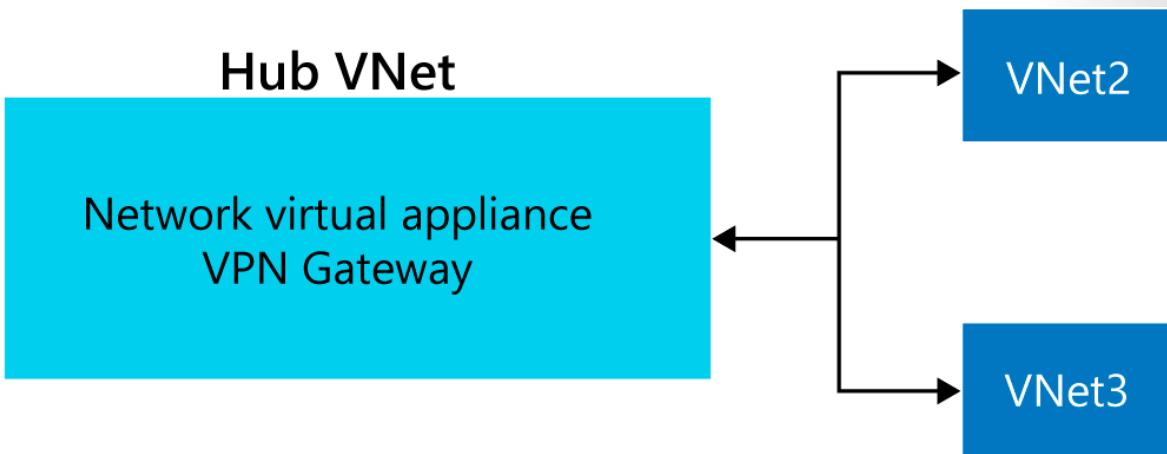
VNet Peering is nontransitive. This means that if you establish VNet Peering between VNet1 and VNet2 and between VNet2 and VNet3, VNet Peering capabilities do not apply between VNet1 and VNet3.

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
Peerings				

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

- **Updating.** When you create the peering to the second virtual network from the first virtual network, the peering status is Initiated.
- **Connected.** When you create the peering from the second virtual network to the first virtual network, the status is changed from Initiated to Connected.

# Demonstration - VNet Peering

- ✓ **Note:** For this demonstration you will need two virtual networks.
- ✓ **Note:** For managing the timing of this demonstration, you do not need to wait for the gateway to finish being creating.

## 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.

## Modify or Delete VNet Peering

Before changing a peering, familiarize yourself with the requirements and constraints and **necessary permissions**<sup>1</sup>.

1. In the search box at the top of the portal, enter *virtual networks* in the search box. When Virtual networks appear in the search results, select it. Do not select Virtual networks (classic) if it appears in the list, as you cannot create a peering from a virtual network deployed through the classic deployment model.
2. Select the virtual network in the list that you want to change peering settings for.
3. Under **SETTINGS**, select **Peerings**.
4. Select the peering you want to view or change settings for.
5. Change the appropriate setting. Read about the options for each setting in **step 5**<sup>2</sup> of Create a peering.
6. Select **Save**.

### Delete a peering

When a peering is deleted, traffic from a virtual network no longer flows to the peered virtual network. When virtual networks deployed through Resource Manager are peered, each virtual network has a peering to the other virtual network. Though deleting the peering from one virtual network disables the communication between the virtual networks, it does not delete the peering from the other virtual network. The peering status for the peering that exists in the other virtual network is Disconnected. You cannot recreate the peering until you re-create the peering in the first virtual network and the peering status for both virtual networks changes to Connected.

If you want virtual networks to communicate sometimes, but not always, rather than deleting a peering, you can set the Allow virtual network access setting to Disabled instead.

1. In the search box at the top of the portal, enter *virtual networks* in the search box. When Virtual networks appear in the search results, select it. Do not select Virtual networks (classic) if it appears in the list, as you cannot create a peering from a virtual network deployed through the classic deployment model.
2. Select the virtual network in the list that you want to delete a peering for.

<sup>1</sup> [https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering?WT.mc\\_id=thomasmaurer-blog-thmaure](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering?WT.mc_id=thomasmaurer-blog-thmaure)

<sup>2</sup> [https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering?WT.mc\\_id=thomasmaurer-blog-thmaure](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering?WT.mc_id=thomasmaurer-blog-thmaure)

3. Under **SETTINGS**, select **Peerings**.
4. On the right side of the peering you want to delete, select ..., select **Delete**, then select Yes to delete the peering from the first virtual network.
5. Complete the previous steps to delete the peering from the other virtual network in the peering.

## Requirements and Constraints

- You can peer virtual networks in the same region, or different regions. Peering virtual networks in different regions is also referred to as Global VNet Peering.
- When creating a global peering, the peered virtual networks can exist in any Azure public cloud region or China cloud regions or Government cloud regions. You cannot peer across clouds. For example, a VNet in Azure public cloud cannot be peered to a VNet in Azure China cloud.
- Resources in one virtual network cannot communicate with the front-end IP address of a Basic internal load balancer in a globally peered virtual network. Support for Basic Load Balancer only exists within the same region. Support for Standard Load Balancer exists for both, VNet Peering and Global VNet Peering.
- You can use remote gateways or allow gateway transit in globally peered virtual networks and locally peered virtual networks.
- The virtual networks can be in the same, or different subscriptions. When you peer virtual networks in different subscriptions, both subscriptions can be associated to the same or different Azure Active Directory tenant. If you don't already have an AD tenant, you can create one. Support for peering across virtual networks from subscriptions associated to different Azure Active Directory tenants is not available in Portal. You can use CLI, PowerShell, or Templates.
- The virtual networks you peer must have non-overlapping IP address spaces.
- You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network. To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.
- You can peer two virtual networks deployed through Resource Manager or a virtual network deployed through Resource Manager with a virtual network deployed through the classic deployment model. You cannot peer two virtual networks created through the classic deployment model
- When peering two virtual networks created through Resource Manager, a peering must be configured for each virtual network in the peering. You see one of the following types for peering status:
  - *Initiated*: When you create the peering to the second virtual network from the first virtual network, the peering status is Initiated.
  - *Connected*: When you create the peering from the second virtual network to the first virtual network, its peering status is Connected. If you view the peering status for the first virtual network, you see its status changed from Initiated to Connected. The peering is not successfully established until the peering status for both virtual network peerings is Connected.
- When peering a virtual network created through Resource Manager with a virtual network created through the classic deployment model, you only configure a peering for the virtual network deployed through Resource Manager. You cannot configure peering for a virtual network (classic), or between two virtual networks deployed through the classic deployment model. When you create the peering from the virtual network (Resource Manager) to the virtual network (Classic), the peering status is *Updating*, then shortly changes to *Connected*.

- A peering is established between two virtual networks. Peerings are not transitive. If you create peerings between:
  - VirtualNetwork1 & VirtualNetwork2
  - VirtualNetwork2 & VirtualNetwork3

There is no peering between VirtualNetwork1 and VirtualNetwork3 through VirtualNetwork2. If you want to create a virtual network peering between VirtualNetwork1 and VirtualNetwork3, you have to create a peering between VirtualNetwork1 and VirtualNetwork3.

- You can't resolve names in peered virtual networks using default Azure name resolution. To resolve names in other virtual networks, you must use **Azure DNS for private domains<sup>3</sup>** or a custom DNS server
- Resources in peered virtual networks in the same region can communicate with each other with the same bandwidth and latency as if they were in the same virtual network. Each virtual machine size has its own maximum network bandwidth however.
- A virtual network can be peered to another virtual network, and also be connected to another virtual network with an Azure virtual network gateway. When virtual networks are connected through both peering and a gateway, traffic between the virtual networks flows through the peering configuration, rather than the gateway.
- Point-to-Site VPN clients must be downloaded again after virtual network peering has been successfully configured to ensure the new routes are downloaded to the client.

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/dns/private-dns-overview?toc=/azure/virtual-network/toc.json>

## Module 3 Review Questions

### Module 3 Review Questions



#### Review Question 1

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 for TCP port 443.
- Create an inbound security rule for TCP port 443.

#### Review Question 2

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.

# Answers

## Review Question 1

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 for TCP port 443.
- Create an inbound security rule for TCP port 443.

### Explanation

*Associate a public IP address to NIC2 and create an inbound security rule for TCP port 443. 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 2

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.

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.*



## Module 4 Implement VMs for Windows and Linux

### Overview - Running Linux and Windows Virtual Machines on Azure

### Checklist for Creating an Azure Virtual Machine

Performing a migration of on-premises servers to Azure requires planning and care. You can move them all at once, or more likely, in small batches or even individually. Before you create a single VM, you should sit down and sketch out your current infrastructure model and see how it might map to the cloud.

### Required resources for IaaS Virtual Machines

Below is a checklist of things to consider as you work through this lesson:

- 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

When you set up a virtual network, you specify the available address spaces, subnets, and security. If the VNet will be connected to other VNets, you must select address ranges that are not overlapping. This is the range of private addresses that the VMs and services in your network can use. You can use unrouteable IP addresses such as 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, or define your own range. Azure will treat any address range as part of the private VNet IP address space if it is only reachable within the

VNet, within interconnected VNets, and from your on-premises location. If someone else is responsible for the internal networks, you should work with that person before selecting your address space to make sure there is no overlap and to let them know what space you want to use, so they don't try to use the same range of IP addresses.

## Segregate the network

After deciding the virtual network address space(s), you can create one or more subnets for your virtual network. You do this to break up your network into more manageable sections. For example, you might assign 10.1.0.0 to VMs, 10.2.0.0 to back-end services, and 10.3.0.0 to SQL Server VMs.

## Secure the network

By default, there is no security boundary between subnets, so services in each of these subnets can talk to one another. However, you can set up Network Security Groups (NSGs), which allow you to control the traffic flow to and from subnets and to and from VMs. NSGs act as software firewalls, applying custom rules to each inbound or outbound request at the network interface and subnet level. This allows you to fully control every network request coming in or out of the VM.

## Plan each VM deployment

Once you have mapped out your communication and network requirements, you can start thinking about the VMs you want to create. A good plan is to select a server and take an inventory:

- Which ports are open?
- Which OS is used?
- How much disk space is in use?
- What kind of data does this use? Are there restrictions (legal or otherwise) with not having it on-premises?
- What sort of CPU, memory, and disk I/O load does the server have? Is there burst traffic to account for?

We can then start to answer some of the questions Azure will have for a new virtual machine.

## Naming 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

Element	Example	Notes
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.

## What is an Azure resource?

An Azure resource is a manageable item in Azure. Just like a physical computer in your datacenter, VMs have several elements that are needed to do their job:

- The VM itself
- Storage account for the disks
- Virtual network (shared with other VMs and services)
- Network interface to communicate on the network
- Network Security Group(s) to secure the network traffic
- Public Internet address (optional)

Azure will create all of these resources if necessary, or you can supply existing ones as part of the deployment process. Each resource needs a name that will be used to identify it. If Azure creates the resource, it will use the VM name to generate a resource name - another reason to be very consistent with your VM names!

## 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. First, the location can limit your available options. Each region has different hardware available and some configurations are not available in all regions. Second, 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.

## 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:

Option	Description
<b>General purpose</b>	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.
<b>Compute optimized</b>	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.
<b>Memory optimized</b>	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.
<b>Storage optimized</b>	Storage optimized VMs are designed to have high disk throughput and IO. Ideal for VMs running databases.
<b>GPU</b>	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.
<b>High performance computes</b>	High performance compute is the fastest and most powerful CPU virtual machines with optional high-throughput network interfaces.
<b>Confidential compute</b>	Designed to protect the confidentiality and the integrity of data and code while it's processed in the cloud.

## 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 upgrade or downgrade 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.

The VM size can be changed while the VM is running, as long as the new size is available in the current hardware cluster the VM is running on. The Azure portal makes this obvious by only showing you available size choices. The command line tools will report an error if you attempt to resize a VM to an unavailable size. Changing a running VM size will automatically reboot the machine to complete the request.

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.

# Virtual Machine Sizes (Windows and Linux)

This section describes the available sizes and options for the Azure virtual machines you can use to run your Linux and Windows apps and workloads. It also provides deployment considerations to be aware of when you're planning to use these resources.

## Sizes for Windows and Linux virtual machines in Azure

Type	Sizes	Description
<b>General purpose</b>	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dv4, Dsv4, Ddv4, Ddsv4	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
<b>Compute optimized</b>	Fsv2	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
<b>Memory optimized</b>	Esv3, Ev3, Easv4, Eav4, Ev4, Esv4, Edv4, Edsv4, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
<b>Storage optimized</b>	Lsv2	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
<b>GPU</b>	NC, NCv2, NCv3, ND, NDv2 (Preview), NV, NVv3, NVv4	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
<b>High performance compute</b>	HB, HBv2, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).
<b>Confidential compute</b>	DCsv2-Series	Supports a larger range of deployment capabilities, have 2x the Enclave Page Cache (EPC) and a larger selection of sizes compared to the DC-Series VMs.

## The Pricing Model

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-second basis. For example, you are only charged for 455 seconds of usage if the VM is deployed for 455 seconds. 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 the following payment options for compute costs.

Option	Description
<b>Pay as you go</b>	With the pay-as-you-go option, you pay for compute capacity by the second, with no long-term commitment or upfront payments. 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.
<b>Reserved Virtual Machine Instances</b>	The Reserved Virtual Machine Instances (RIs) 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.
<b>Spot Pricing</b>	Purchase unused compute capacity at a discount. Spot VMs are for workloads that can be interrupted, providing scalability while reducing costs. Run workloads on Virtual Machines or Virtual Machine Scale Sets.
<b>Azure Hybrid Benefit</b>	For customers who have licenses with Software Assurance, which helps maximize the value of existing on-premises Windows Server and/or SQL Server license investments when migrating to Azure.

## Select an Operating System

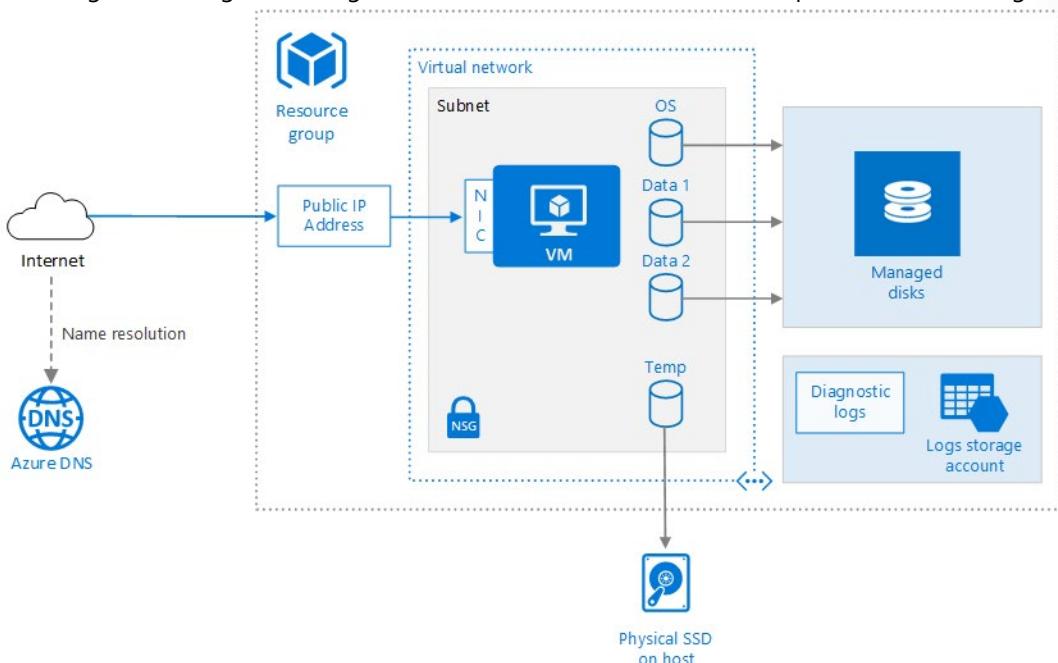
Azure provides a variety of OS images that you can install into the VM, including several versions of Windows and flavors of Linux. As mentioned earlier, the choice of OS will influence your hourly compute pricing as Azure bundles the cost of the OS license into the price.

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.

## Running Linux and Windows Virtual Machines on Azure

Provisioning a virtual machine (VM) in Azure requires some additional components besides the VM itself, including networking and storage resources. This lesson describes best practices for running a Linux or



Windows virtual machine on Azure.

## Resource Groups and Virtual Machines

A resource group is a logical container that holds related Azure resources. In general, group resources based on their lifetime and who will manage them.

Place closely associated resources that share the same lifecycle into the same resource group. Resource groups allow you to deploy and monitor resources as a group and track billing costs by resource group.

You can also delete resources as a set, which is useful for test deployments. Assign meaningful resource names to simplify locating a specific resource and understanding its role.

## Storage for the VM

All Azure virtual machines will have at least two virtual hard disks (VHDs). The first disk stores the operating system, and the second is used as temporary storage. You can add additional disks to store application data; the maximum number is determined by the VM size selection (typically two per CPU). It's

common to create one or more data disks, particularly since the OS disk tends to be quite small. Also, separating out the data to different VHDs allows you to manage the security, reliability, and performance of the disk independently.

The data for each VHD is held in **Azure Storage** as page blobs, which allows Azure to allocate space only for the storage you use. It's also how your storage cost is measured; you pay for the storage you are consuming.

## What is Azure Storage?

Azure Storage is Microsoft's cloud-based data storage solution. It supports almost any type of data and provides security, redundancy, and scalable access to the stored data. A storage account provides access to objects in Azure Storage for a specific subscription. VMs always have one or more storage accounts to hold each attached virtual disk.

Virtual disks can be backed by either **Standard** or **Premium** Storage accounts. Azure Premium Storage leverages solid-state drives (SSDs) to enable high performance and low latency for VMs running I/O-intensive workloads. Use Azure Premium Storage for production workloads, especially those that are sensitive to performance variations or are I/O intensive. For development or testing, Standard storage is fine.

When you create disks, you will have two options for managing the relationship between the storage account and each VHD. You can choose either **unmanaged disks** or **managed disks**.

Option	Description
Unmanaged disks	With unmanaged disks, you are responsible for the storage accounts that are used to hold the VHDs that correspond to your VM disks. You pay the storage account rates for the amount of space you use. A single storage account has a fixed-rate limit of 20,000 I/O operations/sec. This means that a storage account is capable of supporting 40 standard virtual hard disks at full utilization. If you need to scale out with more disks, then you'll need more storage accounts, which can get complicated.
Managed disks	Managed disks are the newer and recommended disk storage model. They elegantly solve this complexity by putting the burden of managing the storage accounts onto Azure. You specify the size of the disk, up to 4 TB, and Azure creates and manages both the disk and the storage. You don't have to worry about storage account limits, which makes managed disks easier to scale out.

# Configure High Availability

## Availability Sets

Workloads are typically spread across different virtual machines to gain high throughput, performance, and to create redundancy in case a VM is impacted due to an update or other event.

There are few options that Azure provides to achieve High Availability.

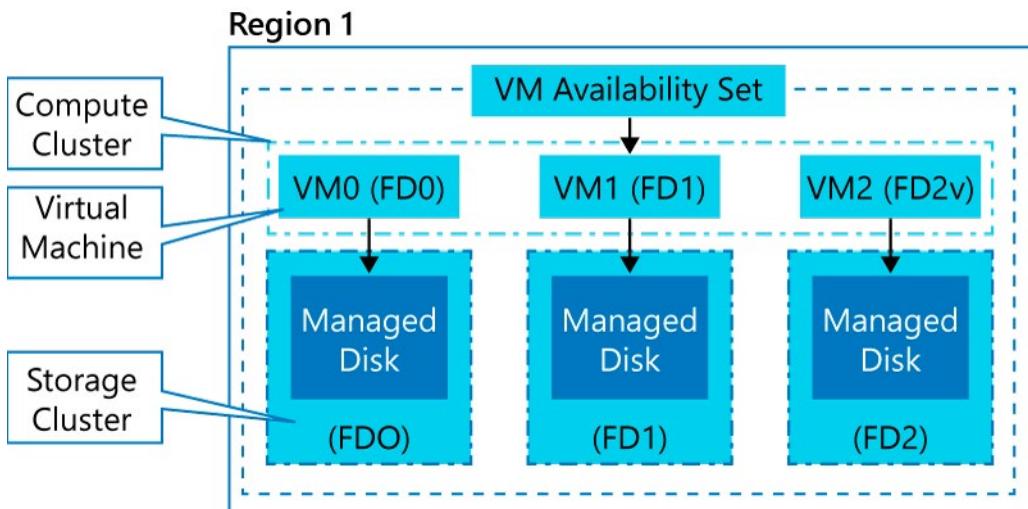
An availability set is a logical grouping of VMs within a datacenter that allows Azure to understand how your application is built to provide for redundancy and availability.

It is recommended that two or more VMs are created within an availability set to provide for a highly available application and to meet the 99.95% Azure SLA. There is no cost for the Availability Set itself, you only pay for each VM instance that you create.

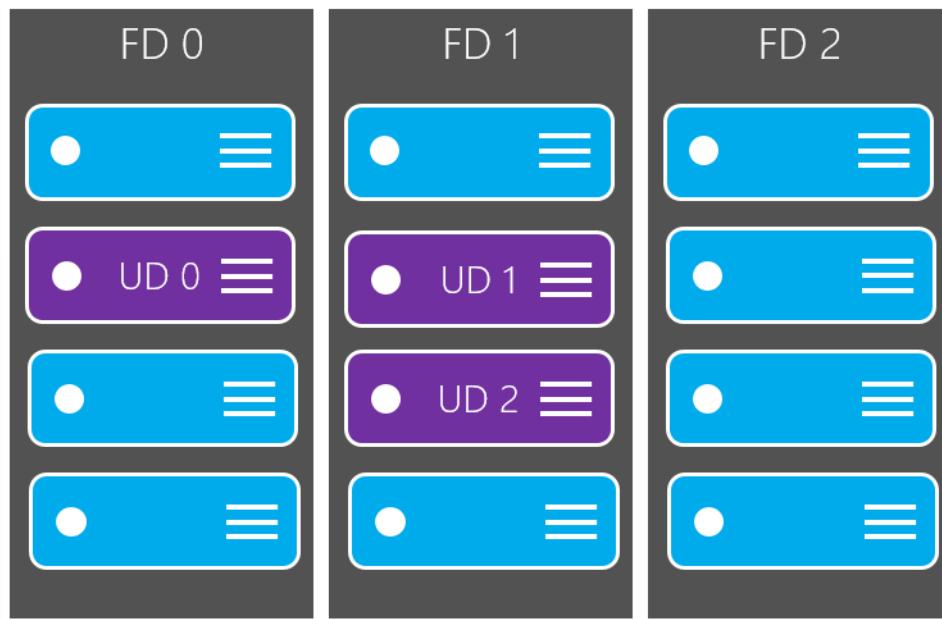
In an availability set, VMs are automatically distributed across these fault domains. This approach limits the impact of potential physical hardware failures, network outages, or power interruptions.

For VMs using Azure Managed Disks, VMs are aligned with managed disk fault domains when using a managed availability set. This alignment ensures that all the managed disks attached to a VM are within the same managed disk fault domain.

Only VMs with managed disks can be created in a managed availability set. The number of managed disk fault domains varies by region - either two or three managed disk fault domains per region.



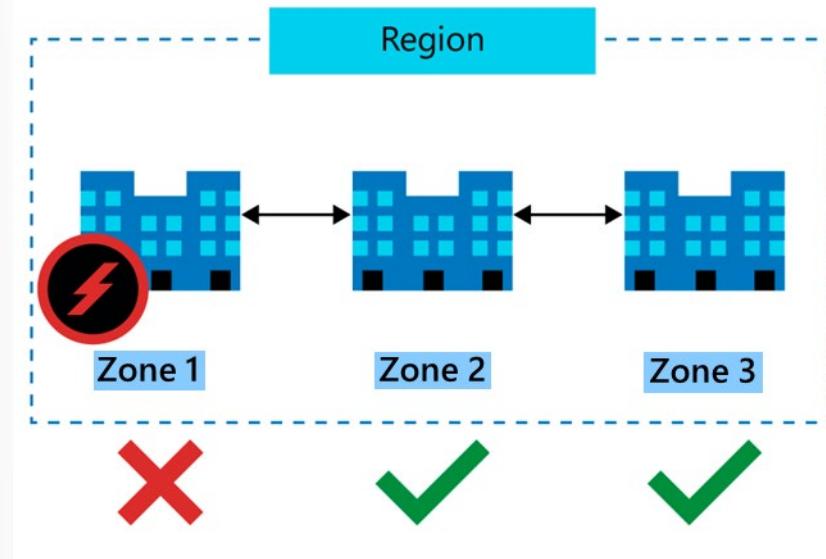
VMs within an availability set are also automatically distributed across update domains.



## Availability Zones

Availability zones expand the level of control you have to maintain the availability of the applications and data on your VMs. An Availability Zone is a physically separate zone, within an Azure region. There are three Availability Zones per supported Azure region.

Each Availability Zone has a distinct power source, network, and cooling. By architecting your solutions to use replicated VMs in zones, you can protect your apps and data from the loss of a datacenter. If one zone is compromised, then replicated apps and data are instantly available in another zone.



### Fault domains

A fault domain is a logical group of underlying hardware that share a common power source and network switch, similar to a rack within an on-premises datacenter.

### Update domains

An update domain is a logical group of underlying hardware that can undergo maintenance or be rebooted at the same time.

This approach ensures that at least one instance of your application always remains running as the Azure platform undergoes periodic maintenance. The order of update domains being rebooted may not proceed sequentially during maintenance, but only one update domain is rebooted at a time.

# Deploy and Configure Scale Sets

## Virtual Machines Scale Sets

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update many VMs. We recommend that two or more VMs are created within a scale set to provide for a highly available application and to meet the 99.95% Azure SLA.

There is no cost for the scale set itself, you only pay for each VM instance that you create. When a single VM is using Azure premium SSDs, the Azure SLA applies for unplanned maintenance events. Virtual machines in a scale set can be deployed across multiple update domains and fault domains to maximize availability and resilience to outages due to data center outages, and planned or unplanned maintenance events.

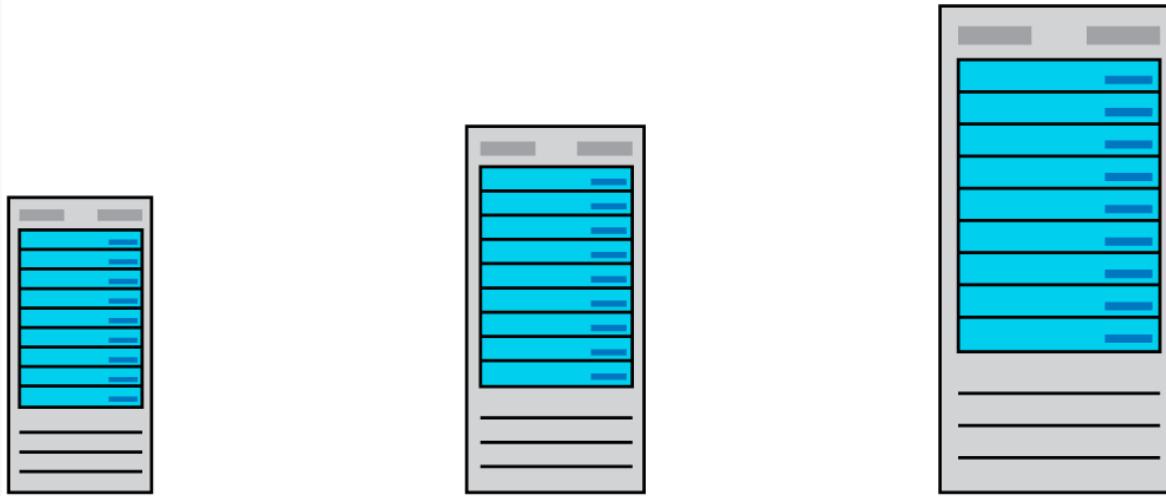
### Fault domains and update domains

Virtual machine scale sets simplify designing for high availability by aligning fault domains and update domains. You will only have to define fault domains count for the scale set. The number of fault domains available to the scale sets may vary by region.

## Scaling Concepts

Generally, there are two types of scaling: vertical scaling and horizontal scaling.

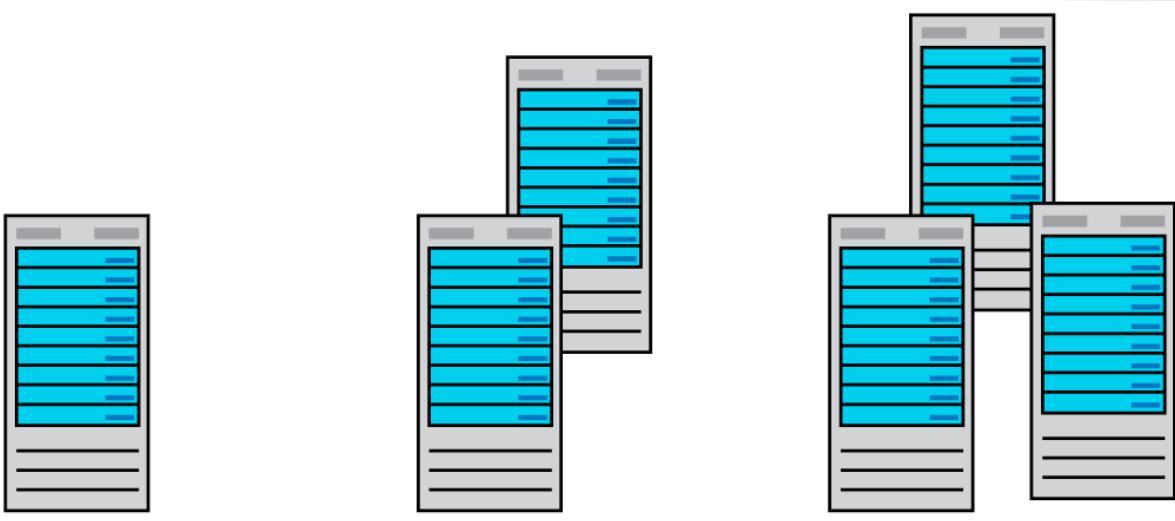
### Vertical scaling



Vertical scaling, also known as scale up and scale down, means increasing or decreasing virtual machine sizes in response to a workload. Vertical scaling makes the virtual machines more (scale up) or less (scale down) powerful. Vertical scaling can be useful when:

- A service built on virtual machines is under-utilized (for example at weekends). Reducing the virtual machine size can reduce monthly costs.
- Increasing virtual machine size to cope with larger demand without creating additional virtual machines.

## Horizontal Scaling



Horizontal scaling, also referred to as scale out and scale in, where the number of VMs is altered depending on the workload. In this case, there is a increase (scale out) or decrease (scale in) in the number of virtual machine instances.

## Considerations

- Vertical scaling generally has more limitations. It's dependent on the availability of larger hardware, which quickly hits an upper limit and can vary by region. Vertical scaling also usually requires a virtual machine to stop and restart.
- Horizontal scaling is generally more flexible in a cloud situation as it allows you to run potentially thousands of virtual machines to handle load.
- Reprovisioning means removing an existing virtual machine and replacing it with a new one. Do you need to retain your data?

## Virtual Machines Scale Sets

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update many VMs. We recommend that two or more VMs are created within a scale set to provide for a highly available application and to meet the 99.95% Azure SLA.

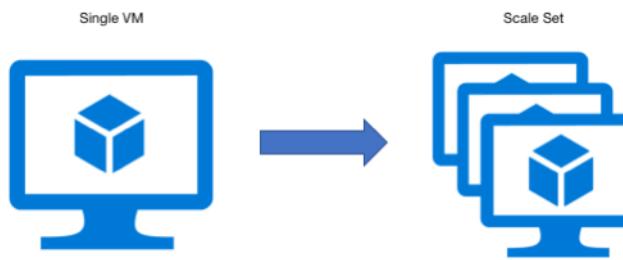
There is no cost for the scale set itself, you only pay for each VM instance that you create. When a single VM is using Azure premium SSDs, the Azure SLA applies for unplanned maintenance events. Virtual machines in a scale set can be deployed across multiple update domains and fault domains to maximize availability and resilience to outages due to data center outages, and planned or unplanned maintenance events.

## Fault Domains and Update Domains

Virtual machine scale sets simplify designing for high availability by aligning fault domains and update domains. You will only have to define fault domains count for the scale set. The number of fault domains available to the scale sets may vary by region.

## Auto-Scaling (VMSS)

Virtual machine scale sets are an Azure Compute resource you can use to deploy and manage a set of **identical** VMs. With all VMs configured the same, VM scale sets are designed to support true auto-scale – no pre-provisioning of VMs is required – and as such makes it easier to build large-scale services targeting big compute, big data, and containerized workloads. So, as demand goes up more virtual machine instances can be added, and as demand goes down virtual machines instances can be removed. The process can be manual or automated or a combination of both.



## Scale Set Benefits

- All VM instances are created from the same base OS image and configuration. This approach lets you easily manage hundreds of VMs without additional configuration tasks or network management.
- Scale sets support the use of the Azure load balancer for basic layer-4 traffic distribution, and Azure Application Gateway for more advanced layer-7 traffic distribution and SSL termination.
- Scale sets are used to run multiple instances of your application. If one of these VM instances has a problem, customers continue to access your application through one of the other VM instances with minimal interruption.
- Customer demand for your application may change throughout the day or week. To match customer demand, scale sets can automatically increase the number of VM instances as application demand increases, then reduce the number of VM instances as demand decreases. This is known as autoscale.
- Scale sets support up to 1,000 VM instances. If you create and upload your own custom VM images, the limit is 600 VM instances.

## Implementing Scale Sets

Below are considerations for implementing Scale Sets.

- **Initial instance count.** Number of virtual machines in the scale set (0 to 1000).
- **Instance size.** The size of each virtual machine in the scale set.
- **Azure spot instance.** Low-priority VMs are allocated from Microsoft Azure's excess compute capacity, enabling several types of workloads to run for a significantly reduced cost.

- **Use managed disks.** Managed disks hide the underlying storage accounts and instead shows the abstraction of a disk. Unmanaged disks expose the underlying storage accounts and VHD blobs.
- **Enable scaling beyond 100 instances.** If No, the scale set will be limited to 1 placement group and can have a max capacity of 100. If Yes, the scale set can span multiple placement groups. This allows for capacity to be up to 1,000 but changes the availability characteristics of the scale set.
- **Spreading algorithm.** We recommend deploying with max spreading for most workloads, as this approach provides the best spreading in most cases.

The screenshot shows the configuration interface for a VM Scale Set. Key settings include:

- Instance:** Initial instance count is set to 2.
- Size:** Standard D2s v3 (2 vcpus, 8 GiB memory, \$85.41/month).
- Azure Spot instance:** No (radio button selected).
- Use managed disks:** Yes (radio button selected).
- Allocation policy:**
  - Enable scaling beyond 100 instances: Yes (radio button selected).
  - Spreading algorithm: Max spreading (radio button selected).

## Create a VM Scale Set in the Azure Portal

Create a public load balancer using the portal. The name and public IP address you create are automatically configured as the load balancer's front end.

1. In the search box, type *load balancer*. Under Marketplace in the search results, pick **Load balancer**.
2. In the **Basics** tab of the Create load balancer page, enter or select the following information:

Setting	Value
Subscription	Select your subscription.
Resource group	Select Create new and type myVMSSResource-Group in the text box.
Name	myLoadBalancer
Region	Select East US.
Type	Select Public.
SKU	Select Standard.
Public IP address	Select Create new.
Public IP address name	MyPip
Assignment	Static

3. Select **Review + create**.
4. Select **Create**.

Home > Create load balancer

## Create load balancer

**Basics** Tags Review + create

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

**Project details**

Subscription \* Pay-As-You-Go

Resource group \* (New) myVMSSResourceGroup [Create new](#)

**Instance details**

Name \* myLoadBalancer

Region \* (US) East US

Type \*  Internal  Public

SKU \*  Basic  Standard

**Public IP address**

Public IP address \*  Create new  Use existing

Public IP address name \* myPip

Public IP address SKU Standard

Assignment \*  Dynamic  Static

Availability zone \* Zone-redundant

**Review + create** < Previous Next : Tags > Download a template for automation

### Create virtual machine scale set

You can deploy a scale set with a Windows Server image or Linux image such as RHEL, CentOS, Ubuntu, or SLES.

1. Type *Scale set* in the search box. In the results, under **Marketplace**, select **Virtual machine scale sets**. The **Create a virtual machine scale set** page will open.
2. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then choose **Create new** resource group. Type *myVMSSResourceGroup* for the name and then select OK .
3. Type *myScaleSet* as the name for your scale set.
4. In **Region**, select a region that is close to your area.

5. Leave the default value of **ScaleSet VMs** for **Orchestrator**.
  6. Select a marketplace image for Image. In this example, we have chosen Ubuntu Server 18.04 LTS.
  7. Enter your desired username, and select which authentication type you prefer.
- A **Password** must be at least 12 characters long and meet three out of the four following complexity requirements: one lower case character, one upper case character, one number, and one special character.
  - If you select a Linux OS disk image, you can instead choose **SSH public key**. Only provide your public key, such as `~/.ssh/id_rsa.pub`. You can use the Azure Cloud Shell from the portal to create and use SSH keys.

Home > Virtual machine scale sets > Create a virtual machine scale set

## Create a virtual machine scale set

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

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs.

[Learn more about virtual machine scale sets](#)

**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) myVMSScaleSet [Create new](#)

**Instance details**

**Virtual machine scale set name \*** myScaleSet

**Region \*** (US) East US

**Availability zone** None

**Orchestrator \*** Virtual Machines **ScaleSet VMs**

**Image \*** Ubuntu Server 18.04 LTS [Browse all public and private images](#)

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

**Administrator account**

**Authentication type**  Password  SSH public key

**Username \***

**SSH public key \***

**Review + create** < Previous Next : Instance >

8. Select **Next** to move to the other pages.

9. Leave the defaults for the **Instance** and **Disks** pages.
10. On the **Networking** page, under **Load balancing**, select **Yes** to put the scale set instances behind a load balancer.
11. In **Load balancing options**, select **Azure load balancer**.
12. In **Select a load balancer**, select **myLoadBalancer** that you created earlier.
13. For Select a **backend pool**, select **Create** new, type *myBackendPool*, and select **Create**.
14. Select **Review + create**.
15. Select **Create** to deploy the scale set.

# Implement Azure Dedicated Hosts

## Azure Dedicated Hosts

Azure Dedicated Host is a service that provides physical servers - able to host one or more virtual machines - dedicated to one Azure subscription. Dedicated hosts are the same physical servers used in our data centers, provided as a resource. You can provision dedicated hosts within a region, availability zone, and fault domain. Then, you can place VMs directly into your provisioned hosts, in whatever configuration best meets your needs.

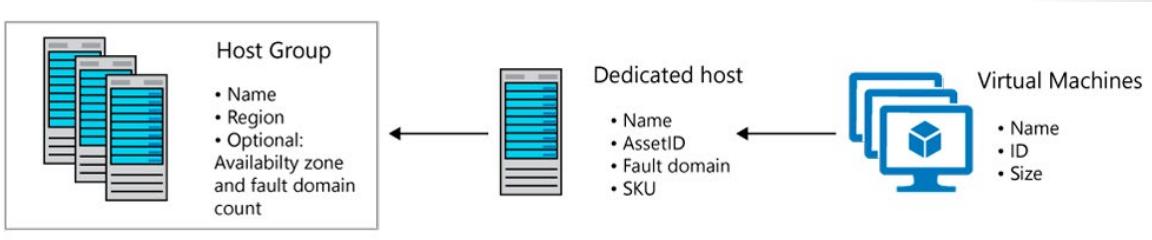
✓ **Note:** Virtual machine scale sets are not currently supported on dedicated hosts.

### Benefits

Reserving the entire host provides the following benefits:

- **Hardware isolation at the physical server level.** No other VMs will be placed on your hosts. Dedicated hosts are deployed in the same data centers and share the same network and underlying storage infrastructure as other, non-isolated hosts.
- **Control over maintenance events initiated by the Azure platform.** While the majority of maintenance events have little to no impact on your virtual machines, there are some sensitive workloads where each second of pause can have an impact. With dedicated hosts, you can opt-in to a maintenance window to reduce the impact to your service.

### Groups, hosts, and VMs



A host group is a resource that represents a collection of dedicated hosts. You create a host group in a region and an availability zone, and add hosts to it.

A host is a resource, mapped to a physical server in an Azure data center. The physical server is allocated when the host is created. A host is created within a host group. A host has a SKU describing which VM sizes can be created. Each host can host multiple VMs, of different sizes, as long as they are from the same size series.

## High Availability Considerations

For high availability, you should deploy multiple VMs, spread across multiple hosts (minimum of 2). With Azure Dedicated Hosts, you have several options to provision your infrastructure to shape your fault isolation boundaries.

### Use Availability Zones for fault isolation

Availability zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. A host group is created in a single availability zone. Once created, all hosts will be placed within that zone.

To achieve high availability across zones, you need to create multiple host groups (one per zone) and spread your hosts accordingly.

If you assign a host group to an availability zone, all VMs created on that host must be created in the same zone.

### Use Fault Domains for fault isolation

A host can be created in a specific fault domain. Just like VM in a scale set or availability set, hosts in different fault domains will be placed on different physical racks in the data center. When you create a host group, you are required to specify the fault domain count.

When creating hosts within the host group, you assign fault domain for each host. The VMs do not require any fault domain assignment.

VMs deployed to hosts with different fault domains, will have their underlying managed disks services on multiple storage stamps, to increase the fault isolation protection.

### Using Availability Zones and Fault Domains

You can use both capabilities together to achieve even more fault isolation. In this case, you will specify the availability zone and fault domain count in for each host group, assign a fault domain to each of your hosts in the group, and assign an availability zone to each of your VMs

## Azure Dedicated Hosts Capacity

Once a dedicated host is provisioned, Azure assigns it to physical server. This guarantees the availability of the capacity when you need to provision your VM. Azure uses the entire capacity in the region (or zone) to pick a physical server for your host.

### Quotas

There is a default quota limit of 3000 vCPUs for dedicated hosts, per region. But, the number of hosts you can deploy is also limited by the quota for the VM size family used for the host. For example, a Pay-as-you-go subscription may only have a quota of 10 vCPUs available for the Dsv3 size series, in the East US region. In this case, you need to request a quota increase to at least 64 vCPUs before you can deploy a dedicated host. Select the **Request increase** button in the upper right corner to file a request if needed.

QUOTA	PROVIDER	LOCATION	USAGE
Standard Dsv3 Family vCPUs	Microsoft.Compute	East US	0 % 0 of 10

### Pricing

Users are charged per dedicated host, regardless how many VMs are deployed. In your monthly statement you will see a new billable resource type of hosts. The VMs on a dedicated host will still be shown in your statement, but will carry a price of 0.

The host price is set based on VM family, type (hardware size), and region. A host price is relative to the largest VM size supported on the host.

Software licensing, storage and network usage are billed separately from the host and VMs. There is no change to those billable items.

## Deploy VMs to Dedicated Hosts

This topic guides you through how to create and deploy an Azure dedicated host to virtual machines.

### Limitations

- Virtual machine scale sets are not currently supported on dedicated hosts.
- The sizes and hardware types available for dedicated hosts vary by region. Create a host group

You can use one or both of the following options with your dedicated hosts:

- Span across multiple availability zones. In this case, you are required to have a host group in each of the zones you wish to use.
- Span across multiple fault domains which are mapped to physical racks.

Below is a procedure for creating a host group using 1 availability zone and 2 fault domains.

- Open the Azure [portal](#)<sup>1</sup>.
- Select **Create a resource** in the upper left corner.
- Search for Host group and then select **Host Groups** from the results.
- In the **Host Groups** page, select **Create**.
- Select the subscription you would like to use, and then select **Create new**.
- Type *myDedicatedHostsRG* as the Name and then select **OK**.
- For **Host group name**, type *myHostGroup*.
- For **Location**, select **East US**.
- For **Availability Zone**, select **1**.
- For **Fault domain count**, select **2**.
- Select **Review + create**.
- Select **Create**.

### Create a dedicated host

- Select **Create a resource** in the upper left corner.
- Search for **Dedicated host** and then select **Dedicated hosts** from the results.
- In the **Dedicated Hosts** page, select **Create**.
- Select the subscription you would like to use.
- Select **myDedicatedHostsRG** as the Resource group.
- In **Instance details**, type *myHost* for the **Name** and **select East US** for the location.
- In **Hardware profile**, select **Standard Es3 family - Type 1** for the Size family, select **myHostGroup** for the Host group and then **select 1** for the Fault domain. Leave the defaults for the remaining fields.
- Select **Review + create**.
- Select **Create**.

<sup>1</sup> <https://portal.azure.com/>

### Create a VM

1. Choose **Create a resource** in the upper left-hand corner of the Azure portal.
2. In the **New** page, under **Popular**, select **Windows Server 2016 Datacenter**.
3. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then select **myDedicatedHostsRG** as the Resource group.
4. Under **Instance details**, type *myVM* for the Virtual machine name and choose **East US** for your Location.
5. In **Availability options** select **Availability zone**, select **1** from the drop-down.
6. For the size, select **Change size**. In the list of available sizes, choose one from the Esv3 series, like **Standard E2s v3**.
7. Under **Administrator** account, provide a username, such as *azureuser* and a password.
8. Under **Inbound port rules**, choose **Allow** selected ports and then select **RDP (3389)** from the drop-down.
9. At the top of the page, select the **Advanced tab** and in the **Host** section, select *myHostGroup* for **Host group** and *myHost* for the **Host**.

Host

Optionally placing your virtual machine in a host [Learn more](#)

Host group ⓘ myHostGroup | Zone 1 | eastus ▾

Host ⓘ myHost ▾

10. Select **Review + create**.

11. Select **Create**.

# Configure Azure Disk Encryption

## Azure Encryption Technologies

The primary encryption-based disk protection technologies for Azure VMs are:

- Storage Service Encryption (SSE)
- Azure Disk Encryption (ADE)

Storage Service Encryption is performed on the physical disks in the data center. If someone were to directly access the physical disk the data would be encrypted. When the data is accessed from the disk, it is decrypted and loaded into memory.

Azure Disk Encryption encrypts the virtual machine's virtual hard disks (VHDs). If VHD is protected with ADE, the disk image will only be accessible by the virtual machine that owns the disk.

It's possible to use both services to protect your data.

### Storage Service Encryption

Azure Storage Service Encryption (SSE) is an encryption service built into Azure used to protect data at rest. The Azure storage platform automatically encrypts data before it's stored to several storage services, including Azure Managed Disks. Encryption is enabled by default using 256-bit AES encryption, and is managed by the storage account administrator.

Storage Service Encryption is enabled for all new and existing storage accounts and cannot be disabled. Your data is secured by default; you don't need to modify your code or applications to take advantage of Storage Service Encryption.

Storage Service Encryption does not affect the performance of Azure storage services.

### Azure Disk Encryption

Azure Disk Encryption (ADE) is managed by the VM owner. It controls the encryption of Windows and Linux VM-controlled disks, using **BitLocker** on Windows VMs and **DM-Crypt** on Linux VMs. BitLocker Drive Encryption is a data protection feature that integrates with the operating system, and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Similarly, DM-Crypt encrypts data at rest for Linux before writing to storage.

ADE ensures that all data on VM disks are encrypted at rest in Azure storage, and ADE is required for VMs backed up to the Recovery Vault.

With ADE, VMs boot under customer-controlled keys and policies. ADE is integrated with Azure Key Vault for the management of these disk-encryption keys and secrets.

#### ✓ Note:

ADE does not support the encryption of Basic tier VMs, and you cannot use an on-premises Key Management Service (KMS) with ADE. Azure Disk Encryption is not available on Basic, A-series VMs, or on virtual machines with a less than 2 GB of memory.

Azure Disk Encryption is not available on Generation 2 VMs and Lsv2-series VMs. See: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview>

## Deciding When to use Encryption

Computer data is at risk when in transit (transmitted across the Internet or other network), and at rest (saved to a storage device). The at-rest scenario is the primary concern when protecting data on Azure VM disks. For example, someone might download the Virtual Hard Disk (VHD) file associated with an

Azure VM, and save it on their laptop. If the VHD is not encrypted, the contents of the VHD are potentially accessible to anyone who can mount the VHD file on their computer.

For operating system (OS) disks, data such as passwords are encrypted automatically, so even if the VHD is not itself encrypted, it's not easy for information to be accessed. Applications may also automatically encrypt their own data. However, even with protections, if someone were to gain access to a data disk, and the disk was unencrypted, they might then be able to exploit weaknesses in that application's data protection. With disk encryption in place, such exploits are not possible.

Storage Service Encryption (SSE) is part of Azure itself, and there should be no noticeable performance impact on the VM disk IO when using SSE. Managed disks with SSE is the default.

Azure Disk Encryption (ADE) makes use of VM operating system tools (**BitLocker** and **DM-Crypt**), so the VM must do some work when encryption or decryption on VM disks is being performed. The impact of this additional VM CPU activity is minimal, except in certain situations. For example, if you have a CPU-intensive application, there may be a case for leaving the OS disk unencrypted to maximize performance.

Azure provides two complementary encryption technologies that are used to secure Azure VM disks. These technologies, **SSE** and **ADE**, encrypt at different layers, and serve different purposes. Both use AES 256-bit encryption. Using both technologies provides a defense-in-depth protection against unauthorized access to your Azure storage, and to specific VHDs.

## Module 4 Review Questions

### Module 4 Review Questions



#### Review Question 1

A company you are advising is planning to use a line-of-business, third-party software package to perform complicated data analysis. The software will use 350 VMs that are based on an Azure Marketplace VM image.

You are asked to design the infrastructure for the software application server. The solution should meet the following needs:

- The number of VMs that are running at any time must change when the user workload changes.
- When a new version of the application is available in the Azure Marketplace it must be deployed without causing application downtime.
- Use VM scale sets.
- Minimize the need for ongoing maintenance.

Which two technologies would you recommend?

- A single placement group
- Managed disks
- Autoscale
- A single storage account
- A point-to-site VPN

#### Review Question 2

An organization you are advising is running a single application that runs on a VM. The traffic to the application has recently been on the increase and continues to rise.

- The application cannot experience downtime must scale dynamically.

- You are asked to recommend an auto-scale approach so the VM can respond well to the workload requirements.

*Which three options would you recommend?*

- Deploy application automatic horizontal scaling
- Implement custom auto-scale
- Create a VM scale set
- Implement an Azure Load Balancer

## Review Question 3

*You are researching Microsoft Azure for your company. The company is considering deploying Windows-based VMs in Azure. However, before moving forward, the management team has asked you to research the costs associated with Azure VMs. You need to document the configuration options that are likely to save the company money on their Azure VMs. Which options should you document? (Each answer presents part of the solution. Select four.)*

- Use HDD instead of SSD for VM storage.
- Use unmanaged premium storage instead of managed standard storage.
- Bring your own Windows custom images.
- Use different Azure regions.
- Use the least powerful VMs that meet your requirements.
- Place all VMs in the same resource group.
- Bring your own Windows license for each VM.

## Review Question 4

*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 5

Another IT administrator creates an Azure virtual machine scale set with 5 VMs. Later, you notice that the VMs are all running at max capacity with the CPU being fully consumed. However, additional VMs are not deploying in the scale set. You need to ensure that additional VMs are deployed when the CPU is 75% consumed. What should you do? Select one.

- Enable the autoscale option.
- Increase the instance count.
- Add the scale set automation script to the library.
- Deploy the scale set automation script.

## Review Question 6

Your company is preparing to deploy an application to Microsoft Azure. The app is a self-contained unit that runs independently on several servers. The company is moving the app to the cloud to provide better performance. To get better performance, the team has the following requirements:

- If the CPU across the servers goes above 85%, a new VM should be deployed to provide additional resources.
- If the CPU across the servers drops below 15%, an Azure VM running the app should be decommissioned to reduce costs.

You need to deploy a solution to meet the requirements while minimizing the administrative overhead to implement and manage the solution. What should you do? Select one.

- Deploy the app in a virtual machine scale set.
- Deploy the app in a virtual machine availability set.
- Deploy the app by using a resource manager template.
- Deploy the app and use PowerShell Desired State Configuration (DSC).

# Answers

## Review Question 1

A company you are advising is planning to use a line-of-business, third-party software package to perform complicated data analysis. The software will use 350 VMs that are based on an Azure Marketplace VM image.

You are asked to design the infrastructure for the software application server. The solution should meet the following needs:

Which two technologies would you recommend?

- A single placement group
- Managed disks
- Autoscale
- A single storage account
- A point-to-site VPN

*Explanation*

*Autoscale facilitates horizontal scaling of VMs depending on a metric such as processor usage or memory usage. Managed disks automate the provisioning of storage capacity for the VMs.*

## Review Question 2

An organization you are advising is running a single application that runs on a VM. The traffic to the application has recently been on the increase and continues to rise.

Which three options would you recommend?

- Deploy application automatic horizontal scaling
- Implement custom auto-scale
- Create a VM scale set
- Implement an Azure Load Balancer

*Explanation*

*Correct Answers: Deploy application automatic horizontal scaling, Implement custom auto-scale, and Create a VM scale set.*

**Review Question 3**

You are researching Microsoft Azure for your company. The company is considering deploying Windows-based VMs in Azure. However, before moving forward, the management team has asked you to research the costs associated with Azure VMs. You need to document the configuration options that are likely to save the company money on their Azure VMs. Which options should you document? (Each answer presents part of the solution. Select four.)

- Use HDD instead of SSD for VM storage.
- Use unmanaged premium storage instead of managed standard storage.
- Bring your own Windows custom images.
- Use different Azure regions.
- Use the least powerful VMs that meet your requirements.
- Place all VMs in the same resource group.
- Bring your own Windows license for each VM.

*Explanation*

*In this scenario, you need to document which of the options presented are likely to save the company money for their Azure VMs. While this isn't an exhaustive list, the correct money-saving configuration options are: Use HDD instead of SSD, use different Azure regions, use the least powerful VMs that meet your requirements, and bring your own Windows license (instead of paying for a license with the VM). The other options usually increase cost.*

**Review Question 4**

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 5**

Another IT administrator creates an Azure virtual machine scale set with 5 VMs. Later, you notice that the VMs are all running at max capacity with the CPU being fully consumed. However, additional VMs are not deploying in the scale set. You need to ensure that additional VMs are deployed when the CPU is 75% consumed. What should you do? Select one.

- Enable the autoscale option.
- Increase the instance count.
- Add the scale set automation script to the library.
- Deploy the scale set automation script.

*Explanation*

*When you have a scale set, you can enable automatic scaling with the autoscale option. When you enable the option, you define the parameters for when to scale. To meet the requirements of this scenario, you need to enable the autoscale option so that additional VMs are created when the CPU is 75% consumed. Note that the automation script is used to automate the deployment of scale sets and not related to automating the building of additional VMs in the scale set.*

**Review Question 6**

Your company is preparing to deploy an application to Microsoft Azure. The app is a self-contained unit that runs independently on several servers. The company is moving the app to the cloud to provide better performance. To get better performance, the team has the following requirements:

You need to deploy a solution to meet the requirements while minimizing the administrative overhead to implement and manage the solution. What should you do? Select one.

- Deploy the app in a virtual machine scale set.
- Deploy the app in a virtual machine availability set.
- Deploy the app by using a resource manager template.
- Deploy the app and use PowerShell Desired State Configuration (DSC).

*Explanation*

*In this scenario, you should use a scale set for the VMs. Scale sets can scale up or down, based on defined criteria (such as the existing set of VMs using a large percentage of the available CPU). This meets the scenario's requirements.*

## Module 5 Implement Load Balancing and Network Security

### Implement Azure Load Balancer

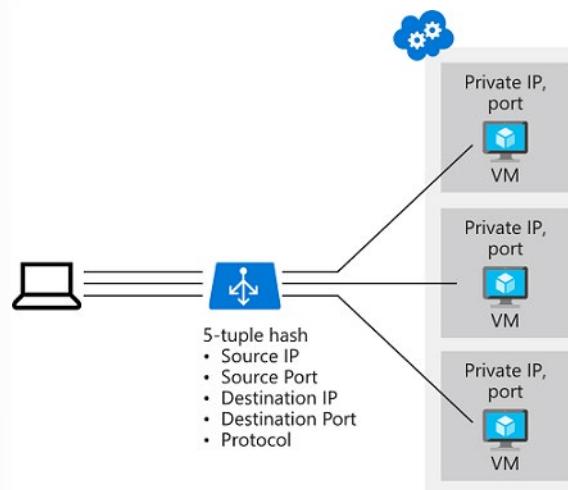
#### Distribute Traffic with Azure Load Balancer

With Azure Load Balancer, you can spread user requests across multiple virtual machines or other services. That way, you can scale the app to larger sizes than a single virtual machine can support, and you ensure that users get service, even when a virtual machine fails.

#### Distribute traffic with Azure Load Balancer

Azure Load Balancer is a service you can use to distribute traffic across multiple virtual machines. Use Load Balancer to scale applications and create high availability for your virtual machines and services. Load balancers use a hash-based distribution algorithm. By default, a five-tuple hash is used to map traffic to available servers. The hash is made from the following elements:

- **Source IP:** The IP address of the requesting client.
- **Source port:** The port of the requesting client.
- **Destination IP:** The destination IP of the request.
- **Destination port:** The destination port of the request.
- **Protocol type:** The specified protocol type, TCP or UDP.



Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all TCP and UDP applications.

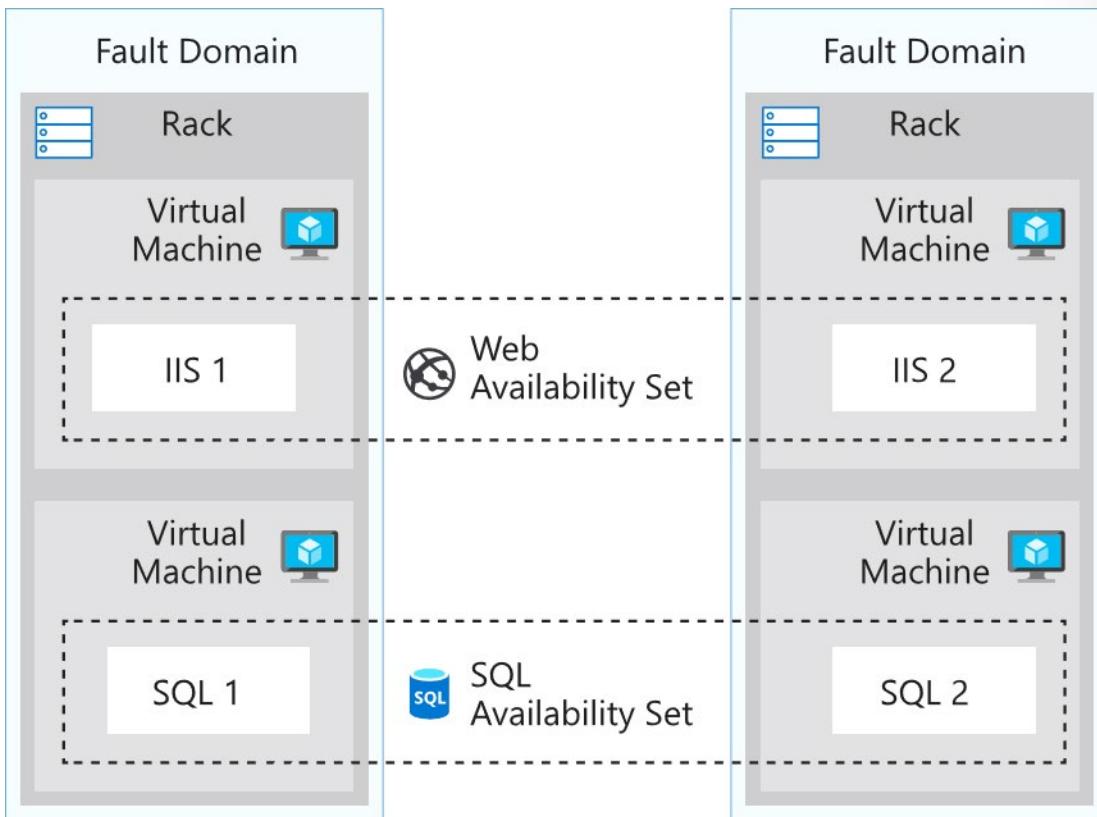
Load balancers aren't physical instances. Load balancer objects are used to express how Azure configures its infrastructure to meet your requirements.

To achieve high availability with Load Balancer, you can choose to use availability sets and availability zones to ensure that virtual machines are always available:

Configuration	Service level agreement (SLA)	Information
Availability set	99.95%	Protection from hardware failures within datacenters
Availability zone	99.99%	Protection from entire datacenter failure

## Availability sets

Mentioned earlier in this course, an availability set is a logical grouping that you use to isolate virtual machine resources from each other when they're deployed. Azure ensures that the virtual machines you put in an availability set run across multiple physical servers, compute racks, storage units, and network switches. If there's a hardware or software failure, only a subset of your virtual machines is affected.

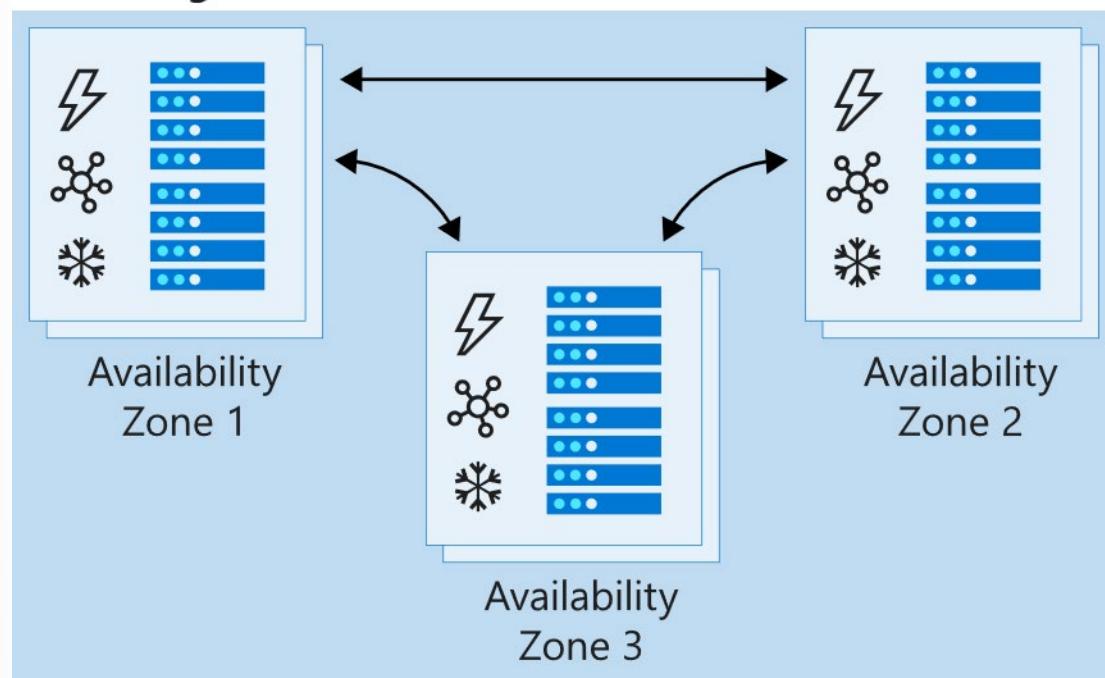


## Availability zones

Mentioned earlier in this course, an availability zone offers groups of one or more datacenters that have independent power, cooling, and networking. The virtual machines in an availability zone are placed in different physical locations within the same region. Use this architecture when you want to ensure that, when an entire datacenter fails, you can continue to serve users.

Availability zones don't support all virtual machine sizes and aren't available in all Azure regions. Check that they are supported in your region before you use them in your architecture.

## Azure Region



## Select a Load Balancer Solution

Two products are available when you create a load balancer in Azure: basic load balancers and standard load balancers.

**Basic load balancers** allow:

- Port forwarding
- Automatic reconfiguration
- Health probes
- Outbound connections through source network address translation (SNAT)
- Diagnostics through Azure Log Analytics for public-facing load balancers

Basic load balancers can be used only with Virtual machines in a single availability set or a virtual machine scale set.

**Standard load balancers** support all of the basic features. They also allow:

- HTTPS health probes
- Availability zones
- Diagnostics through Azure Monitor, for multidimensional metrics
- High availability (HA) ports
- Outbound rules
- A guaranteed SLA (99.99% for two or more virtual machines)

Standard load balancer can use any virtual machines or virtual machine scale sets in a single virtual network.

## Internal and external load balancers

An **external load balancer** operates by distributing client traffic across multiple virtual machines. An external load balancer permits traffic from the internet. The traffic might come from browsers, mobile apps, or other sources.

An **internal load balancer** distributes a load from internal Azure resources to other Azure resources. For example, if you have front-end web servers that need to call business logic that's hosted on multiple middle-tier servers, you can distribute that load evenly by using an internal load balancer. No traffic is allowed from internet sources.

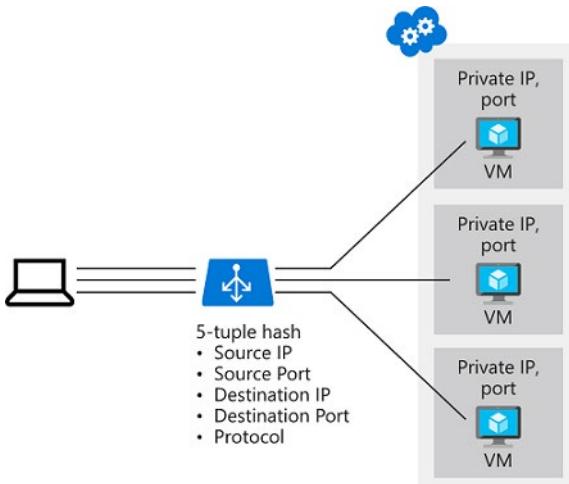
## Configure a Public Load Balancer

A public load balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of a virtual machine in the back-end pool. The responses are then returned to the client. By applying load-balancing rules, you distribute specific types of traffic across multiple virtual machines or services.

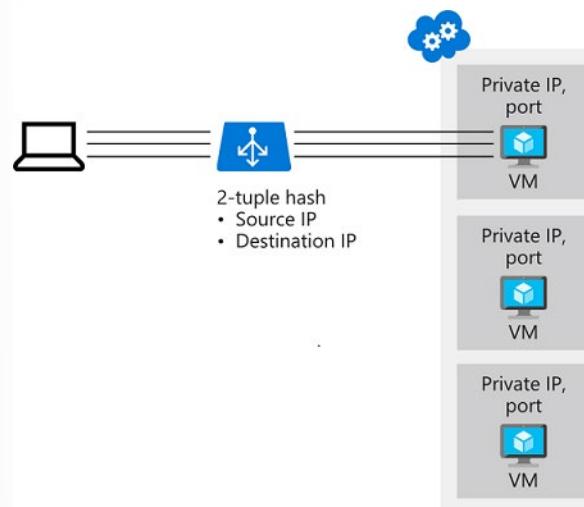
### Distribution modes

By default, Azure Load Balancer distributes network traffic equally among virtual machine instances. The following distribution modes are also possible if a different behavior is required:

**Five-tuple hash.** The default distribution mode for Load Balancer is a five-tuple hash. The tuple is composed of the source IP, source port, destination IP, destination port, and protocol type. Because the source port is included in the hash and the source port changes for each session, clients might be directed to a different virtual machine for each session.



**Source IP affinity.** This distribution mode is also known as session affinity or client IP affinity. To map traffic to the available servers, the mode uses a two-tuple hash (from the source IP address and destination IP address) or three-tuple hash (from the source IP address, destination IP address, and protocol type). The hash ensures that requests from a specific client are always sent to the same virtual machine behind the load balancer.



## Choose a distribution mode

Imagine a scenario where the requirement of the presentation tier is to use in-memory sessions to store the logged user's profile as the user interacts with the portal.

In this scenario, the load balancer must provide source IP affinity to maintain a user's session. The profile is stored only on the virtual machine that the client first connects to because that IP address is directed to the same server. When you create the load balancer endpoint, you must specify the distribution mode by using the following PowerShell example:

```
$lb = Get-AzLoadBalancer -Name MyLb -ResourceGroupName MyResourceGroup  
$lb.LoadBalancingRules[0].LoadDistribution = 'sourceIp'  
Set-AzLoadBalancer -LoadBalancer $lb
```

To add session persistence through the Azure portal:

1. In the Azure portal, open the load balancer resource.
2. Edit the relevant line of the **Load-balancing rules**.
3. Change the value for **Session persistence** to **Client IP**.

myHTTPRule  
myLoadBalancer

Save Discard Delete

\* Name: myHTTPRule

\* IP Version: IPv4

\* Frontend IP address: 52.164.208.78 (myFrontEndPool)

Protocol: TCP

\* Port: 80

\* Backend port: 80

Backend pool: myBackEndPool (1 virtual machine)

Health probe: myHealthProbe (TCP:80)

Session persistence:

- Client IP
- None
- Client IP and protocol
- Floating IP (direct server return)

## Load Balancer and Remote Desktop Gateway

Remote Desktop Gateway is a Windows service that you can use to enable clients on the internet to make Remote Desktop Protocol (RDP) connections through firewalls to Remote Desktop servers on your private network. The default five-tuple hash in Load Balancer is incompatible with this service. If you want to use Load Balancer with your Remote Desktop servers, use source IP affinity.

## Demonstration - Create a Load Balancer to Load Balance VMs

Sign in to the Azure portal at <https://portal.azure.com><sup>1</sup>.

### Create a Load Balancer

In this demonstration, you create a Load Balancer that helps load balance virtual machines. You can create a public Load Balancer or an internal Load Balancer. When you create a public Load Balancer, you must also create a new Public IP address that is configured as the frontend (named as LoadBalancerFrontend by default) for the Load Balancer.

1. Select + **Create a resource**, type *load balancer*.

<sup>1</sup> <https://portal.azure.com/>

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a search bar and several navigation icons. Below the header, there's a section titled 'Azure services' with a 'Create a resource' button highlighted with a red box. Other service icons include Activity log, Log Analytics workspaces, Virtual machine scale sets, Service Health, Network Watcher, Monitor, Azure Workbooks, Metrics, and More services. Below this is a 'Recent resources' table with three items: az303303 (Log Analytics workspace), AZ303Test (Recovery Services vault), and AZ303VM (Virtual machine). There are also 'Navigate' and 'Tools' sections with links to Subscriptions, Resource groups, All resources, Dashboard, Microsoft Learn, Azure Monitor, Security Center, and Cost Management.

2. Click **Create**.

The screenshot shows the Microsoft Azure Load Balancer creation page. The URL is 'All services > New > Load Balancer'. The main heading is 'Load Balancer' with a Microsoft logo. Below it is a purple icon with a network symbol and a 'Create' button highlighted with a red box. Underneath, there are tabs for 'Overview' and 'Plans'. A detailed description of the Azure load balancer is provided, along with configuration options for load balancing and NAT rules. At the bottom left, there are 'Useful Links' for Service overview and Documentation.

3. In the **Basics** tab of the **Create load balancer** page, enter or select the following information, accept the defaults for the remaining settings, and then select **Review + create**:

**Create load balancer**

**Basics** Tags Review + create

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

**Project details**

Subscription \* Azure Pass - Sponsorship

Resource group \* Create new

**Instance details**

Name \*

Region \* (US) East US

Type \*  Internal  Public

SKU \*  Basic  Standard

**Public IP address**

Public IP address \*  Create new  Use existing

Public IP address name \*

Public IP address SKU Basic

Assignment \*  Dynamic  Static

Add a public IPv6 address  No  Yes

**Review + create** < Previous Next : Tags > Download a template for automation

Setting	Value
Subscription	Select your subscription.
Resource group	Select <b>Create new</b> and type <i>myResourceGroupSLB</i> in the text box.
Name	<i>myLoadBalancer</i>
Region	Select <b>West Europe</b> .
Type	Select <b>Public</b> .

Setting	Value
SKU	Select <b>Standard</b> or <b>Basic</b> . Microsoft recommends Standard for production workloads.
Public IP address	Select <b>Create new</b> . If you have an existing Public IP you would like to use, select <b>Use existing</b> .
Public IP address name	Type <i>myPublicIP</i> in the text box. Use <code>-SKU Basic</code> to create a Basic Public IP. Basic Public IPs are not compatible with <b>Standard</b> load balancer. Microsoft recommends using <b>Standard</b> for production workloads.
Availability zone	Type <i>Zone-redundant</i> to create a resilient Load Balancer. To create a zonal Load Balancer, select a specific zone from 1, 2, or 3

✓ **Important**

This demonstration assumes that Standard SKU is chosen during the SKU selection process above.

## Create Load Balancer resources

In this section, you configure Load Balancer settings for a backend address pool, a health probe, and specify a balancer rule.

### Create a Backend pool

To distribute traffic to the VMs, a backend address pool contains the IP addresses of the virtual (NICs) connected to the Load Balancer. Create the backend address pool *myBackendPool* to include virtual machines for load-balancing internet traffic.

1. Select **All services** in the left-hand menu, select **All resources**, and then select **myLoadBalancer** from the resources list.
2. Under **Settings**, select **Backend pools**, then select **Add**.
3. On the **Add a backend pool** page, for name, type *myBackendPool*, as the name for your backend pool, and then select **Add**.

### Create a health probe

To allow the Load Balancer to monitor the status of your app, you use a health probe. The health probe dynamically adds or removes VMs from the Load Balancer rotation based on their response to health checks. Create a health probe *myHealthProbe* to monitor the health of the VMs.

1. Select **All services** in the left-hand menu, select **All resources**, and then select **myLoadBalancer** from the resources list.
2. Under **Settings**, select **Health probes**, then select **Add**.

Setting	Value
Name	Enter <i>myHealthProbe</i> .
Protocol	Select <b>HTTP</b> .
Port	Enter <i>80</i> .

Setting	Value
Interval	Enter 15 for number of <b>Interval</b> in seconds between probe attempts.
Unhealthy threshold	Select 2 for number of <b>Unhealthy threshold</b> or consecutive probe failures that must occur before a VM is considered unhealthy.

3. Select **OK**.

## Create a Load Balancer rule

A Load Balancer rule is used to define how traffic is distributed to the VMs. You define the frontend IP configuration for the incoming traffic and the backend IP pool to receive the traffic, along with the required source and destination port. Create a Load Balancer rule **myLoadBalancerRuleWeb** for listening to port 80 in the frontend **FrontendLoadBalancer** and sending load-balanced network traffic to the backend address pool **myBackEndPool** also using port 80.

1. Select **All services** in the left-hand menu, select **All resources**, and then select **myLoadBalancer** from the resources list.
2. Under **Settings**, select **Load balancing rules**, then select **Add**.
3. Use these values to configure the load balancing rule:

Setting	Value
Name	Enter <i>myHTTPRule</i> .
Protocol	Select <b>TCP</b> .
Port	Enter <i>80</i> .
Backend port	Enter <i>80</i> .
Backend pool	Select <b>myBackendPool</b> .
Health probe	Select <b>myHealthProbe</b> .

4. Leave the rest of the defaults and then select **OK**.

## Create backend servers

In this section, you create a virtual network, create three virtual machines for the backend pool of the Load Balancer, and then install IIS on the virtual machines to help test the Load Balancer.

## Virtual network and parameters

In this section you'll need to replace the following parameters in the steps with the information below:

Parameter	Value
<b>resource-group-name</b>	myResourceGroupSLB
<b>virtual-network-name</b>	myVNet
<b>region-name</b>	West Europe
<b>IPv4-address-space</b>	10.1.0.0\16
<b>subnet-name</b>	myBackendSubnet
<b>subnet-address-range</b>	10.1.0.0\24

## Create the virtual network

In this section, you'll create a virtual network and subnet.

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

Setting	Value
<b>Project Details</b>	
Subscription	Select your Azure subscription
Resource Group	Select <b>Create new</b> , enter <b>resource-group-name</b> , then select <b>OK</b> , or select an existing <b>resource-group-name</b> based on parameters.
<b>Instance details</b>	
Name	Enter <b>virtual-network-name</b>
Region	Select <b>region-name</b>

3. Select the **IP Addresses** tab or select the **Next: IP Addresses** button at the bottom of the page.
4. In the **IP Addresses** tab, enter this information:

Setting	Value
IPv4 address space	Enter <b>IPv4-address-space</b>

5. Under **Subnet name**, select the word **default**.
  6. In **Edit subnet**, enter this information:
- | Setting              | Value                             |
|----------------------|-----------------------------------|
| Subnet name          | Enter <b>subnet-name</b>          |
| Subnet address range | Enter <b>subnet-address-range</b> |
7. Select **Save**.
  8. Select the **Review + create** tab or select the **Review + create** button.
  9. Select **Create**.

## Create virtual machines

Public IP SKUs and Load Balancer SKUs must match. For Standard Load Balancer , use VMs with Standard IP addresses in the backend pool. In this section, you will create three VMs (*myVM1*, *myVM2* and *myVM3*) with a Standard public IP address in three different zones (*Zone 1*, *Zone 2*, and *Zone 3*) that are later added to the backend pool of the Load Balancer that was created earlier. If you selected Basic, use VMs with Basic IP addresses.

1. On the upper-left side of the portal, select **Create a resource > Compute > Windows Server 2019 Datacenter**.
2. In **Create a virtual machine**, type or select the following values in the **Basics** tab:
  - **Subscription > Resource Group**: Select **myResourceGroupSLB**.
  - **Instance Details > Virtual machine** name: Type *myVM1*.
  - **Instance Details > Region** > select **West Europe**.

- **Instance Details > Availability Options** > Select **Availability zones**.
  - **Instance Details > Availability zone** > Select 1.
  - **Administrator account** > Enter the **Username**, **Password** and **Confirm password** information.
  - Select the **Networking** tab, or select **Next: Disks**, then **Next: Networking**.
3. In the **Networking** tab make sure the following are selected:
- **Virtual network**: *myVnet*
  - **Subnet**: *myBackendSubnet*
  - **Public IP** > select **Create new**, and in the **Create public IP address** window, for **SKU**, select **Standard**, and for **Availability zone**, select **Zone-redundant**, and then select **OK**. If you created a Basic Load Balancer, select Basic. Microsoft recommends using Standard SKU for production workloads.
  - To create a new network security group (NSG), a type of firewall, under **Network Security Group**, select **Advanced**.
1. In the **Configure network security group** field, select **Create new**.
  2. Type *myNetworkSecurityGroup*, and select **OK**.
    - To make the VM a part of the Load Balancer's backend pool, complete the following steps:
    - In **Load Balancing**, for **Place this virtual machine behind an existing load balancing solution?**, select **Yes**.
    - In **Load balancing settings**, for **Load balancing options**, select **Azure load balancer**.
    - For **Select a load balancer**, *myLoadBalancer*.
    - Select the **Management** tab, or select **Next > Management**.
  3. In the **Management** tab, under **Monitoring**, set **Boot diagnostics** to **Off**.
  4. Select **Review + create**.
  5. Review the settings, and then select **Create**.
  6. Follow the steps 2 to 6 to create two additional VMs with the following values and all the other settings the same as *myVM1*:

Setting	VM 2	VM 3
Name	<i>myVM2</i>	<i>myVM3</i>
Availability zone	2	3
Public IP	<b>Standard SKU</b>	<b>Standard SKU</b>
Public IP - Availability zone	<b>Zone redundant</b>	<b>Zone redundant</b>
Network security group	Select the existing <i>myNetworkSecurityGroup</i>	Select the existing <i>myNetworkSecurityGroup</i>

## Create NSG rule

In this section, you create a network security group rule to allow inbound connections using HTTP.

1. Select **All services** in the left-hand menu, select **All resources**, and then from the resources list select **myNetworkSecurityGroup** that is located in the **myResourceGroupSLB** resource group.
2. Under **Settings**, select **Inbound security rules**, and then select **Add**.

3. Enter these values for the inbound security rule named **myHTTPRule** to allow for an inbound HTTP connections using port **80**:
  - **Source:** *Service Tag*
  - **Source service tag:** *Internet*
  - **Destination port ranges:** *80*
  - **Protocol:** *TCP*
  - **Action:** *Allow*
  - **Priority:** *100*
  - **Name:** *myHTTPRule*
  - **Description:** *Allow HTTP*
4. Select **Add**.
5. Repeat the steps for the inbound RDP rule, if needed, with the following differing values:
  - **Destination port ranges:** Type *3389*.
  - **Priority:** Type *200*.
  - **Name:** Type *MyRDPRule*.
  - **Description:** Type *Allow RDP*.

## Install IIS

1. Select **All services** in the left-hand menu, select **All resources**, and then from the resources list, select **myVM1** that is located in the *myResourceGroupSLB* resource group.
2. On the **Overview** page, select **Connect** to RDP into the VM.
3. Log into the VM with the credentials that you provided during the creation of this VM. This launches a remote desktop session with virtual machine - *myVM1*.
4. On the server desktop, navigate to**Windows Administrative Tools>Windows PowerShell**.
5. In the PowerShell Window, run the following commands to install the IIS server, remove the default *iisstart.htm* file, and then add a new *iisstart.htm* file that displays the name of the VM:

```
# install IIS server role
Install-WindowsFeature -name Web-Server -IncludeManagementTools

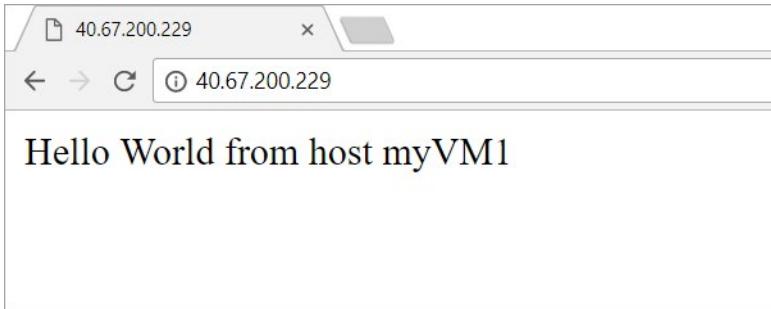
# remove default htm file
remove-item C:\inetpub\wwwroot\iisstart.htm

# Add a new htm file that displays server name
Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $($("Hello World" + $env:computername))
```

6. Close the RDP session with *myVM1*.
7. Repeat steps 1 to 6 to install IIS and the updated *iisstart.htm* file on *myVM2* and *myVM3*.

## Test the Load Balancer

1. Find the public IP address for the Load Balancer on the **Overview** screen. Select **All services** in the left-hand menu, select **All resources**, and then select **myPublicIP**.
2. Copy the public IP address, and then paste it into the address bar of your browser. The default page of IIS Web server is displayed on the browser.

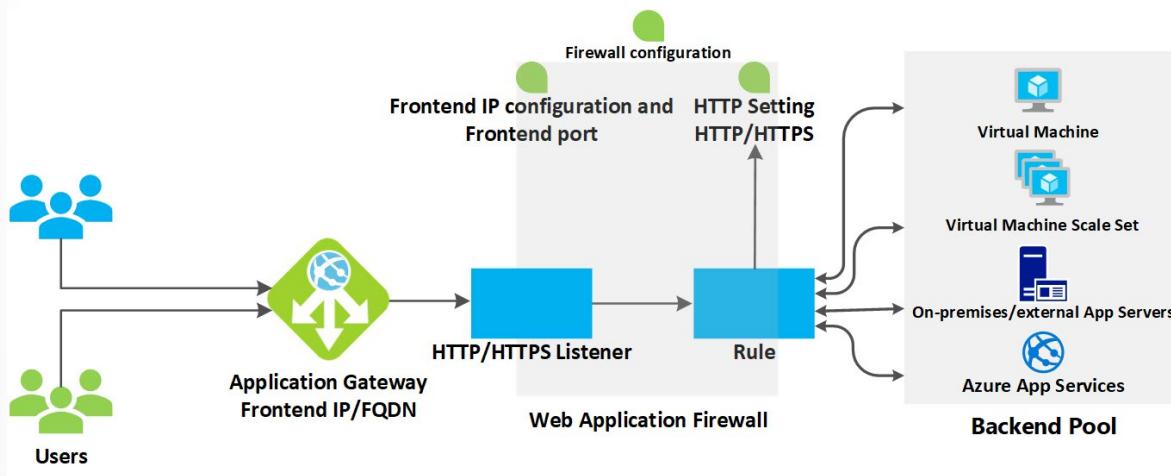


To see the Load Balancer distribute traffic across all three VMs, you can customize the default page of each VM's IIS Web server and then force-refresh your web browser from the client machine.

# Implement an Application Gateway

## Application Gateway

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



## How an application gateway accepts a request

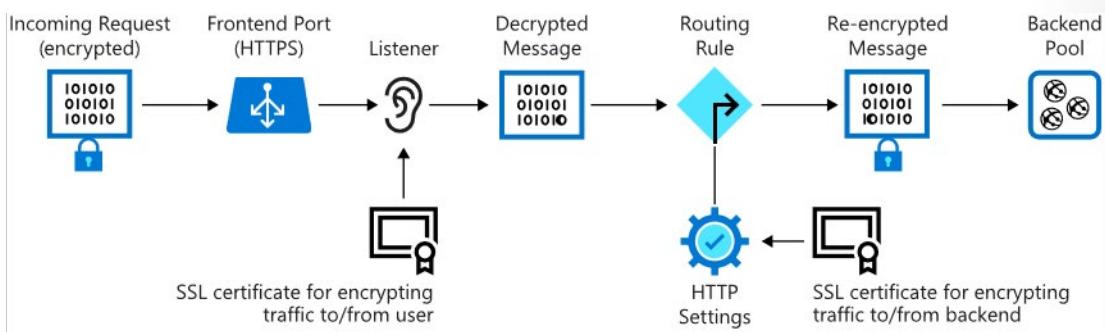
1. Before a client sends a request to an application gateway, it resolves the domain name of the application gateway by using a Domain Name System (DNS) server. Azure controls the DNS entry because all application gateways are in the azure.com domain.
2. The Azure DNS returns the IP address to the client, which is the frontend IP address of the application gateway.
3. The application gateway accepts incoming traffic on one or more listeners. A listener is a logical entity that checks for connection requests. It's configured with a frontend IP address, protocol, and port number for connections from clients to the application gateway.
4. If a web application firewall (WAF) is in use, the application gateway checks the request headers and the body, if present, against WAF rules. This action determines if the request is valid request or a security threat. If the request is valid, it's routed to the backend. If the request isn't valid and WAF is in Prevention mode, it's blocked as a security threat. If it's in Detection mode, the request is evaluated and logged, but still forwarded to the backend server.

Azure Application Gateway can be used as an internal application load balancer or as an internet-facing application load balancer. An internet-facing application gateway uses public IP addresses. The DNS name of an internet-facing application gateway is publicly resolvable to its public IP address. As a result, internet-facing application gateways can route client requests to the internet.

## Application Gateway components

Application Gateway has several components. The main parts for encryption are the frontend port, the listener, and the backend pool.

The following image shows how incoming traffic from a client to Application Gateway over SSL is decrypted and then re-encrypted when it's sent to a server in the backend pool.



## Frontend port and listener

Traffic enters the gateway through a frontend port. You can open many ports, and Application Gateway can receive messages on any of these ports. A listener is the first thing that your traffic meets when entering the gateway through a port. It's set up to listen for a specific host name, and a specific port on a specific IP address. The listener can use an SSL certificate to decrypt the traffic that enters the gateway. The listener then uses a rule that you define to direct the incoming requests to a backend pool.

## Backend pool

The backend pool contains your application servers. These servers might be virtual machines, a virtual machine scale set, or applications running on Azure App Service. Incoming requests can be load balanced across the servers in this pool. The backend pool has an HTTP setting that references a certificate used to authenticate the backend servers. The gateway re-encrypts the traffic by using this certificate before sending it to one of your servers in the backend pool.

If you're using Azure App Service to host the backend application, you don't need to install any certificates in Application Gateway to connect to the backend pool. All communications are automatically encrypted. Application Gateway trusts the servers because Azure manages them.

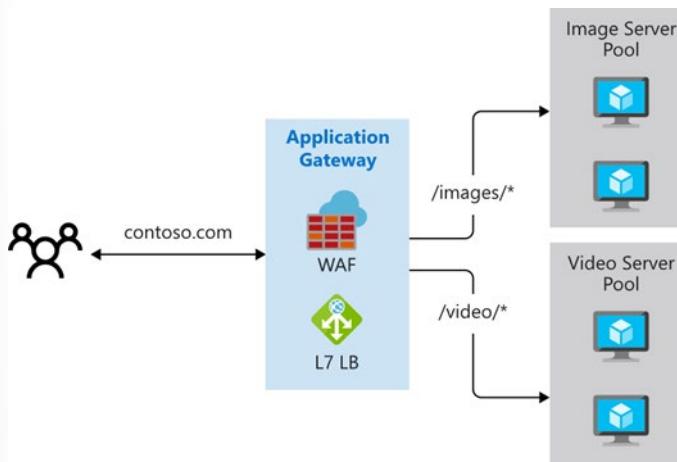
## Application Gateway Routing

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

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

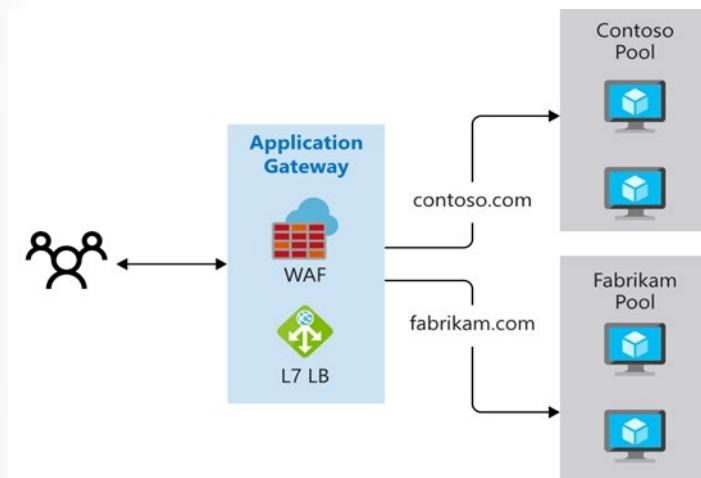
### Path-based routing

Path-based routing enables you to send requests with different paths in the URL to a different pool of back-end servers.



## Multiple site routing

Multiple site hosting enables you to configure more than one web application on the same application gateway instance. In a multi-site configuration, you register multiple DNS names (CNAMEs) for the IP address of the Application Gateway, specifying the name of each site. Application Gateway uses separate listeners to wait for requests for each site. Each listener passes the request to a different rule, which can route the requests to servers in a different back-end pool.



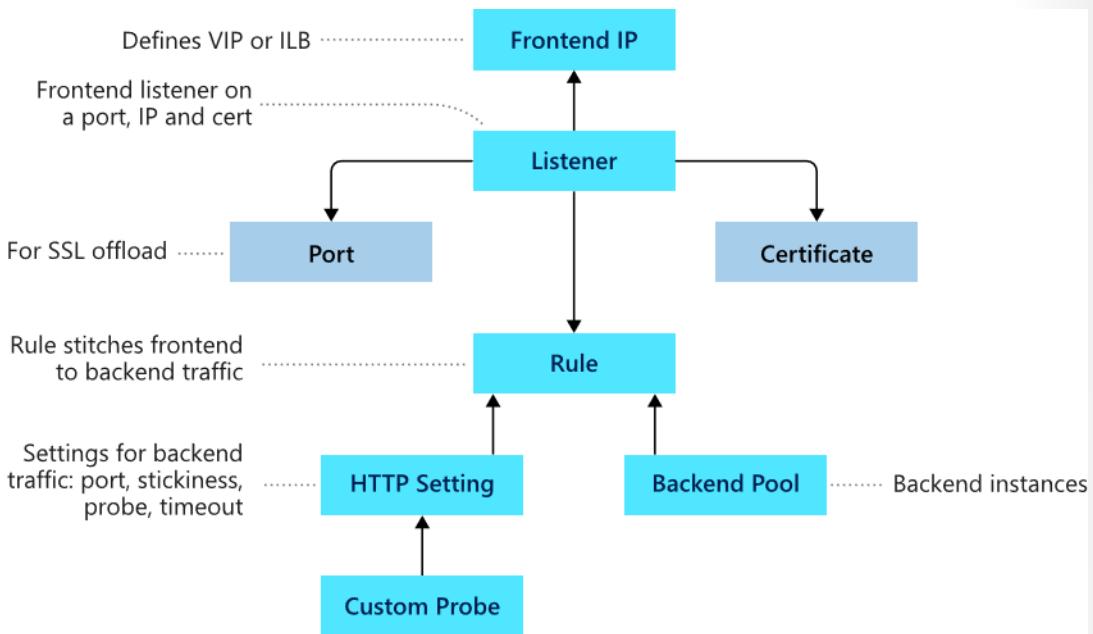
Multi-site configurations are useful for supporting multi-tenant applications, where each tenant has its own set of virtual machines or other resources hosting a web application.

## Additional features

- **Redirection.** Redirection can be used to another site, or from HTTP to HTTPS.
- **Rewrite HTTP headers.** HTTP headers allow the client and server to pass additional information with the request or the response.
- **Custom error pages.** Application Gateway allows you to create custom error pages instead of displaying default error pages. You can use your own branding and layout using a custom error page.

# Application Gateway Configuration

Application Gateway has a series of components that combine to route requests to a pool of web servers and to check the health of these web servers.



## Front-end IP address

Client requests are received through a front-end IP address. You can configure Application Gateway to have a public IP address, a private IP address, or both. Application Gateway can't have more than one public and one private IP address.

## Listeners

Application Gateway uses one or more listeners to receive incoming requests. A listener accepts traffic arriving on a specified combination of protocol, port, host, and IP address. Each listener routes requests to a back-end pool of servers following routing rules that you specify. A listener can be Basic or Multi-site. A Basic listener only routes a request based on the path in the URL. A Multi-site listener can also route requests using the hostname element of the URL.

## Routing rules

A routing rule binds a listener to the back-end pools. A rule specifies how to interpret the hostname and path elements in the URL of a request, and direct the request to the appropriate back-end pool. A routing rule also has an associated set of HTTP settings. These settings indicate whether (and how) traffic is encrypted between Application Gateway and the back-end servers, and other configuration information such as: Protocol, Session stickiness, Connection draining, Request timeout period, and Health probes.

## Back-end pools

A back-end pool references a collection of web servers. You provide the IP address of each web server and the port on which it listens for requests when configuring the pool. Each pool can specify a fixed set

of virtual machines, a virtual machine scale-set, an app hosted by Azure App Services, or a collection of on-premises servers. Each back-end pool has an associated load balancer that distributes work across the pool.

## Web application firewall

The web application firewall (WAF) is an optional component that handles incoming requests before they reach a listener. The web application firewall checks each request for many common threats, based on the Open Web Application Security Project (OWASP). These include: SQL-injection, Cross-site scripting, Command injection, HTTP request smuggling, HTTP response splitting, Remote file inclusion, Bots, crawlers, and scanners, and HTTP protocol violations and anomalies.

WAF is enabled on your Application Gateway by selecting the WAF tier when you create a gateway.

## Health probes

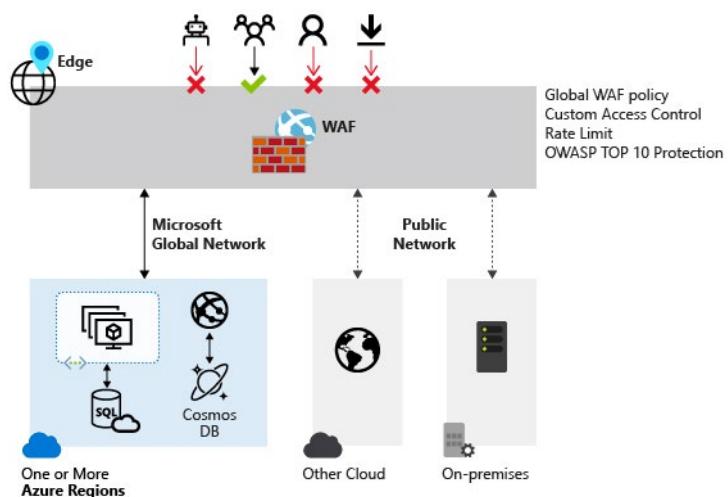
Health probes are an important part in assisting the load balancer to determine which servers are available for load balancing in a back-end pool. Application Gateway uses a health probe to send a request to a server. If the server returns an HTTP response with a status code between 200 and 399, the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

If you don't configure a health probe, Application Gateway creates a default probe that waits for 30 seconds before deciding that a server is unavailable.

# Web Application Firewall

## Web Application Firewall Overview

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.



Preventing such attacks in application code is challenging. It can require rigorous maintenance, patching, and monitoring at multiple layers of the application topology. A centralized web application firewall helps make security management much simpler. A WAF also gives application administrators better assurance of protection against threats and intrusions.

A WAF solution can react to a security threat faster by centrally patching a known vulnerability, instead of securing each individual web application.

### Supported service

WAF can be deployed with Azure Application Gateway, Azure Front Door, and Azure Content Delivery Network (CDN) service from Microsoft. WAF on Azure CDN is currently under public preview.

## Demonstration - Create an Application Gateway with a Web Application Firewall

This demonstration shows how to use the Azure portal to create an Application Gateway with a Web Application Firewall (WAF). The WAF uses **OWASP<sup>2</sup>** rules to protect your application. These rules include protection against attacks such as SQL injection, cross-site scripting attacks, and session hijacks.

Sign in to the Azure portal at [https://portal.azure.com<sup>3</sup>](https://portal.azure.com).

<sup>2</sup> [https://www.owasp.org/index.php/Category:OWASP\\_ModSecurity\\_Core\\_Rule\\_Set\\_Project](https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project)

<sup>3</sup> [https://portal.azure.com/](https://portal.azure.com)

## Create an application gateway

For Azure to communicate between resources, it needs a virtual network. You can either create a new virtual network or use an existing one. In this example, you create a new virtual network. You can create a virtual network at the same time that you create the application gateway. Application Gateway instances are created in separate subnets. You create two subnets in this example: one for the application gateway, and another for the backend servers.

Select **Create a resource** on the left menu of the Azure portal. The **New** window appears.

Select **Networking** and then select **Application Gateway** in the **Featured** list.

### Basics tab

1. On the **Basics** tab, enter these values for the following application gateway settings:
  - **Resource group:** Select **myResourceGroupAG** for the resource group. If it doesn't exist, select **Create new** to create it.
  - **Application gateway name:** Enter *myAppGateway* for the name of the application gateway.
  - **Tier:** select **WAF V2**.

The screenshot shows the 'Create an application gateway' wizard in the Azure portal. The 'Basics' step is selected. Key fields highlighted with red boxes include the Subscription dropdown (VEH Doc Test), Resource group dropdown ((New) myResourceGroupAG), Application gateway name (myAppGateway), Region (US Central US), and Tier (WAF V2). Other visible fields include Minimum instances (2), Maximum instances (empty), Firewall status (Enabled), Firewall mode (Detection), Availability zone (None), and HTTP/2 (Disabled). The 'Configure virtual network' section shows a dropdown for Virtual network (empty). Navigation buttons at the bottom are < Previous and Next : Frontends >.

- For Azure to communicate between the resources that you create, it needs a virtual network. You can either create a new virtual network or use an existing one. In this demonstration, you'll create a new virtual network at the same time that you create the application gateway. Application Gateway instances are created in separate subnets. You create two subnets in this example: one for the application gateway, and another for the backend servers.

Under **Configure virtual network**, create a new virtual network by selecting **Create new**. In the Create virtual network window that opens, enter the following values to create the virtual network and two subnets:

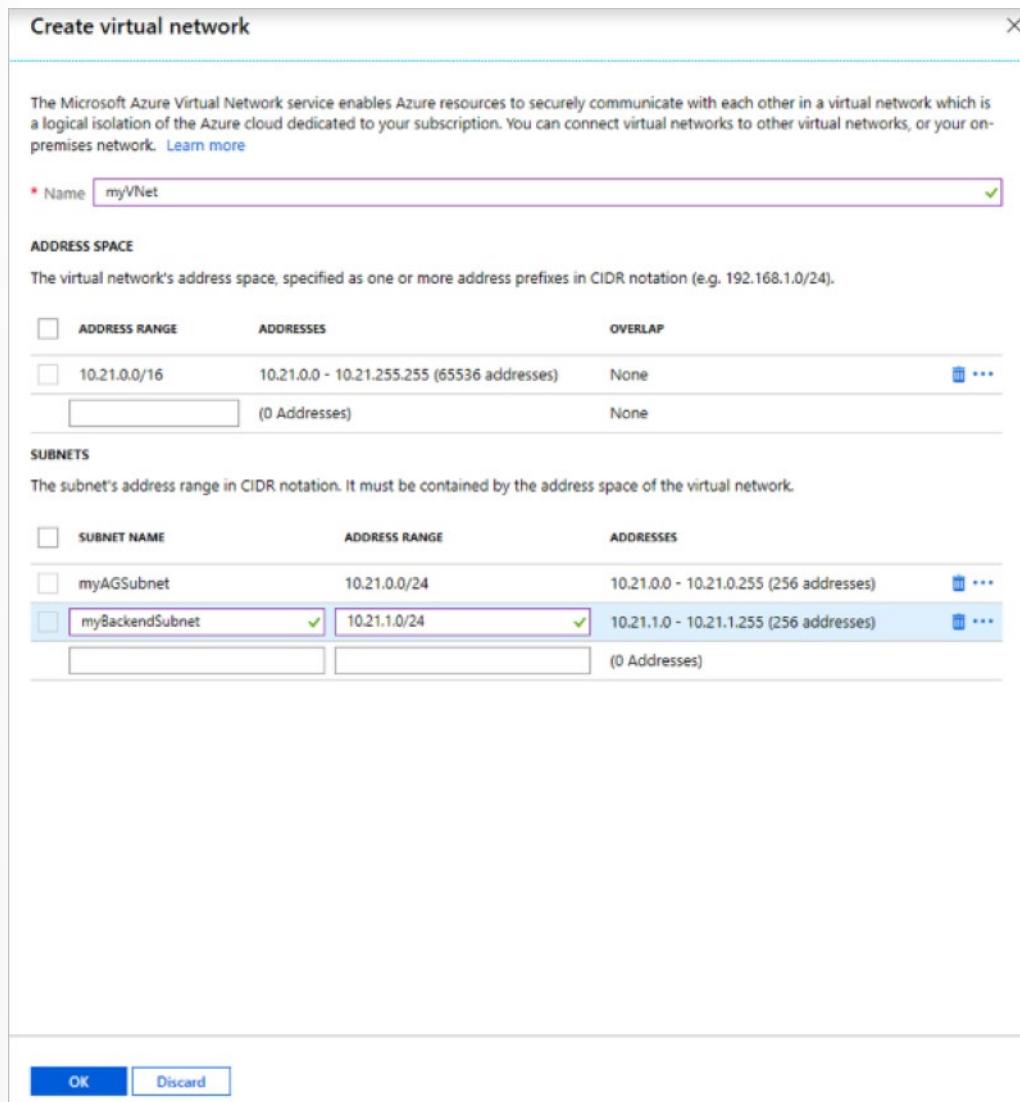
- Name:** Enter *myVNet* for the name of the virtual network.
- Subnet name (Application Gateway subnet):** The **Subnets** grid will show a subnet named Default. Change the name of this subnet to *myAGSubnet*.

The application gateway subnet can contain only application gateways. No other resources are allowed.

- Subnet name (backend server subnet):** In the second row of the **Subnets** grid, enter *myBackendSubnet* in the **Subnet name** column.

- **Address range (backend server subnet):** In the second row of the **Subnets Grid**, enter an address range that doesn't overlap with the address range of *myAGSubnet*. For example, if the address range of *myAGSubnet* is 10.0.0.0/24, enter 10.0.1.0/24 for the address range of *myBackendSubnet*.

Select **OK** to close the Create virtual network window and save the virtual network settings.



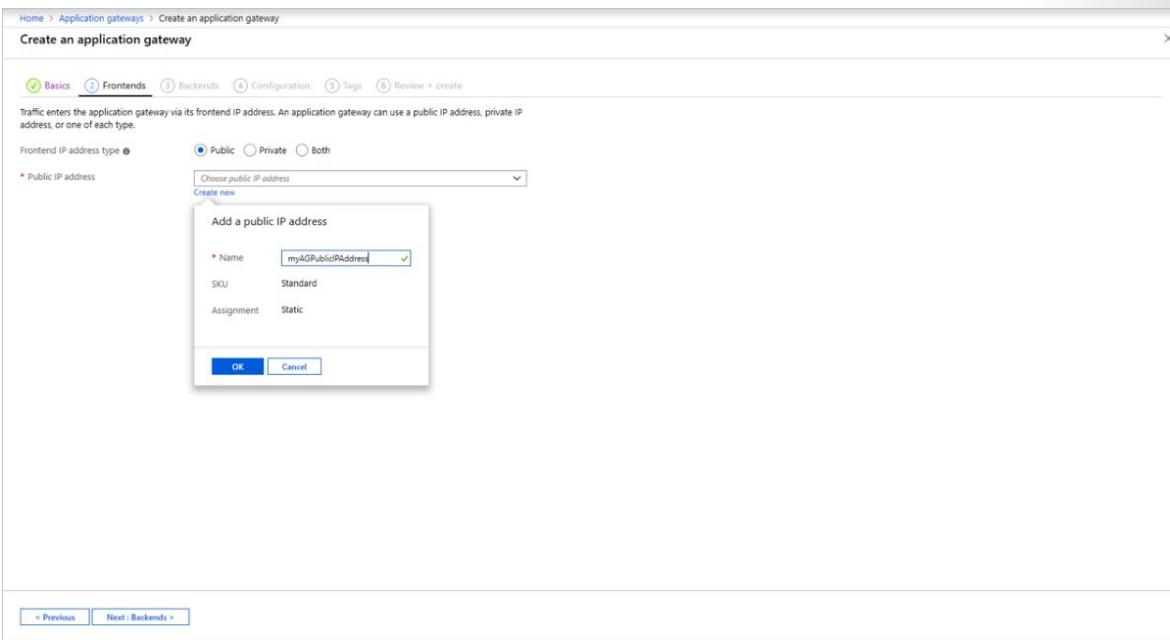
3. On the **Basics** tab, accept the default values for the other settings and then select **Next: Frontends**.

## Frontends tab

1. On the **Frontends** tab, verify **Frontend IP address type** is set to **Public**.

You can configure the Frontend IP to be Public or Private as per your use case. In this demonstration, you'll choose a Public Frontend IP.

2. Choose **Create new** for the **Public IP address** and enter *myAGPublicIPAddress* for the public IP address name, and then select **OK**.

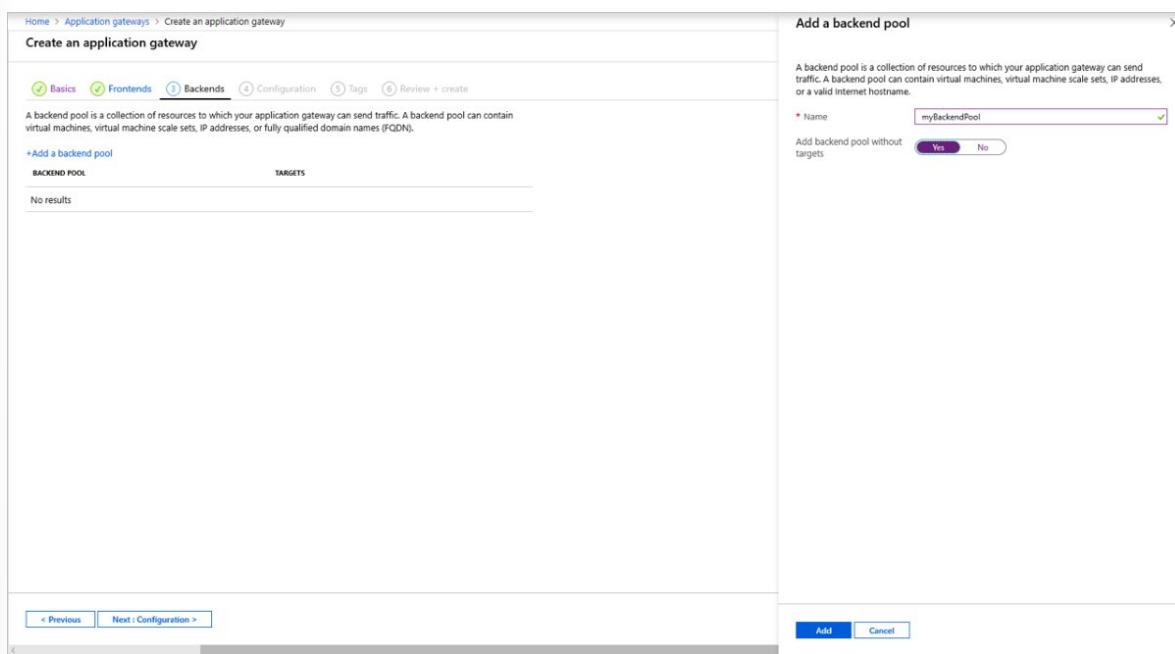


3. Select **Next: Backends**.

## Backends tab

The backend pool is used to route requests to the backend servers that serve the request. Backend pools can be composed of NICs, virtual machine scale sets, public IPs, internal IPs, fully qualified domain names (FQDN), and multi-tenant back-ends like Azure App Service. In this demonstration, you'll create an empty backend pool with your application gateway and then add backend targets to the backend pool.

1. On the **Backends** tab, select **+Add a backend pool**.
2. In the **Add a backend pool** window that opens, enter the following values to create an empty backend pool:
  - Name:** Enter *myBackendPool* for the name of the backend pool.
  - Add backend pool without targets:** Select **Yes** to create a backend pool with no targets. You'll add backend targets after creating the application gateway.
3. In the **Add a backend pool** window, select **Add** to save the backend pool configuration and return to the **Backends** tab.



4. On the **Backends** tab, select **Next: Configuration**.

## Configuration tab

On the **Configuration** tab, you'll connect the frontend and backend pool you created using a routing rule.

1. Select **Add a rule** in the **Routing rules** column.
2. In the **Add a routing rule window** that opens, enter *myRoutingRule* for the **Rule name**.
3. A routing rule requires a listener. On the **Listener** tab within the **Add a routing rule** window, enter the following values for the listener:
  - **Listener name:** Enter *myListener* for the name of the listener.
  - **Frontend IP:** Select **Public** to choose the public IP you created for the frontend.

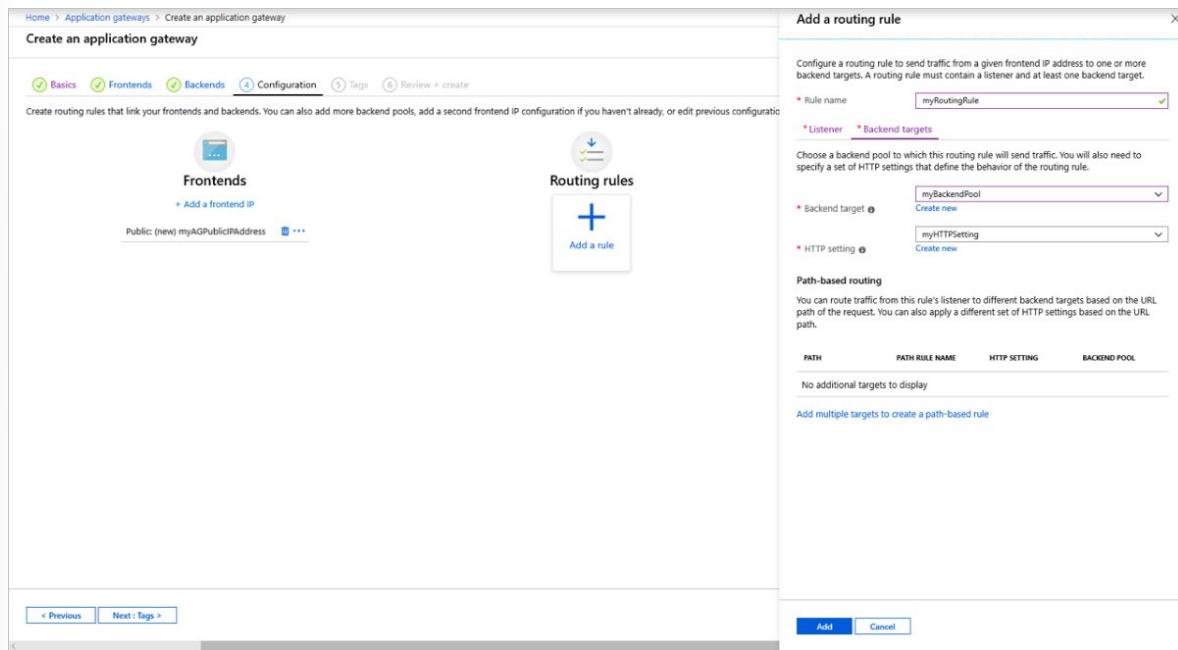
Accept the default values for the other settings on the **Listener** tab, then select the **Backend targets** tab to configure the rest of the routing rule.

The screenshot shows the Azure portal interface for creating an application gateway. The main page has tabs for Basics, Frontends, Backends, Configuration, Tags, and Review + create. The Configuration tab is active. On the right, a modal window titled 'Add a routing rule' is displayed. It contains fields for 'Rule name' (set to 'myRoutingRule'), 'Listener' (set to 'myListener'), 'Frontend IP' (set to 'Public'), 'Protocol' (set to 'HTTP'), and 'Port' (set to '80'). Below these, there are sections for 'Additional settings' (Listener type set to 'Basic') and 'Error page url' (set to 'Yes'). At the bottom of the modal are 'Add' and 'Cancel' buttons.

4. On the **Backend targets** tab, select **myBackendPool** for the **Backend target**.
5. For the **HTTP setting**, select **Create new** to create a new HTTP setting. The HTTP setting will determine the behavior of the routing rule. In the **Add an HTTP setting** window that opens, enter **myHTTPSetting** for the **HTTP setting name**. Accept the default values for the other settings in the **Add an HTTP setting** window, then select **Add** to return to the **Add a routing rule** window.

The screenshot shows the same configuration page as before, but the 'Add an HTTP setting' dialog is now open. It contains fields for 'HTTP setting name' (set to 'myHTTPSetting'), 'Backend protocol' (set to 'HTTP'), and 'Backend port' (set to '80'). Below these, there are sections for 'Additional settings' (Cookie-based affinity set to 'Disable', Connection draining set to 'Disable', Request time-out (seconds) set to '20', and Override backend path left empty), 'Host name' (Override with new host name set to 'No', Host name override set to 'Override with specific domain name' with value 'e.g. contoso.com'), and 'Create custom probes' (set to 'No'). At the bottom are 'Add' and 'Cancel' buttons.

6. On the **Add a routing rule** window, select **Add** to save the routing rule and return to the **Configuration** tab.



7. Select **Next: Tags** and then **Next: Review + create**.

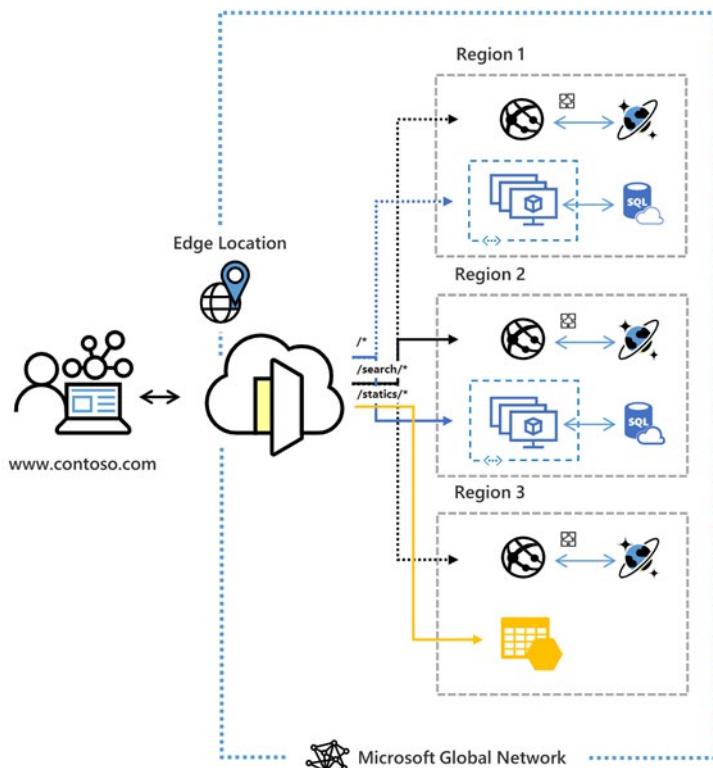
## Review + create tab

Review the settings on the **Review + create** tab, and then select **Create** to create the virtual network, the public IP address, and the application gateway. It may take several minutes for Azure to create the application gateway.

# Implement Azure Front Door

## Azure Front Door

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.



Azure Front Door enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reaches a global audience with Azure.

Front Door works at Layer 7 or HTTP/HTTPS layer and uses anycast protocol with split TCP and Microsoft's global network for improving global connectivity. So, per your routing method selection in the configuration, you can ensure that Front Door is routing your client requests to the fastest and most available application backend. An application backend is any Internet-facing service hosted inside or outside of Azure.

The following features are included with Front Door:

### Accelerate application performance

Using split TCP-based anycast protocol, Front Door ensures that your end users promptly connect to the nearest Front Door POP (Point of Presence).

## Increase application availability with smart health probes

Front Door delivers high availability for your critical applications using its smart health probes, monitoring your backends for both latency and availability and providing instant automatic failover when a backend goes down.

## URL-based routing

URL Path Based Routing allows you to route traffic to backend pools based on URL paths of the request. One of the scenarios is to route requests for different content types to different backend pools.

## Multiple-site hosting

Multiple-site hosting enables you to configure more than one web site on the same Front Door configuration.

## Session affinity

The cookie-based session affinity feature is useful when you want to keep a user session on the same application backend. By using Front Door managed cookies, subsequent traffic from a user session gets directed to the same application backend for processing.

## TLS termination

Front Door supports TLS termination at the edge that is, individual users can set up a TLS connection with Front Door environments instead of establishing it over long haul connections with the application backend.

## Custom domains and certificate management

When you use Front Door to deliver content, a custom domain is necessary if you would like your own domain name to be visible in your Front Door URL.

## URL redirection

Web applications are expected to automatically redirect any HTTP traffic to HTTPS. This ensures that all communication between the users and the application occurs over an encrypted path.

## URL rewrite

Front Door supports **URL rewrite**<sup>4</sup> by allowing you to configure an optional Custom Forwarding Path to use when constructing the request to forward to the backend.

## Protocol support - IPv6 and HTTP/2 traffic

Azure Front Door natively supports end-to-end IPv6 connectivity and also HTTP/2 protocol.

---

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/frontdoor/front-door-url-rewrite>

# Demonstration - Create an Azure Front Door

This practice exercise explains how to create a Front Door profile that delivers high availability and high performance for a global web application.

The scenario described in this exercise includes two instances of a web application running in different Azure regions. A Front Door configuration based on equal weighted and same priority backends is created that helps direct user traffic to the nearest set of site backends running the application. Front Door continuously monitors the web application and provides automatic failover to the next available backend when the nearest site is unavailable.

Sign in to the Azure portal at <https://portal.azure.com>.

## Prerequisites

This exercise requires that you have deployed two instances of a web application running in different Azure regions (East US and West Europe). Both the web application instances run in Active/Active mode, that is, either of them can take traffic at any time unlike a Active/Stand-By configuration where one acts as a failover.

1. On the top left-hand side of the screen, select **Create a resource > Web > Web App > Create**.
2. In **Web App**, enter or select the following information and enter default settings where none are specified:

Setting	Value
<b>Name</b>	Enter a unique name for your web app
<b>Resource group</b>	Select <b>New</b> , and then type <i>myResourceGroupFD1</i>
<b>App Service plan/Location</b>	Select <b>New</b> . In the <b>App Service plan</b> , enter <i>myAppServicePlanEastUS</i> , and then select <b>OK</b> .
<b>Location</b>	<b>East US</b>

3. Select **Create**.
4. A default website is created when the Web App is successfully deployed.
5. Repeat steps 1-3 to create a second website in a different Azure region with the following settings:

Setting	Value
<b>Name</b>	Enter a unique name for your web app
<b>Resource group</b>	Select <b>New</b> , and then type <i>myResourceGroupFD1</i>
<b>App Service plan/Location</b>	Select <b>New</b> . In the <b>App Service plan</b> , enter <i>myAppServicePlanEastUS</i> , and then select <b>OK</b> .
<b>Location</b>	<b>East US</b>

## Create a Front Door for your application

### A. Add a frontend host for Front Door

Create a Front Door configuration that directs user traffic based on lowest latency between the two backends.

1. On the top left-hand side of the screen, select **Create a resource > Networking > Front Door > Create**.
2. In the Create a Front Door, you start with adding the basic info and provide a subscription where you want the Front Door to be configured. Similarly, like any other Azure resource you also need to

provide a ResourceGroup and a Resource Group region if you are creating a new one. Lastly, you need to provide a name for your Front Door.

3. Once the basic info is filled in, the first step you need to define is the frontend host for the configuration. The result should be a valid domain name like *myappfrontend.azurefd.net*. This *hostname* needs to be globally unique but Front Door will take care of that validation.

### B. Add application backend and backend pools

Next, you need to configure your application backend(s) in a backend pool for Front Door to know where your application resides.

1. Click the + icon to add a backend pool and then specify a name for your backend pool, say *myBackendPool*.
2. Next, click on **Add Backends** to add your websites created earlier.
3. Select Target host type as *App Service*, select the subscription in which you created the web site and then choose the first web site from the Target host name, that is, *myAppServicePlanEastUS.azurewebsites.net*.
4. Leave the remaining fields as is for now and click **Add**.
5. Repeat steps 2 to 4 to add the other website, that is, *myAppServicePlanWestEurope.azurewebsites.net*
6. You can optionally choose to update the Health Probes and Load Balancing settings for the backend pool, but the default values should also work. Click **Add**.

### C. Add a routing rule

Lastly, click the + icon on Routing rules to configure a routing rule. This is needed to map your frontend host to the backend pool, which basically is configuring that if a request comes to **myappfrontend.azurefd.net**, then forward it to the backend pool *myBackendPool*. Click **Add** to add the routing rule for your Front Door. You should now be good to creating the Front Door and so click on **Review and Create**.

#### View Front Door in action

Once you create a Front Door, it will take a few minutes for the configuration to be deployed globally everywhere. Once complete, access the frontend host you created, that is, go to a web browser and hit the URL *myappfrontend.azurefd.net*. Your request will automatically get routed to the nearest backend to you from the specified backends in the backend pool.

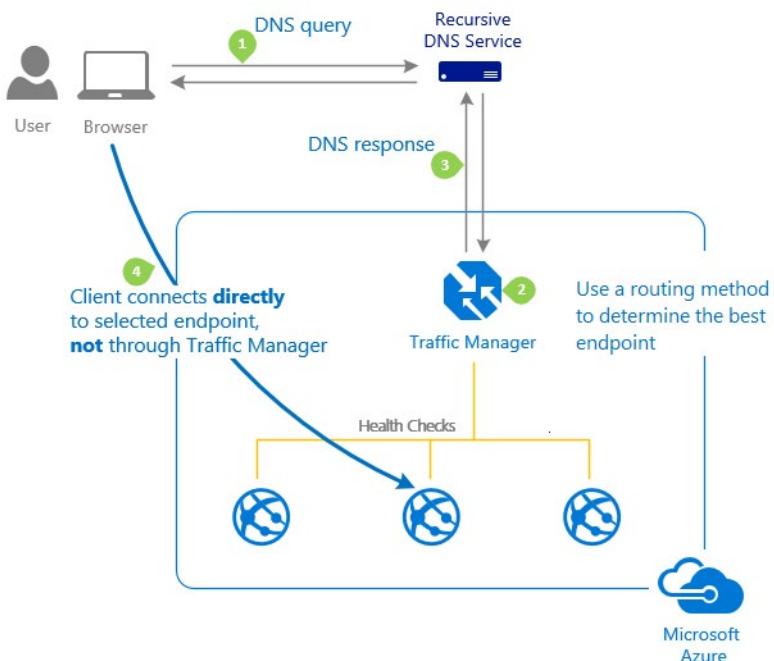
#### View Front Door handle application failover

If you want to test Front Door's instant global failover in action, you can go to one of the web sites you created and stop it. Based on the Health Probe setting defined for the backend pool, we will instantly fail over the traffic to the other web site deployment. You can also test behavior, by disabling the backend in the backend pool configuration for your Front Door.

# Implementing Azure Traffic Manager

## Azure Traffic Manager

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



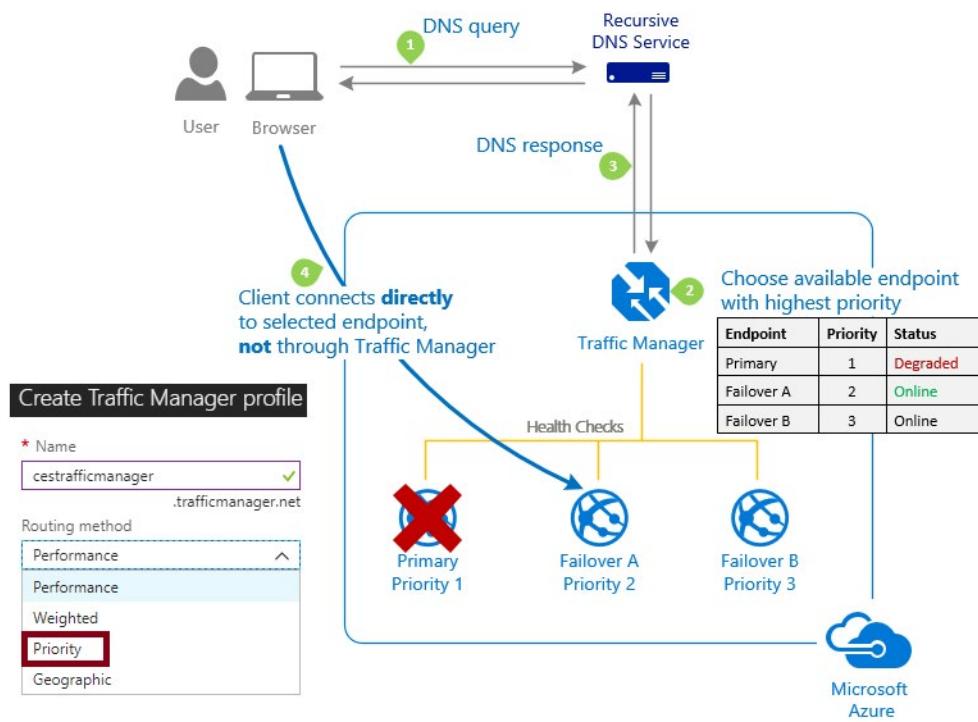
- Traffic Manager works by using the Domain Name System (DNS) to direct end-user requests to the most appropriate endpoint. Service endpoints supported by Traffic Manager include Azure VMs, Web Apps, and cloud services. You can also use Traffic Manager with external, non-Azure endpoints.
- Traffic Manager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

## Traffic Manager Routing Methods

### Priority routing

When a Traffic Manager profile is configured for priority routing it contains a prioritized list of service endpoints. Traffic Manager sends all traffic to the primary (highest-priority) endpoint first. If the primary endpoint is not available, Traffic Manager routes the traffic to the second endpoint, and so on.

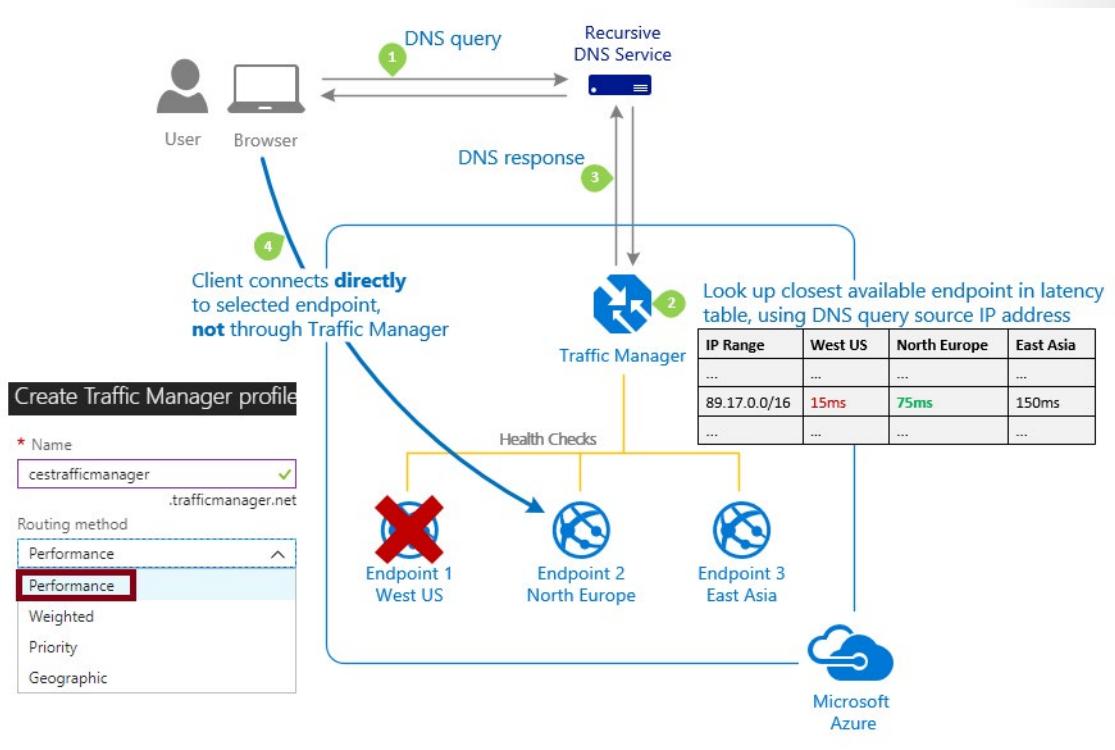
Availability of the endpoint is based on the configured status (enabled or disabled) and the ongoing endpoint monitoring. The Priority traffic routing method allows you to easily implement a failover pattern. You configure the endpoint priority explicitly or use the default priority based on the endpoint order.



## Performance routing

The Performance routing method is designed to improve the responsiveness by routing traffic to the location that is closest to the user. The closest endpoint is not necessarily measured by geographic distance. Instead Traffic Manager determines closeness by measuring network latency.

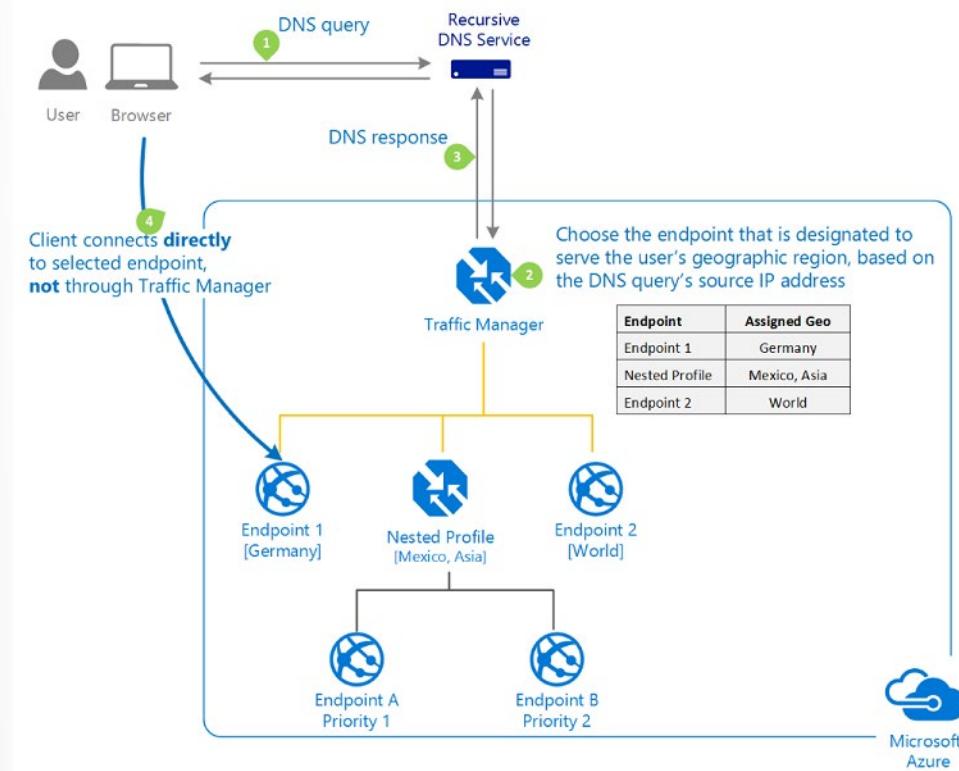
Traffic Manager maintains an Internet Latency Table to track the round-trip time between IP address ranges and each Azure datacenter. With this method Traffic Manager looks up the source IP address of the incoming DNS request in the Internet Latency Table. Traffic Manager chooses an available endpoint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



## Geographic routing

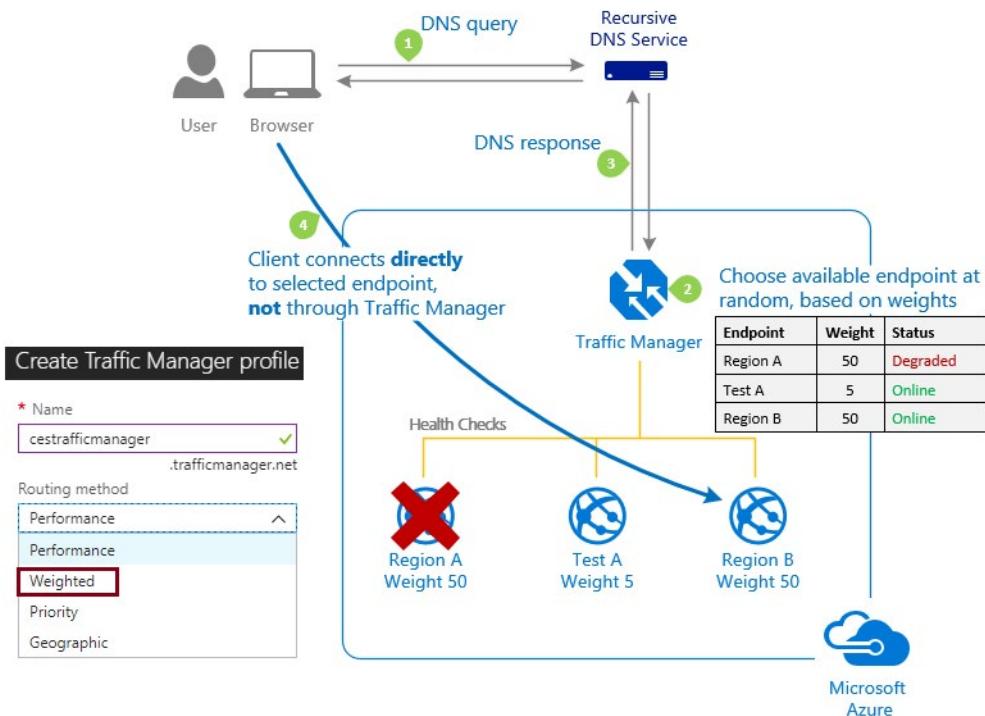
When a Traffic Manager profile is configured for Geographic routing, each endpoint associated with that profile needs will have a set of geographic locations assigned to it. Any requests from those regions gets routed only to that endpoint. Some planning is required when you create a geographical endpoint.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

You build the endpoint from a:



## Weighted routing

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



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

## Distributing Network Traffic

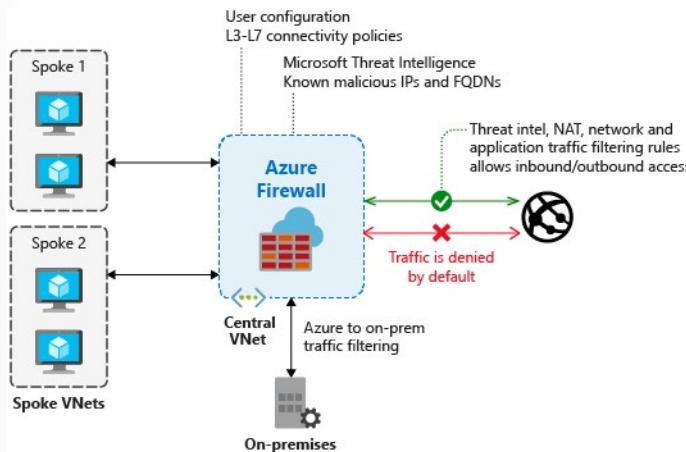
This table compares the Azure Load Balancer, Application Gateway, Traffic Manager, and Front Door. These technologies can be used in isolation or in combination.

Service	Azure Load Balancer	Application Gateway	Traffic Manager	Azure Front Door
<b>Technology</b>	Transport Layer (level 4)	Transport Layer (level 7)	DNS Resolver	Layer 7 or HTTP/HTTPS
<b>Protocols</b>	Any TCP or UDP Protocol	HTTP, HTTPS, HTTP/2, & WebSockets	DNS Resolution	Split TCP-based anycast protocol
<b>Backends and Endpoints</b>	Azure VMs, and Azure VM Scale Sets	Azure VMs, Azure VM Scale Sets, Azure App Services, IP Addresses, and Hostnames	Azure Cloud Services, Azure App Services, Azure App Service Slots, and Public IP Addresses	Internet-facing services hosted inside or outside of Azure
<b>Network connectivity</b>	External and Internal	External and Internal	External	External and Internal

# Implement Azure Firewall

## Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

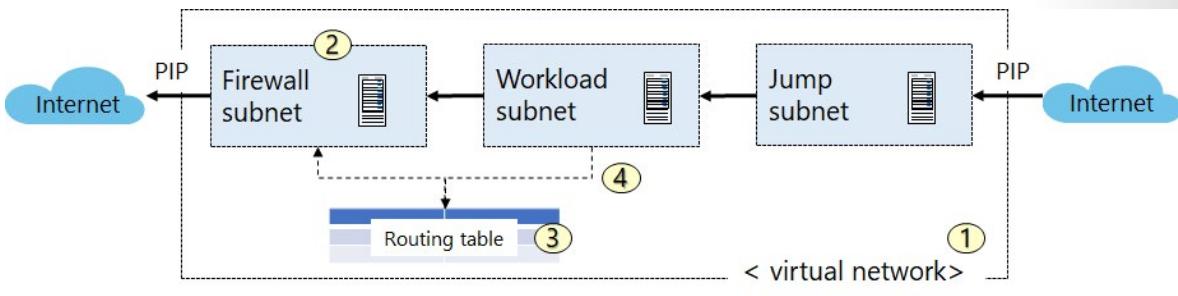


## Azure Firewall features

- **Built-in high availability.** High availability is built in, so no additional load balancers are required and there's nothing you need to configure.
- **Availability Zones.** Azure Firewall can be configured during deployment to span multiple Availability Zones for increased availability.
- **Unrestricted cloud scalability.** Azure Firewall can scale up as much as you need to accommodate changing network traffic flows, so you don't need to budget for your peak traffic.
- **Application FQDN filtering rules.** You can limit outbound HTTP/S traffic or Azure SQL traffic to a specified list of fully qualified domain names (FQDN) including wild cards.
- **Network traffic filtering rules.** You can centrally create allow or deny network filtering rules by source and destination IP address, port, and protocol. Azure Firewall is fully stateful, so it can distinguish legitimate packets for different types of connections. Rules are enforced and logged across multiple subscriptions and virtual networks.
- **Threat intelligence.** Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed.
- **Multiple public IP addresses.** You can associate multiple public IP addresses (up to 100) with your firewall.

# Implementing Azure Firewall

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



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

In production deployments, a **Hub and Spoke model**<sup>5</sup> is recommended, where the firewall is in its own VNET, and workload servers are in peered VNets in the same region with one or more subnets.

## Demonstration - Deploy Azure Firewall

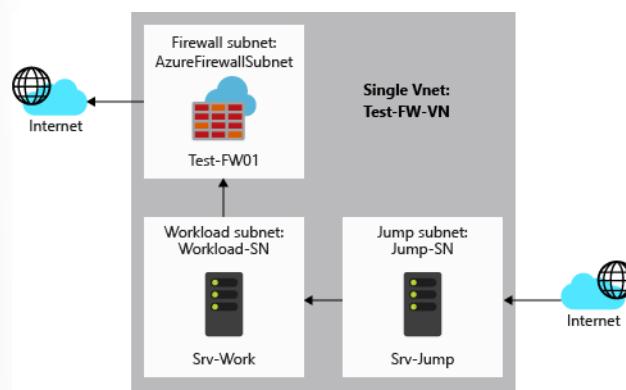
One way to control outbound network access from an Azure subnet is with Azure Firewall. With Azure Firewall, you can configure:

- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
- Network rules that define source address, protocol, destination port, and destination address.

For this demonstration, you create a simplified single VNet with three subnets for easy deployment. For production deployments, a hub and spoke model is recommended. The firewall is in its own VNet. The workload servers are in peered VNets in the same region with one or more subnets.

- **AzureFirewallSubnet** - the firewall is in this subnet.
- **Workload-SN** - the workload server is in this subnet. This subnet's network traffic goes through the firewall.
- **Jump-SN** - The "jump" server is in this subnet. The jump server has a public IP address that you can connect to using Remote Desktop. From there, you can then connect to (using another Remote Desktop) the workload server.

<sup>5</sup> <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>



In this demonstration, you learn how to:

- Set up a test network environment
- Deploy a firewall

## Set up the network

First, create a resource group to contain the resources needed to deploy the firewall.

### Create a resource group

The resource group contains all the resources for the demonstration.

1. Sign in to the Azure portal at <https://portal.azure.com><sup>6</sup>.
2. On the Azure portal menu, select **Resource groups** or search for and select Resource groups from any page. Then select **Add**.
3. For **Resource group name**, enter *Test-FW-RG*.
4. For **Subscription**, select your subscription.
5. For **Resource group location**, select a location. All other resources that you create must be in the same location.
6. Select **Create**.

### Create a VNet

This VNet will contain three subnets.

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. Select **Networking > Virtual network**.
3. For **Name**, type *Test-FW-VN*.
4. For **Address space**, type **10.0.0.0/16**.
5. For **Subscription**, select your subscription.
6. For **Resource group**, select **Test-FW-RG**.
7. For **Location**, select the same location that you used previously.
8. Under **Subnet**, for **Name** type **AzureFirewallSubnet**. The firewall will be in this subnet, and the subnet name must be **AzureFirewallSubnet**.

---

<sup>6</sup> <https://portal.azure.com/>

9. For **Address range**, type *10.0.1.0/26*.
10. Accept the other default settings, and then select **Create**.

#### **Create additional subnets**

Next, create subnets for the jump server, and a subnet for the workload servers.

1. On the Azure portal menu, select **Resource groups** or search for and select Resource groups from any page. Then select **Test-FW-RG**.
2. Select the **Test-FW-VN** virtual network.
3. Select **Subnets > +Subnet**.
4. For **Name**, type *Workload-SN*.
5. For **Address range**, type *10.0.2.0/24*.
6. Select **OK**.

Create another subnet named **Jump-SN**, address range *10.0.3.0/24*.

#### **Create virtual machines**

Now create the jump and workload virtual machines and place them in the appropriate subnets.

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. Select **Compute** and then select **Windows Server 2016 Datacenter** in the Featured list.
3. Enter these values for the virtual machine:

Setting	Value
Resource group	<b>Test-FW-RG</b>
Virtual machine name	<b>Srv-Jump</b>
Region	Same as previous
Administrator user name	<b>azureuser</b>
Password	<b>Azure123456!</b>

4. Under **Inbound port rules**, for **Public inbound ports**, select **Allow selected ports**.
5. For **Select inbound ports**, select **RDP (3389)**.
6. Accept the other defaults and select **Next: Disks**.
7. Accept the disk defaults and select **Next: Networking**.
8. Make sure that **Test-FW-VN** is selected for the virtual network and the subnet is **Jump-SN**.
9. For **Public IP**, accept the default new public ip address name (**Srv-Jump-ip**).
10. Accept the other defaults and select **Next: Management**.
11. Select **Off** to disable boot diagnostics. Accept the other defaults and select **Review + create**.
12. Review the settings on the summary page, and then select **Create**.

Use the information in the following table to configure another virtual machine named **Srv-Work**. The rest of the configuration is the same as the Srv-Jump virtual machine.

Setting	Value
Subnet	<b>Workload-SN</b>
Public IP	<b>None</b>

Setting	Value
Public inbound ports	<b>None</b>

## Deploy the firewall

Deploy the firewall into the VNet.

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. Type *firewall* in the search box and press **Enter**.
3. Select **Firewall** and then select **Create**.
4. On the **Create a Firewall page**, use the following table to configure the firewall:

Setting	Value
Subscription	your subscription
Resource group	<b>Test-FW-RG</b>
Name	<b>Test-FW01</b>
Location	Select the same location that you used previously
Choose a virtual network	<b>Use existing: Test-FW-VN</b>
Public IP address	<b>Add new.</b> The Public IP address must be the Standard SKU type.

5. Select **Review + create**.
6. Review the summary, and then select **Create** to create the firewall.  
This will take a few minutes to deploy.
7. After deployment completes, go to the **Test-FW-RG** resource group, and select the **Test-FW01 firewall**.

# Implement Network Security Groups and Application Security Groups

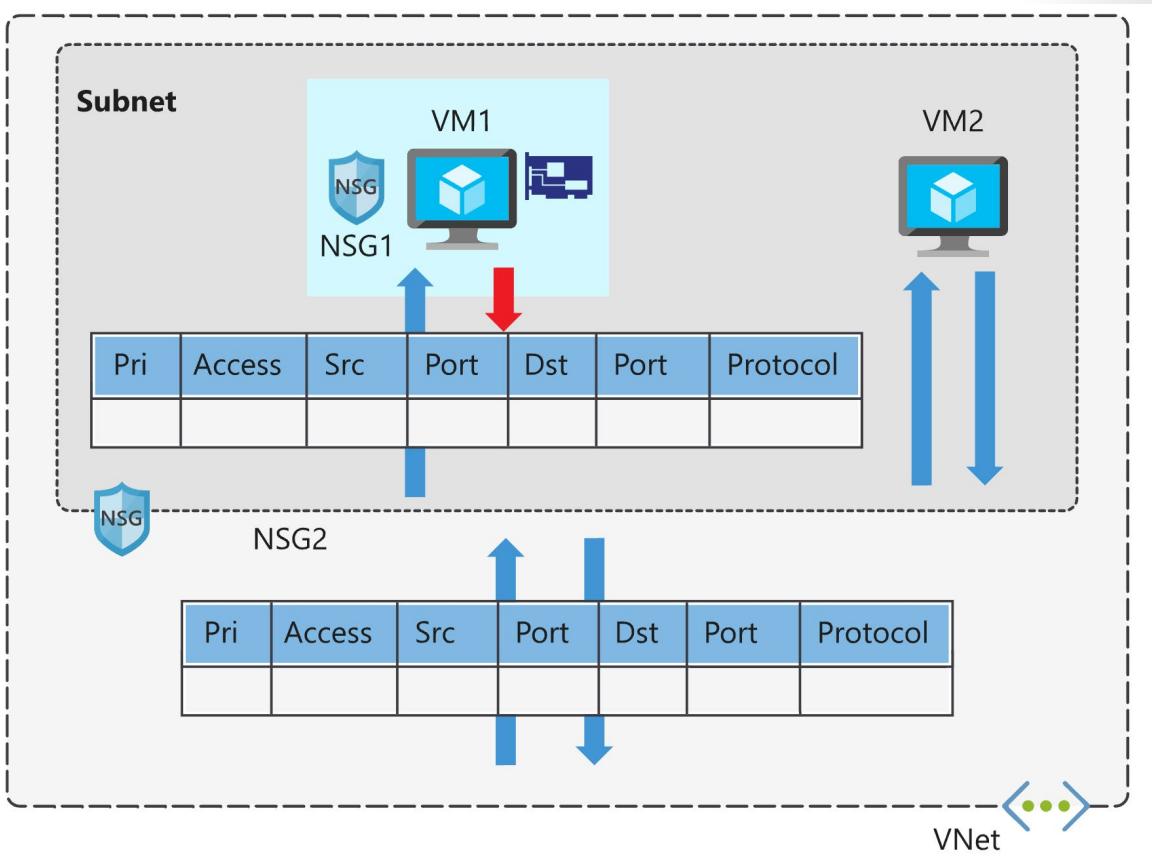
## Network Security Groups (NSGs)

Network security groups filter network traffic to and from Azure resources. Network security groups contain security rules that you configure to allow or deny inbound and outbound traffic. You can use network security groups to filter traffic between virtual machines or subnets, both within a virtual network and from the internet.

### Network security group assignment and evaluation

Network security groups are assigned to a network interface or a subnet. When you assign a network security group to a subnet, the rules apply to all network interfaces in that subnet. You can restrict traffic further by associating a network security group to the network interface of a virtual machine.

When you apply network security groups to both a subnet and a network interface, each network security group is evaluated independently. Inbound traffic is first evaluated by the network security group applied to the subnet, and then by the network security group applied to the network interface. Conversely, outbound traffic from a virtual machine is first evaluated by the network security group applied to the network interface, and then by the network security group applied to the subnet.



Applying a network security group to a subnet instead of individual network interfaces can reduce administration and management efforts. This approach also ensures that all virtual machines within the specified subnet are secured with the same set of rules.

Each subnet and network interface can have one network security group applied to it. Network security groups support TCP, UDP, and ICMP, and operate at Layer 4 of the OSI model.

## Security Rules

A network security group contains one or more security rules. Configure security rules to either allow or deny traffic.

Rules have several properties:

Property	Explanation
<b>Name</b>	A unique name within the network security group.
<b>Priority</b>	A number between 100 and 4096.
<b>Source or destination</b>	Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group.
<b>Protocol</b>	TCP, UDP, or Any.
<b>Direction</b>	Whether the rule applies to inbound, or outbound traffic.
<b>Port range</b>	An individual port or range of ports.
<b>Action</b>	Allow or deny the traffic.

Network security group security rules are evaluated by priority, using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic. When the conditions for a rule match the device configuration, rule processing stops.

With network security groups, the connections are stateful. Return traffic is automatically allowed for the same TCP/UDP session.

## Augmented security rules

You use augmented security rules for network security groups to simplify the management of large numbers of rules. Augmented security rules also help when you need to implement more complex network sets of rules.

Augmented rules let you add the following options into a single security rule:

- multiple IP addresses
- multiple ports
- service tags
- application security groups

## Service tags

You use service tags to simplify network security group security even further. You can allow or deny traffic to a specific Azure service, either globally or per region.

Service tags simplify security for virtual machines and Azure virtual networks, by allowing you to restrict access by resources or services. Service tags represent a group of IP addresses, and help simplify the

configuration of your security rules. For resources that you can specify by using a tag, you don't need to know the IP address or port details.

You can restrict access to many services. Microsoft manages the service tags (you can't create your own). Some examples of the tags are:

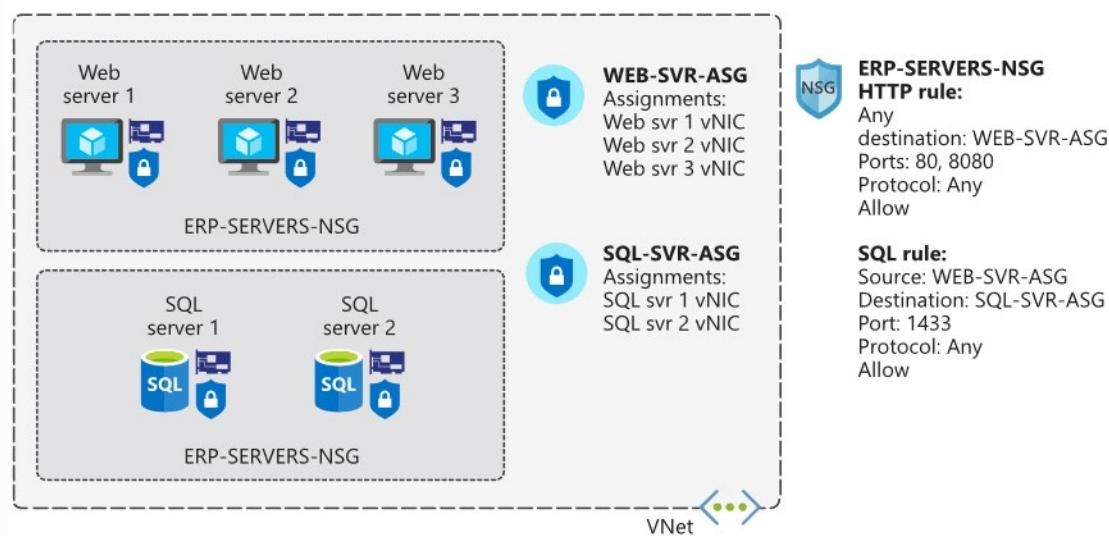
- **VirtualNetwork** - This tag represents all virtual network addresses anywhere in Azure, and in your on-premises network if you're using hybrid connectivity.
- **AzureLoadBalancer** - This tag denotes Azure's infrastructure load balancer. The tag translates to the virtual IP address of the host (168.63.129.16) where Azure health probes originate.
- **Internet** - This tag represents anything outside the virtual network address that is publicly reachable, including resources that have public IP addresses. One such resource is the Web Apps feature of Azure App Service.
- **AzureTrafficManager** - This tag represents the IP address for Azure Traffic Manager.
- **Storage** - This tag represents the IP address space for Azure Storage. You can specify whether traffic is allowed or denied. You can also specify if access is allowed only to a specific region, but you can't select individual storage accounts.
- **SQL** - This tag represents the address for Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure SQL Data Warehouse services. You can specify whether traffic is allowed or denied, and you can limit to a specific region.
- **AppService** - This tag represents address prefixes for Azure App Service.

## Application Security Groups

Use application security groups within a network security group to apply a security rule to a group of resources. It's easier to deploy and scale up specific application workloads. You just add a new virtual machine deployment to one or more application security groups, and that virtual machine automatically picks up your security rules for that workload.

An application security group allows you to group network interfaces together. You can then use that application security group as a source or destination rule within a network security group.

For example, your company has a number of front-end servers in a virtual network. The web servers must be accessible over ports 80 and 8080. Database servers must be accessible over port 1433. You assign the network interfaces for the web servers to one application security group, and the network interfaces for the database servers to another application security group. You then create two inbound rules in your network security group. One rule allows HTTP traffic to all servers in the web server application security group. The other rule allows SQL traffic to all servers in the database server application security group.



Without application security groups, you'd need to create a separate rule for each virtual machine.

# Implement Azure Bastion

## Azure Bastion

The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS. When you connect using Azure Bastion, your virtual machines do not need a public IP address.

Bastion provides secure RDP and SSH connectivity to all the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. With Azure Bastion, you connect to the virtual machine directly from the Azure portal.

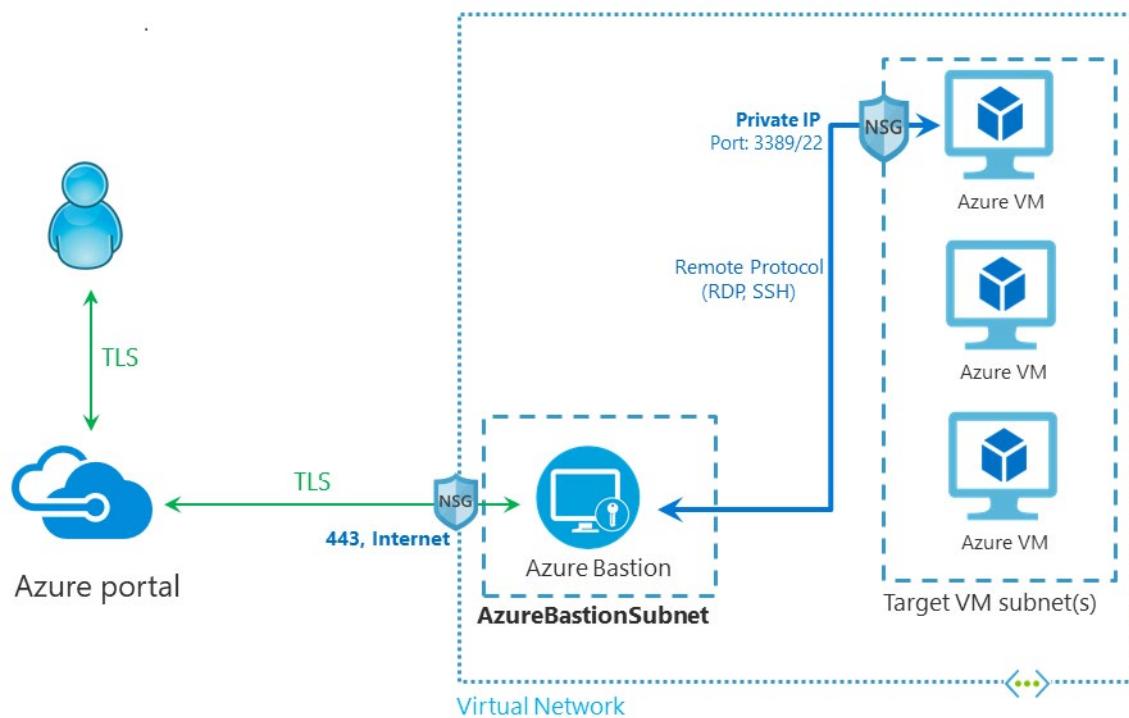
## Architecture

Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine. Once you provision an Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same virtual network.

Exposing RDP/SSH ports over the Internet isn't desired and is seen as a significant threat surface. This is often due to protocol vulnerabilities. To contain this threat surface, you can deploy bastion hosts (also known as jump-servers) at the public side of your perimeter network. Bastion host servers are designed and configured to withstand attacks. Bastion servers also provide RDP and SSH connectivity to the workloads sitting behind the bastion, as well as further inside the network.

This figure below shows the architecture of an Azure Bastion deployment. In this diagram:

- The Bastion host is deployed in the virtual network.
- The user connects to the Azure portal using any HTML5 browser.
- The user selects the virtual machine to connect to.
- With a single click, the RDP/SSH session opens in the browser.
- No public IP is required on the Azure VM.



## Key features

The following features are available:

- **RDP and SSH directly in Azure portal:** You can directly get to the RDP and SSH session directly in the Azure portal using a single click seamless experience.
- **Remote Session over TLS and firewall traversal for RDP/SSH:** Azure Bastion uses an HTML5 based web client that is automatically streamed to your local device, so that you get your RDP/SSH session over TLS on port 443 enabling you to traverse corporate firewalls securely.
- **No Public IP required on the Azure VM:** Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You don't need a public IP on your virtual machine.
- **No hassle of managing NSGs:** Azure Bastion is a fully managed platform PaaS service from Azure that is hardened internally to provide you secure RDP/SSH connectivity. You don't need to apply any NSGs on Azure Bastion subnet. Because Azure Bastion connects to your virtual machines over private IP, you can configure your NSGs to allow RDP/SSH from Azure Bastion only.
- **Protection against port scanning:** Because you do not need to expose your virtual machines to public Internet, your VMs are protected against port scanning by rogue and malicious users located outside your virtual network.
- **Protect against zero-day exploits.** Hardening in one place only: Azure Bastion is a fully platform-managed PaaS service. Because it sits at the perimeter of your virtual network, you don't need to worry about hardening each of the virtual machines in your virtual network.

## Demonstration - Create an Azure Bastion Host

This demonstration shows you how to create an Azure Bastion host using the Azure portal. Once you provision the Azure Bastion service in your virtual network, the seamless RDP/SSH experience is available to all of the VMs in the same virtual network. Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine.

You can create a new bastion host resource in the portal either by specifying all of the settings manually, or by using the settings that correspond to an existing VM.

### Create a new Azure Bastion resource from the Azure portal.

1. On the **Azure portal**<sup>7</sup> menu or from the **Home** page, select **Create a resource**.
2. On the **New** page, in the **Search the Marketplace** field, type *Bastion*, then click **Enter** to get to the search results.
3. From the results, click **Bastion**. Make sure the publisher is *Microsoft* and the category is *Networking*.
4. On the **Bastion** page, click **Create** to open the **Create a bastion** page.
5. On the **Create a bastion** page, configure a new Bastion resource. Specify the configuration settings for your Bastion resource.

<sup>7</sup> <https://portal.azure.com/>

Home > New > Marketplace > Get Started > Bastion (preview) > Create a bastion

## Create a bastion

Basics Tags Review + create

Bastion allows web based RDP access to your vnet VM. [Learn more.](#)

**PROJECT DETAILS**

\* Subscription: [dropdown]

\* Resource group: [dropdown] Select existing... Create new

**INSTANCE DETAILS**

\* Name: [text input]

\* Region: [dropdown]

**CONFIGURE VIRTUAL NETWORKS**

\* Virtual network: [dropdown] Filter virtual networks Create new

Subnet: AzureBastionSubnet

**PUBLIC IP ADDRESS**

\* Public IP address: [radio button] Create new [radio button] Use existing

\* Public IP address name: [text input]

Public IP address SKU: Standard

\* Assignment: [radio button] Dynamic [radio button] Static

**Review + create** Previous Next : Tags > Download a template for automation

- **Subscription:** The Azure subscription you want to use to create a new Bastion resource.
- **Resource Group:** The Azure resource group in which the new Bastion resource will be created in. If you don't have an existing resource group, you can create a new one.
- **Name:** The name of the new Bastion resource
- **Region:** The Azure public region that the resource will be created in.
- **Virtual network:** The virtual network in which the Bastion resource will be created in. You can create a new virtual network in the portal during this process, or use an existing virtual network. If you are using an existing virtual network, make sure the existing virtual network has enough free address space to accommodate the Bastion subnet requirements.

- **Subnet:** The subnet in your virtual network where the new Bastion host will be deployed. The subnet will be dedicated to the Bastion host and must be named as AzureBastionSubnet. This subnet must be at least /27 or larger.

AzureBastionSubnet doesn't support User Defined Routes, but does support Network Security Groups.

- **Public IP address:** The public IP of the Bastion resource on which RDP/SSH will be accessed (over port 443). Create a new public IP, or use an existing one. The public IP address must be in the same region as the Bastion resource you are creating.

- **Public IP address name:** The name of the public IP address resource.

- **Public IP address SKU:** This setting is prepopulated by default to Standard. Azure Bastion uses/supports only the Standard Public IP SKU.

- **Assignment:** This setting is prepopulated by default to Static.

6. When you have finished specifying the settings, click **Review + Create**.

7. On the **Create** a bastion page, click **Create**.

8. You will see a message letting you know that your deployment is underway. Status will display on this page as the resources are created. It takes about 5 minutes for the Bastion resource to be created and deployed.

## Module 5 Review Questions

### Module 5 Review Questions



#### Review Question 1

*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 2

*You are advising a company that is planning to create a virtual network that has a scale set that contains ten VMs.*

*They have a monitoring solution on a separate network that will need to access the VMs within the scale set. They want to define public access to the virtual machines.*

*You recommend that they implement an Azure Load Balancer to for connecting the monitoring solution to the VMs. Does this recommendation fulfill the goal?*

- Yes
- No

#### Review Question 3

*Your organization has Azure VMs deployed to three Azure regions. Each region contains a single virtual network that has four VMs on the same subnet. Each virtual machine runs an application named OEM\_APP\_3.*

*OEM\_APP\_3 is accessible by using HTTPS.*

- The VMs are cannot be accessed from the Internet.
- You are asked to use Azure Front Door to load balance requests from OEM\_SQL\_3 across all the VMs.

- What other Azure service should you enable?
  - An internal Azure Load Balancer
  - Azure Private Link
  - A public Azure Load Balancer
  - Enable High Availability ports

## Lab

# Lab - Implementing Highly Available Azure IaaS Compute Architecture

✓ **Important:** To download the most recent version of this lab, please visit the AZ-303 [GitHub repository](#)<sup>8</sup>.

Direct link to the [Lab: Implementing Highly Available Azure IaaS Compute Architecture](#)<sup>9</sup>.

## Lab scenario



Adatum Corporation has several on-premises workloads running on a mix of physical servers and virtual machines. Most of the workloads require some level of resiliency, including a range of high availability SLAs. Most of the workloads leverage either Windows Server Failover Clustering or Linux Corosync clusters and Pacemaker resource manager, with synchronous replication between cluster nodes. Adatum is trying to determine how the equivalent functionality can be implemented in Azure. In particular, the Adatum Enterprise Architecture team is exploring the Azure platform capabilities that accommodate high availability requirements within the same data center and between data centers in the same region.

In addition, the Adatum Enterprise Architecture team realizes that resiliency alone might not be sufficient to provide the level of availability expected by its business operations. Some of the workloads have highly dynamic usage patterns, which are currently addressed based on continuous monitoring and custom scripting solutions, automatically provisioning and deprovisioning additional cluster nodes. Usage patterns of others are more predictable, but also need to be occasionally adjusted to account for increase demand for disk space, memory, or processing resources.

To accomplish these objectives, the Architecture team wants to test a range of highly available IaaS compute deployments, including:

- Availability sets-based deployment of Azure VMs behind an Azure Load Balancer Basic
- Zone-redundant deployment of Azure VMs behind an Azure Load Balancer Standard
- Zone-redundant deployment of Azure VM scale sets behind an Azure Application Gateway
- Automatic horizontal scaling of Azure VM scale sets (autoscaling)
- Manual vertical scaling (compute and storage) of Azure VM scale sets

An availability set represents a logical grouping of Azure VMs which controls their physical placement within the same Azure datacenter. Azure makes sure that the VMs within the same availability set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays opera-

---

<sup>8</sup> <https://github.com/MicrosoftLearning/AZ-303-Microsoft-Azure-Architect-Technologies>

<sup>9</sup> [https://aka.ms/303\\_Module\\_05\\_Lab](https://aka.ms/303_Module_05_Lab)

tional. Availability Sets are essential for building reliable cloud solutions. With availability sets, Azure offers 99.95% VM uptime SLA.

Availability zones represent unique physical locations within a single Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. The physical separation of availability zones within a region protects applications and data from datacenter failures. Zone-redundant services replicate your applications and data across availability zones to protect from single-points-of-failure. With availability zones, Azure offers 99.99% VM uptime SLA.

Azure virtual machine scale sets let you create and manage a group of identical, load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update many VMs. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

## Objectives

After completing this lab, you will be able to:

- Describe characteristics of highly available Azure VMs residing in the same availability set behind a Azure Load Balancer Basic
- Describe characteristics of highly available Azure VMs residing in different availability zones behind an Azure Load Balancer Standard
- Describe characteristics of automatic horizontal scaling of Azure VM Scale Sets
- Describe characteristics of manual vertical scaling of Azure VM Scale Sets

## Lab Files

- \AZ303\AllFiles\Labs\01\azuredeploy30301suba.json
- \AZ303\AllFiles\Labs\01\azuredeploy30301rga.json
- \AZ303\AllFiles\Labs\01\azuredeploy30301rga.parameters.json
- \AZ303\AllFiles\Labs\01\azuredeploy30301rgb.json
- \AZ303\AllFiles\Labs\01\azuredeploy30301rgb.parameters.json
- \AZ303\AllFiles\Labs\01\azuredeploy30301rgc.json
- \AZ303\AllFiles\Labs\01\azuredeploy30301rgc.parameters.json
- \AZ303\AllFiles\Labs\01\az30301e-configure\_VMSS\_with\_data\_disk.ps1

## Exercise 1: Implement and analyze highly available Azure VM deployments using availability sets and Azure Load Balancer Basic

The main tasks for this exercise are as follows:

1. Deploy highly available Azure VMs into an availability set behind an Azure Load Balancer Basic by using Azure Resource Manager templates
2. Analyze highly available Azure VMs deployed into an availability set behind an Azure Load Balancer Basic

3. Remove Azure resources deployed in the exercise

## **Exercise 2: Implement and analyze highly available Azure VM deployments using availability zones and Azure Load Balancer Standard**

The main tasks for this exercise are as follows:

1. Deploy highly available Azure VMs into availability zones behind an Azure Load Balancer Standard by using Azure Resource Manager templates
2. Analyze highly available Azure VMs deployed across availability zones behind an Azure Load Balancer Standard
3. Remove Azure resources deployed in the exercise

## **Exercise 3: Implement and analyze highly available Azure VM Scale Set deployments using availability zones and Azure Application Gateway.**

The main tasks for this exercise are as follows:

1. Deploy a highly available Azure VM Scale Set into availability zones behind an Azure Application Gateway by using Azure Resource Manager templates
2. Analyze a highly available Azure VM Scale Set deployed across availability zones behind an Azure Application Gateway
3. Remove Azure resources deployed in the exercise

## **Exercise 4: Implementing autoscaling of Azure VM Scale Sets using availability zones and Azure Application Gateway.**

The main tasks for this exercise are as follows:

1. Configuring autoscaling of an Azure VM Scale Set
2. Testing autoscaling of an Azure VM Scale Set

## **Exercise 5: Implementing vertical scaling of Azure VM Scale Sets**

The main tasks for this exercise are as follows:

1. Scaling compute resources of Azure virtual machine scale set instances.
2. Scaling storage resources of Azure virtual machine scale sets instances.

# Answers

## Review Question 1

Your company provides customers a virtual network in the cloud. You have dozens of Linux virtual machines in another virtual network. You need to install an Azure load balancer to direct traffic between the virtual networks. What should you do? Select one.

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

### Explanation

*Install an internal load balancer. Azure has two types of load balancers: public and internal. An internal load balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.*

## Review Question 2

You are advising a company that is planning to create a virtual network that has a scale set that contains ten VMs.

They have a monitoring solution on a separate network that will need to access the VMs within the scale set.

They want to define public access to the virtual machines.

You recommend that they implement an Azure Load Balancer to for connecting the monitoring solution to the VMs. Does this recommendation fulfill the goal?

- Yes
- No

### Explanation

*Correct Answer: The technique of using a round-robin approach with an Azure Load Balancer allows access to a virtual machine within a scale set externally.*

## Review Question 3

Your organization has Azure VMs deployed to three Azure regions. Each region contains a single virtual network that has four VMs on the same subnet. Each virtual machine runs an application named OEM\_APP\_3.

OEM\_APP\_3 is accessible by using HTTPs.

- An internal Azure Load Balancer
- Azure Private Link
- A public Azure Load Balancer
- Enable High Availability ports

### Explanation

*Correct answer: A public Azure Load Balancer.*



# Module 6 Implement Storage Accounts

## 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 scalable, REST based cloud object store. Data Lake Store is Hadoop Distributed File System (HDFS) as a service.
- **Structured Data.** This includes Tables. Tables are a key/value, auto-scaling NoSQL store.

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

- **Standard** storage accounts are backed by magnetic drives (HDD) and provide the lowest cost per GB. They are best for applications that require bulk storage or where data is accessed infrequently.
- **Premium** storage accounts are backed by solid state drives (SSD) and offer consistent low-latency performance. They can only be used with Azure virtual machine disks and are best for I/O-intensive applications, like databases.

**Note:** ✓ 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.

## Azure Storage Services

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

- **Azure Containers (Blobs):** A massively scalable object store for text and binary data.
- **Azure Files:** Managed file shares for cloud or on-premises deployments.
- **Azure Queues:** A messaging store for reliable messaging between application components.
- **Azure Tables:** A NoSQL store for schemaless storage of structured data.

## Container (blob) storage

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

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

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

## Azure Files

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

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.

## Queue storage

The Azure Queue service is used to store and retrieve messages. Queue messages can be up to 64 KB in size, and a queue can contain millions of messages. Queues are generally used to store lists of messages to be processed asynchronously.

For example, say you want your customers to be able to upload pictures, and you want to create thumbnails for each picture. You could have your customer wait for you to create the thumbnails while uploading the pictures. An alternative would be to use a queue. When the customer finishes his upload, write a message to the queue. Then have an Azure Function retrieve the message from the queue and create the thumbnails. Each of the parts of this processing can be scaled separately, giving you more control when tuning it for your usage.

## Table storage

Azure Table storage is now part of Azure Cosmos DB. In addition to the existing Azure Table storage service, there is a new Azure Cosmos DB Table API offering that provides throughput-optimized tables, global distribution, and automatic secondary indexes. To learn more and try out the new premium experience, please check out Azure Cosmos DB Table API.

## Storage Account Types

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

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

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

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

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

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

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

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

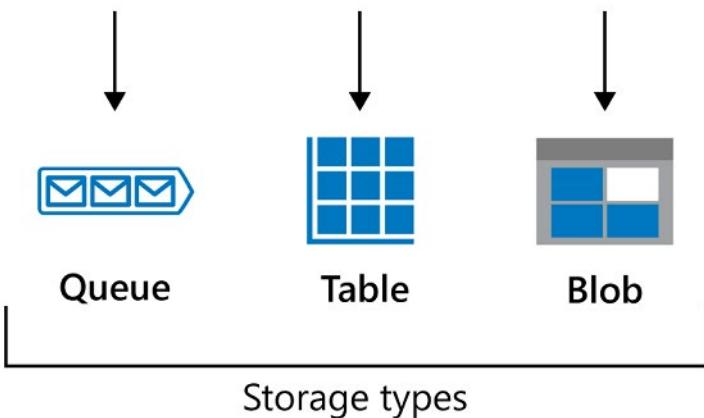
## Azure Storage Account Replication Features

Below is a walk-through of how an Azure storage account is configured to allow for replication and high availability of data.

### Azure storage accounts

As previously mentioned, Azure storage accounts are used to house data objects, such as files, blobs, tables, and disks for virtual machines. The data that you store in a storage account can be accessed from any location globally via HTTP or HTTPS and is highly available and secure.

## Read-Access Geo-Redundant Storage



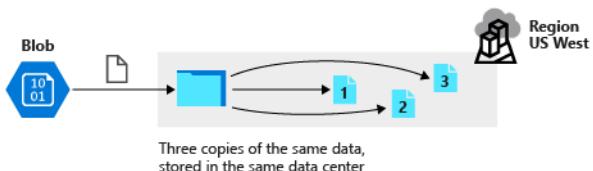
### Data redundancy

Data in Azure is replicated to ensure that it's always available, even if a datacenter or region becomes inaccessible or a specific piece of hardware fails. You have four replication options:

- Locally redundant storage (LRS)
- Zone-redundant storage (ZRS)
- Geographically redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

Each replication option provides a different level of redundancy and durability. The following sections describe these options in more detail.

### What is locally redundant storage (LRS)?



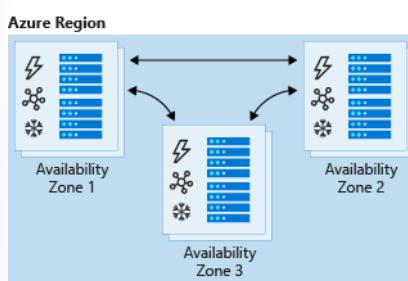
Locally redundant storage replicates data and stores three copies across fault domains, or racks of hardware, within a single datacenter facility in one region. Data is replicated so that if there's a hardware fault or maintenance work, your data is still available and accessible.

LRS protects your data from hardware failures, but you aren't protected if there's a datacenter outage. For example, if Array 1 in UK South suffers a hardware failure, your data is still available on Array 2. If the entire datacenter suffers a failure, you would most likely lose your data.

LRS offers 99.9999999999 percent durability of data.

LRS is the least expensive replication option available. It also offers the least durability, because you can potentially lose all your data during a datacenter outage, depending on the severity of the outage.

### What is zone-redundant storage (ZRS)?



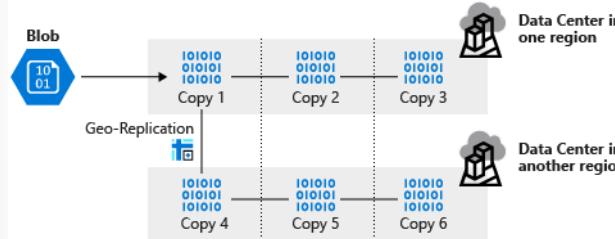
Zone-redundant storage replicates your data across three storage clusters in a region. Each cluster is physically separated from the other two, which means that each cluster is supplied by separate utilities, such as power or networking.

If there's an outage in a datacenter, you can still access your data from another availability zone in that region. Data is normally replicated to two or three availability zones, depending on the region.

An availability zone (AZ) is a physical location that's made up of one or more datacenters in a region. There are typically two or three AZs per region, where each AZ is independent of the other AZs in the region.

ZRS offers 99.999999999 percent durability of data. However, ZRS might not protect you from a regional outage, because all AZs reside in the same region. To migrate data to ZRS from either LRS or GRS requires some planning and manual migration. And it requires a tool such as AZCopy.

### What is geographically redundant storage (GRS)?

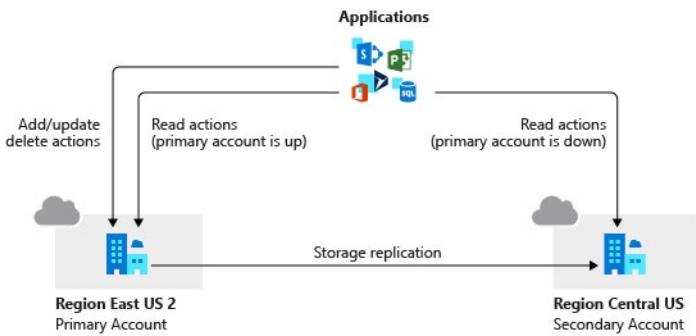


Geographically redundant, or geo-redundant, storage provides multiple levels of replication. Your data is replicated three times within the primary region, and then this set is replicated to a secondary region.

GRS provides the highest level of durability, because you finish with six copies of your data. Such durability means that even if there's a datacenter failure or regional issues in the primary region, your data is always available. If the primary region fails, Azure storage is still available in the secondary region. The secondary region is automatically paired to the primary region based on the primary region you selected. This pairing configuration can't be changed.

Keep in mind that your data in the secondary region is inaccessible until the primary region has failed across to the secondary region. At this point, the secondary region becomes the active region (primary), and your data becomes accessible.

### What is read-access geo-redundant storage (RA-GRS)?



Geo-redundant storage provides 99.9999999999999 percent durability, because it replicates data and objects to a secondary region. When failover starts, DNS entries that point to the primary region are updated to point to the secondary region. Microsoft currently controls the DNS failover process.

When you use RA-GRS, you need to ensure that your application knows which endpoint it's interacting with. The secondary region has "-secondary" appended to the name of the endpoint.

RA-GRS is ideal for applications, which require high availability.

A new feature allows you to start a failover between primary and secondary regions from the Azure portal, PowerShell, or the Azure CLI. When the primary endpoint becomes unavailable, you can fail over to the secondary endpoint. Account failover is supported for all public regions but is not available in sovereign or national clouds at this time.

After the failover and DNS endpoint updates are complete, the storage account is set back to LRS. You're responsible for reverting the replication settings from LRS to RA-GRS or GRS after the primary region becomes available again.

#### **When to use each type of redundant storage**

The most appropriate use of each type of redundant storage is summarized in the following table:

	LRS	ZRS	GRS	RA-GRS
Overview	Replicates data in a single datacenter	Stores copies of data across multiple data-centers	Stores copies in a local datacenter, like LRS, but then stores three more copies in a datacenter in another region	Same as GRS, but offers read access in the secondary datacenter in the other region
Data copies	3	3	6	6
Use case	Ensures that your data is highly available but, for compliance reasons, must be kept local	A higher durability option for block storage, where data can stay in only one region	Where you need to ensure that your data and systems are always available despite datacenter or region outages	Where your applications (especially those with many read requests) can read data from other regions, but also to ensure that read operations are always available even if the primary region is down

## Accessing Storage

Every object that you store in Azure Storage has a unique URL address. The storage account name forms the subdomain of that address. The combination of subdomain and domain name, which is specific to each service, forms an endpoint for your storage account.

For example, if your storage account is named *mystorageaccount*, then the default endpoints for your storage account are:

- Container service: <http://mystorageaccount.blob.core.windows.net>
- Table service: <http://mystorageaccount.table.core.windows.net>
- Queue service: <http://mystorageaccount.queue.core.windows.net>
- File service: <http://mystorageaccount.file.core.windows.net>

The URL for accessing an object in a storage account is built by appending the object's location in the storage account to the endpoint. For example, to access *myblob* in the *mycontainer*, use this format: <http://mystorageaccount.blob.core.windows.net/mycontainer/myblob>.

## Configuring a Custom Domain

You can configure a custom domain for accessing blob data in your Azure storage account. As mentioned previously, the default endpoint for Azure Blob storage is <storage-account-name>.blob.core.windows.net. You can also use the web endpoint that's generated as a part of the static websites feature. If you map a custom domain and subdomain, such as www.contoso.com, to the blob or web endpoint for your storage account, your users can use that domain to access blob data in your storage account. There are two ways to configure this service: Direct CNAME mapping and an intermediary domain.

✓ **Note:** Azure Storage does not yet natively support HTTPS with custom domains. You can currently Use Azure CDN to access blobs by using custom domains over HTTPS.

**Direct CNAME mapping** for example, to enable a custom domain for the blobs.contoso.com sub domain to an Azure storage account, create a CNAME record that points from blobs.contoso.com to the Azure storage account [storage account].blob.core.windows.net. The following example maps a domain to an Azure storage account in DNS:

CNAME record	Target
blobs.contoso.com	contosoblobs.blob.core.windows.net

**Intermediary mapping with asverify** Mapping a domain that is already in use within Azure may result in minor downtime as the domain is updated. 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

**Note:** ✓ 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.

## 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:

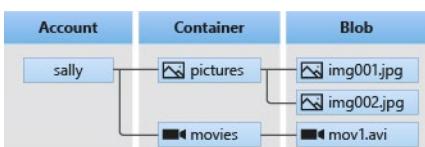
- Serving images or documents directly to a browser.
- Storing files for distributed access, such as installation.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

### 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.



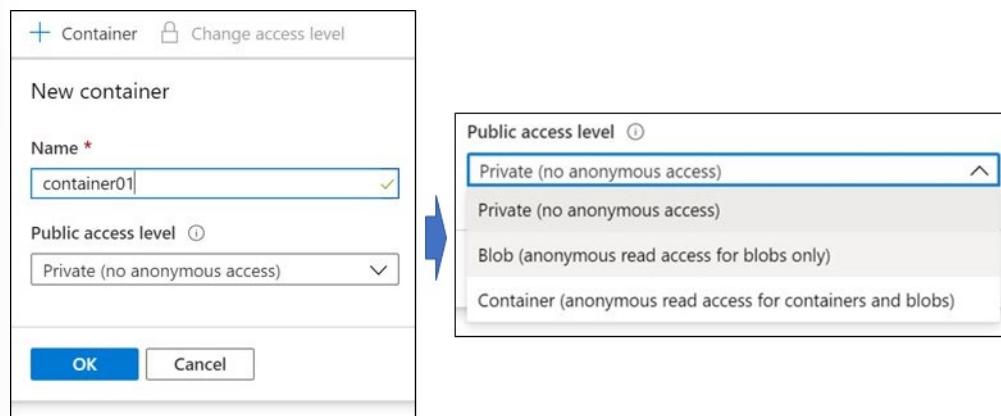
- ✓ Within the storage account, you can group as many blobs as needed in a container.

For more information, [Azure Blob Storage<sup>1</sup>](#).

## 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.

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



**Name:** The name may only contain lowercase letters, numbers, and hyphens, and must begin with a letter or a number. The name must also be between 3 and 63 characters long.

**Public access level:** Specifies whether data in the container may be accessed publicly. By default, container data is private to the account owner.

- Use **Private** to ensure there is no anonymous access to the container and blobs.
  - Use **Blob** to allow anonymous public read access for blobs only.
  - Use **Container** to allow anonymous public read and list access to the entire container, including the blobs.
- ✓ You can also create the Blob container with PowerShell using the **New-AzStorageContainer** command.
- ✓ Have you thought about how you will organize your containers?

## Blob Access Tiers

Azure Storage provides different options for accessing block blob data (as shown in the screenshot), based on usage patterns. Each access tier in Azure Storage is optimized for a particular pattern of data usage. By selecting the correct access tier for your needs, you can store your block blob data in the most cost-effective manner.

### Access Tier

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



- **Hot.** The Hot tier is optimized for frequent access of objects in the storage account. Accessing data in the Hot tier is most cost-effective, while storage costs are somewhat higher. New storage accounts are created in the Hot tier by default.
- **Cool.** The Cool tier is optimized for storing large amounts of data that is infrequently accessed and stored for at least 30 days. Storing data in the Cool tier is more cost-effective, but accessing that data may be somewhat more expensive than accessing data in the Hot tier.

- **Archive.** The Archive tier is optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days. The Archive tier is the most cost-effective option for storing data, but accessing that data is more expensive than accessing data in the Hot or Cool tiers.
- ✓ If there is a change in the usage pattern of your data, you can switch between these access tiers at any time.

## Blob Lifecycle Management

Rule name \*

rule01

**Blobs**

- Move blob to cool storage
 

Days after last modification  
30
- Move blob to archive storage
 

Days after last modification  
180
- Delete blob
 

Days after last modification  
365

**Snapshots**

- Delete snapshot
 

Days after blob is created  
30

Data sets have unique lifecycles. Early in the lifecycle, people access some data often. But the need for access drops drastically as the data ages. Some data stays idle in the cloud and is rarely accessed once stored. Some data expires days or months after creation, while other data sets are actively read and modified throughout their lifetimes. Azure Blob storage lifecycle management offers a rich, rule-based policy for GPv2 and Blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle.

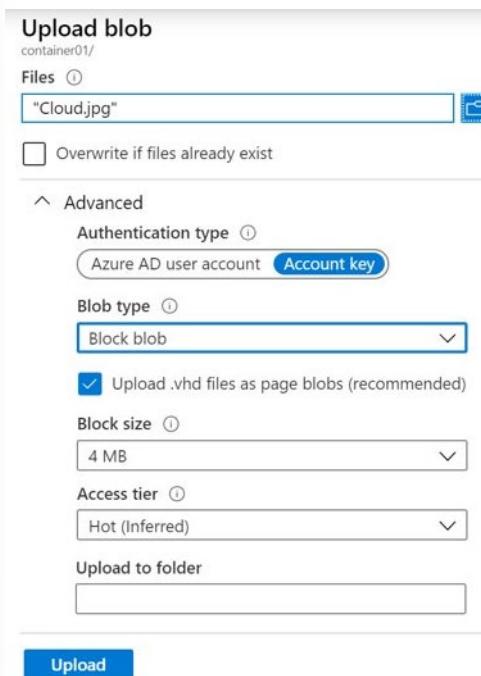
The lifecycle management policy lets you:

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

Consider a scenario where data gets frequent access during the early stages of the lifecycle, but only occasionally after two weeks. Beyond the first month, the data set is rarely accessed. In this scenario, hot storage is best during the early stages. Cool storage is most appropriate for occasional access. Archive storage is the best tier option after the data ages over a month. By adjusting storage tiers in respect to the age of data, you can design the least expensive storage options for your needs. To achieve this transition, lifecycle management policy rules are available to move aging data to cooler tiers.

## Uploading Blobs

A blob can be any type and size file. Azure Storage offers three types of blobs: *block* blobs, *page* blobs, and *append* blobs. You specify the blob type and access tier when you create the blob.



- **Block blobs (default)** consist of blocks of data assembled to make a blob. Most scenarios using Blob storage employ block blobs. Block blobs are ideal for storing text and binary data in the cloud, like files, images, and videos.
- **Append blobs** are like block blobs in that they are made up of blocks, but they are optimized for append operations, so they are useful for logging scenarios.
- **Page blobs** can be up to 8 TB in size and are more efficient for frequent read/write operations. Azure virtual machines use page blobs as OS and data disks.

✓ Once the blob has been created, its type cannot be changed.

## Blob upload tools

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

- **AzCopy** is an easy-to-use command-line tool for Windows and Linux that copies data to and from Blob storage, across containers, or across storage accounts.
- The **Azure Storage Data Movement library** is a .NET library for moving data between Azure Storage services. The AzCopy utility is built with the Data Movement library.
- **Azure Data Factory** supports copying data to and from Blob storage by using the account key, shared access signature, service principal, or managed identities for Azure resources authentications.
- **blobfuse** is a virtual file system driver for Azure Blob storage. You can use blobfuse to access your existing block blob data in your Storage account through the Linux file system.
- **Azure Data Box Disk** is a service for transferring on-premises data to Blob storage when large datasets or network constraints make uploading data over the wire unrealistic. You can use Azure Data

Box Disk to request solid-state disks (SSDs) from Microsoft. You can then copy your data to those disks and ship them back to Microsoft to be uploaded into Blob storage.

- The **Azure Import/Export** service provides a way to export large amounts of data from your storage account to hard drives that you provide and that Microsoft then ships back to you with your data.
- ✓ Of course, you can always use Azure Storage Explorer.

## Storage Pricing

All storage accounts use a pricing model for blob storage based on the tier of each blob. When using a storage account, the following billing considerations apply:

- **Performance tiers:** In addition to, the amount of data stored, the cost of storing data varies depending on the storage tier. The per-gigabyte cost decreases as the tier gets cooler.
- **Data access costs:** Data access charges increase as the tier gets cooler. For data in the cool and archive storage tier, you are charged a per-gigabyte data access charge for reads.
- **Transaction costs:** There is a per-transaction charge for all tiers that increases as the tier gets cooler.
- **Geo-Replication data transfer costs:** This charge only applies to accounts with geo-replication configured, including GRS and RA-GRS. Geo-replication data transfer incurs a per-gigabyte charge.
- **Outbound data transfer costs:** Outbound data transfers (data that is transferred out of an Azure region) incur billing for bandwidth usage on a per-gigabyte basis, consistent with general-purpose storage accounts.
- **Changing the storage tier:** Changing the account storage tier from cool to hot incurs a charge equal to reading all the data existing in the storage account. However, changing the account storage tier from hot to cool incurs a charge equal to writing all the data into the cool tier (GPv2 accounts only).

## Demonstration - Blob Storage

In this demonstration, you will explore blob storage.

**Note:** This demonstration requires a storage account.

### Create a container

1. Navigate to a storage account in the Azure portal.
2. In the left menu for the storage account, scroll to the **Blob service** section, then select **Blobs**.
3. Select the **+ Container** button.
4. Type a **Name** for your new container. The container name must be lowercase, must start with a letter or number, and can include only letters, numbers, and the dash (-) character.
5. Set the level of public access to the container. The default level is Private (no anonymous access).
6. Select **OK** to create the container.

### Upload a block blob

1. In the Azure portal, navigate to the container you created in the previous section.
2. Select the container to show a list of blobs it contains. Since this container is new, it won't yet contain any blobs.
3. Select the **Upload** button to upload a blob to the container.
4. Expand the **Advanced** section.

5. Notice the **Authentication type**, **Blob type**, **Block size**, and the ability to **Upload to a folder**.
6. Notice the default **Authentication type** type is SAS.
7. Browse your local file system to find a file to upload as a block blob, and select **Upload**.
8. Upload as many blobs as you like in this way. You'll observe that the new blobs are now listed within the container.

#### **Download a block blob**

You can download a block blob to display in the browser or save to your local file system.

1. Navigate to the list of blobs that you uploaded in the previous section.
2. Right-click the blob you want to download, and select **Download**.

# Storage Security

## Storage Security

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

- **Encryption.** All data written to Azure Storage is automatically encrypted using Storage Service Encryption (SSE).
- **Authentication.** Azure Active Directory (Azure AD) and Role-Based Access Control (RBAC) are supported for Azure Storage for both resource management operations and data operations, as follows:
  - You can assign RBAC roles scoped to the storage account to security principals and use Azure AD to authorize resource management operations such as key management.
  - Azure AD integration is supported for data operations on the Blob and Queue services.
- **Data in transit.** Data can be secured in transit between an application and Azure by using Client-Side Encryption, HTTPS, or SMB 3.0.
- **Disk encryption.** OS and data disks used by Azure virtual machines can be encrypted using Azure Disk Encryption.
- **Shared Access Signatures.** Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures.

## Authorization options

Every request made against a secured resource in the Blob, File, Queue, or Table service must be authorized. Authorization ensures that resources in your storage account are accessible only when you want them to be, and only to those users or applications to whom you grant access. Options for authorizing requests to Azure Storage include:

- **Azure Active Directory (Azure AD).** Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you can assign fine-grained access to users, groups, or applications via role-based access control (RBAC).
- **Shared Key.** Shared Key authorization relies on your account access keys and other parameters to produce an encrypted signature string that is passed on the request in the Authorization header.
- **Shared access signatures.** Shared access signatures (SAS) delegate access to a particular resource in your account with specified permissions and over a specified time interval.
- **Anonymous access to containers and blobs.** You can optionally make blob resources public at the container or blob level. A public container or blob is accessible to any user for anonymous read access. Read requests to public containers and blobs do not require authorization.

## Storage Account Keys

As mentioned above, Azure Storage accounts can create authorized apps in Active Directory to control access to the data in blobs and queues. This authentication approach is the best solution if the app is using Blob or Queue storage.

For other storage models, clients can use a different approach: a *shared key* or shared secret. This authentication option supports blobs, files, queues, and tables. It's one of the more straightforward approaches

to use: the client embeds the shared key in the `HTTP Authorization` header of every request, and the Storage account validates it.

As an example, an application could issue a `GET` request against a blob resource:

```
GET http://myaccount.blob.core.windows.net/?restype=service&comp=stats
```

The following HTTP headers that control the version of the REST API, the date, and the encoded shared key.

```
x-ms-version: 2018-03-28  
Date: Wed, 23 Oct 2018 21:00:44 GMT  
Authorization: SharedKey myaccount:CY1OP3O3jGFpYFbTCBimLn0Xov0vt0khH/  
E5Gy0fXvg=
```

## Account Keys

Shared keys in Azure Storage accounts are called "Storage Account Access Keys". Azure creates two of these keys (primary and secondary) for each storage account you create and they give access to *everything* in the account. You can view the created storage keys in the Azure portal view of the storage account under **Settings > Access keys** as shown below.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a 'FAVORITES' section with links like Marketplace, Resource groups, All resources, Recent, App Services, Virtual machines, SQL databases, Security Center, Subscriptions, Media services, Azure Active Directory, Monitor, Cost Management + Bill..., and Help + support. The main content area shows the 'Storage accounts' blade for a storage account named 'cs75270e7ced3cex4172xb09'. The 'Access keys' tab is selected. It displays two sets of keys: 'key1' and 'key2'. Each key has a 'Key' field containing a long hex-encoded string and a 'Connection string' field with a URL template. A note at the top right says: 'Use 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.' Below the keys, there are tabs for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Storage Explorer (preview), and Properties.

## Protecting shared keys

Because there are only two keys, and they provide full access to the account, it's recommended to only use these keys with *trusted in-house applications* that you have complete control over. If the keys are compromised, you can change the key values in the Azure portal. There are several other reasons to regenerate your storage account keys.

- You might regenerate them on a regular basis for security reasons.

- You must regenerate your storage account keys if someone managed to hack into an application and retrieve the key that was hardcoded or saved in a configuration file, giving them full access to your storage account.
- Another case for key regeneration is if your team is using a Storage Explorer application that retains the storage account key, and one of the team members leaves. The application would continue to work, giving them access to your storage account after they're gone.

The process to refresh keys is simple:

1. Change each trusted app to use the *secondary* key.
2. Refresh the primary key in the Azure portal. You can consider it the new "secondary" key value.

**✓ IMPORTANT**

Any client attempting to use the old key value will be refused. You must make sure to identify all clients using the shared key and update them to keep them operational.

## Shared Access Signatures

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources (a specific blob in this case). You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time. SAS is a secure way to share your storage resources without compromising your account keys.

\* Permissions ⓘ

Read

Start and expiry date/time ⓘ

Start Expiry

2019-02-27 7:32:03 AM 2019-02-27 3:32:03 PM

(UTC-08:00) --- Current Time Zone --- (UTC-08:00) --- Current Time Zone ---

Allowed IP addresses ⓘ

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

HTTPS  HTTP

Signing key ⓘ

Key 1

Generate blob SAS token and URL

A SAS gives you granular control over the type of access you grant to clients who have the SAS, including:

- An account-level SAS can delegate access to multiple storage services. For example, blob, file, queue, and table.
- An interval over which the SAS is valid, including the start time and the expiry time.

- The permissions granted by the SAS. For example, a SAS for a blob might grant read and write permissions to that blob, but not delete permissions.

Optionally, you can also:

- Specify an IP address or range of IP addresses from which Azure Storage will accept the SAS. For example, you might specify a range of IP addresses belonging to your organization.
  - The protocol over which Azure Storage will accept the SAS. You can use this optional parameter to restrict access to clients using HTTPS.
- ✓ There are two types of SAS: **account** and **service**. The account SAS delegates access to resources in one or more of the storage services. The service SAS delegates access to a resource in just one of the storage services.
- ✓ A stored access policy can provide an additional level of control over service-level SAS on the server side. You can group shared access signatures and provide additional restrictions for signatures that are bound by the policy.

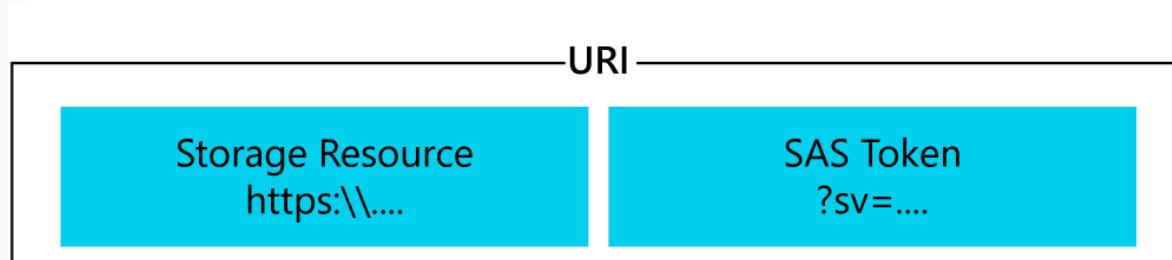
For more information:

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

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

## URI and SAS Parameters

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



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

```
https://myaccount.blob.core.windows.net/?restype=service&comp=proper-
ties&sv=2015-04-05&ss=bf&srt=s&st=2015-04-29T22%3A18%3A26Z&se=2015-04-
30T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.5.60-168.1.5.70&spr=https
&sig=F%6GRVAZ5Cdj2Pw4txxxxx
```

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

Name	SAS portion	Description
Resource URI	https://myaccount.blob.core.windows.net/?restype=service&comp=properties	The Blob service endpoint, with parameters for getting service properties (when called with GET) or setting service properties (when called with SET).
Storage services version	sv=2015-04-05	For storage services version 2012-02-12 and later, this parameter indicates the version to use.
Services	ss=bf	The SAS applies to the Blob and File services
Resource types	srt=s	The SAS applies to service-level operations.
Start time	st=2015-04-29T22%3A18%3A26Z	Specified in UTC time. If you want the SAS to be valid immediately, omit the start time.
Expiry time	se=2015-04-30T02%3A23%3A26Z	Specified in UTC time.
Resource	sr=b	The resource is a blob.
Permissions	sp=rw	The permissions grant access to read and write operations.
IP Range	sip=168.1.5.60-168.1.5.70	The range of IP addresses from which a request will be accepted.
Protocol	spr=https	Only requests using HTTPS are permitted.
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<sup>3</sup>](#).

## 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.

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

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.

The screenshot shows the 'Encryption' blade in the Azure Storage account settings. It includes sections for 'Save' and 'Discard' changes, a description of SSE protection, a note about default encryption using Microsoft Managed Keys, a note about retroactive encryption, and a link to 'Learn More about Azure Storage Encryption'. At the bottom, there is a 'Encryption type' section with radio buttons for 'Microsoft Managed Keys' (selected) and 'Customer Managed Keys'.

- ✓ SSE is enabled for all new and existing storage accounts and cannot be disabled. Because your data is secured by default, you don't need to modify your code or applications.

## Customer Managed keys

If you prefer, you can use the Azure Key Vault to manage your encryption keys. With the Key Vault you can create your own encryption keys and store them in a key vault, or you can use Azure Key Vault's APIs to generate encryption keys.

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

Encryption type

Microsoft Managed Keys

Customer Managed Keys

The storage account named 'storage987123' will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more about customer managed keys](#)

Encryption key

Enter key URI

Select from Key vault

Key vault and key \*

Key vault: keyvault987123  
Key: storagekey  
[Select a key vault and key](#)

- ✓ To use customer-managed keys with SSE, you can either create a new key vault and key or you can use an existing key vault and key. The storage account and the key vault must be in the same region, but they can be in different subscriptions.

## Storage Security Best Practices

### Risks

When you use shared access signatures in your applications, you should be aware of two potential risks.

- If a SAS is compromised, it can be used by anyone who obtains it.
- If a SAS provided to a client application expires and the application is unable to retrieve a new SAS from your service, then the application's functionality may be hindered.

### Recommendations

The following recommendations for using shared access signatures can help mitigate risks.

- **Always use HTTPS to create or distribute a SAS.** If a SAS is passed over HTTP and intercepted, an attacker performing a man-in-the-middle attack is able to read the SAS and then use it just as the intended user could have, potentially compromising sensitive data or allowing for data corruption by the malicious user.
- **Reference stored access policies where possible.** Stored access policies give you the option to revoke permissions without having to regenerate the storage account keys. Set the expiration on these very far in the future (or infinite) and make sure it's regularly updated to move it farther into the future.

- **Use near-term expiration times on an ad hoc SAS.** In this way, even if a SAS is compromised, it's valid only for a short time. This practice is especially important if you cannot reference a stored access policy. Near-term expiration times also limit the amount of data that can be written to a blob by limiting the time available to upload to it.
- **Have clients automatically renew the SAS if necessary.** Clients should renew the SAS well before the expiration, in order to allow time for retries if the service providing the SAS is unavailable. If your SAS is meant to be used for a small number of immediate, short-lived operations that are expected to be completed within the expiration period, then this may be unnecessary as the SAS is not expected to be renewed. However, if you have a client that is routinely making requests via SAS, then the possibility of expiration comes into play. The key consideration is to balance the need for the SAS to be short-lived (as previously stated) with the need to ensure that the client is requesting renewal early enough (to avoid disruption due to the SAS expiring prior to successful renewal).
- **Be careful with SAS start time.** If you set the start time for a SAS to now, then due to clock skew (differences in current time according to different machines), failures may be observed intermittently for the first few minutes. In general, set the start time to be at least 15 minutes in the past. Or, don't set it at all, which will make it valid immediately in all cases. The same generally applies to expiry time as well - remember that you may observe up to 15 minutes of clock skew in either direction on any request. For clients using a REST version prior to 2012-02-12, the maximum duration for a SAS that does not reference a stored access policy is 1 hour, and any policies specifying longer term than that will fail.
- **Be specific with the resource to be accessed.** A security best practice is to provide a user with the minimum required privileges. If a user only needs read access to a single entity, then grant them read access to that single entity, and not read/write/delete access to all entities. This also helps lessen the damage if a SAS is compromised because the SAS has less power in the hands of an attacker
- **Understand that your account will be billed for any usage, including that done with SAS.** If you provide write access to a blob, a user may choose to upload a 200GB blob. If you've given them read access as well, they may choose to download it 10 times, incurring 2 TB in egress costs for you. Again, provide limited permissions to help mitigate the potential actions of malicious users. Use short-lived SAS to reduce this threat (but be mindful of clock skew on the end time).
- **Validate data written using SAS.** When a client application writes data to your storage account, keep in mind that there can be problems with that data. If your application requires that data be validated or authorized before it is ready to use, you should perform this validation after the data is written and before it is used by your application. This practice also protects against corrupt or malicious data being written to your account, either by a user who properly acquired the SAS, or by a user exploiting a leaked SAS.
- **Don't assume SAS is always the correct choice.** Sometimes the risks associated with a particular operation against your storage account outweigh the benefits of SAS. For such operations, create a middle-tier service that writes to your storage account after performing business rule validation, authentication, and auditing. Also, sometimes it's simpler to manage access in other ways. For example, if you want to make all blobs in a container publicly readable, you can make the container Public, rather than providing a SAS to every client for access.
- **Use Storage Analytics to monitor your application.** You can use logging and metrics to observe any spike in authentication failures due to an outage in your SAS provider service or to the inadvertent removal of a stored access policy.

## Accessing Blobs and Queues using AAD

### Authorize access to Blobs and Queues using AAD

Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to Blob and Queue storage. With Azure AD, you can use role-based access control (RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against Blob or Queue storage.

Authorizing requests against Azure Storage with Azure AD provides superior security and ease of use over Shared Key authorization. Microsoft recommends using Azure AD authorization with your blob and queue applications when possible to minimize potential security vulnerabilities inherent in Shared Key.

Authorization with Azure AD is available for all general-purpose and Blob storage accounts in all public regions and national clouds. Only storage accounts created with the Azure Resource Manager deployment model support Azure AD authorization.

Authorization with Azure AD is not supported for Azure Table storage. Use Shared Key to authorize requests to Table storage.

### Overview of Azure AD for Blobs and Queues

When a security principal (a user, group, or application) attempts to access a blob or queue resource, the request must be authorized, unless it is a blob available for anonymous access. With Azure AD, access to a resource is a two-step process. First, the security principal's identity is authenticated and an OAuth 2.0 token is returned. Next, the token is passed as part of a request to the Blob or Queue service and used by the service to authorize access to the specified resource.

The authentication step requires that an application request an OAuth 2.0 access token at runtime. If an application is running from within an Azure entity such as an Azure VM, a virtual machine scale set, or an Azure Functions app, it can use a managed identity to access blobs or queues..

The authorization step requires that one or more RBAC roles be assigned to the security principal. Azure Storage provides RBAC roles that encompass common sets of permissions for blob and queue data. The roles that are assigned to a security principal determine the permissions that the principal will have.

Native applications and web applications that make requests to the Azure Blob or Queue service can also authorize access with Azure AD.

### Assign RBAC roles for Access

Azure Active Directory (Azure AD) authorizes access rights to secured resources through role-based access control (RBAC). Azure Storage defines a set of built-in RBAC roles that encompass common sets of permissions used to access blob and queue data. You can also define custom roles for access to blob and queue data.

When an RBAC role is assigned to an Azure AD security principal, Azure grants access to those resources for that security principal. Access can be scoped to the level of the subscription, the resource group, the storage account, or an individual container or queue. An Azure AD security principal may be a user, a group, an application service principal, or a managed identity for Azure resources.

#### Built-in RBAC roles for blobs and queues

Azure provides the following built-in RBAC roles for authorizing access to blob and queue data using Azure AD and OAuth:

- **Storage Blob Data Owner<sup>4</sup>**: Use to set ownership and manage POSIX access control for Azure Data Lake Storage Gen2. For more information, see [Access control in Azure Data Lake Storage Gen2<sup>5</sup>](#).
- **Storage Blob Data Contributor<sup>6</sup>**: Use to grant read/write/delete permissions to Blob storage resources.
- **Storage Blob Data Reader<sup>7</sup>**: Use to grant read-only permissions to Blob storage resources.
- **Storage Queue Data Contributor<sup>8</sup>**: Use to grant read/write/delete permissions to Azure queues.
- **Storage Queue Data Reader<sup>9</sup>**: Use to grant read-only permissions to Azure queues.
- **Storage Queue Data Message Processor<sup>10</sup>**: Use to grant peek, retrieve, and delete permissions to messages in Azure Storage queues.
- **Storage Queue Data Message Sender<sup>11</sup>**: Use to grant add permissions to messages in Azure Storage queues.

## Resource Scope

Before you assign an RBAC role to a security principal, determine the scope of access that the security principal should have. Best practices dictate that it's always best to grant only the narrowest possible scope.

The following list describes the levels at which you can scope access to Azure blob and queue resources, starting with the narrowest scope:

- **An individual container** At this scope, a role assignment applies to all of the blobs in the container, as well as container properties and metadata.
- **An individual queue** At this scope, a role assignment applies to messages in the queue, as well as queue properties and metadata.
- **The storage account** At this scope, a role assignment applies to all containers and their blobs, or to all queues and their messages.
- **The resource group** At this scope, a role assignment applies to all of the containers or queues in all of the storage accounts in the resource group.
- **The subscription** At this scope, a role assignment applies to all of the containers or queues in all of the storage accounts in all of the resource groups in the subscription.

## Access Data with an Azure AD Account

Access to blob or queue data via the Azure portal, PowerShell, or Azure CLI can be authorized either by using the user's Azure AD account or by using the account access keys (Shared Key authorization).

### Data access from the Azure portal

---

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<sup>5</sup> <https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-access-control>

<sup>6</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<sup>7</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<sup>8</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<sup>9</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<sup>10</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<sup>11</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

The Azure portal can use either your Azure AD account or the account access keys to access blob and queue data in an Azure storage account. Which authorization scheme the Azure portal uses depends on the RBAC roles that are assigned to you.

When you attempt to access blob or queue data, the Azure portal first checks whether you have been assigned an RBAC role with **Microsoft.Storage/storageAccounts/listkeys/action**. If you have been assigned a role with this action, then the Azure portal uses the account key for accessing blob and queue data via Shared Key authorization. If you have not been assigned a role with this action, then the Azure portal attempts to access data using your Azure AD account.

To access blob or queue data from the Azure portal using your Azure AD account, you need permissions to access blob and queue data, and you also need permissions to navigate through the storage account resources in the Azure portal. The built-in roles provided by Azure Storage grant access to blob and queue resources, but they don't grant permissions to storage account resources.

Access to the portal also requires the assignment of an Azure Resource Manager role such as the **Reader<sup>12</sup>** role, scoped to the level of the storage account or higher. The **Reader** role grants the most restricted permissions, but another Azure Resource Manager role that grants access to storage account management resources is also acceptable.

<sup>12</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

# Configure Azure Storage Firewalls and Virtual Networks

## Azure Storage Firewalls and Virtual Networks

Azure Storage provides a layered security model. This model enables you to secure and control the level of access to your storage accounts that your applications and enterprise environments demand, based on the type and subset of networks used. When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).

Storage accounts have a public endpoint that is accessible through the internet. You can also create Private Endpoints for your storage account, which assigns a private IP address from your VNet to the storage account, and secures all traffic between your VNet and the storage account over a private link. The Azure storage firewall provides access control access for the public endpoint of your storage account. You can also use the firewall to block all access through the public endpoint when using private endpoints. Your storage firewall configuration also enables select trusted Azure platform services to access the storage account securely.

An application that accesses a storage account when network rules are in effect still requires proper authorization for the request. Authorization is supported with Azure Active Directory (Azure AD) credentials for blobs and queues, with a valid account access key, or with an SAS token.

### Scenarios

- To secure your storage account, you should first configure a rule to deny access to traffic from all networks (including internet traffic) on the public endpoint, by default. Then, you should configure rules that grant access to traffic from specific VNets. You can also configure rules to grant access to traffic from select public internet IP address ranges, enabling connections from specific internet or on-premises clients. This configuration enables you to build a secure network boundary for your applications.
- You can combine firewall rules that allow access from specific virtual networks and from public IP address ranges on the same storage account. Storage firewall rules can be applied to existing storage accounts, or when creating new storage accounts.
- Storage firewall rules apply to the public endpoint of a storage account. You don't need any firewall access rules to allow traffic for private endpoints of a storage account. The process of approving the creation of a private endpoint grants implicit access to traffic from the subnet that hosts the private endpoint.
- Network rules are enforced on all network protocols to Azure storage, including REST and SMB. To access data using tools such as the Azure portal, Storage Explorer, and AZCopy, explicit network rules must be configured.
- Once network rules are applied, they're enforced for all requests. SAS tokens that grant access to a specific IP address serve to limit the access of the token holder, but don't grant new access beyond configured network rules.
- Virtual machine disk traffic (including mount and unmount operations, and disk IO) is not affected by network rules. REST access to page blobs is protected by network rules.
- Classic storage accounts do not support firewalls and virtual networks.

# Change the Default Network Access Rule

By default, storage accounts accept connections from clients on any network. To limit access to selected networks, you must first change the default action.

**Warning:** Making changes to network rules can impact your applications' ability to connect to Azure Storage. Setting the default network rule to deny blocks all access to the data unless specific network rules that grant access are also applied. Be sure to grant access to any allowed networks using network rules before you change the default rule to deny access.

## Managing default network access rules

As seen below, you can manage default network access rules for storage accounts through the Azure portal or CLIV2.

### Using the Azure portal

1. Go to the storage account you want to secure.
2. Click on the settings menu called **Firewalls and virtual networks**.
3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.
4. Click Save to apply your changes.

### Using CLIV2

1. Install the **Azure CLI**<sup>13</sup> and **sign in**<sup>14</sup>.

2. Display the status of the default rule for the storage account.

```
az storage account show --resource-group "myresourcegroup" --name "mystorageaccount" --query networkRuleSet.defaultAction
```

3. Set the default rule to deny network access by default.

```
az storage account update --resource-group "myresourcegroup" --name "mystorageaccount" --default-action Deny
```

4. Set the default rule to allow network access by default.

```
az storage account update --resource-group "myresourcegroup" --name "mystorageaccount" --default-action Allow  
Grant access from a virtual network
```

# Grant Access from a Virtual Network

You can configure storage accounts to allow access only from specific subnets. The allowed subnets may belong to a VNet in the same subscription, or those in a different subscription, including subscriptions belonging to a different Azure Active Directory tenant.

Enable a Service endpoint for Azure Storage within the VNet. The service endpoint routes traffic from the VNet through an optimal path to the Azure Storage service. The identities of the subnet and the virtual network are also transmitted with each request. Administrators can then configure network rules for the

<sup>13</sup> <https://docs.microsoft.com/en-us/cli/azure/install-azure-cli>

<sup>14</sup> <https://docs.microsoft.com/en-us/cli/azure/authenticate-azure-cli>

storage account that allow requests to be received from specific subnets in a VNet. Clients granted access via these network rules must continue to meet the authorization requirements of the storage account to access the data.

### Available virtual network regions

In general, service endpoints work between virtual networks and service instances in the same Azure region. When using service endpoints with Azure Storage, this scope grows to include the paired region. Service endpoints allow continuity during a regional failover and access to read-only geo-redundant storage (RA-GRS) instances. Network rules that grant access from a virtual network to a storage account also grant access to any RA-GRS instance.

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.

✓ **Note:**

Service endpoints don't apply to traffic outside the region of the virtual network and the designated region pair. You can only apply network rules granting access from virtual networks to storage accounts in the primary region of a storage account or in the designated paired region.

### Required permissions

To apply a virtual network rule to a storage account, the user must have the appropriate permissions for the subnets being added. The permission needed is Join Service to a Subnet and is included in the Storage Account Contributor built-in role. It can also be added to custom role definitions.

Storage account and the virtual networks granted access may be in different subscriptions, including subscriptions that are a part of a different Azure AD tenant.

✓ **Note:**

Configuration of rules that grant access to subnets in virtual networks that are a part of a different Azure Active Directory tenant are currently only supported through Powershell, CLI and REST APIs. Such rules cannot be configured through the Azure portal, though they may be viewed in the portal.

### Managing virtual network rules

You can manage virtual network rules for storage accounts through the Azure portal.

1. Go to the storage account you want to secure.
2. Click on the settings menu called **Firewalls and virtual networks**.
3. Check that you've selected to allow access from **Selected networks**.
4. To grant access to a virtual network with a new network rule, under **Virtual networks**, click **Add existing virtual network**, select **Virtual networks and Subnets** options, and then click **Add**. To create a new virtual network and grant it access, click **Add new virtual network**. Provide the information necessary to create the new virtual network, and then click **Create**.

✓ **Note:**

If a service endpoint for Azure Storage wasn't previously configured for the selected virtual network and subnets, you can configure it as part of this operation.

5. To remove a virtual network or subnet rule, click ... to open the context menu for the virtual network or subnet, and click **Remove**.
6. Click **Save** to apply your changes.

## Grant Access from an Internet IP Range

You can configure storage accounts to allow access from specific public internet IP address ranges. This configuration grants access to specific internet-based services and on-premises networks and blocks general internet traffic.

Provide allowed internet address ranges using **CIDR notation<sup>15</sup>** in the form 16.17.18.0/24 or as individual IP addresses like 16.17.18.19.

IP network rules are only allowed for public internet IP addresses. IP address ranges reserved for private networks (as defined in **RFC 1918<sup>16</sup>**) aren't allowed in IP rules. Private networks include addresses that start with 10., 172.16. - 172.31., and 192.168..

✓ **Note:** IP network rules have no effect on requests originating from the same Azure region as the storage account. Use **Virtual network rules<sup>17</sup>** to allow same-region requests.

✓ **Note:** Services deployed in the same region as the storage account use private Azure IP addresses for communication. Thus, you cannot restrict access to specific Azure services based on their public out-bound IP address range.

Only IPv4 addresses are supported for configuration of storage firewall rules.

Each storage account supports up to 100 IP network rules.

### Configuring access from on-premises networks

To grant access from your on-premises networks to your storage account with an IP network rule, you must identify the internet facing IP addresses used by your network. Contact your network administrator for help.

If you are using **ExpressRoute<sup>18</sup>** from your premises, for public peering or Microsoft peering, you will need to identify the NAT IP addresses that are used. For public peering, each ExpressRoute circuit by default uses two NAT IP addresses applied to Azure service traffic when the traffic enters the Microsoft Azure network backbone. For Microsoft peering, the NAT IP addresses used are either customer provided or are provided by the service provider. To allow access to your service resources, you must allow these public IP addresses in the resource IP firewall setting.

### Managing IP network rules

You can manage IP network rules for storage accounts through the Azure portal.

1. Go to the storage account you want to secure.
2. Click on the settings menu called **Firewalls and virtual networks**.
3. Check that you've selected to allow access from Selected networks.
4. To grant access to an internet IP range, enter the IP address or address range (in CIDR format) under Firewall > Address Range.
5. To remove an IP network rule, click the trash can icon next to the address range.
6. Click **Save** to apply your changes.

<sup>15</sup> <https://tools.ietf.org/html/rfc4632>

<sup>16</sup> <https://tools.ietf.org/html/rfc1918>

<sup>17</sup> [https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?WT.mc\\_id=thomasmaurer-blog-thmaure](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?WT.mc_id=thomasmaurer-blog-thmaure)

<sup>18</sup> <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

## Securing Storage Endpoints

The steps necessary to restrict network access to Azure services varies across services. For accessing a storage account, you would use the **Firewalls and virtual networks** blade to add the virtual networks that will have access. Notice you can also configure to allow access to one or more public IP ranges.

The screenshot shows the 'storage987123 | Firewalls and virtual networks' blade. On the left, there's a sidebar with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Data transfer, Events, and Storage Explorer (preview). The main area has a search bar, Save, Discard, and Refresh buttons. It shows 'Allow access from' set to 'Selected networks'. Below that, it says 'Configure network security for your storage accounts. Learn more.' Under 'Virtual networks', there's a table:

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

The 'Resource Group' column shows 'Demo' for both rows.

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

## Demonstration - Securing Storage Endpoints

In this demonstration, we will create a storage accounts, upload a file, and secure the file endpoint.

### Create a storage account in the portal

1. In the Azure portal, select **All services**. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select **Storage Accounts**.
2. On the Storage Accounts window that appears, choose **Add**.
3. Select the **subscription** in which to create the storage account.
4. Under the Resource group field, select **Create new**. Enter a name for your new resource group.
5. Enter a **name** for your storage account. The name you choose must be unique across Azure. The name also must be between 3 and 24 characters in length, and can include numbers and lowercase letters only.
6. Select a **location** for your storage account, or use the default location.
7. Leave these fields set to their default values:
  - Deployment model: **Resource Manager**
  - Performance: **Standard**
  - Account kind: **StorageV2 (general-purpose v2)**
  - Replication: **Locally redundant storage (LRS)**
  - Access tier: **Hot**
8. Select **Review + Create** to review your storage account settings and create the account.
9. Select **Create**.

10. If you have time, review the PowerShell and CLI code at the end of this demonstration.

#### Upload a file to the storage account

1. Within the Storage Account, create a **file share**, and **upload** a file.
2. For the Storage Account, use the **Shared Access Signature** blade to **Generate SAS and connection string**.
3. Use Storage Explorer and the connection string to access the file share.
4. Ensure you can view your uploaded file.

**Note:** This part of the demonstration requires a virtual network with a subnet.

#### Create a subnet service endpoint

1. Select your virtual network, and then select a subnet in the virtual network.
2. Under **Service Endpoints**, view the **Services** drop-down and the different services that can be secured with an endpoint.
3. Check the **Microsoft.Storage** option.
4. **Save** your changes.

#### Secure the storage to the service endpoint

1. Return to your **storage account**.
2. Select **Firewalls and virtual networks**.
3. Change to **Selected networks**.
4. Add existing virtual network, verify your subnet with the new service endpoint is listed.
5. **Save** your changes.

#### Test the storage endpoint

1. Return to the Storage Explorer.
2. **Refresh** the storage account.
3. You should now have an access error similar to this one:

```
This request is not authorized to perform this operation. RequestId:ae899621-e01a-00e8-12d5-c7876a000000 Time:2019-02-18T22:00:26.4551769Z
```

#### Create a storage account using PowerShell (optional)

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

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

#### Create a storage account using Azure CLI (optional)

Use the following code to create a storage account using Azure CLI. Change the storage types and names to suit your requirements.

```
az group create --name storage-resource-group --location westus  
az account list-locations --query "[].{Region:name}" --out table  
az storage account create --name storagedemo --resource-group storage-re-  
source-group --location westus --sku Standard_LRS --kind StorageV2
```

**Note:** If you plan to use the storage account in other scenarios be sure to return the account to **All networks** in the **Firewalls and virtual networks** blade.

# Managing Storage

## Import and Export Service

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files. With the Azure Import/Export service, you supply your own disk drives and transfer data yourself.

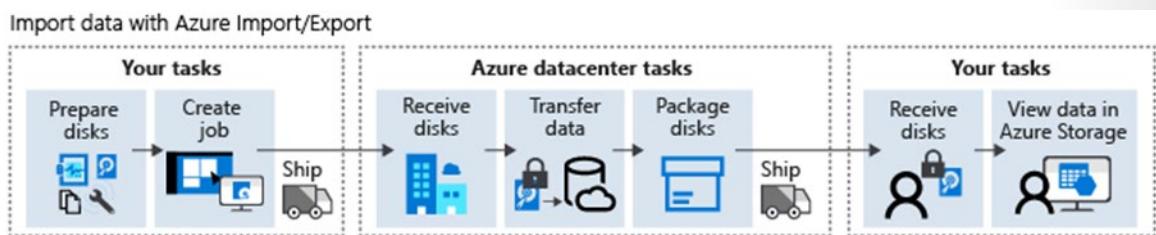
### Usage Cases

Consider using Azure Import/Export service when uploading or downloading data over the network is too slow or getting additional network bandwidth is cost-prohibitive. Scenarios where this would be useful include:

- **Migrating data to the cloud.** Move large amounts of data to Azure quickly and cost effectively.
- **Content distribution.** Quickly send data to your customer sites.
- **Backup.** Take backups of your on-premises data to store in Azure blob storage.
- **Data recovery.** Recover large amount of data stored in blob storage and have it delivered to your on-premises location.

### Import Jobs

An Import job securely transfers large amounts of data to Azure Blob storage (block and page blobs) and Azure Files by shipping disk drives to an Azure datacenter. In this case, you will be shipping hard drives containing your data.



In order to perform an import, follow these steps:

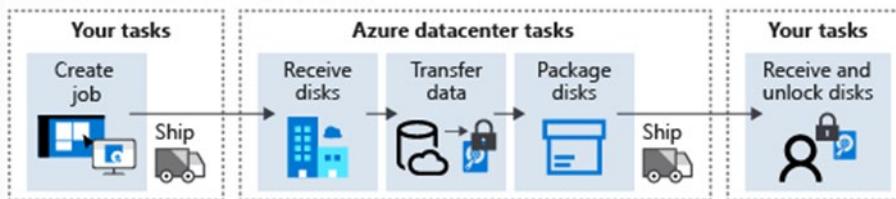
- Create an Azure Storage account.
- Identify the number of disks that you will need to accommodate all the data that you want to transfer.
- Identify a computer that you will use to perform the data copy, attach physical disks that you will ship to the target Azure datacenter, and install the WAIimportExport tool.
- Run the WAIimportExport tool to copy the data, encrypt the drive with BitLocker, and generate journal files.
- Use the Azure portal to create an import job referencing the Azure Storage account. As part of the job definition, specify the destination address representing the Azure region where the Azure Storage account resides.

- Ship the disks to the destination that you specified when creating the import job and update the job by providing the shipment tracking number.
- Once the disks arrive at the destination, the Azure datacenter staff will carry out data copy to the target Azure Storage account and ship the disks back to you.

## Export Jobs

Export jobs transfer data from Azure storage to hard disk drives and ship to your on-premise sites.

Export data with Azure Import/Export



In order to perform an export, follow these steps:

- Identify the data in the Azure Storage blobs that you intend to export.
- Identify the number of disks that you will need to accommodate all the data you want to transfer.
- Use the Azure portal to create an export job referencing the Azure Storage account. As part of the job definition, specify the blobs you want to export, the return address, and your carrier account number. Microsoft will ship your disks back to you after the export process is complete.
- Ship the required number of disks to the Azure region hosting the storage account. Update the job by providing the shipment tracking number.
- Once the disks arrive at the destination, Azure datacenter staff will carry out data copy from the storage account to the disks that you provided, encrypt the volumes on the disks by using BitLocker, and ship them back to you. The BitLocker keys will be available in the Azure portal, allowing you to decrypt the content of the disks and copy them to your on-premises storage.

## Import/Export Tool (WAImportExport)

The **Azure Import/Export Tool** is the drive preparation and repair tool that you can use with the Microsoft Azure Import/Export service. You can use the tool for the following functions:

- Before creating an import job, you can use this tool to copy data to the hard drives you are going to ship to an Azure datacenter.
- After an import job has completed, you can use this tool to repair any blobs that were corrupted, were missing, or conflicted with other blobs.
- After you receive the drives from a completed export job, you can use this tool to repair any files that were corrupted or missing on the drives.

Import/Export service requires the use of internal SATA II/III HDDs or SSDs. Each disk contains a single NTFS volume that you encrypt with BitLocker when preparing the drive. To prepare a drive, you must connect it to a computer running a 64-bit version of the Windows client or server operating system and run the 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.

- ✓ You can create jobs directly from the Azure portal or you can accomplish this programmatically by using Azure Storage Import/Export REST API.

For more information, [Azure Import and Export Service<sup>19</sup>](#).

## AzCopy

An alternative method for transferring data is **AzCopy**. AzCopy v10 is the next-generation command-line utility for copying data to/from Microsoft Azure Blob and File storage, which offers a redesigned command-line interface and new architecture for high-performance reliable data transfers. Using AzCopy, you can copy data between a file system and a storage account, or between storage accounts.

### New features

Synchronize a file system to Azure Blob or vice versa. Ideal for incremental copy scenarios.

- Supports Azure Data Lake Storage Gen2 APIs.
- Supports copying an entire account (Blob service only) to another account.
- Account to account copy is now using the new Put from URL APIs. No data transfer to the client is needed which makes the transfer faster.
- List/Remove files and blobs in a given path.
- Supports wildcard patterns in a path 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:

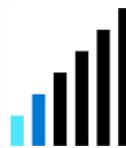
```
AzCopy /Source:<source> /Dest:<destination> [Options]
```

- ✓ AzCopy is available on Windows, Linux, and MacOS.

<sup>19</sup> <https://azure.microsoft.com/en-us/documentation/articles/storage-import-export-service/>

For more information, [Get started with AZCopy<sup>20</sup>](#).

## Data Transfer Tool Selection



Dataset	Network Bandwidth	Solution to use
<b>Large Dataset</b>	Low-bandwidth network or direct connectivity to on-premises storage is limited by organization policies	Azure Import/Export for export; Data Box Disk or Data Box for import where supported; otherwise use Azure Import/Export
<b>Large Dataset</b>	High-bandwidth network: 1 gigabit per second (Gbps) - 100 Gbps	AZCopy for online transfers; or to import data, Azure Stack Edge, or Azure Data Box Gateway
<b>Large Dataset</b>	Moderate-bandwidth network: 100 megabits per second (Mbps) - 1 Gbps	Azure Import/Export for export or Azure Stack Edge for import where supported
<b>Small Dataset:</b> a few GBs to a few TBs	Low to moderate-bandwidth network: up to 1 Gbps	If transferring only a few files, use Azure Storage Explorer, Azure portal, AZCopy, or AZ CLI

## Demonstration - AzCopy

In this demonstration, we will explore AzCopy.

### Install the AzCopy tool

1. Download your version of AZCopy - [Get started with AZCopy<sup>21</sup>](#)
2. Install and launch the tool.

### Explore the help

1. View the help.

```
azcopy /?
```

2. Scroll to the top of the Help information and read about the **Common options**, like: source, destination, source key, and destination key.
3. Scroll down the **Samples** section. We will be trying several of these examples. Are any of these examples particularly interesting to you?

### Download a blob from Blob storage to the file system

<sup>20</sup> <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy>

<sup>21</sup> <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

**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 be 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 be 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.

## Lab

# Lab - Implementing and Configuring Azure Storage File and Blob Services

✓ **Important:** To download the most recent version of this lab, please visit the AZ-303 [GitHub repository<sup>22</sup>](#).

Direct link to the [Lab: Implementing and Configuring Azure Storage File and Blob Services<sup>23</sup>](#).

### Lab scenario



Adatum Corporation hosts large amounts of unstructured and semi-structured data in its on-premises storage. Its maintenance becomes increasingly complex and costly. Some of the data is preserved for extensive amount of time to address data retention requirements. The Adatum Enterprise Architecture team is looking for inexpensive alternatives that would support tiered storage, while, at the same time allow for secure access that minimizes the possibility of data exfiltration. While the team is aware of practically unlimited capacity offered by Azure Storage, it is concerned about the usage of account keys, which grant unlimited access to the entire content of the corresponding storage accounts. While keys can be rotated in an orderly manner, such operation needs to be carried out with proper planning. In addition, access keys constitute exclusively an authorization mechanism, which limits the ability to properly audit their usage.

To address these shortcomings, the Architecture team decided to explore the use of shared access signatures. A shared access signature (SAS) provides secure delegated access to resources in a storage account while minimizing the possibility of unintended data exposure. SAS offers granular control over data access, including the ability to limit access to an individual storage object, such as a blob, restricting such access to a custom time window, as well as filtering network access to a designated IP address range. In addition, the Architecture team wants to evaluate the level of integration between Azure Storage and Azure Active Directory, hoping to address its audit requirements. The Architecture team also decided to determine suitability of Azure Files as an alternative to some of its on-premises file shares.

To accomplish these objectives, Adatum Corporation will test a range of authentication and authorization mechanisms for Azure Storage resources, including:

- Using shared access signatures on the account, container, and object-level
- Configuring access level for blobs
- Implementing Azure Active Directory based authorization
- Using storage account access keys

---

<sup>22</sup> <https://github.com/MicrosoftLearning/AZ-303-Microsoft-Azure-Architect-Technologies>

<sup>23</sup> [https://aka.ms/303\\_Module\\_06\\_Lab](https://aka.ms/303_Module_06_Lab)

## Objectives

After completing this lab, you will be able to:

- Implement authorization of Azure Storage blobs by leveraging shared access signatures
- Implement authorization of Azure Storage blobs by leveraging Azure Active Directory
- Implement authorization of Azure Storage file shares by leveraging access keys

## Lab Environment

Windows Server admin credentials

- User Name: **Student**
- Password: **Pa55w.rd1234**

Estimated Time: 60 minutes

## Lab Files (Located in the GitHub repository listed above)

- \\AZ303\AllFiles\Labs\02\azuredeploy30302suba.json
- \\AZ303\AllFiles\Labs\02\azuredeploy30302rga.json
- \\AZ303\AllFiles\Labs\02\azuredeploy30302rga.parameters.json

## Exercise 0: Prepare the lab environment

The main tasks for this exercise are as follows:

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

## Exercise 1: Configure Azure Storage account authorization by using shared access signature.

The main tasks for this exercise are as follows:

1. Create an Azure Storage account
2. Install Storage Explorer
3. Generate an account-level shared access signature
4. Create a blob container by using Azure Storage Explorer
5. Upload a file to a blob container by using AzCopy
6. Access a blob by using a blob-level shared access signature

## Exercise 2: Configure Azure Storage blob service authorization by using Azure Active Directory

The main tasks for this exercise are as follows:

1. Create an Azure AD user
2. Enable Azure Active Directory authorization for Azure Storage blob service

3. Upload a file to a blob container by using AzCopy

## Exercise 3: Implement Azure Files.

The main tasks for this exercise are as follows:

1. Create an Azure Storage file share
2. Map a drive to an Azure Storage file share from Windows
3. Remove Azure resources deployed in the lab

# Module 6 Review Questions

## Module 6 Review Questions



### Review Question 1

You are the Solution Architect for your company. Your company has an Azure subscription that contains the following resource groups.

Name: ResourceGroup\_Red

- Region: East US

Name: ResourceGroup\_Blue

- Region: West US

Also, the subscription contains the following storage accounts.

Name: Team\_Storage1

- Resource Group: ResourceGroup\_Red
- Region: West US
- Account Type: BlobStorage

Name: Team\_Storage2

- Group: ResourceGroup\_Blue
- Region: West US
- Account Type: Storage - general purpose v1

Name: Team\_Storage3

- Resource Group: ResourceGroup\_Red
- Region: East US

- Account Type: StorageV2 - general purpose v2

You advise that they create a Recovery Service vault named Vault1 in ResourceGroup\_Red in the West US location.

Diagnostics logs should be in same region as the monitored resources.

They will need to identify which storage accounts can be used to generate the diagnostic logs for Vault1.

Which storage account(s) should you identify?

- Team\_Storage1 only
- Team\_Storage2 only
- Team\_Storage3 only
- Team\_Storage1 and Team\_Storage2

## Review Question 2

You are advising a company that has an Azure subscription containing two storage accounts named TailwindStorage1 and TailwindStorage2. Both storage accounts contains a queue service, table service, and a blob service.

- You recommend they develop two separate applications named TaiwindApp\_1 and TaiwindApp\_2.
- They will need to configure the applications to store different types of data to all the storage services on TailwindStorage1 and TailwindStorage2.

How many endpoints should you recommend they configure for each of the applications?

- 2
- 3
- 6
- 12

## Review Question 3

Your organization has a SQL Server on an Azure virtual machine named OEM\_SQL\_3.

You've been asked to provide a solution to automate backup of the databases on OEM\_SQL\_3 using Automated Backup V2 for the virtual machines.

The requirements are as follows:

- Meet the RPO of 15 minutes
- Retain the backups for 30 days
- Encrypt the backups at rest

As part the solution you will be providing, what should you include?

- An Azure Storage account
- A Key Vault
- An Azure SQL Managed Instance
- An Azure Logic App

## Review Question 4

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 5

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 6

*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.

# Answers

## Review Question 1

You are the Solution Architect for your company. Your company has an Azure subscription that contains the following resource groups.

Name: ResourceGroup\_Red

Name: ResourceGroup\_Blue

Also, the subscription contains the following storage accounts.

Name: Team\_Storage1

Name: Team\_Storage2

Name: Team\_Storage3

You advise that they create a Recovery Service vault named Vault1 in ResourceGroup\_Red in the West US location.

Diagnostics logs should be in same region as the monitored resources.

They will need to identify which storage accounts can be used to generate the diagnostic logs for Vault1. Which storage account(s) should you identify?

- Team\_Storage1 only
- Team\_Storage2 only
- Team\_Storage3 only
- Team\_Storage1 and Team\_Storage2

### Explanation

*Correct Answer: Diagnostics settings can be archived to a storage account that resides in the same Azure region irrespective of the storage account type. Because Vault1 resides in West US, diagnostics settings can be set for Team\_Storage1 and Team\_Storage2 only.*

## Review Question 2

You are advising a company that has an Azure subscription containing two storage accounts named TailwindStorage1 and TailwindStorage2. Both storage accounts contains a queue service, table service, and a blob service.

How many endpoints should you recommend they configure for each of the applications?

- 2
- 3
- 6
- 12

*Explanation*

*Correct Answer: 6 endpoints each. Each storage service in storage account, queue service, table service and blob service has its own endpoint. Because each app must write to three storage services in two different accounts, each of them has different endpoint, which means that you should configure six endpoints for each app.*

**Review Question 3**

Your organization has a SQL Server on an Azure virtual machine named OEM\_SQL\_3.

You've been asked to provide a solution to automate backup of the databases on OEM\_SQL\_3 using Automated Backup V2 for the virtual machines.

The requirements are as follows:

As part the solution you will be providing, what should you include?

- An Azure Storage account
- A Key Vault
- An Azure SQL Managed Instance
- An Azure Logic App

*Explanation*

*Correct answer: An Azure Storage account. Azure Storage supports almost any type of data and provides security, redundancy, and scalable access to the stored data. A storage account provides access to objects in Azure Storage for a specific subscription. VMs always have one or more storage accounts to hold each attached virtual disk.*

**Review Question 4**

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. 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 5**

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 6**

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.*

## Module 7 Implement NoSQL Databases

### Configure Storage Account Tables

#### Azure Table Storage

Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schemaless design. Because Table storage is schemaless, it's easy to adapt your data as the needs of your application evolve. Access to Table storage data is fast and cost-effective for many types of applications and is typically lower in cost than traditional SQL for similar volumes of data.

You can use Table storage to store flexible datasets like user data for web applications, address books, device information, or other types of metadata your service requires. You can store any number of entities in a table, and a storage account may contain any number of tables, up to the capacity limit of the storage account.

#### What is Table storage

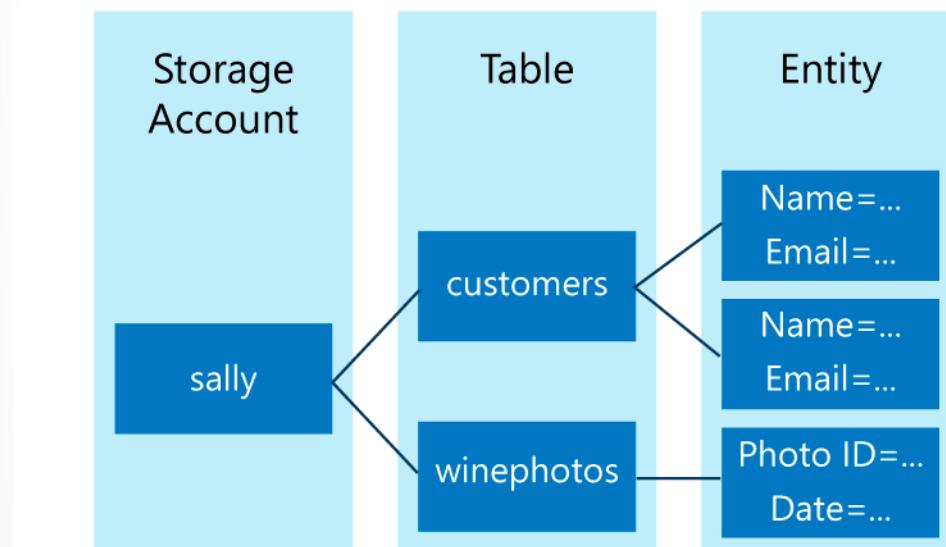
Azure Table storage stores large amounts of structured data. The service is a NoSQL datastore which accepts authenticated calls from inside and outside the Azure cloud. Azure tables are ideal for storing structured, non-relational data. Common uses of Table storage include:

- Storing TBs of structured data capable of serving web scale applications
- Storing datasets that don't require complex joins, foreign keys, or stored procedures and can be denormalized for fast access
- Quickly querying data using a clustered index
- Accessing data using the OData protocol and LINQ queries with WCF Data Service .NET Libraries

You can use Table storage to store and query huge sets of structured, non-relational data, and your tables will scale as demand increases.

#### Table storage concepts

Table storage contains the following components:



- **URL format:**
  - **Azure Table Storage accounts use this format:** `http://<storage account>.table.core.windows.net/<table>`
  - **Azure Cosmos DB Table API accounts use this format:** `http://<storage account>.table.cosmosdb.azure.com/<table>`
- **Accounts:** All access to Azure Storage is done through a storage account.
- **Table:** A table is a collection of entities. Tables don't enforce a schema on entities, which means a single table can contain entities that have different sets of properties.
- **Entity:** An entity is a set of properties, similar to a database row. An entity in Azure Storage can be up to 1MB in size. An entity in Azure Cosmos DB can be up to 2MB in size.
- **Properties:** A property is a name-value pair. Each entity can include up to 252 properties to store data. Each entity also has three system properties that specify a partition key, a row key, and a timestamp. Entities with the same partition key can be queried more quickly, and inserted/updated in atomic operations. An entity's row key is its unique identifier within a partition.

## Table Service Data Model

The Table service offers structured storage in the form of tables. The following sections outline the Table service data model.

### Storage Account

A storage account is a globally unique entity within the storage system. The storage account is the parent namespace for the Table service and is the basis for authorization. You can create any number of tables within a given storage account, if each table is uniquely named.

The storage account must always be specified in the request URI. The base URI for accessing the Table service is as follows:

`https://myaccount.table.core.windows.net`

## Tables, Entities, and Properties

Tables store data as collections of entities. Entities are similar to rows. An entity has a primary key and a set of properties. A property is a name, typed-value pair, similar to a column.

The Table service does not enforce any schema for tables, so two entities in the same table may have different sets of properties. Developers may choose to enforce a schema on the client side. A table may contain any number of entities.

## Table Names

Table names must conform to these rules:

- Table names must be unique within an account.
- Table names may contain only alphanumeric characters.
- Table names cannot begin with a numeric character.
- Table names are case-insensitive.
- Table names must be from 3 to 63 characters long.
- Some table names are reserved, including "tables". Attempting to create a table with a reserved table name returns error code 404 (Bad Request).

These rules are also described by the regular expression "`^([A-Za-z][A-Za-z0-9]{2,62}$)`".

Table names preserve the case with which they were created but are case-insensitive when used.

## Property Names

Property names are case-sensitive strings up to 255 characters in size. Property names should follow naming rules for C# identifiers.

## Property Limitations

An entity can have up to 255 properties, including 3 system properties described in the following section. Therefore, the user may include up to 252 custom properties, in addition to the 3 system properties. The combined size of all data in an entity's properties cannot exceed 1 MB.

## System Properties

An entity always has the following system properties:

- PartitionKey property
- RowKey property
- Timestamp property

These system properties are automatically included for every entity in a table. The names of these properties are reserved and cannot be changed. The developer is responsible for inserting and updating the values of PartitionKey and RowKey. The server manages the value of Timestamp, which cannot be modified.

## Characters Disallowed in Key Fields

The following characters are not allowed in values for the `PartitionKey` and `RowKey` properties:

- The forward slash (/) character
- The backslash (\) character
- The number sign (#) character
- The question mark (?) character
- Control characters from U+0000 to U+001F, including:
  - The horizontal tab (\t) character
  - The linefeed (\n) character
  - The carriage return (\r) character
- Control characters from U+007F to U+009F

## PartitionKey Property

Tables are partitioned to support load balancing across storage nodes. A table's entities are organized by partition. A partition is a consecutive range of entities possessing the same partition key value. The partition key is a unique identifier for the partition within a given table, specified by the `PartitionKey` property. The partition key forms the first part of an entity's primary key. The partition key may be a string value up to 1 KB in size.

You must include the `PartitionKey` property in every insert, update, and delete operation.

## RowKey Property

The second part of the primary key is the row key, specified by the `RowKey` property. The row key is a unique identifier for an entity within a given partition. Together the `PartitionKey` and `RowKey` uniquely identify every entity within a table.

The row key is a string value that may be up to 1 KB in size.

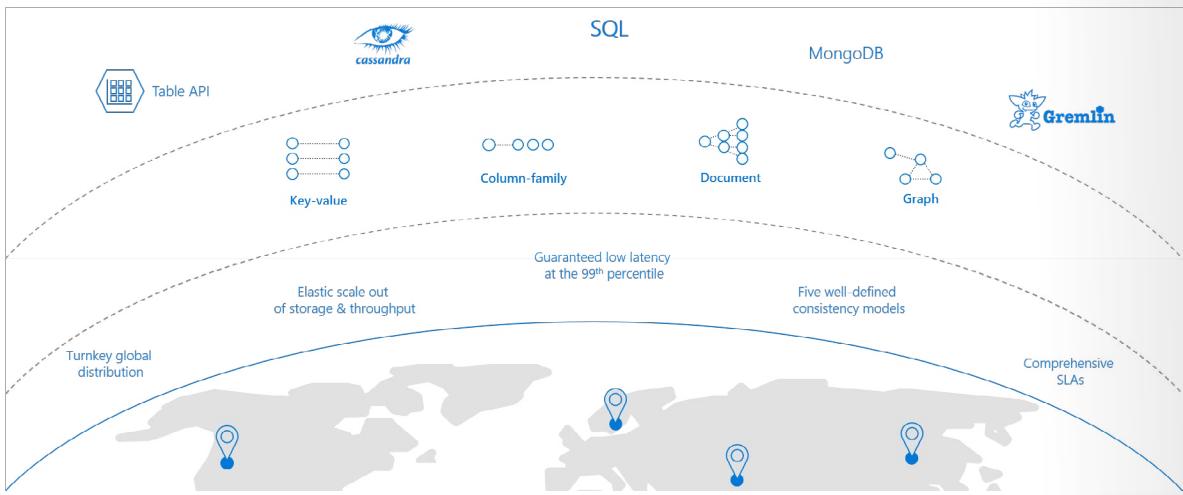
You must include the `RowKey` property in every insert, update, and delete operation.

## Timestamp Property

The `Timestamp` property is a `DateTime` value that is maintained on the server side to record the time an entity was last modified. The Table service uses the `Timestamp` property internally to provide optimistic concurrency. The value of `Timestamp` is a monotonically increasing value, meaning that each time the entity is modified, the value of `Timestamp` increases for that entity. This property should not be set on insert or update operations (the value will be ignored).

# Select Appropriate CosmosDB APIs

## Overview of Azure Cosmos DB



Azure Cosmos DB is a globally distributed and elastically scalable database. It has a guaranteed low latency that is backed by a comprehensive set of Service Level Agreements (SLAs). Consistency can sometimes be an issue when you are working with distributed systems, but Azure Cosmos DB alleviates this situation by offering you five different consistency levels: strong, bounded staleness, session, consistent prefix, and eventual.

## SQL

Core (SQL) is the default API for Azure Cosmos DB, which provides you with a view of your data that resembles a traditional NoSQL document store. You can query the hierarchical JSON documents with a SQL-like language. Core (SQL) uses JavaScript's type system, expression evaluation, and function invocation.

For a e-commerce website, you could choose to use Core (SQL) to store your product catalog.

## MongoDB

Azure Cosmos DB's API for MongoDB supports the MongoDB wire protocol. This API allows existing MongoDB client SDKs, drivers, and tools to interact with the data transparently, as if they are running against an actual MongoDB database. The data is stored in document format, which is the same as using Core (SQL).



Azure Cosmos DB's support for the Cassandra API makes it possible to query data by using the Cassandra Query Language (CQL), and your data will appear to be a partitioned row store. Just like the MongoDB API, any clients or tools should be able to connect transparently to Azure Cosmos DB; only your connection settings should need to be updated.

For developers who have experience with the CQL query language, Azure Cosmos DB provides several familiar CQL statements and clauses.



Azure Cosmos DB's Azure Table API provides support for applications that are written for Azure Table Storage that need premium capabilities like global distribution, high availability, scalable throughput. The original Table API only allows for indexing on the Partition and Row keys; there are no secondary indexes. Storing table data in Comsos DB automatically indexes all the properties and requires no index management.

Querying is accomplished by using OData and LINQ queries in code, and the original REST API for GET operations.

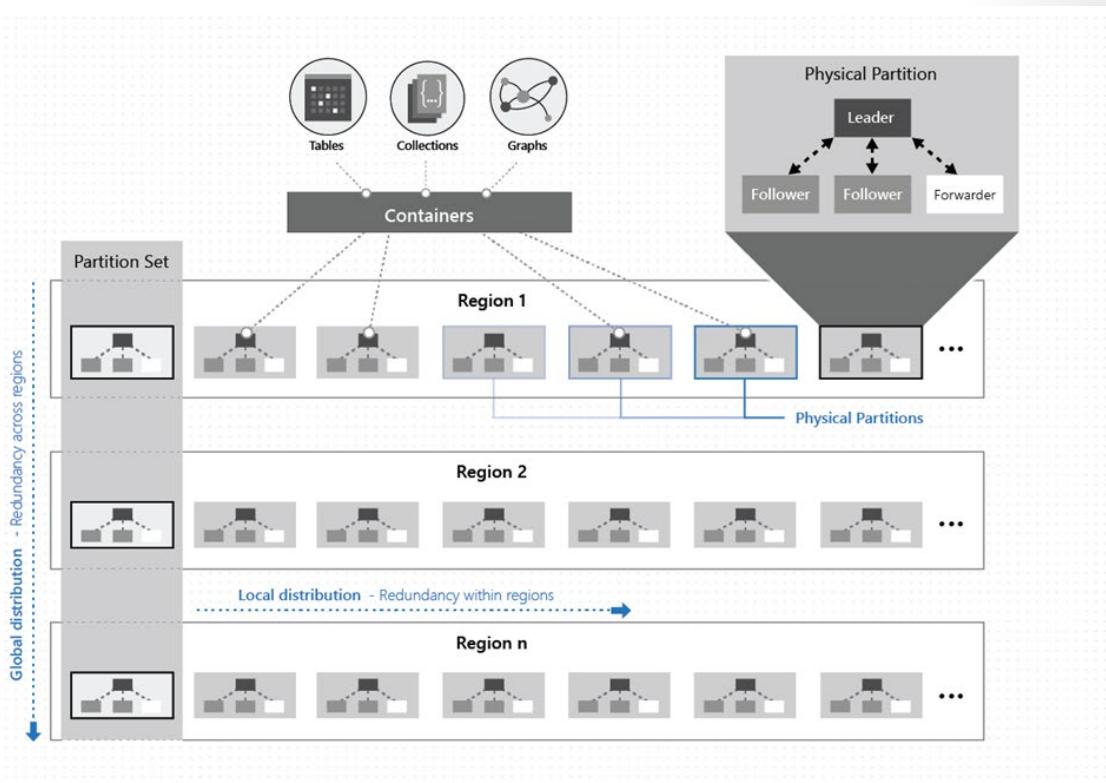


Choosing Gremlin as the API provides a graph-based view over the data. Remember that at the lowest level, all data in any Azure Cosmos DB is stored in an ARS format. A graph-based view on the database means data is either a vertex (which is an individual item in the database), or an edge (which is a relationship between items in the database).

You typically use a traversal language to query a graph database, and Azure Cosmos DB supports Apache Tinkerpop's Gremlin language.

## High Availability with CosmosDB

Azure Cosmos DB transparently replicates your data across all the Azure regions associated with your Cosmos account. Cosmos DB employs multiple layers of redundancy for your data as shown in the following image:



- The data within Cosmos containers is horizontally partitioned.
- Within each region, every partition is protected by a replica-set with all writes replicated and durably committed by most replicas. Replicas are distributed across as many as 10-20 fault domains.
- Each partition across all the regions is replicated. Each region contains all the data partitions of a Cosmos container and can accept writes and serve reads.

If your Cosmos account is distributed across \*N \* regions, there will be at least  $N \times 4$  copies of all your data. In addition to providing low latency data access and scaling write/read throughput across the regions associated with your Cosmos account, having more regions (higher N) further improves availability.

## SLAs for availability

As a globally distributed database, Cosmos DB provides comprehensive SLAs that encompass throughput, latency at the 99th percentile, consistency, and high availability. The table below shows the guarantees for high availability provided by Cosmos DB for single and multi-region accounts. For high availability, always configure your Cosmos accounts to have multiple write regions.

Operation type	Single region	Multi-region (single region writes)	Multi-region (multi-region writes)
Writes	99.99	99.99	99.999
Reads	99.99	99.999	99.999

## High availability with Cosmos DB in the event of regional outages

Regional outages aren't uncommon, and Azure Cosmos DB makes sure your database is always highly available. The following details capture Cosmos DB behavior during an outage, depending on your Cosmos account configuration:

- With Cosmos DB, before a write operation is acknowledged to the client, the data is durably committed by a quorum of replicas within the region that accepts the write operations.
- Multi-region accounts configured with multiple-write regions will be highly available for both writes and reads. Regional failovers are instantaneous and don't require any changes from the application.

## Multi-region accounts with a single-write region (write region outage)

- During a write region outage, the Cosmos account will automatically promote a secondary region to be the new primary write region when **enable automatic failover** is configured on the Azure Cosmos account. When enabled, the failover will occur to another region in the order of region priority you've specified.
- When the previously impacted region is back online, any write data that was not replicated when the region failed, is made available through the conflicts feed. Applications can read the conflicts feed, resolve the conflicts based on the application-specific logic, and write the updated data back to the Azure Cosmos container as appropriate.
- Once the previously impacted write region recovers, it becomes automatically available as a read region. You can switch back to the recovered region as the write region.

## Multi-region accounts with a single-write region (read region outage)

- During a read region outage, Cosmos accounts using any consistency level or strong consistency with three or more read regions will remain highly available for reads and writes.
- The impacted region is automatically disconnected and will be marked offline. The Azure Cosmos DB SDKs will redirect read calls to the next available region in the preferred region list.
- If none of the regions in the preferred region list is available, calls automatically fall back to the current write region.

## Availability Zone support

In addition to cross region resiliency, you can now enable **zone redundancy** when selecting a region to associate with your Azure Cosmos database.

With Availability Zone support, Azure Cosmos DB will ensure replicas are placed across multiple zones within a given region to provide high availability and resiliency during zonal failures.

## Azure Cosmos DB Cassandra API

Azure Cosmos DB Cassandra API can be used as the data store for apps written for Apache Cassandra. This means that by using existing Apache drivers compliant with CQLv4, your existing Cassandra application can now communicate with the Azure Cosmos DB Cassandra API. In many cases, you can switch from

using Apache Cassandra to using Azure Cosmos DB's Cassandra API, by just changing a connection string.

The Cassandra API enables you to interact with data stored in Azure Cosmos DB using the Cassandra Query Language (CQL), Cassandra-based tools (like cqlsh) and Cassandra client drivers that you're already familiar with.

## Benefits of using Apache Cassandra API for Azure Cosmos DB

**No operations management:** As a fully managed cloud service, Azure Cosmos DB Cassandra API removes the overhead of managing and monitoring a myriad of settings across OS, JVM, and yaml files and their interactions. Azure Cosmos DB provides monitoring of throughput, latency, storage, availability, and configurable alerts.

**Open source standard:** Despite being a fully managed service, Cassandra API still supports a large surface area of the native Apache Cassandra wire protocol, allowing you to build applications on a widely used and cloud agnostic open source standard.

**Performance management:** Azure Cosmos DB provides guaranteed low latency reads and writes at the 99th percentile, backed up by the SLAs. Users do not have to worry about operational overhead to ensure high performance and low latency reads and writes. This means that users do not need to deal with scheduling compaction, managing tombstones, setting up bloom filters and replicas manually. Azure Cosmos DB removes the overhead to manage these issues and lets you focus on the application logic.

**Ability to use existing code and tools:** Azure Cosmos DB provides wire protocol level compatibility with existing Cassandra SDKs and tools. This compatibility ensures you can use your existing codebase with Azure Cosmos DB Cassandra API with trivial changes.

**Throughput and storage elasticity:** Azure Cosmos DB provides guaranteed throughput across all regions and can scale the provisioned throughput with Azure portal, PowerShell, or CLI operations. You can elastically scale storage and throughput for your tables as needed with predictable performance.

**Global distribution and availability:** Azure Cosmos DB provides the ability to globally distribute data across all Azure regions and serve the data locally while ensuring low latency data access and high availability. Azure Cosmos DB provides 99.99% high availability within a region and 99.999% read and write availability across multiple regions with no operations overhead. Learn more in Distribute data globally article.

**Choice of consistency:** Azure Cosmos DB provides the choice of five well-defined consistency levels to achieve optimal tradeoffs between consistency and performance. These consistency levels are strong, bounded-staleness, session, consistent prefix and eventual. These well-defined, practical, and intuitive consistency levels allow developers to make precise trade-offs between consistency, availability, and latency. Learn more in consistency levels article.

**Enterprise grade:** Azure cosmos DB provides compliance certifications to ensure users can use the platform securely. Azure Cosmos DB also provides encryption at rest and in motion, IP firewall, and audit logs for control plane activities.

**Event Sourcing:** Cassandra API provides access to a persistent change log, the Change Feed, which can facilitate event sourcing directly from the database. In Apache Cassandra, the only equivalent is change data capture (CDC), which is merely a mechanism to flag specific tables for archival as well as rejecting writes to those tables once a configurable size-on-disk for the CDC log is reached (these capabilities are redundant in Cosmos DB as the relevant aspects are automatically governed).

## Azure Cosmos DB API for MongoDB

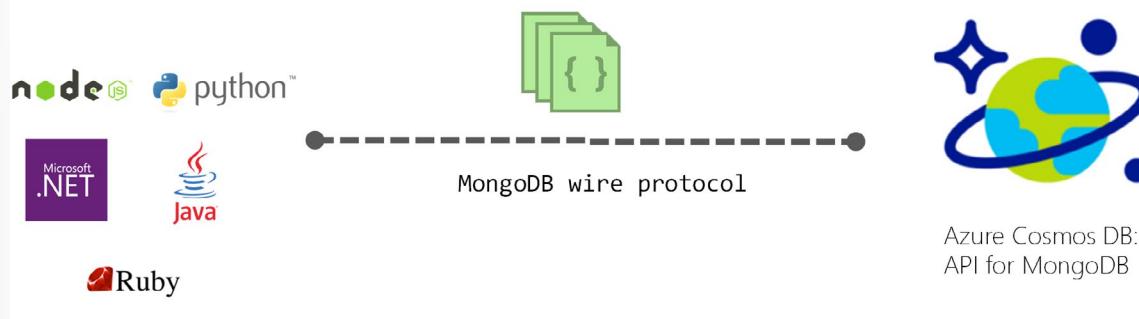
Azure Cosmos DB is a globally distributed, multi-model database service for mission-critical applications. Azure Cosmos DB provides turn-key global distribution, elastic scaling of throughput and storage worldwide, single-digit millisecond latencies at the 99th percentile, and guaranteed high availability supported by industry-leading SLAs.

Azure Cosmos DB automatically indexes data without schema and index management. It is multi-model and supports document, key-value, graph, and columnar data models. By default, you can interact with Cosmos DB using SQL API. Additionally, the Cosmos DB service implements wire protocols for common NoSQL APIs including Cassandra, MongoDB, Gremlin, and Azure Table Storage. This allows you to use familiar NoSQL client drivers and tools to interact with your Cosmos database.

### Wire protocol compatibility

Azure Cosmos DB implements wire protocols of common NoSQL databases including Cassandra, MongoDB, Gremlin, and Azure Tables Storage. By providing a native implementation of the wire protocols directly and efficiently inside Cosmos DB, it allows existing client SDKs, drivers, and tools of the NoSQL databases to interact with Cosmos DB transparently. Cosmos DB does not use any source code of the databases for providing wire-compatible APIs for any of the NoSQL databases.

By default, new accounts created using Azure Cosmos DB's API for MongoDB are compatible with version 3.6 of the MongoDB wire protocol. Any MongoDB client driver that understands this protocol version should be able to natively connect to Cosmos DB.



### Key benefits

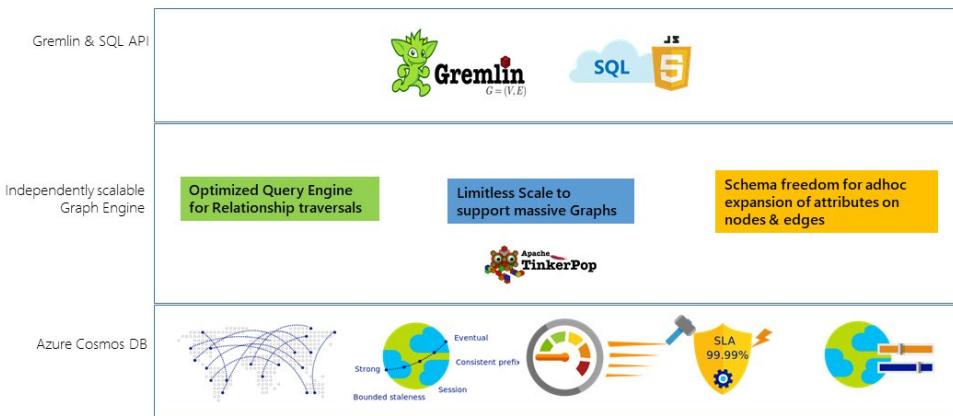
By natively implementing wire protocols of NoSQL APIs, Cosmos DB provides the following benefits:

- Migrate applications to Cosmos DB while preserving significant portions of your application logic.
- Keep applications portable and continue to remain cloud vendor-agnostic.
- Financially backed SLAs for the common NoSQL APIs powered by Cosmos DB.
- Turnkey, global distribution with multi-master replication.

## Azure Cosmos DB Gremlin API

Azure Cosmos DB is a multi-model database and supports document, key-value, graph, and column-family data models. The Azure Cosmos DB Gremlin API is used to store and operate with graph data on a fully managed database service designed for any scale.

## Azure Cosmos DB – Graph API PaaS



This topic provides an overview of the Azure Cosmos DB Gremlin API and explains how you can use it to store massive graphs with billions of vertices and edges. You can query the graphs with millisecond latency and evolve the graph structure easily. Azure Cosmos DB's Gremlin API is based on the Apache TinkerPop graph database standard, and uses the Gremlin query language.

Azure Cosmos DB's Gremlin API combines the power of graph database algorithms with highly scalable, managed infrastructure to provide a unique, flexible solution to most common data problems associated with lack of flexibility and relational approaches.

## Features of Azure Cosmos DB graph database

Azure Cosmos DB is a fully managed graph database that offers global distribution, elastic scaling of storage and throughput, automatic indexing and query, tunable consistency levels, and support for the TinkerPop standard.

The following are the differentiated features that Azure Cosmos DB Gremlin API offers:

### Elastically scalable throughput and storage

Graphs in the real world need to scale beyond the capacity of a single server. Azure Cosmos DB supports horizontally scalable graph databases that can have a virtually unlimited size in terms of storage and provisioned throughput. As the graph database scale grows, the data will be automatically distributed using graph partitioning.

### Multi-region replication

Azure Cosmos DB can automatically replicate your graph data to any Azure region worldwide. Global replication simplifies the development of applications that require global access to data. In addition to minimizing read and write latency anywhere around the world, Azure Cosmos DB provides automatic regional failover mechanism that can ensure the continuity of your application in the rare case of a service interruption in a region.

### Fast queries and traversals with the most widely adopted graph query standard

Store heterogeneous vertices and edges and query them through a familiar Gremlin syntax. Gremlin is an imperative, functional query language that provides a rich interface to implement common graph algorithms.

### Fully managed graph database

Azure Cosmos DB eliminates the need to manage database and machine resources. Most existing graph database platforms are bound to the limitations of their infrastructure and often require a high degree of maintenance to ensure its operation.

As a fully managed service, Cosmos DB removes the need to manage virtual machines, update runtime software, manage sharding or replication, or deal with complex data-tier upgrades. Every graph is automatically backed up and protected against regional failures. These guarantees allow developers to focus on delivering application value instead of operating and managing their graph databases.

### Automatic indexing

By default, Azure Cosmos DB automatically indexes all the properties within nodes and edges in the graph and doesn't expect or require any schema or creation of secondary indices.

### Tunable consistency levels

Azure Cosmos DB provides five well-defined consistency levels to achieve the right tradeoff between consistency and performance for your application. For queries and read operations, Azure Cosmos DB offers five distinct consistency levels: strong, bounded-staleness, session, consistent prefix, and eventual. These granular, well-defined consistency levels allow you to make sound tradeoffs among consistency, availability, and latency.

## Graph databases

Data as it appears in the real world is naturally connected. Traditional data modeling focuses on defining entities separately and computing their relationships at runtime. While this model has its advantages, highly connected data can be challenging to manage under its constraints.

A graph database approach relies on persisting relationships in the storage layer instead, which leads to highly efficient graph retrieval operations. Azure Cosmos DB's Gremlin API supports the property graph model.

## Property graph objects

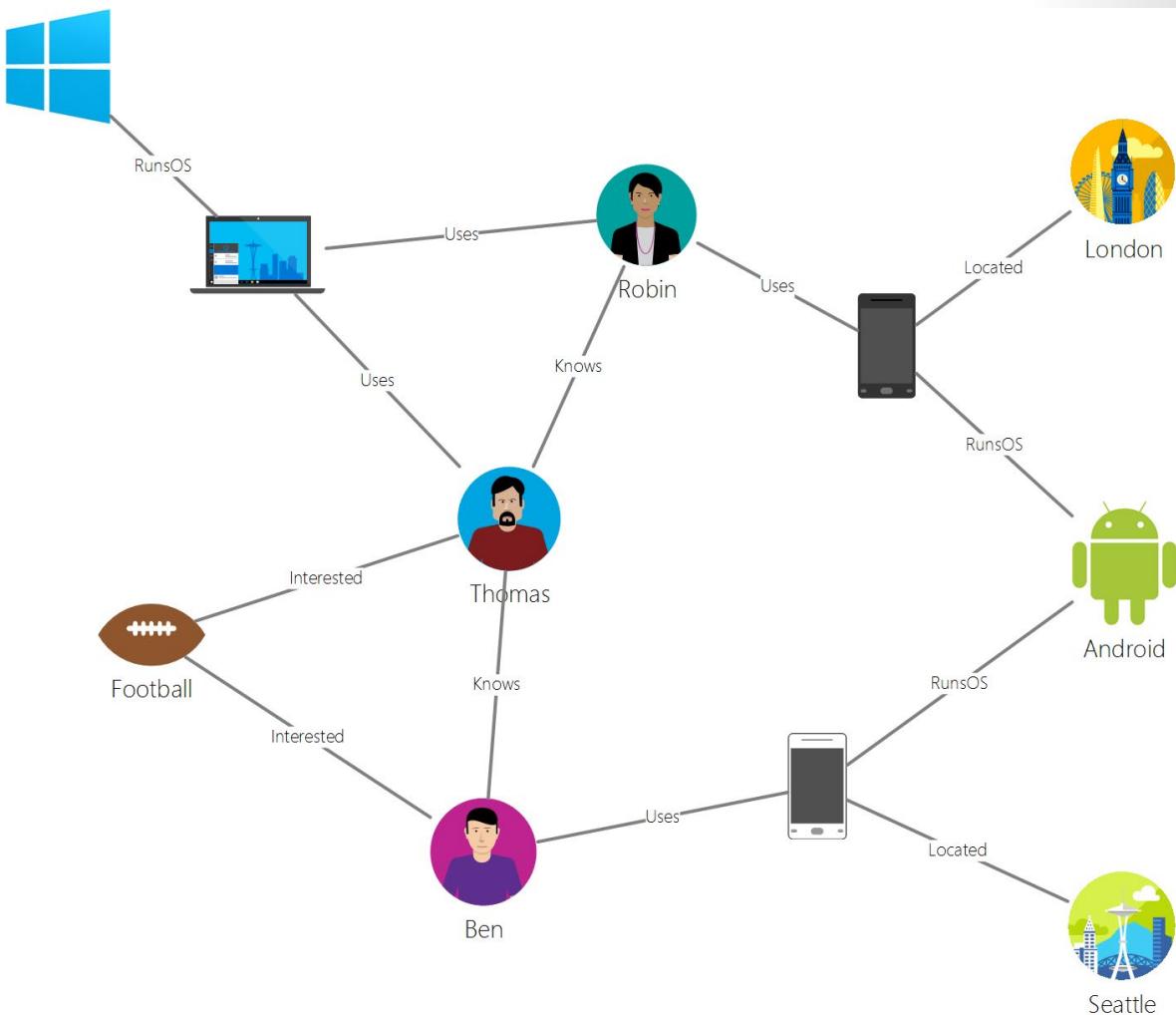
A property graph is a structure that's composed of vertices and edges. Both objects can have an arbitrary number of key-value pairs as properties.

- **Vertices** - Vertices denote discrete entities, such as a person, a place, or an event.
- **Edges** - Edges denote relationships between vertices. For example, a person might know another person, be involved in an event, and recently been at a location.
- **Properties** - Properties express information about the vertices and edges. There can be any number of properties in either vertices or edges, and they can be used to describe and filter the objects in a query. Example properties include a vertex that has name and age, or an edge, which can have a time stamp and/or a weight.

Graph databases are often included within the NoSQL or non-relational database category, since there is no dependency on a schema or constrained data model. This lack of schema allows for modeling and storing connected structures naturally and efficiently.

## Gremlin example

Below is sample graph to help understand how queries can be expressed in Gremlin. The following figure shows a business application that manages data about users, interests, and devices in the form of a graph.



This graph has the following vertex types (called "label" in Gremlin):

- **People:** The graph has three people, Robin, Thomas, and Ben
- **Interests:** Their interests, in this example, the game of Football
- **Devices:** The devices that people use
- **Operating Systems:** The operating systems that the devices run on

We represent the relationships between these entities via the following edge types/labels:

- **Knows:** For example, "Thomas knows Robin"
- **Interested:** To represent the interests of the people in our graph, for example, "Ben is interested in Football"
- **RunsOS:** Laptop runs the Windows OS

- **Uses:** To represent which device a person uses. For example, Robin uses a Motorola phone with serial number 77

## Azure Cosmos DB Table API

Azure Cosmos DB provides the Table API for applications that are written for Azure Table storage and that need premium capabilities like:

- Turnkey global distribution.
- Dedicated throughput worldwide.
- Single-digit millisecond latencies at the 99th percentile.
- Guaranteed high availability.
- Automatic secondary indexing.

Applications written for Azure Table storage can migrate to Azure Cosmos DB by using the Table API with no code changes and take advantage of premium capabilities. The Table API has client SDKs available for .NET, Java, Python, and Node.js.

**Important:** The .NET Framework SDK Microsoft.Azure.CosmosDB.Table is in maintenance mode and it will be deprecated soon. Please upgrade to the new .NET Standard library Microsoft.Azure.Cosmos.Table to continue to get the latest features supported by the Table API.

## Table offerings

If you currently use Azure Table Storage, you gain the following benefits by moving to the Azure Cosmos DB Table API:

	Azure Table storage	Azure Cosmos DB Table API
<b>Latency</b>	Fast, but no upper bounds on latency.	Single-digit millisecond latency for reads and writes, backed with <10 ms latency for reads and writes at the 99th percentile, at any scale, anywhere in the world.
<b>Throughput</b>	Variable throughput model. Tables have a scalability limit of 20,000 operations/s.	Highly scalable with dedicated reserved throughput per table that's backed by SLAs. Accounts have no upper limit on throughput and support >10 million operations/s per table.
<b>Global distribution</b>	Single region with one optional readable secondary read region for high availability. You can't initiate failover.	Turnkey global distribution from one to any number of regions. Support for automatic and manual failovers at any time, anywhere in the world. Multi-master capability to let any region accept write operations.
<b>Indexing</b>	Only primary index on PartitionKey and RowKey. No secondary indexes.	Automatic and complete indexing on all properties by default, with no index management.

	<b>Azure Table storage</b>	<b>Azure Cosmos DB Table API</b>
<b>Query</b>	Query execution uses index for primary key, and scans otherwise.	Queries can take advantage of automatic indexing on properties for fast query times.
<b>Consistency</b>	Strong within primary region. Eventual within secondary region.	Five well-defined consistency levels to trade off availability, latency, throughput, and consistency based on your application needs.
<b>Pricing</b>	Storage-optimized.	Throughput-optimized.
<b>SLAs</b>	99.9% to 99.99% availability, depending on the replication strategy.	99.999% read availability, 99.99% write availability on a single-region account and 99.999% write availability on multi-region accounts. Comprehensive SLAs covering availability, latency, throughput and consistency.

## Module 7 Review Questions

### Module 7 Review Questions



#### Review Question 1

A company you are advising wants to create the following Azure Cosmos DB databases for their dev team.  
*OEM\_Cosmos\_Database\_A:*

- 1500 RU/sec throughput
- Multiple write regions
- Uses the Core (SQL) API

*OEM\_Cosmos\_Database\_B:*

- 1100 RU/sec throughput
- Use the MongoDB API

*OEM\_Cosmos\_Database\_C:*

- 1500 RU/sec throughput
- Single write region
- Uses the Core (SQL) API

*OEM\_Cosmos\_Database\_D:*

- 900 RU/sec throughput
- Use the MongoDB API

As a part of the solution, they want to reduce costs.

You advise they create the Azure Cosmos DBs with two of the following recommendations:

- Create three Azure Cosmos DB accounts, one for DBs that use MongoDB API, one for OEM\_Cosmos\_Database\_A, and one for OEM\_Cosmos\_Database\_C.
- Create a single Azure Cosmos DB that includes the OEM\_Cosmos\_Database\_A, OEM\_Cosmos\_Database\_B, OEM\_Cosmos\_Database\_C, and OEM\_Cosmos\_Database\_D.
- Create one Azure Cosmos DB account for each DBs listed above.
- Create two Azure Cosmos DB accounts, one for those that use the Core (SQL) API and one for those that use MongoDB API.

## Review Question 2

*The same company also wants to create an app that uses a separate NoSQL DB that will be used to store transactions and supplier information using JSON files.*

*You recommend their developers use which of the two Cosmos DB APIs for the app:*

- Core (SQL) API
- Azure SQL Database REST API
- MongoDB API
- Cassandra

# Answers

## Review Question 1

A company you are advising wants to create the following Azure Cosmos DB databases for their dev team.

OEM\_Cosmos\_Database\_A:

OEM\_Cosmos\_Database\_B:

OEM\_Cosmos\_Database\_C:

OEM\_Cosmos\_Database\_D:

As a part of the solution, they want to reduce costs.

You advise they create the Azure Cosmos DBs with two of the following recommendations:

- Create three Azure Cosmos DB accounts, one for DBs that use MongoDB API, one for OEM\_Cosmos\_Database\_A, and one for OEM\_Cosmos\_Database\_C.
- Create a single Azure Cosmos DB that includes the OEM\_Cosmos\_Database\_A, OEM\_Cosmos\_Database\_B, OEM\_Cosmos\_Database\_C, and OEM\_Cosmos\_Database\_D.
- Create one Azure Cosmos DB account for each DBs listed above.
- Create two Azure Cosmos DB accounts, one for those that use the Core (SQL) API and one for those that use MongoDB API.

### Explanation

Correct Answer: A and C. *Create three Azure Cosmos DB accounts, one for DBs that use MongoDB API, one for OEM\_Cosmos\_Database\_A, and one for OEM\_Cosmos\_Database\_C. And, Create one Azure Cosmos DB account for each of Azure Cosmos DB databases.*

## Review Question 2

The same company also wants to create an app that uses a separate NoSQL DB that will be used to store transactions and supplier information using JSON files.

You recommend their developers use which of the two Cosmos DB APIs for the app:

- Core (SQL) API
- Azure SQL Database REST API
- MongoDB API
- Cassandra

### Explanation

Correct Answer: A and C. *Both Core (SQL) API and MongoDB API can be used for the NoSQL database.*

## Module 8 Implement Azure SQL Databases

### Configure Azure SQL Database Settings

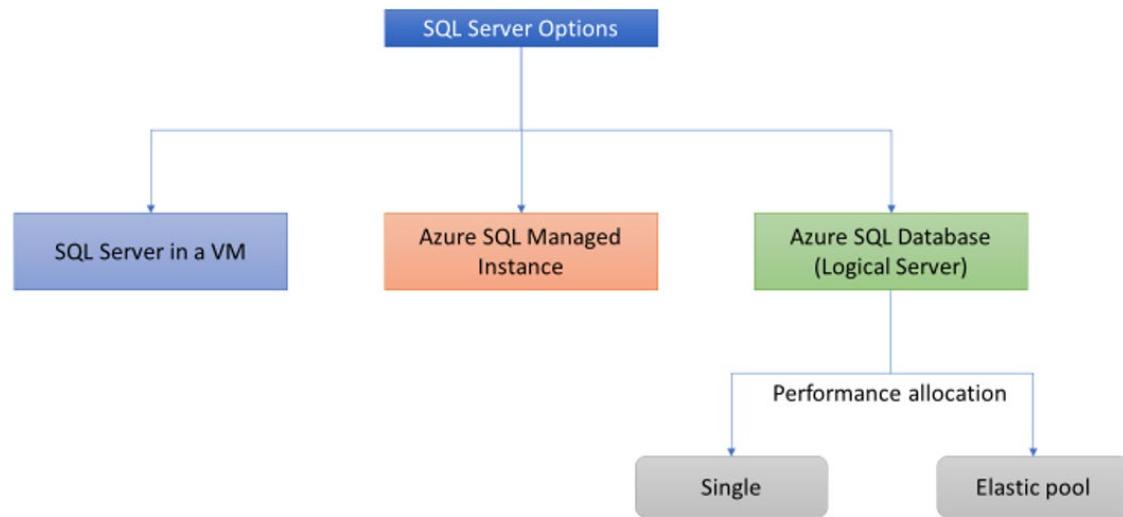
#### Azure SQL Database Service

SQL Database is a fully managed Platform as a Service (PaaS) Database Engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement. Azure SQL Database is always running on the latest stable version of SQL Server Database Engine and patched OS with 99.99% availability.

With Azure SQL Database, you can create a highly available and high-performance data storage layer for the applications and solutions in Azure. SQL Database can be the right choice for a variety of modern cloud applications because it enables you to process both relational data and non-relational structures, such as graphs, JSON, spatial, and XML.

#### Deployment models

Azure SQL Database provides the following deployment options for an Azure SQL database:



- Single database represents a fully managed, isolated database. You might use this option if you have modern cloud applications and microservices that need a single reliable data source. A single database is similar to a contained database in Microsoft SQL Server Database Engine.
- Managed instance is a fully managed instance of the Microsoft SQL Server Database Engine. It contains a set of databases that can be used together. Use this option for easy migration of on-premises SQL Server databases to the Azure cloud, and for applications that need to use the database features that SQL Server Database Engine provides.
- Elastic pool is a collection of single databases with a shared set of resources, such as CPU or memory. Single databases can be moved into and out of an elastic pool.

## Demonstration - Create an Azure SQL Database Single Database

In this demonstration, you use the Azure portal to create an Azure SQL Database single database. You then query the database using Query editor in the Azure portal.

A single database is the quickest and simplest deployment option for Azure SQL Database. You manage a single database within a SQL Database server, which is inside an Azure resource group in a specified Azure region. In this demonstration, you create a new resource group and SQL server for the new database.

You can create a single database in the *provisioned* or *serverless* compute tier. A provisioned database is pre-allocated a fixed amount of compute resources, including CPU and memory, and uses one of two purchasing models. This demonstration creates a provisioned database using the vCore-based purchasing model.

### Create a single database

In this step, you create an Azure SQL Database server and a single database that uses AdventureWorksLT sample data. You can create the database by using Azure portal menus and screens, or by using an Azure CLI or PowerShell script in the Azure Cloud Shell.

To create a resource group, SQL server, and single database in the Azure portal:

1. Sign in to the [portal<sup>1</sup>](#).
2. From the Search bar, search for and select **Azure SQL**.
3. On the Azure SQL page, select **Add**.

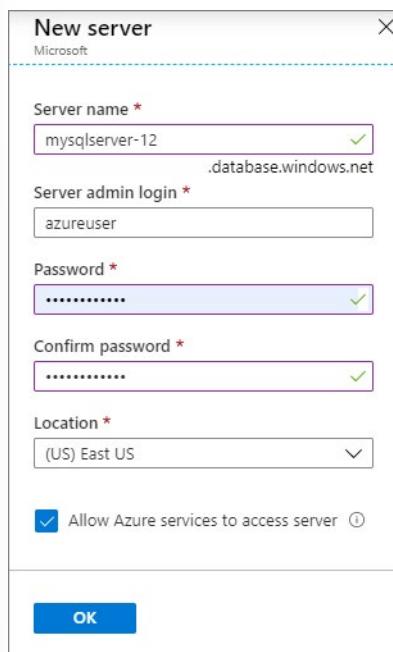
The screenshot shows the Microsoft Azure portal interface. In the top navigation bar, the search bar contains the text 'azure sql'. Below the search bar, the 'Services' section is visible, with 'Azure SQL' highlighted by a red box. Other service options listed include 'Azure Database for MySQL servers', 'SQL databases', 'Azure Cosmos DB', and 'Azure Synapse Analytics (formerly SQL DW)'. To the right of the services, there's a 'Marketplace' section with links to 'Azure SQL', 'Azure SQL Analytics (Preview)', 'Azure SQL Managed Instance', and 'CloudBeam Azure SQL Data Warehouse-BYOL'. At the bottom right of the screen, the user's email address 'admin@M365x125231...@contoso.com' is displayed.

4. On the **Select SQL deployment option** page, select the **SQL databases** tile, with **Single database** under **Resource** type. You can view more information about the different databases by selecting **Show details**.
5. Select **Create**.

The screenshot shows the 'Select SQL deployment option' page. At the top, it says 'How do you plan to use the service?'. There are three options: 'SQL databases', 'SQL managed instances', and 'SQL virtual machines'. The 'SQL databases' option is selected, showing its description: 'Best for modern cloud applications. Hyperscale and serverless options are available.' Below this, a dropdown menu shows 'Resource type: Single database' and a 'Create' button, which is highlighted with a red box. The other two options ('SQL managed instances' and 'SQL virtual machines') also have their descriptions and 'Create' buttons below them.

6. On the **Basics** tab of the Create SQL database form, under **Project details**, select the correct Azure Subscription if it isn't already selected.
  7. Under **Resource group**, select **Create new**, enter *myResourceGroup*, and select **OK**.
  8. Under **Database details**, for **Database name** enter *mySampleDatabase*.
  9. For **Server**, select **Create new**, and fill out the New server form as follows:
    - **Server name:** Enter *mysqlserver*, and some characters for uniqueness.
    - **Server admin login:** Enter *azureuser*.
    - **Password:** Enter a password that meets requirements, and enter it again in the **Confirm password** field.
    - **Location:** Drop down and choose a location, such as **(US) East US**.
- Select **OK**.

<sup>1</sup> <https://portal.azure.com/>



Record the server admin login and password so you can log in to the server and databases. If you forget your login or password, you can get the login name or reset the password on the **SQL server** page after database creation. To open the **SQL server** page, select the server name on the database **Overview** page.

10. Under **Compute + storage**, if you want to reconfigure the defaults, select **Configure database**.

On the **Configure** page, you can optionally:

- Change the **Compute tier** from **Provisioned** to **Serverless**.
- Review and change the settings for **vCores** and **Data max size**.
- Select **Change configuration** to change the hardware generation.

After making any changes, select **Apply**.

11. Select **Next: Networking** at the bottom of the page.

**Create SQL Database**

**Basics** Networking Additional settings Tags Review + create

Create a SQL database with your preferred configurations. Complete the Basics tab then go to Review + Create to provision with smart defaults, or visit each tab to customize. [Learn more](#)

**Project details**

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

Subscription \* ⓘ A Subscription

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

**Database details**

Enter required settings for this database, including picking a logical server and configuring the compute and storage resources

Database name \* mySampleDatabase

Server ⓘ (new) mysqlserver-12 (East US) [Create new](#)

Want to use SQL elastic pool? \* ⓘ  Yes  No

Compute + storage \* ⓘ

**General Purpose**  
Gen5, 2 vCores, 32 GB storage  
[Configure database](#)

**Review + create** **Next : Networking >**

12. On the **Networking** tab, under **Connectivity method**, select **Public endpoint**.
13. Under **Firewall rules**, set **Add current client IP address** to **Yes**.
14. Select **Next: Additional** settings at the bottom of the page.

**Create SQL Database**

Microsoft

Basics Networking Additional settings Tags Review + create

Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'mysqlserver-12' and all databases it manages. [Learn more](#)

**Network connectivity**

Choose an option for configuring connectivity to your server via public endpoint or private endpoint. Choosing no access creates with defaults and you can configure connection method after server creation. [Learn more](#)

Connectivity method \* ⓘ

No access  
 Public endpoint  
 Private endpoint (preview)

**Firewall rules**

Setting 'Allow Azure services and resources to access this server' to Yes allows communications from all resources inside the Azure boundary, that may or may not be part of your subscription. [Learn more](#)

Setting 'Add current client IP address' to Yes will add an entry for your client IP address to the server firewall.

Allow Azure services and resources to access this server \*

No Yes

Add current client IP address \*

No Yes

**Review + create** < Previous Next : Additional settings >

15. On the **Additional settings** tab, in the **Data source** section, for **Use existing data**, select **Sample**.
16. Select **Review + create** at the bottom of the page.

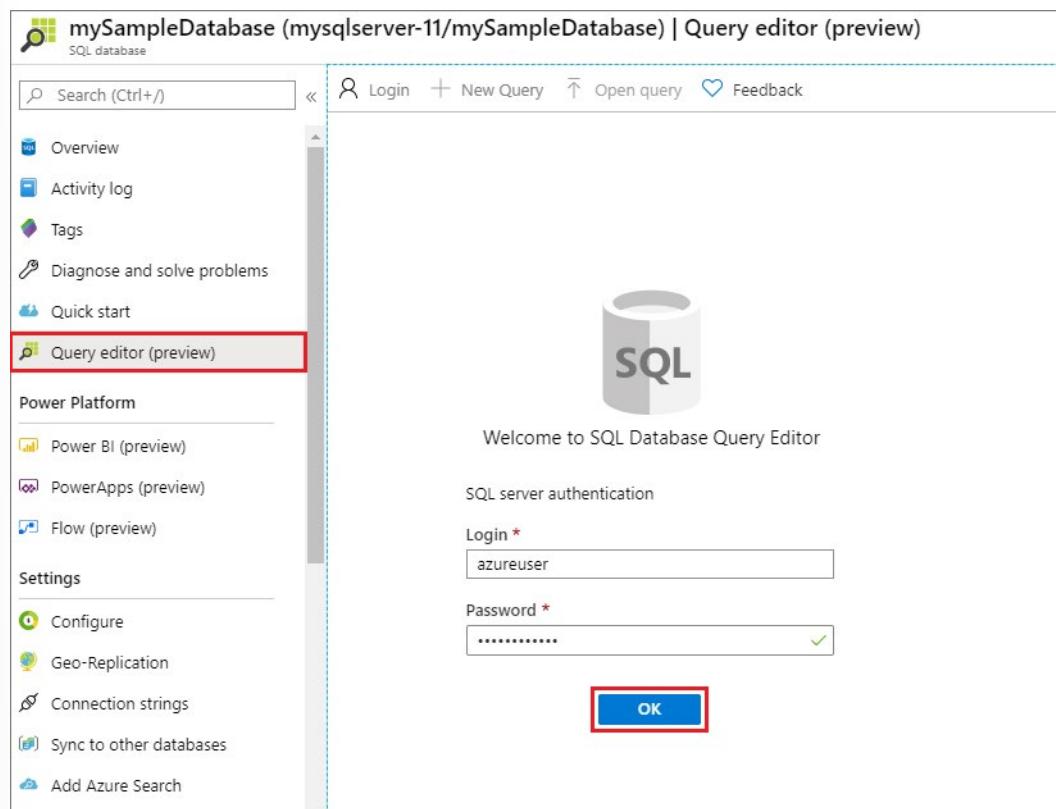
The screenshot shows the 'Create SQL Database' wizard interface. At the top, there are tabs: Basics, Networking, Additional settings (which is underlined), Tags, and Review + create. Below the tabs, a note says 'Customize additional configuration parameters including collation & sample data.' Under 'Data source', it says 'Start with a blank database, restore from a backup or select sample data to populate your new database.' A radio button for 'Use existing data \*' is followed by three options: None, Backup, and Sample, with Sample being selected. A note below says 'AdventureWorksLT will be created as the sample database.' Under 'Database collation', it says 'Database collation defines the rules that sort and compare data, and cannot be changed after database creation. The default database collation is SQL\_Latin1\_General\_CI\_AS.' A link 'Learn more' is provided. A dropdown menu shows 'SQL\_Latin1\_General\_CI\_AS'. Under 'Advanced data security', it says 'Protect your data using advanced data security, a unified security package including data classification, vulnerability assessment and advanced threat protection for your server.' A link 'Learn more' is provided. At the bottom, there are buttons for 'Review + create' (highlighted with a red box), '< Previous', and 'Next : Tags >'.

17. After reviewing settings, select **Create**.

## Query the database

Once your database is created, you can use the built-in Query editor in the Azure portal to connect to the database and query the data.

1. In the portal, search for and select **SQL databases**, and then select your database from the list.
2. On the **SQL Database** page for your database, select **Query editor** in the left menu.
3. Enter your server admin login information, and select **OK**.



4. Enter the following query in the Query editor pane.

```
SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName  
  
FROM SalesLT.ProductCategory pc  
  
JOIN SalesLT.Product p  
  
ON pc.productcategoryid = p.productcategoryid;
```

5. Select **Run**, and then review the query results in the **Results** pane.

The screenshot shows the Azure portal interface for a database named 'mySampleDatabase'. On the left, there's a sidebar with various management options like Overview, Activity log, Tags, and Query editor (preview). The main area is titled 'Query editor (preview)' and contains a query editor window. In the query editor, a SQL script is written:

```
1 SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName
2 FROM SalesLT.ProductCategory pc
3 JOIN SalesLT.Product p
4 ON pc.productcategoryId = p.productcategoryId;
```

The results tab is selected, displaying the output of the query:

CATEGORYNAME	PRODUCTNAME
Road Frames	HL Road Frame - Black, 58
Road Frames	HL Road Frame - Red, 58
Helmets	Sport-100 Helmet, Red
Helmets	Sport-100 Helmet, Black
Socks	Mountain Bike Socks, M
Socks	Mountain Bike Socks, L
Helmets	Sport-100 Helmet, Blue
Can	AWC Logo Can

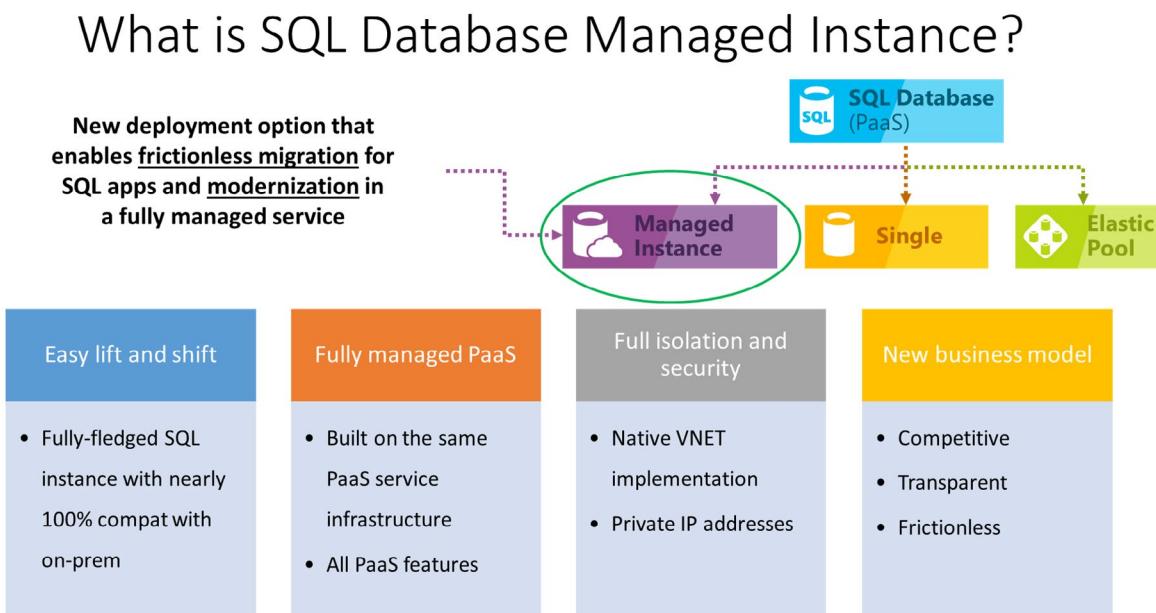
6. Close the **Query editor** page, and select **OK** when prompted to discard your unsaved edits.

# Implement Azure SQL Database Managed Instances

## Azure SQL Database Managed Instance

Managed instance is a new deployment option of Azure SQL Database, providing near 100% compatibility with the latest SQL Server on-premises (Enterprise Edition) Database Engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for on-premises SQL Server customers. The managed instance deployment model allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes.

The following diagram outlines key features of managed instances:



The managed instance deployment model is designed for customers looking to migrate a large number of apps from on-premises or IaaS, self-built, or ISV provided environment to fully managed PaaS cloud environment, with as low migration effort as possible. Using the fully automated Data Migration Service (DMS) in Azure, customers can lift and shift their on-premises SQL Server to a managed instance that offers compatibility with SQL Server on-premises and complete isolation of customer instances with native VNet support.

The managed instance deployment option aims delivers close to 100% surface area compatibility with the latest on-premises SQL Server version through a staged release plan.

## Features and capabilities

Managed instance combines the best features that are available both in Azure SQL Database and SQL Server Database Engine.

PaaS benefits	Business continuity
No hardware purchasing and management	99.99% uptime SLA
No management overhead for managing underlying infrastructure	Built in high-availability
Quick provisioning and service scaling	Data protected with automated backup. Customer configurable backup retention period
Automated patching and version upgrade	User-initiated backups
Integration with other PaaS data services	Point in time database restore capability

The key features of managed instances are shown in the following table:

Feature	Description
SQL Server version / build	SQL Server Database Engine (latest stable)
Managed automated backups	Yes
Built-in instance and database monitoring and metrics	Yes
Automatic software patching	Yes
The latest Database Engine features	Yes
Number of data files (ROWS) per the database	Multiple
Number of log files (LOG) per database	1
VNet - Azure Resource Manager deployment	Yes
VNet - Classic deployment model	No
Portal support	Yes
Built-in Integration Service (SSIS)	No - SSIS is a part of Azure Data Factory PaaS
Built-in Analysis Service (SSAS)	No - SSAS is separate PaaS
Built-in Reporting Service (SSRS)	No - use Power BI paginated reports instead or host SSRS on Azure VM.

## Demonstration - Create an Azure SQL Database Managed Instance

This demonstration walks you through how to create an Azure SQL Database managed instance in Azure portal.

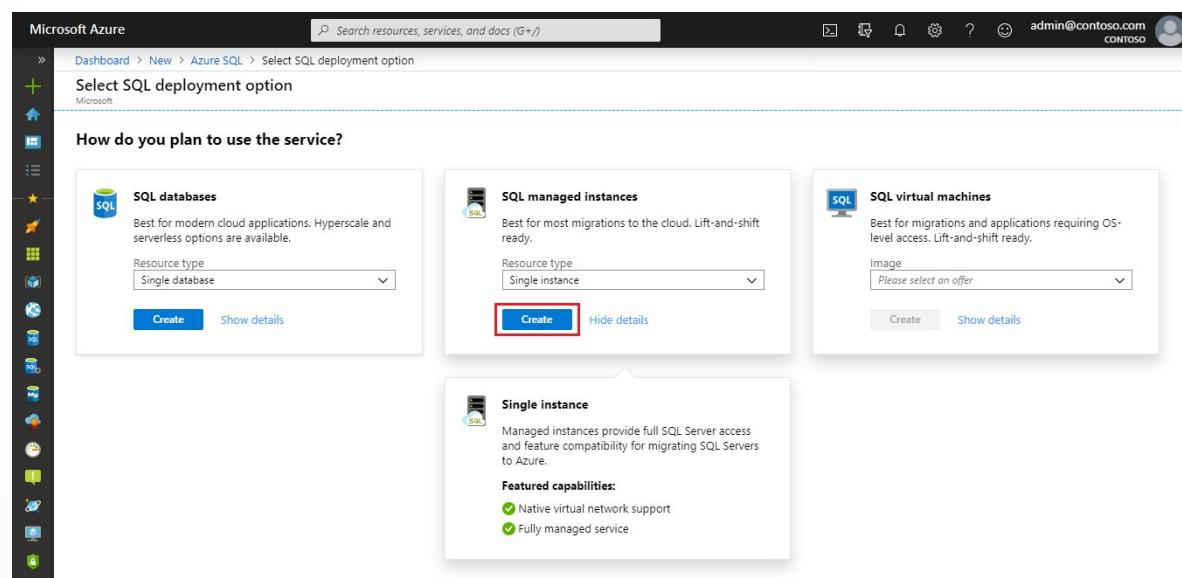
Sign in to [Azure portal<sup>2</sup>](#).

### Create a managed instance

The following steps show you how to create a managed instance:

1. Select **Azure SQL** on the left menu of Azure portal. If **Azure SQL** is not in the list, select **All services**, and then enter *Azure SQL* in the search box.
2. Select **+Add** to open the **Select SQL deployment option** page. You can view additional information about an Azure SQL Database managed instance by selecting **Show details** on the **Managed instances** tile.
3. Select **Create**.

<sup>2</sup> <https://portal.azure.com/>



4. Use the tabs on the **Create Azure SQL Database Managed Instance** provisioning form to add required and optional information. The following sections describe these tabs.

## Basics

- Fill out mandatory information required on the **Basics** tab.

Use the table below as a reference for information required at this tab.

Setting	Suggested value	Description
<b>Virtual network</b>	Select either Create new virtual network or a valid virtual network and subnet.	If a network or subnet is unavailable, it must be modified to satisfy the network requirements before you select it as a target for the new managed instance. For information about the requirements for configuring the network environment for a managed instance, see Configure a virtual network for a managed instance.
<b>Connection type</b>	Choose between a proxy and a redirect connection type.	For more information about connection types, see Azure SQL Database connection policy.

Setting	Suggested value	Description
<b>Public endpoint</b>	Select Enable.	For a managed instance to be accessible through the public data endpoint, you need to enable this option.
<b>Allow access from (if Public endpoint is enabled)</b>	Select one of the options.	The portal experience enables configuring a security group with a public endpoint.

- Select **Configure Managed Instance** to size compute and storage resources and to review the pricing tiers. Use the sliders or text boxes to specify the amount of storage and the number of virtual cores. When you're finished, select **Apply** to save your selection.

The screenshot shows the Azure portal interface for creating a managed instance. The top navigation bar includes 'Microsoft Azure', a search bar, and a user profile for 'admin@contoso.com'. The main content area is titled 'Configure performance' under 'Create Azure SQL Database Managed Instance'. On the left, there's a sidebar with various icons. The main panel has two tabs: 'General Purpose' (selected) and 'Business Critical'. Under 'General Purpose', it says 'For most production workloads' with options 4 / 8 / 16 / 24 / 32 / 40 / 64 / 80 vCores, 32 GB - 8TB storage capacity, and Fast storage. The 'Business Critical' tab says 'For IO-intensive and compute-intensive workloads' with options 4 / 8 / 16 / 24 / 32 / 40 / 64 / 80 vCores, 32 GB - 4 TB storage capacity, and Super fast storage. Below these are sections for 'Compute Generation' (Gen4 and Gen5, with Gen5 selected), 'vCores' (set to 4), 'Storage' (set to 256), 'Days of backup retention' (set to 7), and a 'Save money' checkbox for 'Azure Hybrid Benefit for SQL Server' (set to No). At the bottom is a large blue 'Apply' button.

- To review your choices before you create a managed instance, you can select **Review + create**. Or, configure networking options by selecting **Next: Networking**.

## Networking

- Fill out optional information on the **Networking** tab. If you omit this information, the portal will apply default settings.

The screenshot shows the Microsoft Azure portal interface for creating a new Azure SQL Database Managed Instance. The 'Networking' tab is active. Under 'Virtual network', a dropdown menu shows '(new) vnet-my-managed-instance/ManagedInstance'. A note says 'New virtual network will be created. Network configuration required for Managed Instance will be applied to the subnet automatically.' Under 'Connection type', it shows 'Proxy (Default)'. Under 'Public endpoint', there's a note about accelerated networking being automatically enabled on Gen5 hardware. At the bottom, there are 'Review + create', '< Previous', and 'Next : Additional settings >' buttons.

Use the table below as a reference for information required at this tab.

Setting	Suggested value	Description
<b>Virtual network</b>	Select either Create new virtual network or a valid virtual network and subnet.	If a network or subnet is unavailable, it must be modified to satisfy the network requirements before you select it as a target for the new managed instance. For information about the requirements for configuring the network environment for a managed instance, see Configure a virtual network for a managed instance.
<b>Connection type</b>	Choose between a proxy and a redirect connection type.	For more information about connection types, see Azure SQL Database connection policy.
<b>Public endpoint</b>	Select Enable.	For a managed instance to be accessible through the public data endpoint, you need to enable this option.

Setting	Suggested value	Description
<b>Allow access from (if Public endpoint is enabled)</b>	Select one of the options.	The portal experience enables configuring a security group with a public endpoint.

- Select **Review + create** to review your choices before you create a managed instance. Or, configure more custom settings by selecting **Next: Additional settings**.

## Additional settings

- Fill out optional information on the **Additional settings** tab. If you omit this information, the portal will apply default settings.

The screenshot shows the Microsoft Azure portal interface for creating a new Azure SQL Database Managed Instance. The top navigation bar includes 'Microsoft Azure', a search bar, and a user profile for 'admin@contoso.com'. The main title is 'Create Azure SQL Database Managed Instance'. Below it, the 'Additional settings' tab is active, indicated by a dashed blue border. The page content includes sections for 'Collation', 'Time zone', and 'Geo-Replication', each with configuration fields and help links. At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next : Review + create >'.

Use the table below as a reference for information required at this tab.

Setting	Suggested value	Description
<b>Collation</b>	Choose the collation that you want to use for your managed instance. If you migrate databases from SQL Server, check the source collation by using <code>SELECT SERVERPROPERTY('N'Collation')</code> and use that value.	For information about collations, see Set or change the server collation.
<b>Time zone</b>	Select the time zone that your managed instance will observe.	For more information, see Time zones.

Setting	Suggested value	Description
<b>Use as failover secondary</b>	Select Yes.	Enable this option to use the managed instance as a failover group secondary.
<b>Primary managed instance (if Use as failover secondary is set to Yes)</b>	Choose an existing primary managed instance that will be joined in the same DNS zone with the managed instance you're creating.	This step will enable post-creation configuration of the failover group.

## Review + create

5. Select **Review + create** tab to review your choices before you create the managed instance.

6. Select **Create** to start provisioning the managed instance.

# High-Availability and Azure SQL Database

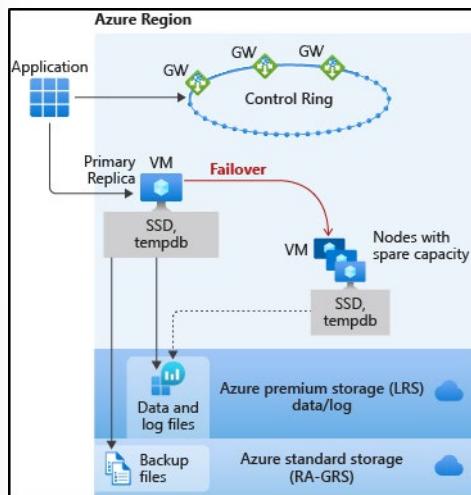
## High-Availability and Azure SQL Database

There are two high-availability architectural models that are used in Azure SQL Database:

- **Standard availability model that is based on a separation of compute and storage.** It relies on high availability and reliability of the remote storage tier. This architecture targets budget-oriented business applications that can tolerate some performance degradation during maintenance activities.
- **Premium availability model that is based on a cluster of database engine processes.** It relies on the fact that there is always a quorum of available database engine nodes. This architecture targets mission critical applications with high IO performance, high transaction rate and guarantees minimal performance impact to your workload during maintenance activities.

## Basic, Standard, and General-Purpose service tier availability

The Basic, Standard, and General-Purpose service tiers leverage the standard availability architecture for both serverless and provisioned compute. The following figure shows four different nodes with the separated compute and storage layers.



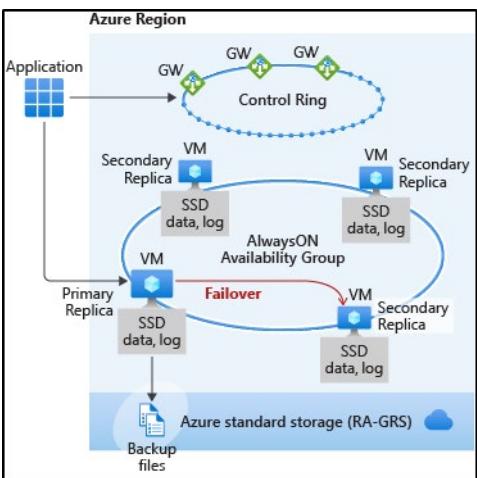
The standard availability model includes two layers:

- A **stateless compute layer** that runs the `sqlservr.exe` process and contains only transient and cached data, such as TempDB, model databases on the attached SSD, and plan cache, buffer pool, and columnstore pool in memory. This stateless node is operated by Azure Service Fabric that initializes `sqlservr.exe`, controls health of the node, and performs failover to another node if necessary.
- A **stateful data layer** with the database files (.mdf/.ldf) that are stored in Azure Blob storage. Azure blob storage has built-in data availability and redundancy feature. It guarantees that every record in the log file or page in the data file will be preserved even if SQL Server process crashes.

## Premium and Business Critical service tier availability

Premium and Business Critical service tiers leverage the Premium availability model, which integrates compute resources (SQL Server Database Engine process) and storage (locally attached SSD) on a single

node. High availability is achieved by replicating both compute and storage to additional nodes creating a three to four-node cluster.

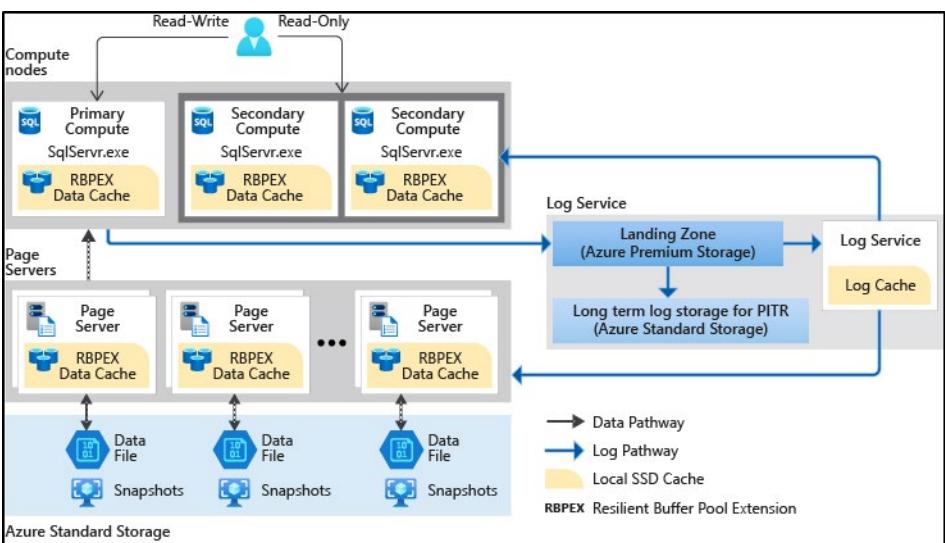


The underlying database files (.mdf/.ldf) are placed on the attached SSD storage to provide very low latency IO to your workload. High availability is implemented using a technology similar to SQL Server Always On Availability Groups. The cluster includes a single primary replica (SQL Server process) that is accessible for read-write customer workloads, and up to three secondary replicas (compute and storage) containing copies of data.

The primary node constantly pushes changes to the secondary nodes in order and ensures that the data is synchronized to at least one secondary replica before committing each transaction. This process guarantees that if the primary node crashes for any reason, there is always a fully synchronized node to fail over to.

The failover is initiated by the Azure Service Fabric. Once the secondary replica becomes the new primary node, another secondary replica is created to ensure the cluster has enough nodes (quorum set). Once failover is complete, SQL connections are automatically redirected to the new primary node.

## Hyperscale service tier availability



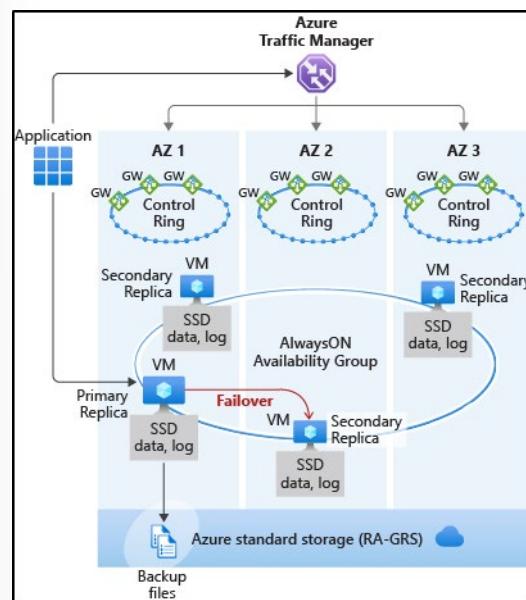
The availability model in Hyperscale includes four layers:

- A **stateless compute layer** that runs the `sqlservr.exe` processes and contains only transient and cached data, such as non-covering RBPEX cache, TempDB, model database, etc. on the attached SSD, and plan cache, buffer pool, and columnstore pool in memory.
- A **stateless storage layer** formed by page servers. This layer is the distributed storage engine for the `sqlservr.exe` processes running on the compute replicas. Each page server contains only transient and cached data, such as covering RBPEX cache on the attached SSD, and data pages cached in memory.
- A **stateful transaction log storage layer** formed by the compute node running the Log service process, the transaction log landing zone, and transaction log long term storage.
- A **stateful data storage layer** with the database files (.mdf/.ndf) that are stored in Azure Storage and are updated by page servers. This layer uses data availability and redundancy features of Azure Storage. Compute nodes in all Hyperscale layers run on Azure Service Fabric, which controls health of each node and performs failovers to available healthy nodes as necessary.

## Zone redundant configuration

By default, the cluster of nodes for the premium availability model is created in the same datacenter. With the introduction of Azure Availability Zones, SQL Database can place different replicas of the Business Critical database to different availability zones in the same region. To eliminate a single point of failure, the control ring is also duplicated across multiple zones as three gateway rings (GW). The routing to a specific gateway ring is controlled by Azure Traffic Manager (ATM).

The zone redundant version of the high availability architecture is illustrated by the following diagram:



## Module 8 Review Questions

### Module 8 Review Questions



#### Review Question 1

You are advising a auto parts company that has the following:

- OEMDabaBase\_1: Microsoft SQL Server
- OEMDabaBase\_2: Microsoft SQL Server
- OEMApplication\_1: Uses data from both databases listed above

The company wants to move both databases to Azure and they are asking for recommendations for services needed to host in Azure.

Also, the recommendation must include support for server-side transactions between the two databases.

You recommend they deploy both databases as Azure SQL Databases on the same Azure SQL Database server.

Is this the right solution?

- Yes  
 No

#### Review Question 2

You are advising a auto parts company that has the following:

- OEMDabaBase\_1: Microsoft SQL Server
- OEMDabaBase\_2: Microsoft SQL Server
- OEMApplication\_1: Uses data from both databases listed above

The company wants to move both databases to Azure and they are asking for recommendations for services needed to host in Azure.

Also, the recommendation must include support for server-side transactions between the two databases.

You recommend they deploy both databases (OEMDabaBase\_1 and OEMDabaBase\_2) to sQL Server on an Azure VM.

Is this the right solution?

- Yes  
 No

## Review Question 3

You are advising an auto parts company that is running the following Azure SQL Database servers:

*OEM\_SQLSvr\_1:*

- Resource Group: Resource\_Group\_1
- Location: East US

*OEM\_SQLSvr\_2:*

- Resource Group: Resource\_Group\_1
- Location: East US

*OEM\_SQLSvr\_3:*

- Resource Group: Resource\_Group\_1
- Location: North Europe

*OEM\_SQLSvr\_4:*

- Resource Group: Resource\_Group\_2
- Location: North Europe

The plan to make OEM\_SQLSvr\_1 as the primary server within a failover group.  
Which server should you recommend as the secondary server?

- OEM\_SQLSvr\_3 and OEM\_SQLSvr\_4
- OEM\_SQLSvr\_2 and OEM\_SQLSvr\_3
- OEM\_SQLSvr\_2 and OEM\_SQLSvr\_4

# Answers

## Review Question 1

You are advising a auto parts company that has the following:

The company wants to move both databases to Azure and they are asking for recommendations for services needed to host in Azure.

Also, the recommendation must include support for server-side transactions between the two databases. You recommend they deploy both databases as Azure SQL Databases on the same Azure SQL Database server.

Is this the right solution?

- Yes
- No

*Explanation*

*No. You should deploy both databases (OEMDabaBase\_1 and OEMDabaBase\_2) to an Azure SQL managed instance.*

## Review Question 2

You are advising a auto parts company that has the following:

The company wants to move both databases to Azure and they are asking for recommendations for services needed to host in Azure.

Also, the recommendation must include support for server-side transactions between the two databases. You recommend they deploy both databases (OEMDabaBase\_1 and OEMDabaBase\_2) to sQL Server on an Azure VM.

Is this the right solution?

- Yes
- No

*Explanation*

*Yes. You should deploy both databases (OEMDabaBase\_1 and OEMDabaBase\_2) to an Azure SQL managed instance.*

## Review Question 3

You are advising an auto parts company that is running the following Azure SQL Database servers:  
OEM\_SQLSvr\_1:

OEM\_SQLSvr\_2:

OEM\_SQLSvr\_3:

OEM\_SQLSvr\_4:

The plan to make OEM\_SQLSvr\_1 as the primary server within a failover group.  
Which server should you recommend as the secondary server?

- OEM\_SQLSvr\_3 and OEM\_SQLSvr\_4
- OEM\_SQLSvr\_2 and OEM\_SQLSvr\_3
- OEM\_SQLSvr\_2 and OEM\_SQLSvr\_4

*Explanation*

*Correct answer: OEM\_SQLSvr\_3 and OEM\_SQLSvr\_4. OEM\_SQLSvr\_1 is located in East US, and both OEM\_SQLSvr\_3 and OEM\_SQLSvr\_4 are located in North Europe.*

# Module 9 Automate Deployment and Configuration of Resources

## Azure Resource Manager Templates

### Overview of Resource Manager Templates

Azure Resource Manager is the interface for managing and organizing cloud resources. Think of Resource Manager as a way to deploy cloud resources.

If you're familiar with Azure resource groups, you know that they enable you to treat sets of related resources as a single unit. Resource Manager is what organizes the resource groups that let you deploy, manage, and delete all of the resources together in a single action.

With Resource Manager, you deploy assets into the same resource group and manage and monitor them together. When you're done, you can delete all of the resources in a resource group in one operation.

#### What are Resource Manager templates?

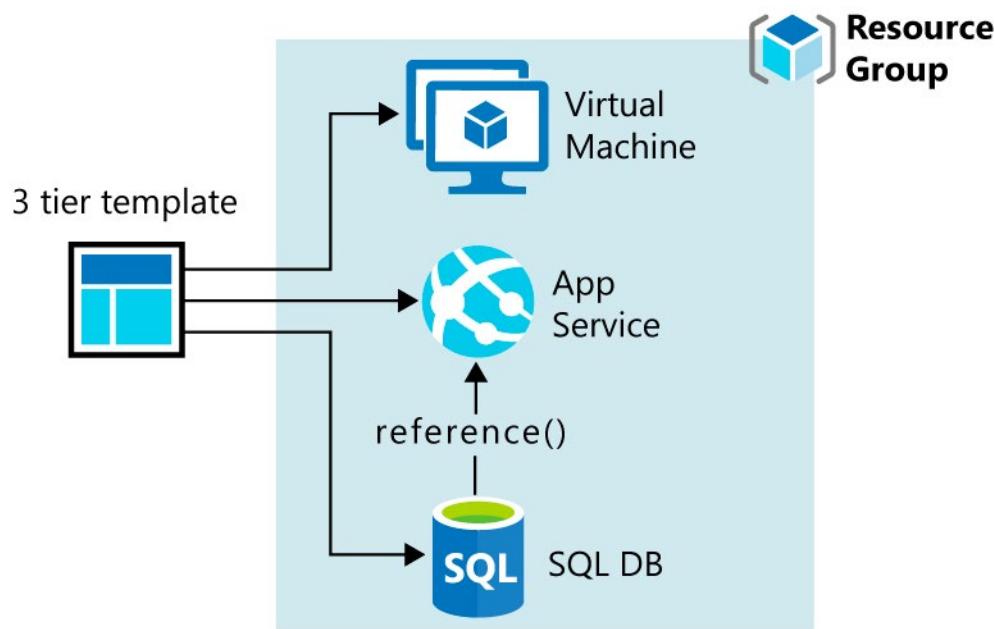
A Resource Manager template precisely defines all the Resource Manager resources in a deployment. You can deploy a Resource Manager template into a resource group as a single operation.

A Resource Manager template is a JSON file, making it a form of declarative automation. Declarative automation means that you define what resources you need but not how to create them. Put another way, you define what you need, and it is Resource Manager's responsibility to ensure that resources are deployed correctly.

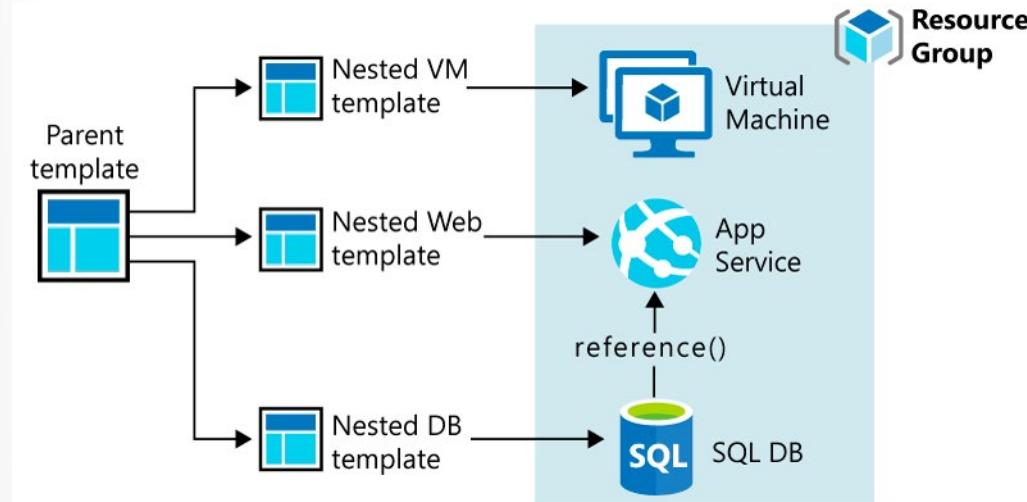
You can think of declarative automation similar to how web browsers display HTML files. The HTML file describes what elements appear on the page, but doesn't describe how to display them. The "how" is the web browser's responsibility.

#### Template design

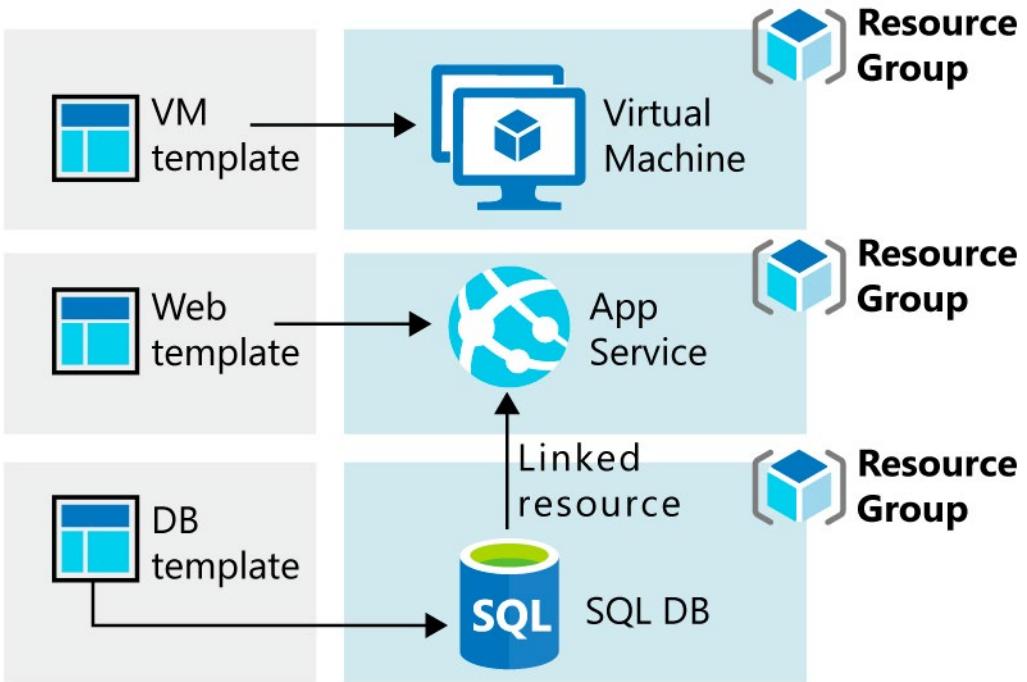
How you define templates and resource groups is entirely up to you and how you want to manage your solution. For example, you can deploy your three-tier application through a single template to a single resource group.



But, you don't have to define your entire infrastructure in a single template. Often, it makes sense to divide your deployment requirements into a set of targeted, purpose-specific templates. You can easily reuse these templates for different solutions. To deploy a solution, you create a master template that links all the required templates. The following image shows how to deploy a three-tier solution through a parent template that includes three nested templates.



If you envision your tiers having separate lifecycles, you can deploy your three tiers to separate resource groups. Notice the resources can still be linked to resources in other resource groups.



## What's in a Resource Manager Template

Below are code examples to give you a sense of how each section of the template is structured.

You use JSON to send data between servers and web applications. JSON is also a way to describe how applications and infrastructure are configured.

JSON allows us 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; its value can be a string, a number, a Boolean expression, a list of values, or an object (which is a collection of other key-value pairs).

A Resource Manager template can contain the following sections. These sections 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": { }
}
```

### Parameters

Parameters specify which values are configurable when the template runs.

Below is an example that illustrates two parameters – one for a 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."
        }
    }
}
```

## Variables

Variables define values used throughout the template. For example, you can define a storage account name one time as a variable and use that variable throughout the template. If the storage account name changes, you need to only update the variable.

Below is 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"
}
```

## Functions

Functions define procedures that you don't want to repeat throughout the template. Below is an example that creates a function to create a unique name that could be used when creating resources that have globally unique naming requirements.

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

```
        }
    }
}
],

```

## Resources

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

Below is an example that creates a public IP address resource.

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

In the above sample, the type of resource is `Microsoft.Network/publicIPAddresses`. Its name is read from the variables section and its location, or Azure region, is read from the parameters section.

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

## Outputs

Outputs define any information you'd like to receive when the template runs.

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

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

# Azure Quickstart Templates

Azure Quickstart templates are Resource Manager templates that are provided by the Azure community. Quickstart templates are available on GitHub.

To find a Resource Manager template that brings up a basic VM configuration, do the following.

1. Browse the **Quickstart template gallery**<sup>1</sup> to see what's available.

The screenshot shows the 'Most popular' section of the Azure Quickstart template gallery. It displays four templates in a grid:

- Create a Standard Storage Account**: This template creates a Standard Storage Account. It was created by Kay Singh and last updated on 12/4/2018.
- Create a Virtual Network with two Subnets**: This template allows you to create a Virtual Network with two subnets. It was created by Telmo Sampaio and last updated on 10/12/2018.
- Create an Azure VM with a new AD Forest**: This template creates a new Azure VM, it configures the VM to be an AD DC for a new Forest. It was created by Simon Davies and last updated on 7/4/2018.
- Join a VM to an existing domain**: This template demonstrates domain join to a private AD domain up in cloud. It was created by Kay Singh and last updated on 5/25/2018.

2. Select a Deploy a simple Windows VM template.

The screenshot shows the details page for the 'Deploy a simple Windows VM' template. It includes the following information:

- Templates / Deploy a simple Windows VM**
- Deploy a simple Windows VM**
- Created by Brian Moore
- Deploy to Azure** and **Browse on GitHub** buttons
- Description: 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.

The Deploy to Azure button enables you to deploy the template directly through the Azure portal. Additionally, you can use the Azure CLI to deploy the template from Cloud Shell.

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

<sup>1</sup> <https://azure.microsoft.com/resources/templates/>

## Very simple deployment of a Windows VM

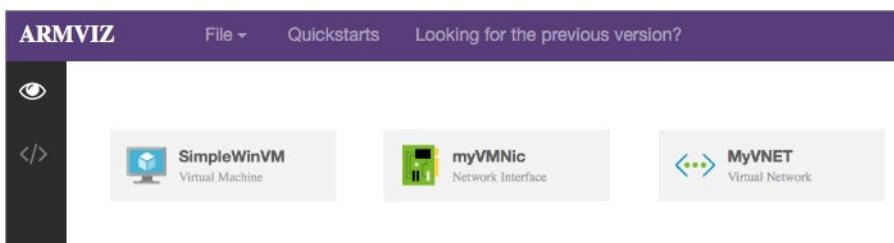
 Deploy to Azure

 Visualize

This template allows you to deploy a simple Windows VM using a few different options. You can choose the latest patched version. This will deploy a A2 size VM in the resource group location you specified. The name of the VM.

- Click **Visualize** to navigate to the Azure Resource Manager Visualizer.

You see the resources that make up the deployment, including a VM, a storage account, and network resources. You can use your mouse to arrange the resources.



- Click on the Virtual Machine resource labeled **SimpleWinVM**.

Below is the JSON that defines the VM resource.

The screenshot shows the ARMVIZ interface with a purple header bar. The header contains the title 'ARMVIZ' and navigation links 'File ▾', 'Quickstarts', and 'Looking for the previous version?'. Below the header, there's a sidebar with icons for 'eye' and 'refresh'. The main area displays the JSON code for the 'SimpleWinVM' resource, which is a 'Microsoft.Compute/virtualMachines' type resource. The code includes variables for name, location, apiVersion, dependsOn, properties (hardwareProfile, osProfile), and storageProfile (imageReference).

```

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        },

```

- The resource's type is `Microsoft.Compute/virtualMachines`.
- It's 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.

## Save a Template for a VM

### Download the Template for a VM

When you create a VM in Azure using the portal or PowerShell, a Resource Manager template is automatically created for you. You can use this template to quickly duplicate a deployment.

The template contains information about all the resources in a resource group. For a virtual machine, this means the template contains everything that is created in support of the VM in that resource group, including the networking resources.

#### Download the template using the portal

1. Log in to the [Azure portal<sup>2</sup>](https://portal.azure.com/).
2. On the left menu, select **Virtual Machines**.
3. Select the virtual machine from the list.
4. Select **Export template**.
5. Select **Download** from the menu at the top and save the .zip file to your local computer.
6. Open the .zip file and extract the files to a folder. The .zip file contains:
  - parameters.json
  - template.json

The template.json file is the template.

### Download the Template using PowerShell

You can also download the .json template file using the PowerShell Export-AzResourceGroup cmdlet. You can use the `-path` parameter to provide the **filename** and path for the .json file.

This example shows how to download the template for the resource group named **myResourceGroup** to the C:\users\public\downloads folder on your local computer.

```
Export-AzResourceGroup -ResourceGroupName "myResourceGroup" -Path "C:\users\public\downloads"
```

---

<sup>2</sup> <https://portal.azure.com/>

# Configure a Virtual Hard Disk Template

## Virtual Disk Images for Azure VMs

An Azure virtual machine runs in the cloud, in an Azure datacenter. When you create a virtual machine, you specify a virtual machine image to use. This image contains the operating system and (optionally) other preconfigured software.

Azure uses this image to create a new virtual hard disk (VHD) from which it can start your virtual machine. You can then customize the virtual machine by configuring and installing additional applications, according to your requirements.

In this topic, you'll see how you can use VHDs to create standard customized disks for building virtual machines for your organization.

### What is an Azure virtual hard disk?

A virtual machine can contain multiple VHDs. Typically, a virtual machine has an operating system VHD on which the operating system is installed. It also has one or more data VHDs that contain the applications and other user-specific data used by the virtual machine.

The difference between a VHD and a physical hard disk is that a VHD is stored as a virtual file in Azure. It isn't a piece of physical hardware.

### What is a virtual machine image?

If you consider a VHD to be like a physical disk, a virtual machine image is a template from which you can create the VHDs to run a virtual machine. The VHDs for a typical virtual machine image contain a pre-configured version of an operating system.

Azure Marketplace supplies many virtual machine images that you can use as a starting point for your own systems. Examples include:

- Various versions of Windows Server, optionally with SQL Server installed.
- Linux variants with software such as MySQL, MongoDB, Cassandra, or other databases already configured.

### What is a generalized image?

You can create your own custom virtual machine image in one of two ways:

- If you're building an image from scratch by using Hyper-V, you first create a blank virtual disk, and then create a virtual machine with this disk. When you start the virtual machine, you install the operating system and any other additional software from source disks (typically DVDs) and other packages.
- If you're customizing an image from Azure Marketplace, you build a virtual machine by using an existing image. The image provides the operating system and base functionality. You add your own software, operating system updates, and other packages as required. Unit 3 describes this process in more detail.

After you build and customize a virtual machine, you can save the new image as a set of VHDs.

### What is a specialized virtual image?

A specialized virtual image is a copy of a live virtual machine after it has reached a specific state. For example, a specialized image might contain a copy of the configured operating system, software, user accounts, databases, connection information, and other data for your system.

You can use a specialized virtual image as a backup of your system at a particular point in time. If you need to recover after a catastrophic failure, or you need to roll back the virtual machine, you can restore your virtual machine from this image.

If you use a specialized image to create a new virtual machine, the new virtual machine will retain all of the data from the image. That data includes the host name, user accounts, and other settings.

## Deploy an Azure VM from a VHD

This topic describes how to deploy a generalized VHD image to create a new Azure VM resource, using the supplied Azure Resource Manager template and Azure PowerShell script.

### VHD deployment template

Use the Azure Resource Manager template for **VHD deployment**<sup>3</sup> seen in the subsequent topic to a local file named *VHDtoImage.json*. Edit the file to provide values for the following parameters.

Parameter	Description
<b>ResourceGroupName</b>	Existing Azure resource group name. Typically use the same RG associated with your key vault
<b>TemplateFile</b>	Full pathname to the file <i>VHDtoImage.json</i>
<b>userStorageAccountName</b>	Name of the storage account
<b>sNameForPublicIP</b>	DNS name for the public IP. Must be lowercase
<b>subscriptionId</b>	Azure subscription identifier
<b>Location</b>	Standard Azure geographic location of the resource group
<b>vmName</b>	Name of the virtual machine
<b>vaultName</b>	Name of the key vault
<b>vaultResourceGroup</b>	Resource group of the key vault
<b>certificateUrl</b>	Url of the certificate, including version stored in the key vault, for example: <a href="https://testault.vault.azure.net/secrets/testcert/b621es1db241e56a72d037479xab1r7">https://testault.vault.azure.net/secrets/testcert/b621es1db241e56a72d037479xab1r7</a>
<b>vhdUrl</b>	URL of the virtual hard disk
<b>vmSize</b>	Size of the virtual machine instance
<b>publicIPAddressName</b>	Name of the public IP address
<b>virtualNetworkName</b>	Name of the virtual network
<b>nicName</b>	Name of the network interface card for the virtual network
<b>adminUserName</b>	Username of the administrator account
<b>adminPassword</b>	Administrator password

### Powershell script

Copy and edit the following script to supply values for the \$storageaccount and \$vhdUrl variables. Execute it to create an Azure VM resource from your existing generalized VHD.

```
# storage account of existing generalized VHD
$storageaccount = "testwinrm11815"
```

---

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/marketplace/cloud-partner-portal/virtual-machine/cpp-deploy-json-template>

```
# generalized VHD URL
$vhdUrl = "https://testwinrm11815.blob.core.windows.net/vhds/test-
vm1234562016651857.vhd"

echo "New-AzResourceGroupDeployment -Name "dplisvvm$postfix" -ResourceGroupName "$rgName" -TemplateFile "C:\certLocation\VHDtoImage.json" -userStorageAccountName "$storageaccount" -dnsNameForPublicIP "$vmName" -subscriptionId "$mysubid" -location "$location" -vmName "$vmName" -vaultName "$kvname" -vaultResourceGroup "$rgName" -certificateUrl $objAzureKeyVaultSecret.Id -vhdUrl "$vhdUrl" -vmSize "Standard_A2" -publicIPAddressName "myPublicIP1" -virtualNetworkName "myVNET1" -nicName "myNIC1" -adminUserName "isv" -adminPassword $pwd"

#deploying VM with existing VHD
New-AzResourceGroupDeployment -Name "dplisvvm$postfix" -ResourceGroupName "$rgName" -TemplateFile "C:\certLocation\VHDtoImage.json" -userStorageAccountName "$storageaccount" -dnsNameForPublicIP "$vmName" -subscriptionId "$mysubid" -location "$location" -vmName "$vmName" -vaultName "$kvname" -vaultResourceGroup "$rgName" -certificateUrl $objAzureKeyVaultSecret.Id -vhdUrl "$vhdUrl" -vmSize "Standard_A2" -publicIPAddressName "myPublicIP1" -virtualNetworkName "myVNET1" -nicName "myNIC1" -adminUserName "isv" -adminPassword $pwd
```

## Virtual Hard Disk Deployment Template

The Azure Resource Manager template below defines a new Azure virtual machine (VM) instance, created from local virtual hard disk (VHD).

The template below is for reference only, and is used in the previous topic entitled *Deploy an Azure VM from a VHD*.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2014-04-01-pre-
view/deploymentTemplate.json",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "userStorageAccountName": {
            "type": "string"
        },
        "userStorageContainerName": {
            "type": "string",
            "defaultValue": "vhds"
        },
        "dnsNameForPublicIP": {
            "type": "string"
        },
        "adminUserName": {
            "defaultValue": "isv",
            "type": "string"
        },
        "adminPassword": {
```

```
        "type": "securestring",
        "defaultValue": "Password@123"
    },
    "osType": {
        "type": "string",
        "defaultValue": "windows",
        "allowedValues": [
            "windows",
            "linux"
        ]
    },
    "subscriptionId": {
        "type": "string"
    },
    "location": {
        "type": "string"
    },
    "vmSize": {
        "type": "string"
    },
    "publicIPAddressName": {
        "type": "string"
    },
    "vmName": {
        "type": "string"
    },
    "virtualNetworkName": {
        "type": "string"
    },
    "nicName": {
        "type": "string"
    },
    "vaultName": {
        "type": "string",
        "metadata": {
            "description": "Name of the KeyVault"
        }
    },
    "vaultResourceGroup": {
        "type": "string",
        "metadata": {
            "description": "Resource Group of the KeyVault"
        }
    },
    "certificateUrl": {
        "type": "string",
        "metadata": {
            "description": "Url of the certificate with version in
KeyVault e.g. https://testault.vault.azure.net/secrets/testcert/b621es1d-
b241e56a72d037479xab1r7"
        }
    }
}
```

```
        },
        "vhdUrl": {
            "type": "string",
            "metadata": {
                "description": "VHD Url..."
            }
        }
    },
    "variables": {
        "addressPrefix": "10.0.0.0/16",
        "subnet1Name": "Subnet-1",
        "subnet2Name": "Subnet-2",
        "subnet1Prefix": "10.0.0.0/24",
        "subnet2Prefix": "10.0.1.0/24",
        "publicIPAddressType": "Dynamic",
        "vnetID": "[resourceId('Microsoft.Network/virtualNetworks',parameters('virtualNetworkName'))]",
        "subnet1Ref": "[concat(variables('vnetID'), '/subnets/', variables('subnet1Name'))]",
        "osDiskVhdName": "[concat('http://', parameters('userStorageAccountName'), '.blob.core.windows.net/', parameters('userStorageContainerName'), '/', parameters('vmName'), 'osDisk.vhd')]"
    },
    "resources": [
        {
            "apiVersion": "2015-05-01-preview",
            "type": "Microsoft.Network/publicIPAddresses",
            "name": "[parameters('publicIPAddressName')]",
            "location": "[parameters('location')]",
            "properties": {
                "publicIPAllocationMethod": "[variables('publicIPAddressType')]",
                "dnsSettings": {
                    "domainNameLabel": "[parameters('dnsNameForPublicIP')]"
                }
            }
        },
        {
            "apiVersion": "2015-05-01-preview",
            "type": "Microsoft.Network/virtualNetworks",
            "name": "[parameters('virtualNetworkName')]",
            "location": "[parameters('location')]",
            "properties": {
                "addressSpace": {
                    "addressPrefixes": [
                        "[variables('addressPrefix')]"
                    ]
                },
                "subnets": [
                    {

```

```
        "name": "[variables('subnet1Name')]",
        "properties": {
            "addressPrefix": "[variables('subnet1Pre-
fix')]"
        }
    },
    {
        "name": "[variables('subnet2Name')]",
        "properties": {
            "addressPrefix": "[variables('subnet2Pre-
fix')]"
        }
    }
]
}
},
{
    "apiVersion": "2015-05-01-preview",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[parameters('nicName')]",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[concat('Microsoft.Network/publicIPAddresses/', parameters('publicIPAddressName'))]",
        "[concat('Microsoft.Network/virtualNetworks/', parameters('virtualNetworkName'))]"
    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "privateIPAllocationMethod": "Dynamic",
                    "publicIPAddress": {
                        "id": "[resourceId('Microsoft.Network/
publicIPAddresses', parameters('publicIPAddressName'))]"
                    },
                    "subnet": {
                        "id": "[variables('subnet1Ref')]"
                    }
                }
            }
        ]
    }
},
{
    "apiVersion": "2015-06-15",
    "type": "Microsoft.Compute/virtualMachines",
    "name": "[parameters('vmName')]",
    "location": "[parameters('location')]",
    "dependsOn": [
```

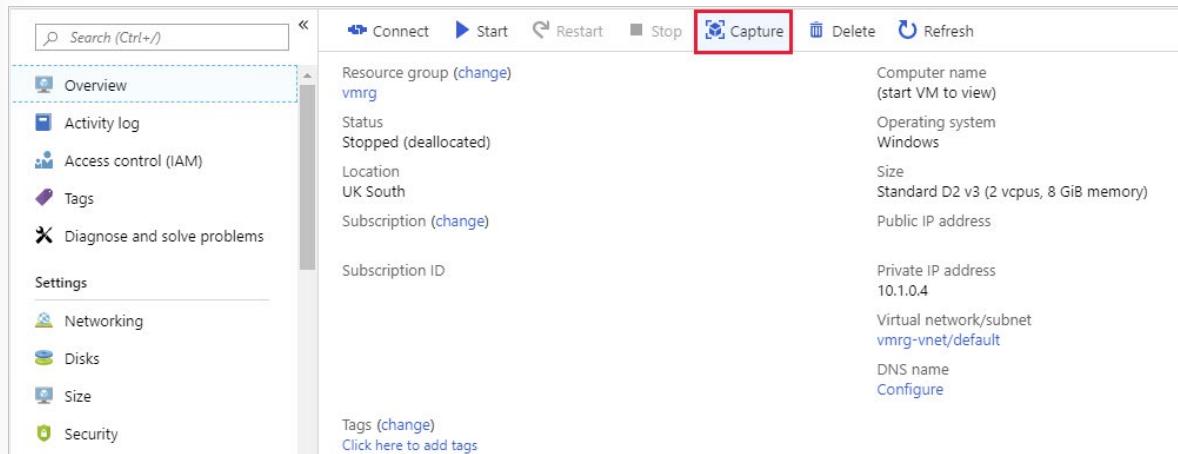
```
    "[concat('Microsoft.Network/networkInterfaces/', parameters('nicName'))]"
],
"properties": {
    "hardwareProfile": {
        "vmSize": "[parameters('vmSize')]"
    },
    "osProfile": {
        "computername": "[parameters('vmName')]",
        "adminUsername": "[parameters('adminUsername')]",
        "adminPassword": "[parameters('adminPassword')]",
        "secrets": [
            {
                "sourceVault": {
                    "id": "[resourceId(parameters('vaultResourceGroup'), 'Microsoft.KeyVault/vaults', parameters('vaultName'))]"
                },
                "vaultCertificates": [
                    {
                        "certificateUrl": "[parameters('certificateUrl')]",
                        "certificateStore": "My"
                    }
                ]
            }
        ],
        "windowsConfiguration": {
            "provisionVMAgent": "true",
            "winRM": {
                "listeners": [
                    {
                        "protocol": "http"
                    },
                    {
                        "protocol": "https",
                        "certificateUrl": "[parameters('certificateUrl')]"
                    }
                ]
            }
        },
        "enableAutomaticUpdates": "true"
    }
},
"storageProfile": {
    "osDisk": {
        "name": "[concat(parameters('vmName'), '-os-Disk')]",
        "osType": "[parameters('osType')]",
        "caching": "ReadWrite",
        "image": {
            "uri": "[parameters('vhdUrl')]"
        }
    }
}
```

```
        },
        "vhd": {
            "uri": "[variables('osDiskVhdName')]"
        },
        "createOption": "FromImage"
    }
},
"networkProfile": {
    "networkInterfaces": [
        {
            "id": "[resourceId('Microsoft.Network/networkInterfaces', parameters('nicName'))]"
        }
    ]
},
"diagnosticsProfile": {
    "bootDiagnostics": {
        "enabled": true,
        "storageUri": "[concat('http://', parameters('userStorageAccountName'), '.blob.core.windows.net')]"
    }
}
}
```

## Create a VM from a VHD

After you have generalized the virtual machine, you can create an image. The image will include all the disks associated with the virtual machine. You can create an image from the generalized virtual machine by using the Azure portal, the Azure CLI, or PowerShell.

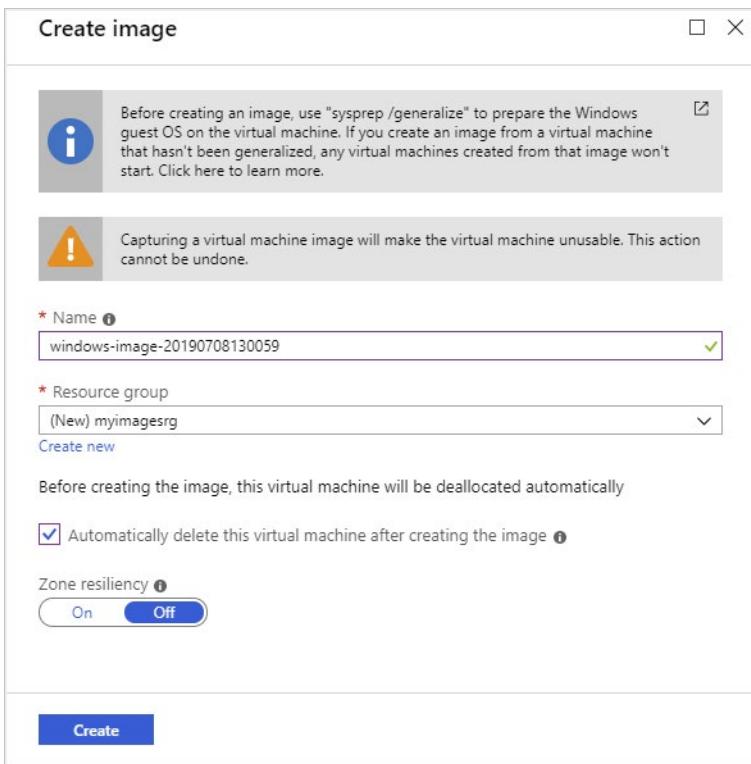
To create an image in the Azure portal, go to the page for the virtual machine and select Capture:



The screenshot shows the Azure portal interface for a virtual machine named 'vmrg'. The 'Capture' button in the top navigation bar is highlighted with a red box. The main content area displays the following details:

Setting	Value
Resource group (change)	vmrg
Status	Stopped (deallocated)
Location	UK South
Subscription (change)	
Subscription ID	
Computer name (start VM to view)	
Operating system	Windows
Size	Standard D2 v3 (2 vcpus, 8 GiB memory)
Public IP address	
Private IP address	10.1.0.4
Virtual network/subnet	vmrg-vnet/default
DNS name	Configure
Tags (change)	
Click here to add tags	

On the **Create image** page that follows, give your image a name and specify a resource group in which to store the image. You can optionally remove the virtual machine after the image is created.



### ✓ Important

When you create a virtual machine image in this way, the original virtual machine becomes unusable. You can't restart it. Instead, you must create a new virtual machine from the image, as described later in this unit.

If you're using PowerShell or the Azure CLI, you can create a virtual machine image from a generalized and deallocated virtual machine by using the following commands. In both examples, the image will be created in the same resource group as the original virtual machine:

```
$vm = Get-AzVM -ResourceGroupName <resource group>
-Name <generalized virtual machine>

$image = New-AzImageConfig -SourceVirtualMachineId ` 
$vm.ID -Location<virtual machine location>

New-AzImage -Image $image ` 
-ImageName <image name> ` 
-ResourceGroupName <resource group>

az image create \
--name <image name> \
--resource-group <resource group> \
--source <generalized virtual machine>
```

### Create a new virtual machine from a generalized image

You can build a new virtual machine by using your generalized image. The simplest way is to use the Azure portal. Go to the page for your image, and **select + Create VM**. You'll be prompted for the ma-

chine-specific details, such as the virtual machine name, user account, virtual machine size, and network ports to open.

Alternatively, you can use the PowerShell New-AzVm command, or the Azure CLI az vm create command. The following examples illustrate the syntax:

```
New-AzVm ` 
    -ResourceGroupName <resource group> ` 
    -Name <new virtual machine name> ` 
    -ImageName <image name> ` 
    -Location <location of image> ` 

az vm create \ 
    --resource-group <resource group> \ 
    --name <new virtual machine name> \ 
    --image <image name> \ 
    --location <location of image>
```

### Create a snapshot of a VHD

A virtual machine image contains an image of every VHD in the virtual machine. You can also create separate snapshot images of a VHD at any time.

Unlike creating an image of a virtual machine, capturing a snapshot of a VHD is a non-destructive process. You can continue running virtual machines by using the VHD afterward.

### Create a virtual machine from VHD snapshots

Rebuilding a virtual machine from a set of VHD snapshots is a two-step process:

1. For each snapshot, create a new managed disk. Specify the snapshot as the source of the managed disk. The simplest way is to use the Azure portal, as shown in the following image:

Home > New > Managed Disks > Create managed disk

## Create managed disk

Basics Tags Review + create

Select the disk type and size needed for your workload. Azure Disks are designed for 99.999% availability. Azure Managed Disks encrypt your data at rest, by default, using Storage Service Encryption. [Learn more about disks.](#)

PROJECT DETAILS

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

\* Subscription

  \* Resource group   
    (New) restoredisksrg   
    Create new

DISK DETAILS

\* Disk name

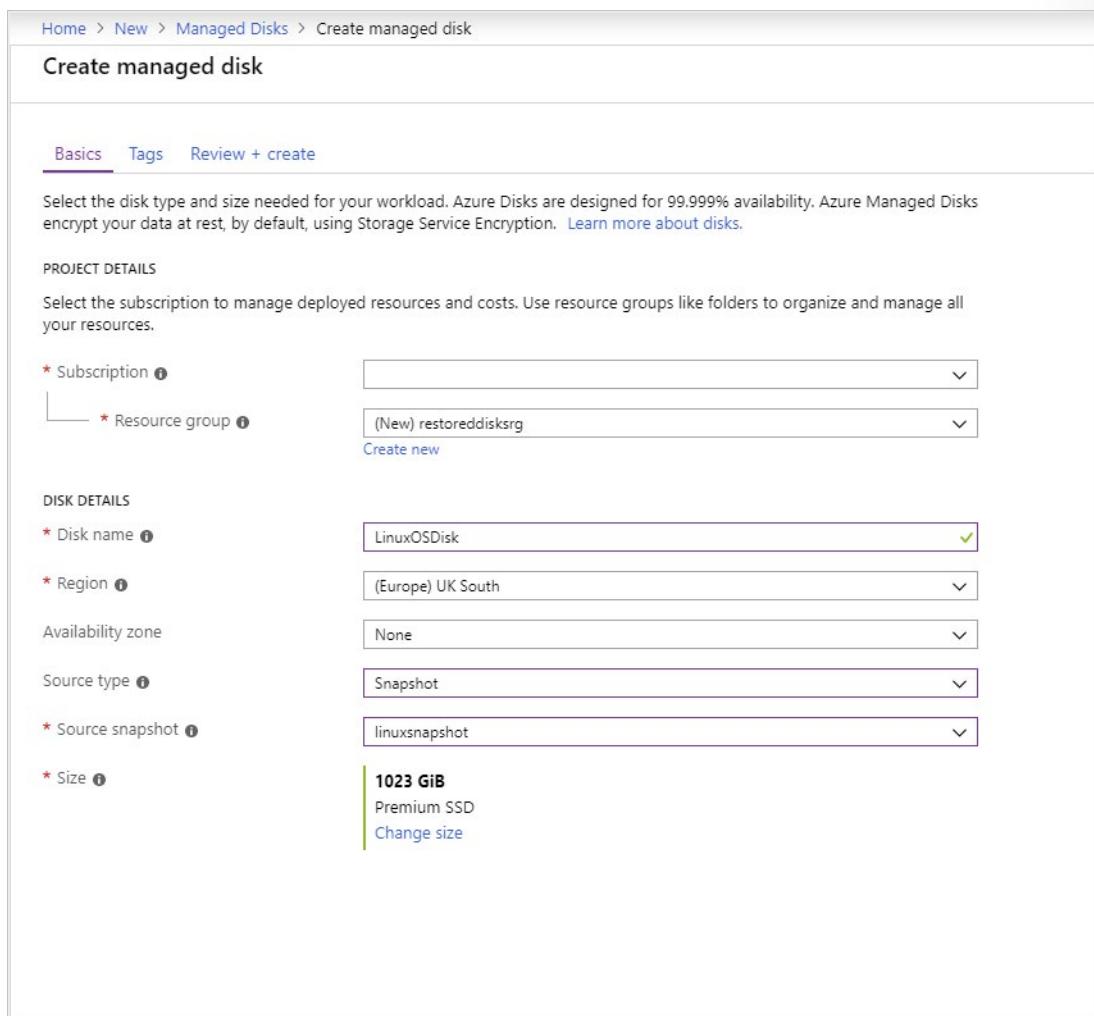
\* Region   
  (Europe) UK South

Availability zone   
  None

Source type   
  Snapshot

\* Source snapshot   
  linuxsnapshot

\* Size   
  1023 GiB  
  Premium SSD  
  Change size



2. Create the new virtual machine by using the managed disk. You can do this through PowerShell, the Azure CLI, or the portal.

# Deploy from a Template

## Create and Deploy from a ARM Template

This topic demonstrates how to create a simple ARM template and deploy it to Azure using Azure CLI.

**✓ Note:**

It is recommended you use Visual Studio Code with the Resource Manager Tools extension. If you need to install these tools, see **Use Visual Studio Code to create ARM templates<sup>4</sup>**.

### Command-line deployment

You need Azure CLI to deploy the template. For the installation instructions, see:

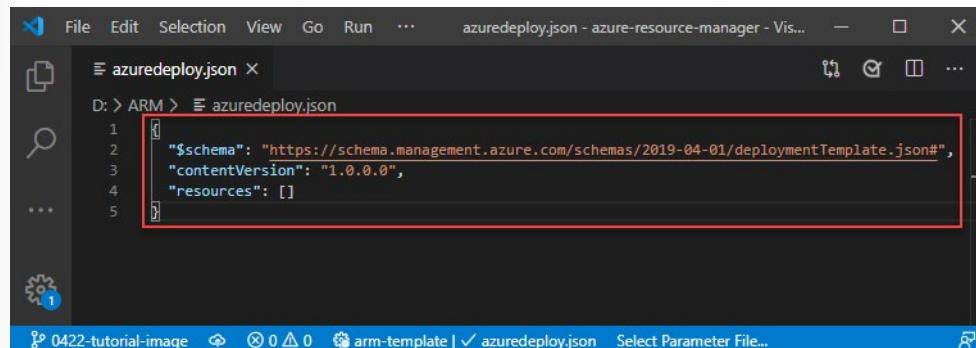
- **Install Azure CLI on Windows<sup>5</sup>**
- **Install Azure CLI on Linux<sup>6</sup>**

### Create the ARM template

1. Open Visual Studio Code with the Resource Manager Tools extension installed.
2. From the **File** menu, select **New File** to create a new file.
3. From the **File** menu, select **Save as**.
4. Name the file *azuredeploy* and select the JSON file extension. The complete name of the file is *azuredeploy.json*.
5. Save the file to your workstation.
6. Copy and paste the following JSON into the file:

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/  
deploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "resources": []  
}
```

Below is a sample of what the VS Code environment looks like:



**4** <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/use-vs-code-to-create-template>

**5** <https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows>

**6** <https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-linux>

Notice that this template doesn't deploy any resources. We're starting with a blank template so you can get familiar with the steps to deploy a template.

The JSON file has the following elements:

- `$schema`: Specifies the location of the JSON schema file. The schema file describes the properties that are available within a template. For example, the schema defines resources as one of the valid properties for a template.
- `contentVersion`: Specifies the 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.
- `resources`: Contains the resources you want to deploy or update. Currently, it's empty, but you'll add resources later.

7. Save the file.

### Sign in to Azure using Azure CLI

```
az login
```

### Create resource group

When you deploy a template, you specify a resource group that will contain the resources. Before running the deployment command, create the resource group with Azure CLI.

```
az group create \
--name myResourceGroup \
--location "Central US"
```

### Deploy template

To deploy the template you use Azure CLI. Use the resource group you created. Give a name to the deployment so you can easily identify it in the deployment history. For convenience, also create a variable that stores the path to the template file. This variable makes it easier for you to run the deployment commands because you don't have to retype the path every time you deploy.

```
templateFile="{provide-the-path-to-the-template-file}"
az deployment group create \
--name blanktemplate \
--resource-group myResourceGroup \
--template-file $templateFile
```

Look for `ProvisioningState` to see whether the deployment succeeded.

```
"parameters": {},  
"parametersLink": null,  
"providers": [],  
"provisioningState": "Succeeded",  
"template": null,  
"templateHash": "9132645722898483367",
```

### Verify deployment

You can verify the deployment by exploring the resource group from the Azure portal.

1. Sign in to the [Azure portal](#)<sup>7</sup>.
2. From the left menu, select **Resource groups**.
3. Select the resource group deploy in the last procedure. The default name is “myResourceGroup”. You should see no resources deployed within the resource group.
4. Notice in the upper right of the overview, the status of the deployment is displayed. Select **1 Succeeded**.

The screenshot shows the 'myResourceGroup - Deployments' page in the Azure portal. At the top, there are buttons for Delete, Cancel, Redeploy, View template, and Refresh. Below is a search bar with the placeholder 'Filter by deployment name or resources in the deployment...'. A table lists deployments with columns: DEPLOYMENT NAME, STATUS, LAST MODIFIED, DURATION, and RELATED EVENTS. One row is highlighted with a red box around the 'blanktemplate' name, showing a green checkmark icon and the text 'Succeeded'.

DEPLOYMENT NAME	STATUS	LAST MODIFIED	DURATION	RELATED EVENTS
blanktemplate	Succeeded	9/7/2019, 11:49:17 AM	4 seconds	<a href="#">Related events</a>

5. You see a history of deployment for the resource group. Select blanktemplate.

This screenshot is identical to the one above, showing the 'myResourceGroup - Deployments' page. It displays the same deployment history, with the 'blanktemplate' entry highlighted by a red box.

6. You see a summary of the deployment. Notice on the left you can view inputs, outputs, and the template used during deployment.

The screenshot shows the 'blanktemplate - Overview' page. On the left is a navigation sidebar with links for Overview, Inputs, Outputs, and Template. The main area has a search bar and buttons for Delete, Cancel, Redeploy, and Refresh. A prominent message says 'Your deployment is complete' with a green checkmark icon. To the right, deployment details are listed: Deployment name: blanktemplate, Subscription: Documentation Testing 1, Resource group: myResourceGroup. Below this, deployment details are shown with a download link. A table at the bottom shows resource status with the message 'No results.'

### Clean up resources

1. From the Azure portal, select **Resource group** from the left menu.

<sup>7</sup> <https://portal.azure.com/>

2. Enter the resource group name in the Filter by name field.
3. Select the resource group name.
4. Select **Delete resource group** from the top menu.

## Deploy an Azure Resource Manager Template using CLI

This topic is based upon the sample template for deploying an Azure Storage Account using CLI further below.

This topic and dives deeper into the underlying JSON demonstrated in the previous topic.

### Create resource group

When you deploy a template, you specify a resource group that will contain the resources. Before running the deployment command, create the resource group with either Azure CLI or Azure PowerShell.

Use the following Azure CLI to specify a resource group.

```
echo "Enter a project name that is used to generate resource and resource
group names:"
read projectName
resourceGroupName="${projectName}rg"

az group create \
--name $resourceGroupName \
--location "Central US"
```

### Deploy template

Use the following Azure CLI to deploy the template.

```
echo "Enter the same project name:"
read projectName
echo "Enter the template file path and file name:"
read templateFile
resourceGroupName="${projectName}rg"

az deployment group create \
--name DeployLocalTemplate \
--resource-group $resourceGroupName \
--template-file $templateFile \
--parameters projectName=$projectName \
--verbose
```

### Sample deployment of an Azure storage account

Below is the JSON for demonstrating the creating a resource group and deploying a ARM template.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploy-
mentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
```

```
"projectName": {
    "type": "string",
    "minLength": 3,
    "maxLength": 11,
    "metadata": {
        "description": "Specify a project name that is used to generate resource names."
    }
},
"location": {
    "type": "string",
    "defaultValue": "[resourceGroup().location]",
    "metadata": {
        "description": "Specify a location for the resources."
    }
},
"storageSKU": {
    "type": "string",
    "defaultValue": "Standard_LRS",
    "allowedValues": [
        "Standard_LRS",
        "Standard_GRS",
        "Standard_RAGRS",
        "Standard_ZRS",
        "Premium_LRS",
        "Premium_ZRS",
        "Standard_GZRS",
        "Standard_RAGZRS"
    ],
    "metadata": {
        "description": "Specify the storage account type."
    }
},
"linuxFxVersion": {
    "type": "string",
    "defaultValue": "php|7.0",
    "metadata": {
        "description": "Specify the Runtime stack of current web app"
    }
}
},
"variables": {
    "storageAccountName": "[concat(parameters('projectName'), 'store')]",
    "webAppName": "[concat(parameters('projectName'), 'WebApp')]",
    "appServicePlanName": "[concat(parameters('projectName'), 'Plan')]"
},
"resources": [
{
    "type": "Microsoft.Storage/storageAccounts",
    "apiVersion": "2019-04-01",
    "name": "[variables('storageAccountName')]"
},
```

```
    "location": "[parameters('location')]",
    "sku": {
        "name": "[parameters('storageSKU')]"
    },
    "kind": "StorageV2",
    "properties": {
        "supportsHttpsTrafficOnly": true
    }
},
{
    "type": "Microsoft.Web/serverfarms",
    "apiVersion": "2016-09-01",
    "name": "[variables('appServicePlanName')]",
    "location": "[parameters('location')]",
    "sku": {
        "name": "B1",
        "tier": "Basic",
        "size": "B1",
        "family": "B",
        "capacity": 1
    },
    "kind": "linux",
    "properties": {
        "perSiteScaling": false,
        "reserved": true,
        "targetWorkerCount": 0,
        "targetWorkerSizeId": 0
    }
},
{
    "type": "Microsoft.Web/sites",
    "apiVersion": "2018-11-01",
    "name": "[variables('webAppName')]",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[resourceId('Microsoft.Web/serverfarms', variables('appServicePlanName'))]"
    ],
    "kind": "app",
    "properties": {
        "serverFarmId": "[resourceId('Microsoft.Web/serverfarms', variables('appServicePlanName'))]",
        "siteConfig": {
            "linuxFxVersion": "[parameters('linuxFxVersion')]"
        }
    }
},
{
    "outputs": {
        "storageEndpoint": {
            "type": "object",

```

```
        "value": "[reference(variables('storageAccountName')).primaryEnd-
points]"
    }
}
}
```

# Create and Execute an Automation Runbook

## Runbooks in Azure Automation

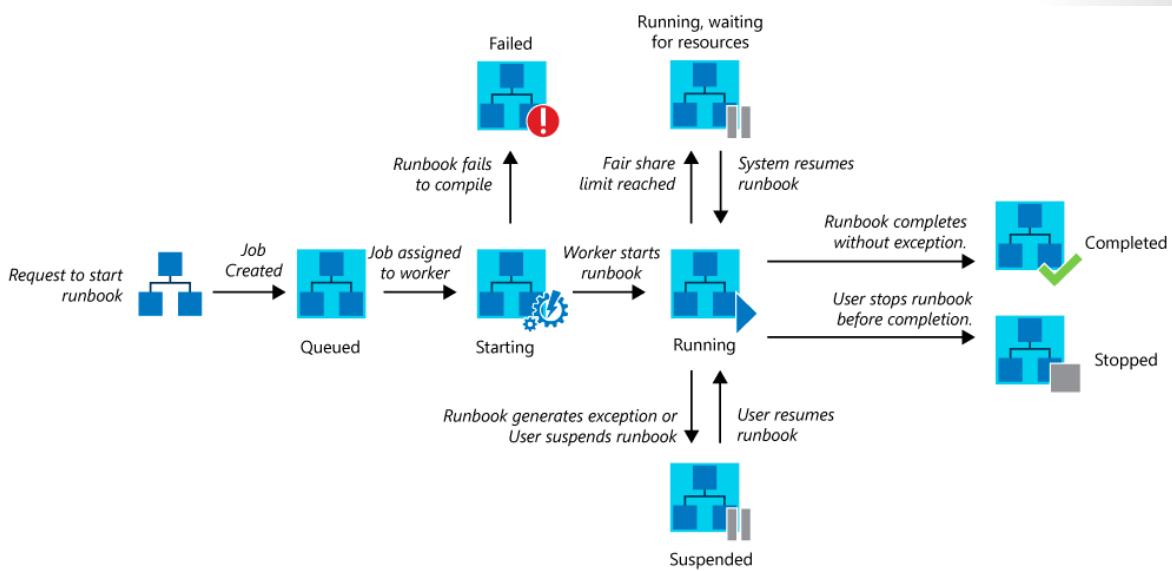
Process automation in Azure Automation allows you to create and manage PowerShell, PowerShell Workflow, and graphical runbooks.

Automation executes your runbooks based on the logic defined inside them. If a runbook is interrupted, it restarts at the beginning. This behavior requires you to write runbooks that support being restarted if transient issues occur.

Starting a runbook in Azure Automation creates a job, which is a single execution instance of the runbook. Each job accesses Azure resources by making a connection to your Azure subscription. The job can only access resources in your data center if those resources are accessible from the public cloud.

Azure Automation assigns a worker to run each job during runbook execution. While workers are shared by many Azure accounts, jobs from different Automation accounts are isolated from one another. You can't control which worker services your job requests.

The following diagram shows the lifecycle of a runbook job for PowerShell runbooks, PowerShell Workflow runbooks, and graphical runbooks.



### Where to run runbooks

Runbooks in Azure Automation can run on either an Azure sandbox or a Hybrid Runbook Worker. When runbooks are designed to authenticate and run against resources in Azure, they run in an Azure sandbox, which is a shared environment that multiple jobs can use. Jobs using the same sandbox are bound by the resource limitations of the sandbox.

You can use a Hybrid Runbook Worker to run runbooks directly on the computer that hosts the role and against local resources in the environment. Azure Automation stores and manages runbooks and then delivers them to one or more assigned computers.

The following table lists some runbook execution tasks with the recommended execution environment listed for each.

Task	Recommendation	Notes
Integrate with Azure resources	Azure Sandbox	Hosted in Azure, authentication is simpler. If you're using a Hybrid Runbook Worker on an Azure VM, you can use managed identities for Azure resources.
Obtain optimal performance to manage Azure resources	Azure Sandbox	Script is run in the same environment, which has less latency.
Minimize operational costs	Azure Sandbox	There is no compute overhead and no need for a VM.
Execute long-running script	Hybrid Runbook Worker	Azure sandboxes have resource limits.
Interact with local services	Hybrid Runbook Worker	Can directly access the host machine, or resources in other cloud environments, or in your on-premises environment.
Require third-party software and executables	Hybrid Runbook Worker	You manage the operating system and can install software.
Monitor a file or folder with a runbook	Hybrid Runbook Worker	Use a Watcher task on a Hybrid Runbook Worker.
Run a resource-intensive script	Hybrid Runbook Worker	Azure sandboxes have resource limits.
Use modules with specific requirements	Hybrid Runbook Worker	Some examples are: WinSCP - dependency on winscp.exe IIS administration - dependency on enabling or managing IIS.
Install a module with an installer	Hybrid Runbook Worker	Modules for sandbox must support copying.
Use runbooks or modules that require .NET Framework version different from 4.7.2	Hybrid Runbook Worker	Automation sandboxes support .NET Framework 4.7.2, and upgrading to a different version is not supported.
Run scripts that require elevation	Hybrid Runbook Worker	Sandboxes don't allow elevation. With a Hybrid Runbook Worker, you can turn off UAC and use Invoke-Command when running the command that requires elevation.
Run scripts that require access to Windows Management Instrumentation (WMI)	Hybrid Runbook Worker	Jobs running in sandboxes in the cloud can't access WMI provider.

## Import a PowerShell Runbook from the Runbook Gallery

1. In the Azure portal, open your Automation account.
2. Select **Runbooks gallery** under **Process Automation**.

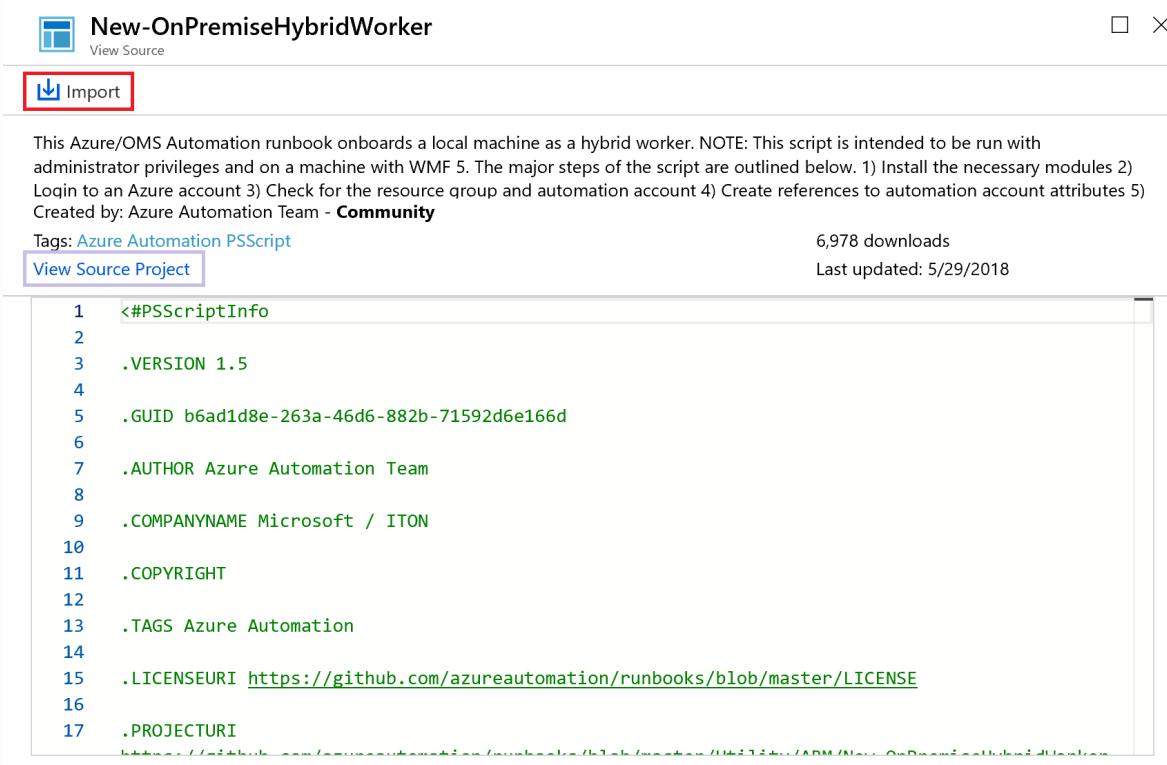
3. Select **Source: PowerShell Gallery**.
4. Locate the gallery item you want and select it to view its details. On the left, you can enter additional search parameters for the publisher and type.

The screenshot shows the 'TestAzureAuto - Runbooks gallery' page. On the left, there's a sidebar with categories like 'Process Automation' (Runbooks, Jobs, Runbooks gallery), 'Shared Resources' (Schedules, Modules, Modules gallery, Python 2 packages, Credentials), and a search bar. The main area displays three PowerShell Runbook items:

- Get-WindowsAutoPilotInfo**: PowerShell Runbook. Description: This script uses WMI to retrieve properties needed by the Microsoft Store for Business to support Windows AutoPilot deployment. See <https://blogs.technet.microsoft.com/mniehaus/2017/12/12/gathering-windows-autopilot-tags/>. Created by: Michael Niehaus, 195,361 downloads, Last updated: 2/16/2018.
- Install-DockerOnWS2016UsingDSC**: PowerShell Runbook. Description: Installs Docker on a Windows Server 2016 server using DSC. This function will: Tags: DSC Docker Containers PSScript. Created by: Daniel Scott-Raynsford, 62,759 downloads, Last updated: 10/15/2016.
- SharePointDSC.Reverse**: PowerShell Runbook. Description: Extracts the DSC Configuration of an existing SharePoint 2013, 2016 or 2019 environment, allowing you to analyze it or to replicate the farm. Tags: SharePoint ReverseDSC DesiredStateConfiguration DSC DSCResourceKit DSCResource PSScript. Created by: Microsoft Corporation, 32,507 downloads, Last updated: 2/6/2019.

5. Click on **View source project** to view the item in the **TechNet Script Center**<sup>8</sup>.
6. To import an item, click on it to view its details and then click **Import**.

<sup>8</sup> <https://gallery.technet.microsoft.com/>



This Azure/OMS Automation runbook onboards a local machine as a hybrid worker. NOTE: This script is intended to be run with administrator privileges and on a machine with WMF 5. The major steps of the script are outlined below. 1) Install the necessary modules 2) Login to an Azure account 3) Check for the resource group and automation account 4) Create references to automation account attributes 5) Created by: Azure Automation Team - **Community**

Tags: Azure Automation PSScript      6,978 downloads  
View Source Project      Last updated: 5/29/2018

```
1 <#PSScriptInfo
2
3 .VERSION 1.5
4
5 .GUID b6ad1d8e-263a-46d6-882b-71592d6e166d
6
7 .AUTHOR Azure Automation Team
8
9 .COMPANYNAME Microsoft / ITON
10
11 .COPYRIGHT
12
13 .TAGS Azure Automation
14
15 .LICENSEURI https://github.com/azureautomation/runbooks/blob/master/LICENSE
16
17 .PROJECTURI
```

**ATTENTION**

Each runbook is licensed to you under a license agreement by its owner, not Microsoft. Microsoft is not responsible for runbooks provided & licensed by the community members and does not screen for security, compatibility or performance. The runbooks are not supported under any Microsoft support program or service. The runbooks are provided AS IS without warranty of any kind.

7. Optionally, change the name of the runbook and then click **OK** to import the runbook.
8. The runbook appears on the **Runbooks** tab for the Automation account.

**Add a PowerShell runbook to the gallery**

Microsoft encourages you to add runbooks to the PowerShell Gallery that you think would be useful to other customers. The PowerShell Gallery accepts PowerShell modules and PowerShell scripts. You can add a runbook by [uploading it to the PowerShell Gallery<sup>9</sup>](#).

**Import a module from the module gallery with the Azure portal**

1. In the Azure portal, open your Automation account.
2. Select **Modules** under **Shared Resources** to open the list of modules.
3. Click **Browse gallery** from the top of the page.

<sup>9</sup> <https://docs.microsoft.com/en-us/powershell/scripting/gallery/how-to/publishing-packages/publishing-a-package>

The screenshot shows the 'TestAzureAuto - Modules' page in the Azure portal. The left sidebar has 'Modules' selected. The main area displays a table of modules:

NAME	LAST MODIFIED	STATUS	VERSION
Azure	1/2/2018 1:14 PM	Available	5.1.1
Azure.Storage	1/2/2018 1:12 PM	Available	4.0.2
AzureRM.Automation	1/2/2018 1:12 PM	Available	4.1.1
AzureRM.Compute	1/2/2018 1:12 PM	Available	4.1.1
AzureRM.Profile	1/2/2018 1:11 PM	Available	4.1.1
AzureRM.Resources	1/2/2018 1:12 PM	Available	5.1.1

4. On the **Browse gallery** page, you can search by the following fields:
  - Module Name
  - Tags
  - Author
  - Cmdlet/DSC resource name
5. Locate a module that you're interested in and select it to view its details.

The screenshot shows the 'Posh-SSH' PowerShell Module page on the PowerShell Gallery. The top navigation bar says 'PowerShell Module'. The main content includes:

- Import** button
- Description: Provide SSH and SCP functionality for executing commands against remote hosts.
- Created by:** cperez
- Tags:** PSModule
- View Source Project**
- Learn more** section with links to View in PowerShell Gallery, Documentation, and Licensing Information (PowerShell Gallery Default).
- Version:** 2.0.2
- 320,993 downloads**
- Last updated:** 10/13/2017

**Content** table:

TYPE	NAME
Cmdlet	Get-SCPFile
Cmdlet	Get-SCPFolder
Cmdlet	Get-SFTPFile
Cmdlet	Set-SFTPFile
Cmdlet	New-SFTPSession
Cmdlet	New-SSHSession
Cmdlet	Set-SCPFile

6. To install the module directly into Azure Automation, click **Import**.

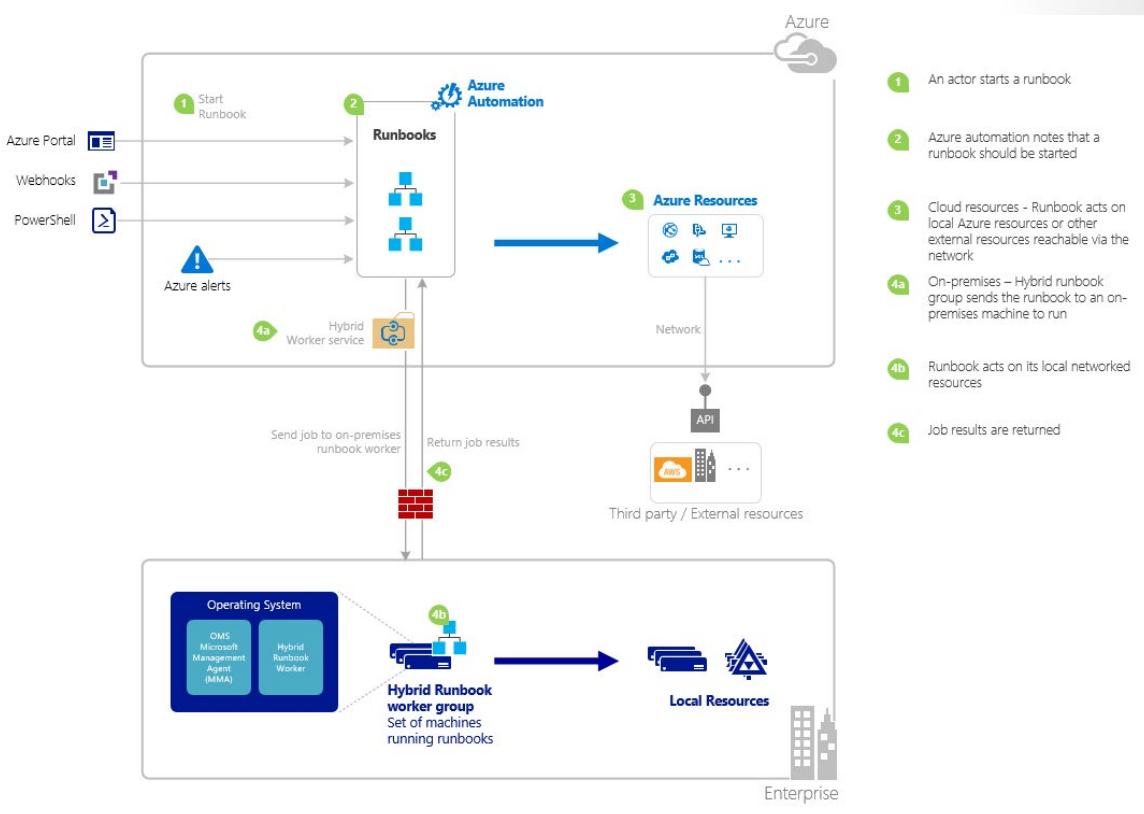
7. On the **Import** pane, you can see the name of the module to import. If all the dependencies are installed, the **OK** button is activated.
8. On the **Import** pane, click **OK** to import the module. While Azure Automation imports a module to your account, it extracts metadata about the module and the cmdlets.
9. You receive an initial notification that the module is being deployed and another notification when it has completed.

## Start a Runbook in Azure Automation

The following table helps you determine the method to start a runbook in Azure Automation that is most suitable to your scenario. This topic includes details on starting a runbook with the Azure portal and with Windows PowerShell.

Method	Characteristics
Azure portal	Simplest method with interactive user interface. Form to provide simple parameter values. Easily track job state. Access authenticated with Azure sign in.
Windows PowerShell	Call from command line with Windows PowerShell cmdlets. Can be included in automated solution with multiple steps. Request is authenticated with certificate or OAuth user principal / service principal. Provide simple and complex parameter values. Track job state. Client required to support PowerShell cmdlets.

The following image illustrates detailed step-by-step process in the life cycle of a runbook. It includes different ways a runbook starts in Azure Automation, which components required for Hybrid Runbook Worker to execute Azure Automation runbooks and interactions between different components.



## Runbook parameters

When you start a runbook from the Azure portal or Windows PowerShell, the instruction is sent through the Azure Automation web service. This service doesn't support parameters with complex data types. If you need to provide a value for a complex parameter, then you must call it inline from another runbook as described in **Child runbooks in Azure Automation**<sup>10</sup>.

### Start a runbook with the Azure portal

1. In the Azure portal, select **Automation** and then click the name of an Automation account.
2. On the Hub menu, select **Runbooks**.
3. On the **Runbooks** page, select a runbook, and then click **Start**.
4. If the runbook has parameters, you're prompted to provide values with a text box for each parameter. For more information on parameters, see **Runbook Parameters**<sup>11</sup>.
5. On the **Job** pane, you can view the status of the runbook job.

### Start a runbook with PowerShell

You can use the `Start-AzAutomationRunbook` to start a runbook with Windows PowerShell. The following sample code starts a runbook called `Test-Runbook`.

```
Start-AzAutomationRunbook -AutomationAccountName "MyAutomationAccount"
-Name "Test-Runbook" -ResourceGroupName "ResourceGroup01"
```

<sup>10</sup> <https://docs.microsoft.com/en-us/azure/automation/automation-child-runbooks>

<sup>11</sup> [https://docs.microsoft.com/en-us/azure/automation/start-runbooks?WT.mc\\_id=thomasmaurer-blog-thmaure](https://docs.microsoft.com/en-us/azure/automation/start-runbooks?WT.mc_id=thomasmaurer-blog-thmaure)

`Start-AzAutomationRunbook` returns a job object that you can use to track status once the runbook is started. You can then use this job object with `Get-AzAutomationJob` to determine the status of the job and `Get-AzAutomationJobOutput` to retrieve its output. The following example starts a runbook called `Test-Runbook`, waits until it has completed, and then displays its output.

```
$runbookName = "Test-Runbook"
$ResourceGroup = "ResourceGroup01"
$AutomationAcct = "MyAutomationAccount"

$job = Start-AzAutomationRunbook -AutomationAccountName $AutomationAcct
-Name $runbookName -ResourceGroupName $ResourceGroup

$doLoop = $true
While ($doLoop) {
    $job = Get-AzAutomationJob -AutomationAccountName $AutomationAcct -Id
$job.JobId -ResourceGroupName $ResourceGroup
    $status = $job.Status
    $doLoop = (($status -ne "Completed") -and ($status -ne "Failed") -and
($status -ne "Suspended") -and ($status -ne "Stopped"))
}
Get-AzAutomationJobOutput -AutomationAccountName $AutomationAcct -Id $job.
JobId -ResourceGroupName $ResourceGroup -Stream Output
```

If the runbook requires parameters, then you must provide them as a hashtable. The key of the hashtable must match the parameter name and the value is the parameter value. The following example shows how to start a runbook with two string parameters named **FirstName** and **LastName**, an integer named **RepeatCount**, and a boolean parameter named **Show**.

```
$params = @{"FirstName"="Joe"; "LastName"="Smith"; "RepeatCount"=2; "-
Show"=$true}
Start-AzureRmAutomationRunbook -AutomationAccountName "MyAutomationAccount"
-Name "Test-Runbook" -ResourceGroupName "ResourceGroup01" -Parameters
$params
```

## Demonstration-Create and run a workflow run-book

This walkthrough will create a new PowerShell workflow runbook, test, publish and then run the runbook.

### Prerequisites

- ✓ Note: You require an Azure subscription to perform the following steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today<sup>12</sup>](#) webpage.

---

<sup>12</sup> [https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm\\_source=microsoft.com&utm\\_medium=docs&utm\\_campaign=visualstudio](https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio)

## Steps

### Create a new runbook

1. In the **Azure portal**, open your Automation account.
2. Under **Process Automation**, select **Runbooks** to open the list of runbooks.
3. Create a new runbook by selecting the **Create a new runbook**.
4. Give the runbook the name **MyFirstRunbook-Workflow**.
5. You're going to create a PowerShell Workflow runbook, so for **Runbook type**, select **Powershell Workflow**.
6. Select **Create** to create the runbook and open the text editor.

### Add code to a runbook

You have two options when adding code to a runbook. You can type code directly into the runbook, or you can select cmdlets, runbooks, and assets from the Library control and have them added to the runbook, along with any related parameters.

For this walkthrough, you'll use the type directly into the runbook method, as detailed in the following steps:

1. Type **Write-Output "Hello World."** between the braces, as per the below:

```
Workflow MyFirstRunbook-Workflow
{
    Write-Output "Hello World"
}
```

2. Save the runbook by selecting **Save**.



### Test the runbook

Before you publish the runbook to production, you want to test it to ensure that it works properly. When you test a runbook, you run the draft version and view its output interactively, as demonstrated in the following steps:

1. Select the **Test** pane.

The screenshot shows the 'Edit PowerShell Workflow Runbook\*' interface for 'MyFirstRunbook-Workflow'. On the left, there's a sidebar with 'CMDLETS', 'RUNBOOKS', and 'ASSETS' sections. The main area contains the PowerShell script:

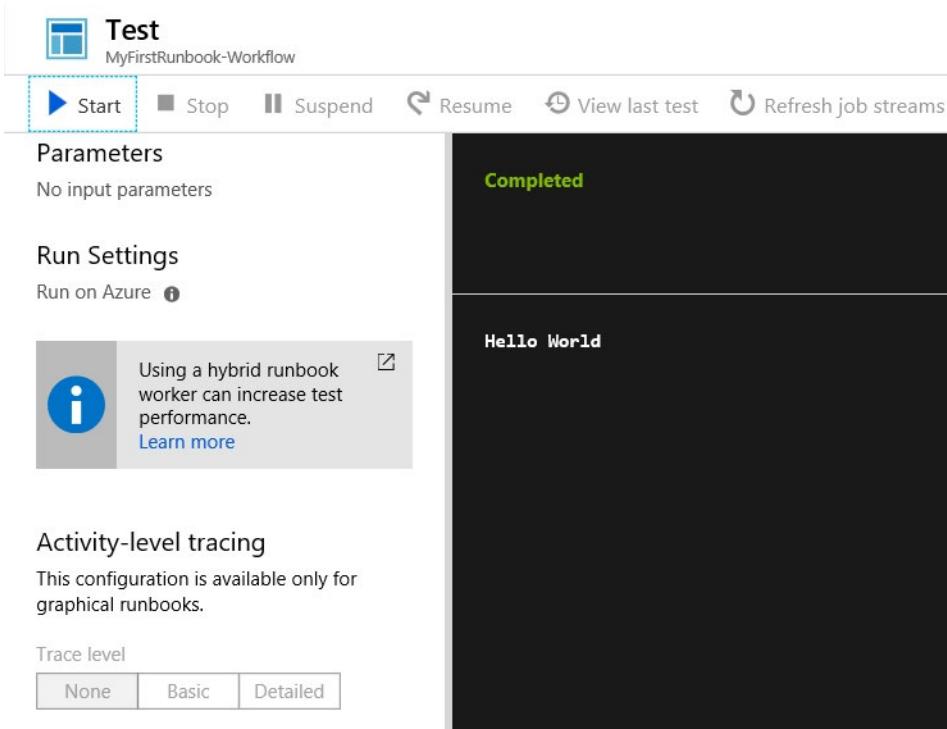
```
1 workflow MyFirstRunbook-Workflow
2 {
3     Write-Output "Hello World"
4 }
```

2. Select **Start** to start the test. This should be the only enabled option.

The screenshot shows the 'Test' page for 'MyFirstRunbook-Workflow'. The top navigation bar includes 'Start' (highlighted with a red box), 'Stop', 'Suspend', 'Resume', 'View last test', and 'Refresh job streams'. Below this, the 'Parameters' section indicates 'No input parameters'. The 'Run Settings' section shows 'Run on Azure' with a status icon. A tooltip message says: 'Using a hybrid runbook worker can increase test performance.' A link to 'Learn more' is provided. The main pane displays a message: 'Click 'Start' to begin the test run. Streams will display when the test completes.' At the bottom, there's an 'Activity-level tracing' section with a note about graphical runbooks and trace level options: 'None', 'Basic', and 'Detailed'.

A runbook job is created and its status displayed. The job status will start as Queued indicating that it is waiting for a runbook worker in the cloud to come available. It moves to Starting when a worker claims the job, and then Running when the runbook actually starts running. When the runbook job completes, its output displays. In your case, you should see Hello World.

3. When the runbook job finishes, close the **Test pane**.



## Publish and run the runbook

The runbook that you created is still in draft mode. You need to publish it before you can run it in production. When you publish a runbook, you overwrite the existing published version with the draft version. In your case, you don't have a published version yet because you just created the runbook.

Use the following steps to publish your runbook:

1. In the runbook editor, select **Publish** to publish the runbook.
2. When prompted, select **Yes**.
3. Scroll left to view the runbook in the Runbooks pane, and ensure that it shows an **Authoring Status of Published**.
4. Scroll back to the right to view the pane for **MyFirstRunbook-Workflow**. Notice the options across the top:
  - Start
  - View
  - Edit
  - Link to schedule to start at some time in the future
  - Add a webhook
  - Delete
  - Export

The screenshot shows the Azure portal interface for a runbook named 'MyFirstRunbook-Workflow'. The left sidebar has a search bar and links for Overview, Activity log, Tags, Diagnose and solve problems, Jobs, Schedules, Webhooks, Runbook settings, and Properties. The main content area displays the runbook's properties:

Resource group	az-auto-rg	Account	az-auto-ac-1	Location	West Europe
Subscription	Pay-As-You-Go	Subscription ID	974e6e39-73eb-48b0-9226-dae31425c367	Status	Published
Runbook type	PowerShell Workflow Runbook	Last modified	1/11/2019 10:14 AM		
Tags ( <a href="#">change</a> ) Click here to add tags					
<b>Recent Jobs</b>					
<b>STATUS</b>		<b>CREATED</b>		<b>LAST UPDATED</b>	
No jobs found.					

5. You just want to start the runbook, so select **Start**, and then when prompted, select **Yes**.
6. When the job pane opens for the runbook job that you created, leave it open so you can watch the job's progress.
7. Verify that at when the job completes, the job statuses that display in **Job Summary** match the statuses that you saw when you tested the runbook.

 MyFirstRunbook-Workflow 1/11/2019 10:16 AM

□ X

► Resume ■ Stop || Suspend

Essentials ^

Job Id d91f3e85-7196-4fa8-8355-d88c0790ec8c	Created 1/11/2019 10:16 AM
Job status Completed	Last Update 1/11/2019 10:17 AM
Run As User	Runbook <a href="#">MyFirstRunbook-Workflow</a>
Ran on Azure	Source snapshot <a href="#">View source snapshot</a>

Overview

<b>Input</b> 0 	<b>Output</b>  Output	 All Logs
<b>Errors</b> 0 	<b>Warnings</b> 0 	

Exception

None

## Module 9 Review Questions

### Module 9 Review Questions



#### Review Question 1

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

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

#### Review Question 2

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

- Resources can be in only one resource group.
- Resources can be moved from one resource group to another resource group.
- Resource groups can be nested.
- Role-based access control can be applied to the resource group.

#### Review Question 3

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

- Location
- Name
- Region
- Subscription
- Tag

# Answers

## Review Question 1

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

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

*Explanation*

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

## Review Question 2

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

- Resources can be in only one resource group.
- Resources can be moved from one resource group to another resource group.
- Resource groups can be nested.
- Role-based access control can be applied to the resource group.

*Explanation*

*Resource groups cannot be nested.*

## Review Question 3

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

- Location
- Name
- Region
- Subscription
- Tag

*Explanation*

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



## Module 10 Implement and Manage Azure Governance Solutions

### Overview of Role-Based Access Control (RBAC)

#### Role-Based Access Control (RBAC)

Role-based access control (RBAC) is an authorization system built on Azure Resource Manager that provides fine-grained access management of resources in Azure. With RBAC, you can grant the exact access that users need to do their jobs.

#### What is role-based access control?

You grant access by assigning the appropriate RBAC role to users, groups, and applications at a certain scope. The scope of a role assignment can be a subscription, a resource group, or a single resource. A role assigned at a parent scope also grants access to the child scopes contained within it.

Below are scenarios you can implement with RBAC.

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

#### RBAC in the Azure portal

In several areas in the Azure portal, you'll see a pane named **Access control (IAM)**, also known as identity and access management. On this pane, you can see who has access to that area and their role. Using this same pane, you can grant or remove access.

The following shows an example of the Access control (IAM) pane for a resource group. In this example, Alain Charon has been assigned the Backup Operator role for this resource group.

The screenshot shows the Azure portal's Access control (IAM) blade for the 'sales-projectforecast' resource group. The 'Access control (IAM)' tab is selected. On the left, there's a sidebar with various navigation options like Overview, Activity log, and Tags. The main area displays a table of role assignments:

NAME	TYPE	ROLE	SCOPE
AC	User	Backup Operator	This resource
SA	Group	Billing Reader	Subscription (Inherited)

## How RBAC Works

You control access to resources using RBAC by creating role assignments, which control how permissions are enforced. To create a role assignment, you need three elements: a security principal, a role definition, and a scope. You can think of these elements as "who", "what", and "where".

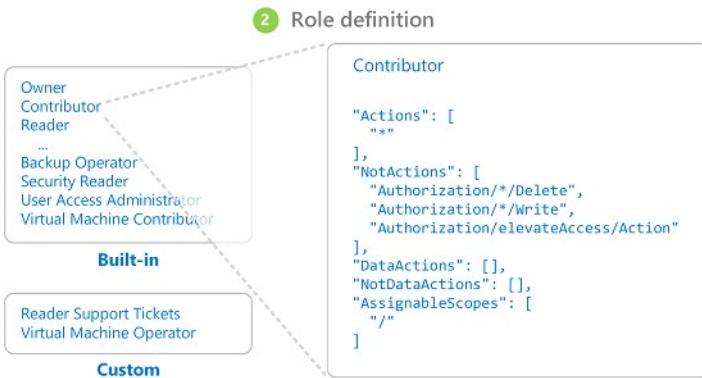
### 1. Security principal (who)

A *security principal* is a user, group, service principal, or managed identity that is requesting access to Azure resources.



### 2. Role definition (what you can do)

A role definition is a collection of permissions. It's sometimes just called a role. A role definition lists the permissions that can be performed, such as read, write, and delete. Roles can be high-level, like Owner, or specific, like Virtual Machine Contributor.



Azure includes several built-in roles that you can use. The following lists four fundamental built-in roles:

- **Owner** - Has full access to all resources, including the right to delegate access to others.
- **Contributor** - Can create and manage all types of Azure resources, but can't grant access to others.
- **Reader** - Can view existing Azure resources.
- **User Access Administrator** - Lets you manage user access to Azure resources.

If the built-in roles don't meet the specific needs of your organization, you can create your own custom roles.

### 3. Scope (where)

Scope is where the access applies to. This is helpful if you want to make someone a Website Contributor, but only for one resource group.

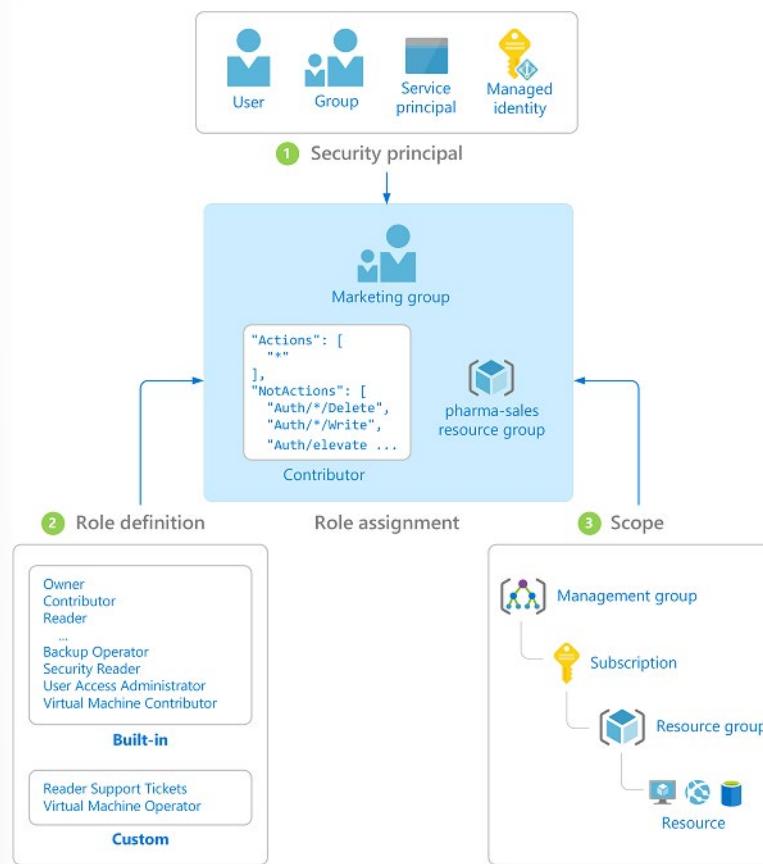
In Azure, you can specify a scope at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent-child relationship. When you grant access at a parent scope, those permissions are inherited by the child scopes. For example, if you assign the Contributor role to a group at the subscription scope, that role is inherited by all resource groups and resources in the subscription.



## Role assignment

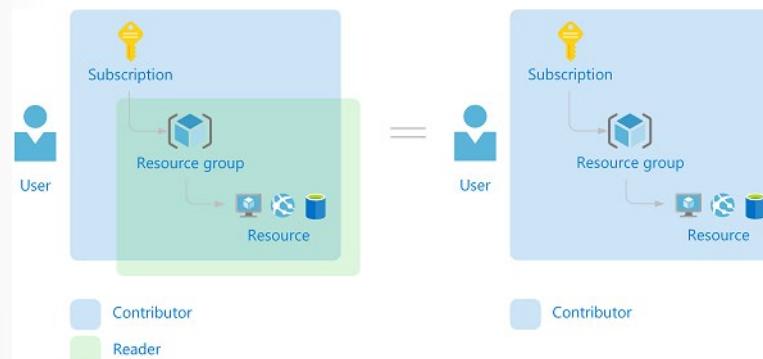
Once you have determined the who, what, and where, you can combine those elements to grant access. A role assignment is the process of binding a role to a security principal at a particular scope, for the purpose of granting access. To grant access, you create a role assignment. To revoke access, you remove a role assignment.

The following example shows how the Marketing group has been assigned the Contributor role at the sales resource group scope.



## Multiple role assignments

Azure RBAC is an additive model, so your effective permissions are the sum of your role assignments. Consider the following example where a user is granted the Contributor role at the subscription scope and the Reader role on a resource group. The sum of the Contributor permissions and the Reader permissions is effectively the Contributor role for the resource group. Therefore, in this case, the Reader role assignment has no impact.



## Deny assignments

Previously, Azure RBAC was an allow-only model with no deny, but now Azure RBAC supports deny assignments in a limited way. Similar to a role assignment, a deny assignment attaches a set of deny actions to a user, group, service principal, or managed identity at a particular scope for the purpose of denying access. A role assignment defines a set of actions that are allowed, while a deny assignment defines a set of actions that are not allowed. In other words, deny assignments block users from performing specified actions even if a role assignment grants them access. Deny assignments take precedence over role assignments.

# Role-Based Access Control (RBAC) Roles

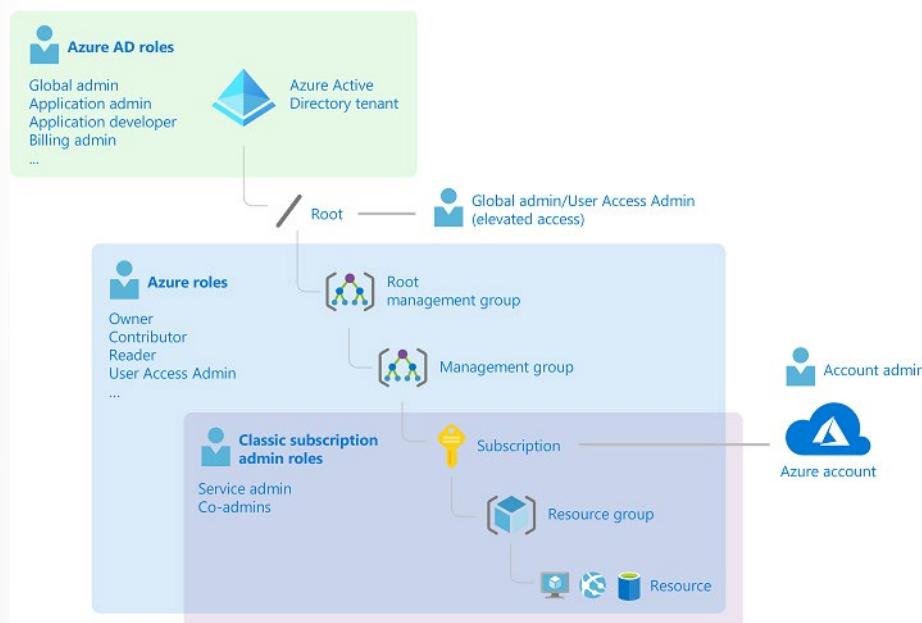
## Administrator Roles, Azure Roles, and Azure AD Roles

This topic explain the following roles and when you would use each:

- Classic subscription administrator roles
- Azure roles
- Azure Active Directory (Azure AD) roles

### How the roles are related

The following diagram is a high-level view of how the classic subscription administrator roles, Azure roles, and Azure AD roles are related.



### Classic subscription administrator roles

Account Administrator, Service Administrator, and Co-Administrator are the three classic subscription administrator roles in Azure. Classic subscription administrators have full access to the Azure subscription. They can manage resources using the Azure portal.

The following table describes the differences between these three classic subscription administrative roles.

Classic subscription administrator	Limit	Permissions	Notes
<b>Account Administrator</b>	1 per Azure account	Access the Azure Account Center Manage all subscriptions in an account Create new subscriptions Cancel subscriptions Change the billing for a subscription Change the Service Administrator	Conceptually, the billing owner of the subscription. The Account Administrator has no access to the Azure portal.
<b>Service Administrator</b>	1 per Azure subscription	Manage services in the Azure portal Cancel the subscription Assign users to the Co-Administrator role	By default, for a new subscription, the Account Administrator is also the Service Administrator. The Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope. The Service Administrator has full access to the Azure portal.
<b>Co-Administrator</b>	200 per subscription	Same access privileges as the Service Administrator, but can't change the association of subscriptions to Azure directories Assign users to the Co-Administrator role, but cannot change the Service Administrator	The Co-Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.

In the Azure portal, you can manage Co-Administrators or view the Service Administrator by using the **Classic administrators** tab.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a tree view with 'Access control (IAM)' selected. The main content area shows a table of users with the following data:

Name	Role	
AK	Archana Kulkarni	Service administrator
AB	Amporn Boonluang	Co-administrator

In the Azure portal, you can view or change the Service Administrator or view the Account Administrator on the properties blade of your subscription.

The screenshot shows the Microsoft Azure portal interface with the 'Properties' blade open for a subscription. The left sidebar has a tree view with 'Properties' selected. The main content area shows the following details:

- OFFER: Free Trial
- OFFER ID: (redacted)
- ACCOUNT ADMIN: (redacted)
- SERVICE ADMIN: (redacted)

## Azure roles

Azure RBAC includes over 70 built-in roles. There are four fundamental Azure roles. The first three apply to all resource types:

Azure role	Permissions	Notes
<b>Owner</b>	Full access to all resources Delegate access to others	The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope Applies to all resource types.
<b>Contributor</b>	Create and manage all of types of Azure resources Create a new tenant in Azure Active Directory- Cannot grant access to others	Applies to all resource types.
<b>Reader</b>	View Azure resources	Applies to all resource types.
<b>User Access Administrator</b>	Manage user access to Azure resources	

In the Azure portal, role assignments using Azure RBAC appear on the **Access control (IAM)** blade. This blade can be found throughout the portal, such as management groups, subscriptions, resource groups, and various resources.

Name	Type	Role	Scope
Ashish (AK)	User	Billing Contributor	This resource
admin (AD)	User	CheckAccess Test Role	Root (Inherited)
abene (AB)	User	Contributor	This resource

When you click the **Roles** tab, you will see the list of built-in and custom roles.

NAME	TYPE	USERS	GROUPS
Owner	BuiltInRole	0	1
Contributor	BuiltInRole	0	0
Reader	BuiltInRole	1	0
AcrImagePuller	BuiltInRole	0	0
AcrImagePusher	BuiltInRole	0	0
AcrImageSigner	BuiltInRole	0	0
AcrQuarantineReader	BuiltInRole	0	0
AcrQuarantineWriter	BuiltInRole	0	0
API Management Service Contributor	BuiltInRole	0	0
API Management Service Operator Role	BuiltInRole	0	0
API Management Service Reader Role	BuiltInRole	0	0

## Azure AD roles

Azure AD roles are used to manage Azure AD resources in a directory such as create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains. The following table describes a few of the more important Azure AD roles.

### Global Administrator

The following permissions apply:

- Manage access to all administrative features in Azure Active Directory, as well as services that federate to Azure Active Directory
- Assign administrator roles to others
- Reset the password for any user and all other administrators

### User Administrator

The following permissions apply:

- Create and manage all aspects of users and groups
- Manage support tickets
- Monitor service health
- Change passwords for users, Helpdesk administrators, and other User Administrators

### Billing Administrator

The following permissions apply:

- Make purchases

- Manage subscriptions
- Manage support tickets
- Monitors service health

In the Azure portal, you can see the list of Azure AD roles on the **Roles and administrators** blade.

ROLE	DESCRIPTION	...
Application administrator	Can create and manage all aspects of app registrations and enterprise...	...
Application developer	Can create application registrations independent of the 'Users can reg...	...
Billing administrator	Can perform common billing related tasks like updating payment info...	...
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise...	...
Cloud device administrator	Full access to manage devices in Azure AD.	...
Compliance administrator	Can read and manage compliance configuration and reports in Azure ...	...
Conditional Access administrator	Can manage conditional access capabilities.	...
Customer LockBox access approver	Can approve Microsoft support requests to access customer organizatio...	...
Desktop Analytics administrator	Can access and manage Desktop management tools and services.	...
Dynamics 365 administrator	Can manage all aspects of the Dynamics 365 product.	...
Exchange administrator	Can manage all aspects of the Exchange product.	...
Global administrator	Can manage all aspects of Azure AD and Microsoft services that use A...	...
Guest inviter	Can invite guest users independent of the 'members can invite guests...	...
Information Protection administrator	Can manage all aspects of the Azure Information Protection product.	...

## Differences between Azure roles and Azure AD roles

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

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

# Demonstration - Add an Azure Role Assignment

## Prerequisites

To add or remove role assignments, you must have:

- Microsoft.Authorization/roleAssignments/write and Microsoft.Authorization/roleAssignments/delete permissions, such as *User Access Administrator* or *Owner*.

**Access control (IAM)** is the blade that you use to assign roles to grant access to Azure resources. It's also known as identity and access management and appears in several locations in the Azure portal. The following shows an example of the Access control (IAM) blade for a subscription.

The screenshot shows the Azure portal interface for managing access control (IAM) within a specific subscription. The left sidebar contains links to various Azure services. The main area is focused on IAM, with tabs for 'Check access', 'Role assignments', 'Deny assignments', 'Classic administrators', and 'Roles'. The 'Check access' tab is active. It includes a search bar and dropdown for selecting the type of identity (Azure AD user, group, or service principal). To the right, there are three main callout boxes: one for adding a role assignment, another for viewing existing role assignments, and a third for viewing deny assignments. Each box includes a 'View' button and a 'Learn more' link.

To be the most effective with the Access control (IAM) blade, it helps if you can answer the following three questions when you are trying to assign a role:

### 1. Who needs access?

Who refers to a user, group, service principal, or managed identity. This is also called a *security principal*.

### 2. What role do they need?

Permissions are grouped together into roles. You can select from a list of several built-in roles or you can use your own custom roles.

### 3. Where do they need access?

Where refers to the set of resources that the access applies to. Where it can be a management group, subscription, resource group, or a single resource such as a storage account. This is called the *scope*.

## Add a role assignment

In Azure RBAC, to grant access to an Azure resource, you add a role assignment. Follow these steps to assign a role.

1. In the Azure portal, click **All services** and then select the scope that you want to grant access to.
2. Click the specific resource for that scope.
3. Click **Access control (IAM)**.
4. Click the **Role assignments** tab to view the role assignments at this scope.

The screenshot shows the Azure portal interface for managing access control. The left sidebar lists various service categories like Overview, Activity log, and Access control (IAM). The main content area is titled "Pay-As-You-Go - Access control (IAM)" and shows the "Role assignments" tab selected. A summary bar indicates there are 20 role assignments for this subscription, with a maximum limit of 2000. Below this, a table lists five role assignments: "Billing Reader" (User), "Sales Admins" (Group), and "user-assigned-identity" (App).

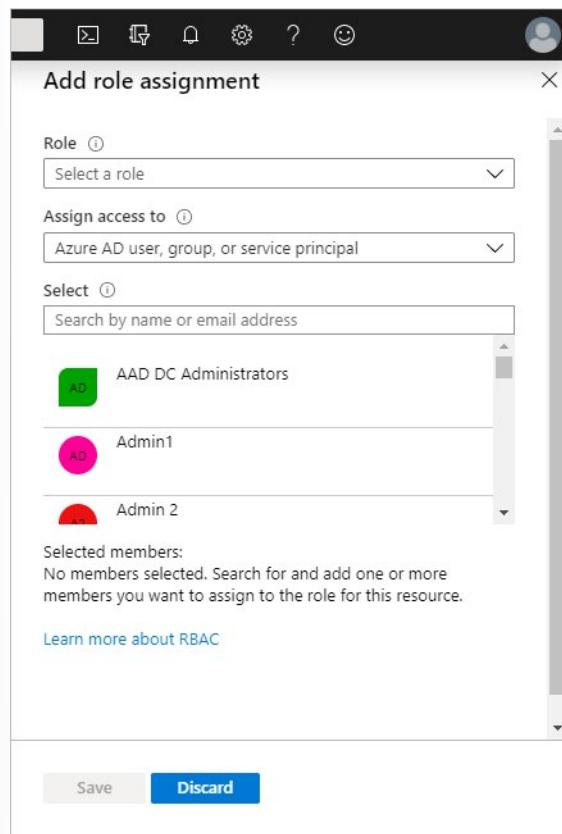
Name	Type	Role
Billing Reader	User	Billing Reader
Sales Admins	Group	Billing Reader
user-assigned-identity	App	Billing Reader

5. Click **Add > Add role assignment**.

If you don't have permissions to assign roles, the **Add role assignment** option will be disabled.

This screenshot shows the "Add role assignment" pane open. The top navigation bar includes "Add", "Edit columns", "Refresh", and "Remove" buttons. The "Add role assignment" button is highlighted with a red box. Below the buttons, there's a note about managing access to Azure resources for users, groups, and service principals. A summary bar shows 20 role assignments out of a limit of 2000. The pane is currently empty, showing only the header and a note about permissions.

The **Add role assignment** pane opens.



6. In the **Role** drop-down list, select a role such as **Virtual Machine Contributor**.
7. In the **Select** list, select a user, group, service principal, or managed identity. If you don't see the security principal in the list, you can type in the **Select** box to search the directory for display names, email addresses, and object identifiers.
8. Click **Save** to assign the role.

After a few moments, the security principal is assigned the role at the selected scope.

Virtual Machine Contributor				
<input type="checkbox"/>	Alain Charon	User	Virtual Machine Contributor ⓘ	This resource

# Azure AD Access Reviews

## Azure AD Access Reviews

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

User's access can be reviewed on a regular basis to make sure only the right people have continued access.

### Why are access reviews important?

Azure AD enables you to collaborate internally within your organization and with users from external organizations, such as partners.

- As new employees join, how do you ensure they have the right access to be productive?
- As people move teams or leave the company, how do you ensure their old access is removed, especially when it involves guests?
- Excessive access rights can lead to audit findings and compromises as they indicate a lack of control over access.
- You must proactively engage with resource owners to ensure they regularly review who has access to their resources.

### When to use access reviews?

- Too many users in privileged roles
- When a group is used for a new purpose
- Business critical data access
- To maintain a policy's exception list
- Ask group owners to confirm they still need guests in their groups

### Where do you create reviews?

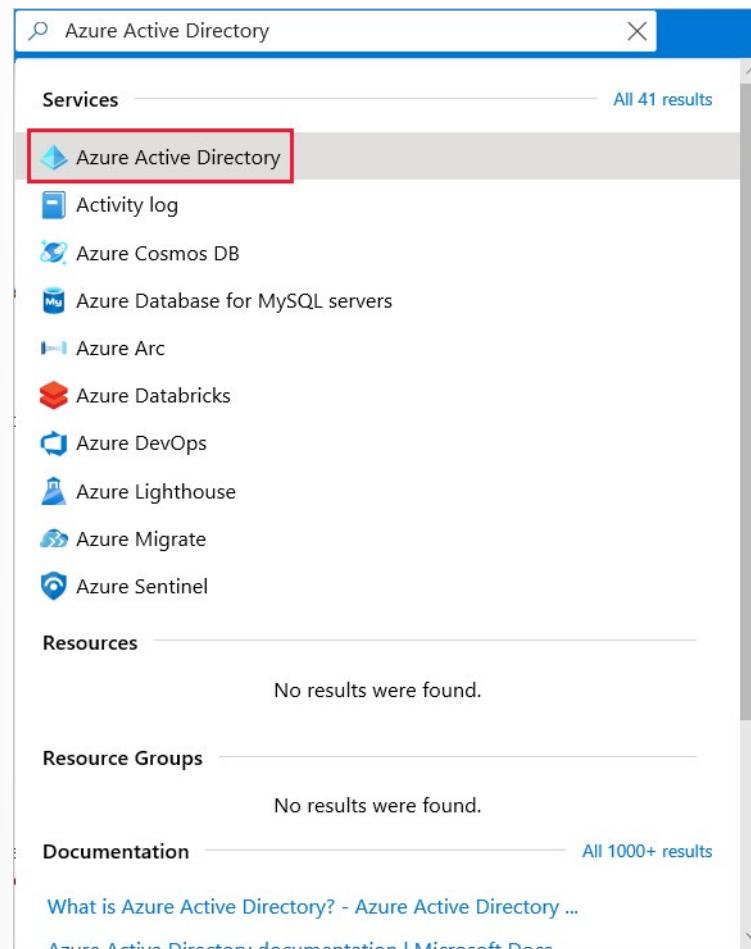
Depending on what you want to review, you will create your access review in Azure AD access reviews, Azure AD enterprise apps (in preview), or Azure AD PIM.

Access rights of users	Reviewers can be...	Review created in...	Reviewer experience
<b>Security group members</b> <b>Office group members</b>	Specified reviewers Group owners Self-review	Azure AD access reviews Azure AD groups	Access panel
<b>Assigned to a connected app</b>	Specified reviewers Self-review	Azure AD access reviews Azure AD enterprise apps (in preview)	Access panel
<b>Azure AD role</b>	Specified reviewers Self-review	Azure AD PIM	Azure portal
<b>Azure resource role</b>	Specified reviewers Self-review	Azure AD PIM	Azure portal

## Create an Azure AD Access Review

To create an access reviews, follow these steps:

1. Go to the [Azure portal<sup>1</sup>](https://portal.azure.com/) to manage access reviews and sign in as a Global administrator or User administrator.
2. Search for and select **Azure Active Directory**.



The screenshot shows the Azure portal search interface. The search bar at the top contains the text "Azure Active Directory". Below the search bar, there are two main sections: "Services" and "Resources". In the "Services" section, "Azure Active Directory" is listed first and has a red box drawn around it. Other services listed include Activity log, Azure Cosmos DB, Azure Database for MySQL servers, Azure Arc, Azure Databricks, Azure DevOps, Azure Lighthouse, Azure Migrate, and Azure Sentinel. In the "Resources" section, it says "No results were found." Below the "Services" section, there is a "Resource Groups" section which also says "No results were found." At the bottom, there is a "Documentation" section with a link to "What is Azure Active Directory? - Azure Active Directory ...".

3. Select **Identity Governance**.
4. On the **Getting started** page, click the **Create an access review** button.

<sup>1</sup> <https://portal.azure.com/>

**Identity Governance**

Getting started   Got feedback?

Entitlement management

- Access packages
- Catalogs
- Connected organizations
- Reports
- Settings

Access reviews

- Overview
- Access reviews
- Programs

Privileged Identity Management

- Azure AD roles
- Azure resources

Terms of use

- Terms of use

Activity

- Audit logs

Getting started Learn more

Ensure the right people have the right access at the right time

Azure AD Identity Governance helps you to protect, monitor, and audit access to critical assets while ensuring employee productivity

**Entitlement management**  
Govern the lifecycle of access to groups, applications, and SharePoint Online sites for both employees and guests.

**Create an access package**

**Access reviews**  
Enable organizations to recertify group memberships, application access, and privileged role assignments.

**Create an access review**

# Implement and Configure an Azure Policy

## Azure Policy Overview

Azure Policy is an Azure service you use to create, assign and, manage policies. These policies enforce different rules and effects over your resources so that those resources stay compliant with your corporate standards and service level agreements.

## How are Azure Policy and RBAC different?

At first glance, it might seem like Azure Policy is a way to restrict access to specific resource types similar to role-based access control (RBAC). However, they solve different problems. RBAC focuses on user actions at *different scopes*. You might be added to the contributor role for a resource group, allowing you to make changes to anything in that resource group. Azure Policy focuses on *resource properties during deployment* and for already-existing resources. Azure Policy controls properties such as the types or locations of resources. Unlike RBAC, Azure Policy is a **default-allow-and-explicit-deny system**.

## Creating a policy

The process of creating and implementing an Azure Policy begins with creating a *policy definition*. Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met. To apply a policy, you will:

1. Create a policy definition
2. Assign a definition to a scope of resources
3. View policy evaluation results

## What is a policy definition?

A *policy definition* expresses what to evaluate and what action to take. For example, you could ensure all public websites are secured with HTTPS, prevent a storage type from being created, or force a specific version of SQL Server to be used.

Below are the most common policy definitions you can apply.

Policy definition	Description
<b>Allowed Storage Account SKUs</b>	This policy definition has a set of conditions/rules that determine whether a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
<b>Allowed Resource Type</b>	This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of this defined list.
<b>Allowed Locations</b>	This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geographic compliance requirements.

Policy definition	Description
<b>Allowed Virtual Machine SKUs</b>	This policy enables you to specify a set of VM SKUs that your organization can deploy.
<b>Not allowed resource types</b>	Prevents a list of resource types from being deployed.

The policy definition itself is represented as a JSON file - you can use one of the pre-defined definitions in the portal or create your own (either modifying an existing one or starting from scratch).

Below is an example of a Compute policy that only allows specific virtual machine sizes:

```
{
  "if": {
    "allof": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "not": {
          "field": "Microsoft.Compute/virtualMachines/sku.name",
          "in": "[parameters('listOfAllowedSKUs')]"
        }
      }
    ],
    "then": {
      "effect": "Deny"
    }
  }
}
```

Notice the `[parameters('listofAllowedSKUs')]` value; this value is a *replacement token* that will be filled in when the policy definition is applied to a scope. When a parameter is defined, it's given a name and optionally given a value.

## What is an initiative definition?

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions. They simplify by grouping a set of policies as one single item.

## Demonstration - Create and Manage Policies to Enforce Compliance

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

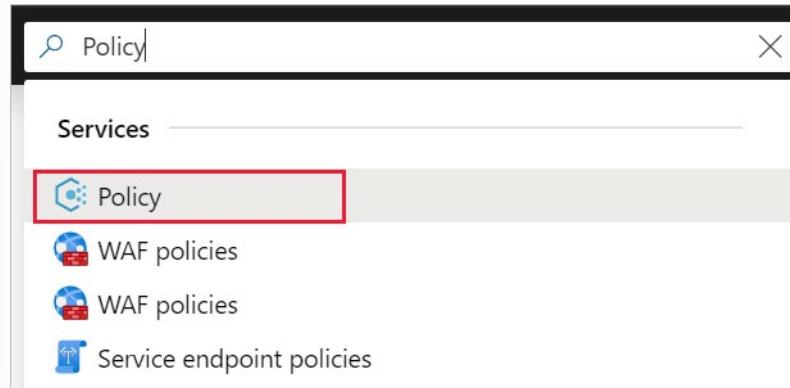
- Assign a policy to enforce a condition for resources you create in the future
- Create and assign an initiative definition to track compliance for multiple resources
- Resolve a non-compliant or denied resource

- Implement a new policy across an organization

## Assign a policy

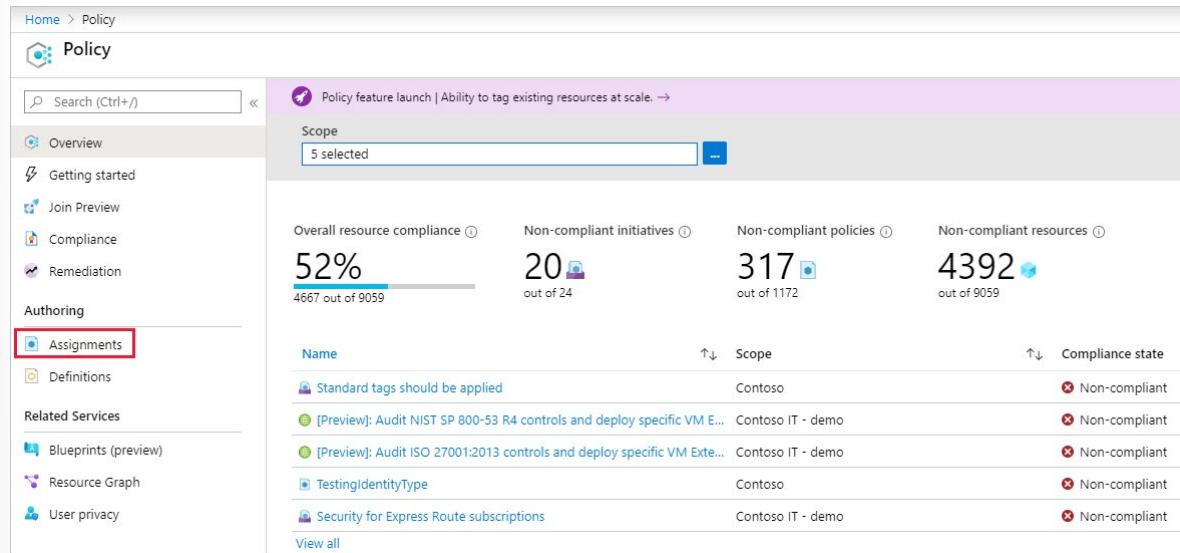
The first step in enforcing compliance with Azure Policy is to assign a policy definition. A policy definition defines under what condition a policy is enforced and what effect to take. In this example, assign the built-in policy definition called *Inherit a tag from the resource group if missing* to add the specified tag with its value from the parent resource group to new or updated resources missing the tag.

1. Go to the Azure portal to assign policies. Search for and select **Policy**.



A screenshot of the Azure portal search interface. The search bar at the top contains the text "Policy". Below the search bar, there is a list of services. The "Policy" service is highlighted with a red box. Other listed services include "WAF policies" (listed twice) and "Service endpoint policies".

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.



A screenshot of the Azure Policy - Assignments page. The left sidebar shows navigation links: Home, Policy, Overview, Getting started, Join Preview, Compliance, Remediation, Authoring, and Assignments (which is highlighted with a red box). The main content area displays performance metrics: Overall resource compliance (52%, 4667 out of 9059), Non-compliant initiatives (20, out of 24), Non-compliant policies (317, out of 1172), and Non-compliant resources (4392, out of 9059). Below these metrics is a table listing assignments:

Name	Scope	Compliance state
Standard tags should be applied	Contoso	Non-compliant
[Preview]: Audit NIST SP 800-53 R4 controls and deploy specific VM E...	Contoso IT - demo	Non-compliant
[Preview]: Audit ISO 27001:2013 controls and deploy specific VM Exte...	Contoso IT - demo	Non-compliant
TestingIdentityType	Contoso	Non-compliant
Security for Express Route subscriptions	Contoso IT - demo	Non-compliant

3. Select **Assign Policy** from the top of the **Policy - Assignments** page.

The screenshot shows the 'Policy - Assignments' blade in the Azure portal. On the left, there's a navigation menu with items like Overview, Getting started, Join Preview, Compliance, Remediation, Authoring, Assignments (which is selected), and Definitions. The main area has a search bar, buttons for 'Assign initiative' and 'Assign policy' (the latter is highlighted with a red box), and a 'Refresh' button. A 'Scope' section shows '5 selected'. Below that, it displays 'Total Assignments: 15' and 'Initiative Assignments: 1' (with a small icon). There are two dropdown menus under 'name': 'Apply tag and its default value' and 'Require tag and its value'.

4. On the **Assign Policy** page and **Basics** tab, select the **Scope** by selecting the ellipsis and selecting either a management group or subscription. Optionally, select a resource group. A scope determines what resources or grouping of resources the policy assignment gets enforced on. Then select **Select** at the bottom of the **Scope** page.
5. Resources can be excluded based on the Scope. Exclusions start at one level lower than the level of the **Scope**. **Exclusions** are optional, so leave it blank for now.
6. Select the **Policy definition** ellipsis to open the list of available definitions. You can filter the policy definition **Type** to *Built-in* to view all and read their descriptions.
7. Select **Inherit a tag from the resource group if missing**. Select **Select** at the bottom of the **Available Definitions** page once you have found and selected the policy definition.

The screenshot shows the 'Available Definitions' page. It has a search bar with the text 'inherit a tag from the r' (partially visible) highlighted with a red box. Below the search bar, there's a dropdown for 'Type' set to 'All types'. The main area shows 'Policy Definitions (2)'.

**Inherit a tag from the resource group**  
Built-in  
Adds or replaces the specified tag and value from the parent resource group when any resource is created or updated. Existing resources can be remediated by triggering a remediation task.

**Inherit a tag from the resource group if missing**  
Built-in  
Adds the specified tag with its value from the parent resource group when any resource missing this tag is created or updated. Existing resources can be remediated by triggering a remediation task. If the tag exists with a different value it will not be changed.

8. The **Assignment name** is automatically populated with the policy name you selected, but you can change it. For this example, leave *Inherit a tag from the resource group if missing*. You can also add an optional **Description**. The description provides details about this policy assignment.
9. Leave **Policy enforcement** as *Enabled*. When *Disabled*, this setting allows testing the outcome of the policy without triggering the effect.
10. **Assigned by** is automatically filled based on who is logged in.
11. Select the **Parameters** tab at the top of the wizard.

12. For **Tag Name**, enter *Environment*.
13. Select the **Remediation** tab at the top of the wizard.
14. Leave **Create a remediation task** unchecked. This box allows you to create a task to alter existing resources in addition to new or updated resources.
15. **Create a Managed Identity** is automatically checked since this policy definition uses the modify effect. **Permissions** is set to *Contributor* automatically based on the policy definition.
16. Select the **Review + create** tab at the top of the wizard.
17. Review your selections, then select **Create** at the bottom of the page.

## Implement a New Custom Policy

**Scenario:** create a new custom policy to save costs by validating that VMs created in your environment can't be in the G series. This way, every time a user in your organization tries to create VM in the G series, the request is denied.

1. Select **Definitions** under **Authoring** in the left side of the Azure Policy page.

The screenshot shows the Azure Policy - Definitions page. On the left, there's a navigation sidebar with links for Home, Policy - Definitions, Overview, Getting started, Join Preview, Compliance, Remediation, Authoring (which is selected), Assignments, and Definitions. The main area has a search bar, a 'Scope' dropdown set to '5 selected', and a 'Definition type' dropdown set to 'All definition types'. Below these are several policy definitions listed in a table with columns for Name and Description. The descriptions include audit rules for Windows VMs regarding Administrators group members, Log Analytics agent connection, IRS1075 controls, and CIS Microsoft Azure Foundations Benchmark recommendations.

2. Select **+ Policy definition** at the top of the page. This button opens to the **Policy definition** page.
3. Enter the following information:
  - The management group or subscription in which the policy definition is saved. Select by using the ellipsis on **Definition location**.
  - The name of the policy definition - *\*\_Require VM SKUs smaller than the G series*.
  - The description of what the policy definition is intended to do – *This policy definition enforces that all VMs created in this scope have SKUs smaller than the G series to reduce cost*.
  - Choose from existing options (such as *Compute*), or create a new category for this policy definition.
  - Copy the following JSON code and then update it for your needs with:
    - The policy parameters.
    - The policy rules/conditions, in this case – VM SKU size equal to G series
    - The policy effect, in this case – **Deny**.

Here's what the JSON should look like. Paste your revised code into the Azure portal.

```
{  
    "policyRule": {  
        "if": {  
            "allof": [{  
                "field": "type",  
                "equals": "Microsoft.Compute/virtualMachines"  
            },  
            {  
                "field": "Microsoft.Compute/virtualMachines/sku.name",  
                "like": "Standard_G*"  
            }  
        ]  
    },  
    "then": {  
        "effect": "deny"  
    }  
}
```

The *field* property in the policy rule must be a supported value. A full list of values is found on **policy definition structure** fields. An example of an alias might be Microsoft.Compute/VirtualMachines/Size.

4. Select **Save**.

## Azure Blueprints

### Azure Blueprints

Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Azure Blueprints makes it possible for development teams to rapidly build and deploy new environments with the trust they're building within organizational compliance using a set of built-in components, such as networking, to speed up development and delivery.

The screenshot shows the Azure Blueprints interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below that is a breadcrumb trail: 'Home > Blueprints - Getting started'. The main title is 'Blueprints - Getting started'. On the left, a sidebar has a 'Getting started' section with three items: 'Blueprint definitions', 'Assigned blueprints', and 'Create a blueprint' (which is highlighted with a red box). The main content area features a 'Welcome to Azure Blueprints PREVIEW' section with a diagram showing various Azure services like Storage, Compute, and Network connected by arrows. Below this, there are three cards: 'Create a blueprint' (with a 'Create' button), 'Apply to a scope' (with an 'Apply' button), and 'Track assignments' (with a 'Track' button). To the right of the 'Create a blueprint' card, there's a link to 'Blueprints Overview'.

Azure Blueprints is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

Azure Blueprints are also useful in Azure DevOps scenarios, where blueprints are associated with specific build artifacts and release pipelines and can be tracked more rigorously.

The process of implementing Azure Blueprint consists of the following high-level steps:

1. Create an Azure Blueprint
2. Assign the blueprint

### 3. Track the blueprint assignments

With Azure Blueprint, the relationship between the blueprint definition (what *should be* deployed) and the blueprint assignment (what *was* deployed) is preserved. This connection supports improved deployment tracking and auditing.

The Azure Blueprints service is backed by the globally distributed Azure Cosmos database. Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, regardless of which region Blueprints deploys your resources to.

## How is it different from Resource Manager templates?

The Azure Blueprints service is designed to help with environment setup. This setup often consists of a set of resource groups, policies, role assignments, and Resource Manager template deployments. A blueprint is a package to bring each of these artifact types together and allow you to compose and version that package—including through a CI/CD pipeline. Ultimately, each setup is assigned to a subscription in a single operation that can be audited and tracked.

Nearly everything that you want to include for deployment in Blueprints can be accomplished with a Resource Manager template. However, a Resource Manager template is a document that doesn't exist natively in Azure. Resource Manager templates are stored either locally or in source control. The template gets used for deployments of one or more Azure resources, but once those resources deploy there's no active connection or relationship to the template.

With Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

Each blueprint can consist of zero or more Resource Manager template artifacts. This support means that previous efforts to develop and maintain a library of Resource Manager templates are reusable in Blueprints.

## How it's different from Azure Policy

A blueprint is a package or container for composing focus-specific sets of standards, patterns, and requirements related to the implementation of Azure cloud services, security, and design that can be reused to maintain consistency and compliance.

A policy is a default-allow and explicit-deny system focused on resource properties during deployment and for already existing resources. It supports cloud governance by validating that resources within a subscription adhere to requirements and standards.

Including a policy in a blueprint enables the creation of the right pattern or design during assignment of the blueprint. The policy inclusion makes sure that only approved or expected changes can be made to the environment to protect ongoing compliance to the intent of the blueprint.

A policy can be included as one of many artifacts in a blueprint definition. Blueprints also support using parameters with policies and initiatives.

## Demonstration - Create a Blueprint

The first step in defining a standard pattern for compliance is to compose a blueprint from the available resources. In this demonstration, create a new blueprint named **MyBlueprint** to configure role and policy

assignments for the subscription. Then add a new resource group, and create a Resource Manager template and role assignment on the new resource group.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Blueprint definitions** from the page on the left and select the **+ Create blueprint** button at the top of the page.

The screenshot shows the 'Blueprints - Blueprint definitions' page. At the top right, there is a 'Create blueprint' button with a plus sign, which is highlighted with a red box. Below it is a 'Scope' section showing '4 selected'. On the left, there is a navigation bar with 'Getting started', 'Blueprint definitions' (which is selected and highlighted in blue), and 'Assigned blueprints'. The main area is titled 'NAME'.

3. Select **Start with blank blueprint** from the card at the top of the built-in blueprints list.
4. Provide a **Blueprint name** such as **MyBlueprint**. Leave **Blueprint description** blank for now.
5. In the **Definition location** box, select the ellipsis on the right, select the management group or subscription where you want to save the blueprint, and choose **Select**.
6. Verify that the information is correct. The **Blueprint name** and **Definition location** fields can't be changed later. Then select **Next : Artifacts** at the bottom of the page or the **Artifacts** tab at the top of the page.
7. Add a role assignment at the subscription level:
  - Select the **+ Add artifact** row under **Subscription**. The **Add artifact** window opens on the right side of the browser.
  - Select **Role assignment** for **Artifact type**.
  - Under **Role**, select **Contributor**. Leave the **Add user, app or group** box with the check box that indicates a dynamic parameter.
  - Select **Add** to add this artifact to the blueprint.

The screenshot shows the 'Add artifact' window for a 'Role assignment'. It has a dropdown menu for 'Artifact type' set to 'Role assignment'. A message box says 'You can choose to fill these parameters in now or when assigning the blueprint.' Below it, the 'Role' dropdown is set to 'Contributor'. There is a 'Search by name or email' input field and a checked checkbox that says 'This value should be specified when the blueprint is assigned'.

8. Add a policy assignment at the subscription level:
  - Select the **+ Add artifact** row under the role assignment artifact.
  - Select **Policy assignment** for **Artifact type**.
  - Change **Type** to **Built-in**. In **Search**, enter **tag**.

- Click out of **Search** for the filtering to occur. Select **Append tag and its default value to resource groups**.
  - Select **Add** to add this artifact to the blueprint.
9. Select the row of the policy assignment **Append tag and its default value to resource groups**.
10. The window to provide parameters to the artifact as part of the blueprint definition opens and allows setting the parameters for all assignments (static parameters) based on this blueprint instead of during assignment (dynamic parameters). This example uses dynamic parameters during blueprint assignment, so leave the defaults and select **Cancel**.
11. Add a resource group at the subscription level:
- Select the **+ Add artifact** row under **Subscription**.
  - Select **Resource group** for **Artifact type**.
  - Leave the **Artifact display name**, **Resource Group Name**, **Location** boxes blank, but make sure that the check box is checked for each parameter property to make them dynamic parameters.
  - Select **Add** to add this artifact to the blueprint.
12. Add a template under the resource group:
- Select the **+ Add artifact** row under the **ResourceGroup** entry.
  - Select **Azure Resource Manager template** for **Artifact type**, set **Artifact display name** to **StorageAccount**, and leave **Description** blank.
  - On the **Template** tab in the editor box, paste the following Resource Manager template. After you paste the template, select the **Parameters** tab and note that the template parameters **storageAccountType** and **location** were detected. Each parameter was automatically detected and populated but configured as a dynamic parameter.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/
deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "storageAccountType": {
            "type": "string",
            "defaultValue": "Standard_LRS",
            "allowedValues": [
                "Standard_LRS",
                "Standard_GRS",
                "Standard_ZRS",
                "Premium_LRS"
            ],
            "metadata": {
                "description": "Storage Account type"
            }
        },
        "location": {
            "type": "string",
            "defaultValue": "[resourceGroup().location]",
            "metadata": {
                "description": "Location for all resources."
            }
        }
    }
}
```

```
        }
    },
    "variables": {
        "storageAccountName": "[concat('store', uniquestring(resourceGroup().id))]"
    },
    "resources": [
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[variables('storageAccountName')]",
            "location": "[parameters('location')]",
            "apiVersion": "2018-07-01",
            "sku": {
                "name": "[parameters('storageAccountType')]"
            },
            "kind": "StorageV2",
            "properties": {}
        }],
    "outputs": {
        "storageAccountName": {
            "type": "string",
            "value": "[variables('storageAccountName')]"
        }
    }
}
```

- Clear the **storageAccountType** check box and note that the drop-down list contains only values included in the Resource Manager template under **allowedValues**. Select the box to set it back to a dynamic parameter.
  - Select **Add** to add this artifact to the blueprint.
13. Your completed blueprint should look like the following. Notice that each artifact has **x out of y parameters populated** in the **Parameters** column. The dynamic parameters are set during each assignment of the blueprint.

The screenshot shows the 'Parameters' tab of a Blueprint configuration page. It includes an information icon and a note: 'You can choose to fill these parameters in now or when assigning the blueprint.' Below are two parameter entries:

- storageAccountType**: A dropdown menu showing 'Standard\_LRS' with a checked checkbox below it: 'This value should be specified when the blueprint is assigned'.
- location**: A text input field containing '[resourceGroups('ResourceGroup').location]' with a checked checkbox below it: 'This value should be specified when the blueprint is assigned'.

14. Now that all planned artifacts have been added, select **Save Draft** at the bottom of the page.

# Lab

## Lab: Managing Azure Role-Based Access Control

✓ **Important:** To download the most recent version of this lab, please visit the AZ-303 [GitHub repository<sup>2</sup>](#).

Direct link to the [Lab: Managing Azure Role-Based Access Control<sup>3</sup>](#).

### Lab scenario



With Azure Active Directory (Azure AD) becoming integral part of its identity management environment, the Adatum Enterprise Architecture team must also determine the optimal authorization approach. In the context of controlling access to Azure resources, such approach must involve the use of Azure Role-Based Access Control (RBAC). Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources.

The key concept of Azure RBAC is role assignment. A role assignment consists of three elements: security principal, role definition, and scope. A security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources. A role definition is a collection of the operations that the role assignments will grant, such as read, write, or delete. Roles can be generic or resource specific. Azure includes four built-in generic roles (Owner, Contributor, Reader, and User Access Administrator) and a fairly large number of built-in resource-specific roles (such as, for example, Virtual Machine Contributor, which includes permissions to create and manage Azure virtual machines). It is also possible to define custom roles. A scope is the set of resources that the access applies to. A scope can be set at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent-child relationship.

The Adatum Enterprise Architecture team wants to test delegation of Azure management by using custom Role-Based Access Control roles. To start its evaluation, the team intends to create a custom role that provides restricted access to Azure virtual machines.

### Objectives

After completing this lab, you will be able to:

- Define a custom RBAC role
- Assign a custom RBAC role

### Lab Environment

Windows Server admin credentials

- User Name: **Student**
- Password: **Pa55w.rd1234**

<sup>2</sup> <https://github.com/MicrosoftLearning/AZ-303-Microsoft-Azure-Architect-Technologies>

<sup>3</sup> [https://aka.ms/303\\_Module\\_10\\_Lab](https://aka.ms/303_Module_10_Lab)

Estimated Time: 60 minutes

## Lab Files (Located in the GitHub repository listed above)

- \\AZ303\\AllFiles\\Labs\\11\\azuredeploy30311suba.json
- \\AZ303\\AllFiles\\Labs\\11\\azuredeploy30311rga.json
- \\AZ303\\AllFiles\\Labs\\11\\azuredeploy30311rga.parameters.json
- \\AZ303\\AllFiles\\Labs\\11\\roledefinition30311.json

## Exercise 0: Prepare the lab environment

The main tasks for this exercise are as follows:

1. Deploy an Azure VM by using an Azure Resource Manager template
2. Create an Azure Active Directory user

## Exercise 1: Define a custom RBAC role

The main tasks for this exercise are as follows:

1. Identify actions to delegate via RBAC
2. Create a custom RBAC role in an Azure AD tenant

## Exercise 2: Assign and test a custom RBAC role

The main tasks for this exercise are as follows:

1. Create an RBAC role assignment
2. Test the RBAC role assignment

# Module 10 Review Questions

## Module 10 Review Questions



### Review Question 1

You are asked to make recommendation to a company whose network contains an on-premises Active Directory and an Azure AD tenant.

- They have deployed Azure AD Connect and have configured pass-through authentication.
- Their Azure subscription contains many web apps that are accessed from the Internet.
- They plan to use Azure MFA with the Azure AD tenant.

You are asked to recommend a solution that prevents users from being prompted for Azure MFA while accessing apps from the on-premises network. What do you advise?

- Trusted IPs
- A site-to-site VPN between the on-premises network and Azure
- Azure ExpressRoute
- Azure Policy

### Review Question 2

An organization has an Azure subscription named *Tailwind\_Subscription\_1* that contains an Azure VM named *Tailwind\_VM\_1* within the resource group named *Tailwind\_RG\_1*.

- *Tailwind\_VM\_1* runs services that are used to deploy resources in *Tailwind\_RG\_1*.
- They want to ensure that the service on running *Tailwind\_VM\_1* can manage the resources in *Tailwind\_RG\_1* by using the identity of *Tailwind\_VM\_1*.
- Managed Identity has not been enabled on the VM.

What do you advise they do first?

- From the Azure portal, modify the Identity Access Control (IAM) settings for *Tailwind\_VM\_1*.
- From the Azure portal, modify the value of the Identity option for *Tailwind\_VM\_1*.
- From the Azure portal, modify the Policies settings for *Tailwind\_RG\_1*.
- From the Azure portal, modify the Access Control (IAM) settings or *Tailwind\_RG\_1*.

## Review Question 3

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

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

## Review Question 4

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.

# Answers

## Review Question 1

You are asked to make recommendation to a company whose network contains an on-premises Active Directory and an Azure AD tenant.

You are asked to recommend a solution that prevents users from being prompted for Azure MFA while accessing apps from the on-premises network. What do you advise?

- Trusted IPs
- A site-to-site VPN between the on-premises network and Azure
- Azure ExpressRoute
- Azure Policy

*Explanation*

*Correct Answer: Trusted IPs. Trusted IPs are an multi-factor authentication feature that bypasses the two-step verification for users who signing in from IP addresses that are on the Trusted IP list.*

## Review Question 2

An organization has an Azure subscription named Tailwind\_Subscription\_1 that contains an Azure VM named Tailwind\_VM\_1 within the resource group named Tailwind\_RG\_1.

What do you advise they do first?

- From the Azure portal, modify the Identity Access Control (IAM) settings for Tailwind\_VM\_1.
- From the Azure portal, modify the value of the Identity option for Tailwind\_VM\_1.
- From the Azure portal, modify the Policies settings for Tailwind\_RG\_1.
- From the Azure portal, modify the Access Control (IAM) settings or Tailwind\_RG\_1.

*Explanation*

*Correct Answer: From the Azure portal, modify the value of the Identity option for Tailwind\_VM\_1 because you must first enable Managed Service Identity.*

## Review Question 3

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

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

*Explanation*

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

**Review Question 4**

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

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

*Explanation*

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

# Module 11 Manage Security for Applications

## Azure Managed Identity

### Authentication with Azure Managed Identities

Azure managed identity automatically creates identities to allow apps to authenticate with Azure resources and services.

In this lesson, you'll explore the managed identity feature. You'll see how it works and what resources you can access in Azure.

#### What are managed identities in Azure?

You use managed identities to authenticate any Azure service that supports the feature. To use managed identities, you don't need to provide authentication credentials in code. The managed identity feature solves the credential problem by granting an automatically managed identity. You use this service principal to authenticate to Azure services.

A managed identity combines Azure AD authentication and Azure role-based access control (RBAC).

When you use managed identities, you don't need to rotate credentials or worry about expiring certifications. Azure handles credential rotation and expiration in the background. To configure an application to use a managed identity, you use the provided token to call the service.

#### How managed identities work

When you work with managed identities, you should know some common terms:

- **Client ID:** A unique ID that's linked to the Azure AD application and service principal that was created when you provisioned the identity.
- **Object ID:** The service principal object of the managed identity.
- **Azure Instance Metadata Service:** A REST API that's enabled when Azure Resource Manager provisions a VM. The endpoint is accessible only from within the VM.

You can create two types of managed identity: system-assigned identity and user-assigned managed identity. These types are similar, but they're used differently.

## System-assigned managed identity

You enable system-assigned identity directly on an Azure service instance, such as a VM. When you enable that identity, Azure creates a service principal through Azure Resource Manager.

The service principal is for the resource that's connected to the information about the managed identity on the Azure AD tenant. For example, if you have two VMs, managed identity must be enabled on each VM.

The status of the managed identity is directly linked to the status of the resource. If the resource is deleted, so is the managed identity. A resource can have only one system-assigned managed identity.

## User-assigned managed identity

User-assigned managed identity is created as a standalone Azure resource. It's independent of any app. When user-assigned identity is provisioned, Azure creates a service principal just as it does for a system-assigned identity.

However, a user-assigned identity isn't tied to a specific resource, so you can assign it to more than one application. For example, if your web app is deployed on 10 front-end VMs, you create a user-assigned managed identity for the app and then associate it with all 10 VMs. If you used system-assigned identity, you would need 10 identities, and then you would have to manage the access for each one.

# Using Managed Identities with Azure Resources

To set up a managed identity:

1. In the Azure portal, go to the VM that hosts the app.
2. On the overview page, under **Settings**, select **Identity**.
3. Choose a system-assigned identity or a user-assigned identity. To do so, change the status to **On**.
4. Save the changes.

Next, the system reminds you that the server will be registered with Azure AD and that you can grant permissions to resources there.

You can always see the current managed identities for the subscription in Azure AD, on the **Enterprise applications** page. On the overview page, you can assign users and change permissions.

AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

Microsoft Azure

Search resources, services, and docs (G+/)

Home > TestVM-12

## TestVM-12 | Identity

Virtual machine

Search (Ctrl+ /)

System assigned User assigned

A system assigned managed identity enables Azure resources to authenticate based-access-control. The lifecycle of this type of managed identity is tied to Managed identities.

Save Discard Refresh Got feedback?

Status: On

Networking

Connect

Disks

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

Identity

Properties

Locks

## Azure Key Vault

### Azure Key Vault

Azure Key Vault is a centralized cloud service for storing application secrets such as encryption keys, certificates, and server-side tokens. Key Vault helps you control your applications' secrets by keeping them in a single central location and providing secure access, permissions control, and access logging.

There are three primary concepts used in an Azure Key Vault: *vaults*, *keys*, and *secrets*.

### Vaults

You use Azure Key Vault to create multiple secure containers, called vaults. Vaults help reduce the chances of accidental loss of security information by centralizing application secrets storage. Organizations will have several key vaults. Each key vault is a collection of cryptographic keys and cryptographically protected data (call them "secrets") managed by one or more responsible individuals within your organization. These key vaults represent the logical groups of keys and secrets for your organization; those that you want to manage together. They are like folders in the file system. Key vaults also control and log the access to anything stored in them.

You can create and manage vaults using command line tools such as Azure PowerShell or the Azure CLI, using the REST API, or through the Azure portal.

For example, here's a sample Azure CLI command line to create a new vault in a resource group:

```
az keyvault create \
    --resource-group <resource-group> \
    --name <your-unique-vault-name>
```

Here's the same command using Azure PowerShell:

```
New-AzKeyVault -Name <your-unique-vault-name> -ResourceGroupName <re-
source-group>
```

### Keys

Keys are the central actor in the Azure Key Vault service. A given key in a key vault is a cryptographic asset destined for a particular use such as the asymmetric master key of Microsoft Azure RMS, or the asymmetric keys used for SQL Server TDE (Transparent Data Encryption), CLE (Column Level Encryption) and Encrypted backup.

Microsoft and your apps don't have access to the stored keys directly once a key is created or added to a key vault. Applications must use your keys by calling cryptography methods on the Key Vault service. The Key Vault service performs the requested operation within its hardened boundary. The application never has direct access to the keys.

Keys can be single instanced (only one key exists) or be versioned. In the versioned case, a key is an object with a primary (active) key and a collection of one or more secondary (archived) keys created when keys are rolled (renewed). Key Vault supports asymmetric keys (RSA 2048). Your applications may use these for encryption or digital signatures.

There are two variations on keys in Key Vault: hardware-protected, and software-protected.

## Hardware protected keys

The Key Vault service supports using HSMs that provide a hardened, tamper-resistant environment for cryptographic processing and key generation. Azure has dedicated HSMs validated to FIPS 140-2 Level 2 that Key Vault uses to generate or store keys. These HSM-backed keys are always locked to the boundary of the HSM. When you ask the Key Vault service to decrypt or sign with a key, the operation is performed inside an HSM.

You can import keys from your own hardware security modules (HSMs) and transfer them to Key Vault without leaving the HSM boundary. This scenario is often referred to as bring your own key, or BYOK. More details on generating your own HSM-protected key and then transferring it to Azure Key Vault is available in the summary of this module. You can also use these Azure HSMs directly through the Microsoft Azure Dedicated Hardware Security Module (HSM) service if you need to migrate HSM-protected apps or maintain a high security compliance requirement.

## Software protected keys

Key Vault can also generate and protect keys using software-based RSA and ECC algorithms. In general, software-protected keys offer most of the features as HSM-protected keys except the FIPS 140-2 Level 2 assurance:

- Your key is still isolated from the application (and Microsoft) in a container that you manage
- It's stored at rest encrypted with HSMs
- You can monitor usage using Key Vault logs

The primary difference (besides price) with a software-protected key is when cryptographic operations are performed, they are done in software using Azure compute services while for HSM-protected keys the cryptographic operations are performed within the HSM.

You determine the key generation type when you create the key. For example, the Azure PowerShell command `Add-AzureKeyVaultKey` has a `Destination` parameter that can be set to either Software or HSM:

```
$key = Add-AzureKeyVaultKey -VaultName 'contoso' -Name 'MyFirstKey' -Destination 'HSM'
```

## Secrets

Secrets are small (less than 10K) data blobs protected by a HSM-generated key created with the Key Vault. Secrets exist to simplify the process of persisting sensitive settings that almost every application has: storage account keys, .PFX files, SQL connection strings, data encryption keys, etc.

## Key Vault Uses

With these three elements, an Azure Key Vault helps address the following issues:

- **Secrets management.** Azure Key Vault can securely store (with HSMs) and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
- **Key management.** Azure Key Vault is a cloud-based key management solution, making it easier to create and control the encryption keys used to encrypt your data. Azure services such as App Service

integrate directly with Azure Key Vault and can decrypt secrets without knowledge of the encryption keys.

- **Certificate management.** Azure Key Vault is also a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with Azure and your internal connected resources. It can also request and renew TLS certificates through partnerships with certificate authorities, providing a robust solution for certificate lifecycle management.
- ✓ **Important:Key Vault is designed to store configuration secrets for server applications.** It's not intended for storing data belonging to your app's users, and it shouldn't be used in the client-side part of an app. This is reflected in its performance characteristics, API, and cost model.

User data should be stored elsewhere, such as in an Azure SQL database with Transparent Data Encryption, or a storage account with Storage Service Encryption. Secrets used by your application to access those data stores can be kept in Key Vault.

## Best practices

Below are security best practices for using Azure Key Vault.

Best practice	Solution
<b>Grant access to users, groups, and applications at a specific scope.</b>	Use RBAC's predefined roles. For example, to grant access to a user to manage key vaults, you would assign the predefined role Key Vault Contributor to this user at a specific scope. The scope, in this case, would be a subscription, a resource group, or just a specific key vault. If the predefined roles don't fit your needs, you can define your own roles.
<b>Control what users have access to.</b>	Access to a key vault is controlled through two separate interfaces: management plane, and data plane. The management plane and data plane access controls work independently. Use RBAC to control what users have access to. For example, if you want to grant an application the rights to use keys in a key vault, you only need to grant data plane access permissions by using key vault access policies, and no management plane access is needed for this application. Conversely, if you want a user to be able to read vault properties and tags but not have any access to keys, secrets, or certificates, you can grant this user read access by using RBAC, and no access to the data plane is required.
<b>Store certificates in your key vault.</b>	Azure Resource Manager can securely deploy certificates stored in Azure Key Vault to Azure VMs when the VMs are deployed. By setting appropriate access policies for the key vault, you also control who gets access to your certificate. Another benefit is that you manage all your certificates in one place in Azure Key Vault.

Best practice	Solution
<b>Ensure that you can recover a deletion of key vaults or key vault objects.</b>	Deletion of key vaults or key vault objects can be either inadvertent or malicious. Enable the soft delete and purge protection features of Key Vault, particularly for keys that are used to encrypt data at rest. Deletion of these keys is equivalent to data loss, so you can recover deleted vaults and vault objects if needed. Practice Key Vault recovery operations regularly.

## Demonstration - Configure Certificate Auto-Rotation in Key Vault

Certificates can be public and private Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificates signed by a certificate authority (CA), or a self-signed certificate. Key Vault can also request and renew certificates through partnerships with CAs, providing a robust solution for certificate lifecycle management.

In this demonstration, you will update a certificate's validity period, auto-rotation frequency, and CA attributes.

- Manage a certificate by using the Azure portal.
- Add a CA provider account.
- Update the certificate's validity period.
- Update the certificate's auto-rotation frequency.
- Update the certificate's attributes by using Azure PowerShell.

### Sign in to Azure

Sign in to the Azure portal at <https://portal.azure.com><sup>1</sup>.

### Create a vault

Create a key vault or select your existing vault to perform operations (If needed, see **Steps to create a key vault**<sup>2</sup>).

In this demonstraton, the key vault name is **Example-Vault**.

<sup>1</sup> <https://portal.azure.com/>

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/key-vault/quick-create-portal>

The screenshot shows the Azure Key Vault Overview page for a vault named 'example-vault'. On the left, there's a navigation menu with sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events (preview), Settings (Keys, Secrets, Certificates, Access policies, Networking, Properties, Locks, Export template), Monitoring (Alerts, Metrics, Diagnostic settings, Logs), Support + troubleshooting (Resource health, New support request), and Help & feedback.

On the right, there's a summary card with the following details:

- Resource group (change) : Contoso-Vault
- Location : Central US
- Subscription (change) : jalichwa Projects
- Subscription ID : 9ddb6ca6-f086-4796-8c53-ea831f1df369
- DNS Name : https://example-vault.vault.azure.net/
- Sku (Pricing tier) : Standard
- Directory ID : 72f988bf-86f1-41af-91ab-2d7cd011db47
- Directory Name : Microsoft

Below this, there's a warning message: "The soft delete feature has been enabled on this key vault. After you soft delete this key vault, it will remain in your subscription as a hidden vault. It will get purged after the retention period you specified. You may purge it sooner, or restore the vault, using Azure PowerShell or Azure CLI. Click this for more details."

Under the monitoring section, there are two charts:

- Total requests**: A line chart showing request volume over time. A sharp spike is visible at 6 AM UTC-07:00 on March 31st.
- Average latency**: A line chart showing average response time in milliseconds. The value is consistently around 40ms.

## Create a certificate in Key Vault

Create a certificate or import a certificate into the key vault (If needed, see **Steps to create a certificate in Key Vault<sup>3</sup>**).

In this demo, you'll work on a certificate called **ExampleCertificate**.

## Update certificate lifecycle attributes

In Azure Key Vault, you can update a certificate's lifecycle attributes both before and after the time of certificate creation.

A certificate created in Key Vault can be:

- A self-signed certificate.
- A certificate created with a CA that's partnered with Key Vault.
- A certificate with a CA that isn't partnered with Key Vault.

The following CAs are currently partnered providers with Key Vault:

- **DigiCert**: Key Vault offers OV TLS/SSL certificates.
- **GlobalSign**: Key Vault offers OV TLS/SSL certificates.

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/key-vault/quick-create-portal>

Key Vault auto-rotates certificates through established partnerships with CAs. Because Key Vault automatically requests and renews certificates through the partnership, auto-rotation capability is not applicable for certificates created with CAs that are not partnered with Key Vault.

- ✓ **Note** An account admin for a CA provider creates credentials that Key Vault uses to create, renew, and

The screenshot shows the 'Certificate Authorities' blade in the Azure Key Vault interface. On the left, there's a table with columns 'Name' and 'Provider'. A note at the bottom says 'There are no certificate authorities available.' On the right, a modal window titled 'Create a certificate authority' is open, containing fields for 'Name' (set to 'Example DigiCert'), 'Provider' (set to 'DigiCert'), 'Account ID' (set to 'Username'), 'Account Password' (redacted), and 'Organization ID' (set to 'IDname').

use TLS/SSL certificates.

## Update certificate lifecycle attributes at the time of creation

1. On the Key Vault properties pages, select **Certificates**.
2. Select **Generate/Import**.
3. On the **Create a certificate** screen, update the following values:
  - **Validity Period:** Enter the value (in months). Creating short-lived certificates is a recommended security practice. By default, the validity value of a newly created certificate is 12 months.
  - **Lifetime Action Type:** Select the certificate's auto-renewal and alerting action and then update **percentage lifetime** or **Number of days before expiry**. By default, a certificate's auto-renewal is set at 80 percent of its lifetime. From the drop-down menu, select one of the following options.

Automatically renew at a given time	Email all contacts at a given time
Selecting this option will turn on autorotation.	Selecting this option will not auto-rotate but will only alert the contacts.

4. Select **Create**.

### Create a certificate

Method of Certificate Creation  
Generate

Certificate Name \* ⓘ  
ExampleCertificate

Type of Certificate Authority (CA) ⓘ  
Self-signed certificate

Subject \* ⓘ  
CN=ExampleDomain

DNS Names ⓘ >  
0 DNS names

Validity Period (in months)  
12

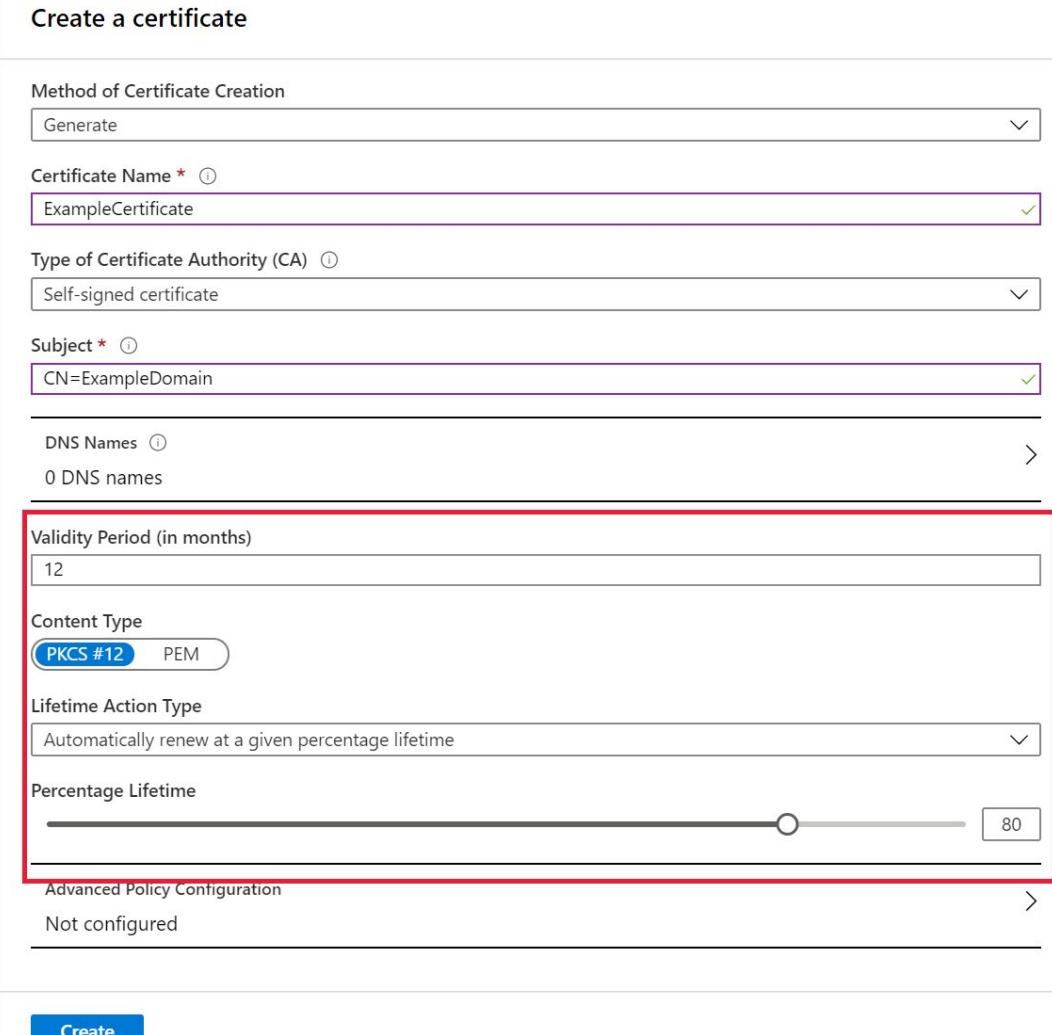
Content Type  
PKCS #12 PEM

Lifetime Action Type  
Automatically renew at a given percentage lifetime

Percentage Lifetime  
 80

Advanced Policy Configuration >  
Not configured

**Create**



## Update lifecycle attributes of a stored certificate

1. Select the key vault.
2. On the Key Vault properties pages, select **Certificates**.
3. Select the certificate you want to update. In this case, you'll work on a certificate called **ExampleCertificate**.
4. Select **Issuance Policy** from the top menu bar.

The screenshot shows the 'ExampleCertificate' page in the Azure Key Vault interface. At the top, there are several buttons: 'New Version', 'Refresh', 'Delete', 'Download Backup', 'Issuance Policy' (which is highlighted with a red box), and 'Certificate Operation'. Below these buttons is a table with columns: 'Version', 'Thumbprint', 'Status', 'Activation Date', and 'Expiration Date'. A single row is listed under 'CURRENT VERSION' with the following values: d8e8263cb363473a... (Version), 6550B28B2DB3316F62... (Thumbprint), Enabled (Status), 3/24/2020 (Activation Date), and 3/24/2021 (Expiration Date).

5. On the **Issuance Policy** screen, update the following values:

- **Validity Period:** Update the value (in months).
- **Lifetime Action Type:** Select the certificate's auto-renewal and alerting action and then update the percentage lifetime or **Number of days before expiry**.

The screenshot shows the 'Issuance Policy' configuration page. It includes a 'Save' and 'Discard' button at the top left. A note below states: 'Issuance policies only affect certificates that will be issued in the future. Modifying this issuance policy will not affect any existing certificates.' The page displays the following details:
 

- Type of Certificate Authority (CA):** Certificate issued by a non-integrated CA.
- Subject:** CN=ExampleCertificate.
- DNS Names:** 0 DNS names.
- Validity Period (in months):** 13 (highlighted with a red box).
- Content Type:** PKCS #12 (selected) and PEM.
- Enabled?**: Yes (selected).
- Lifetime Action Type:** E-mail all contacts at a given percentage lifetime (highlighted with a red box).
- Percentage Lifetime:** A slider set to 80% (highlighted with a red box).

 At the bottom, there are links for 'Advanced Policy Configuration' and 'Not configured'.

6. Select **Save**.

**Important** Changing the Lifetime Action Type for a certificate will record modifications for the existing certificates immediately.

## Update certificate attributes by using PowerShell

```
Set-AzureKeyVaultCertificatePolicy -VaultName $vaultName  
    -Name $certificateName  
    -RenewAtNumberOfDaysBeforeExpiry [276 or  
appropriate calculated value]
```

# Module 11 Review Questions

## Module 11 Review Questions



### Review Question 1

*You download an Azure Resource Manager template based on an existing virtual machine.*

- The template will be used to deploy 300 virtual machines.
- You need to modify the template to reference an administrative password. You must prevent the password from being stored in plain text.

*What should you create to store the password?*

- Azure AD Identity Protection and an Azure Policy
- A Recovery Services vault and a backup policy
- An Azure Key Vault and an access policy
- An Azure Storage account and an access policy

### Review Question 2

*A company has an Azure subscription that contains the Azure virtual machines shown below.*

*Name: TeamVM1*

- Operating System: Windows Server 2012 R2
- Location: East US

*Name: TeamVM2*

- Operating System: Windows Server 2016
- Location: East US

*Name: TeamVM3*

- Operating System: Windows Server 2019
- Location: West US

*Name: TeamVM4*

- Operating System: Ubuntu Server 18.04

- Location: East US  
They create an Azure Key Vault named Vault1 in East US location.

*They need to identify which virtual machines can enable Azure Disk Encryption using Vault1.  
Which virtual machines would you identify?*

- TeamVM3 only
- TeamVM2 and TeamVM3 only
- TeamVM1, TeamVM2, and TeamVM4 only
- TeamVM1, TeamVM2, and TeamVM3 only

# Answers

## Review Question 1

You download an Azure Resource Manager template based on an existing virtual machine.

What should you create to store the password?

- Azure AD Identity Protection and an Azure Policy
- A Recovery Services vault and a backup policy
- An Azure Key Vault and an access policy
- An Azure Storage account and an access policy

*Explanation*

*Correct Answer: An Azure Key Vault and an access policy. Key Vault is a store for credential information that can be accessed from VM deployments. The relevant access policy must be set on the Vault that allows access for VM deployment.*

## Review Question 2

A company has an Azure subscription that contains the Azure virtual machines shown below.

Name: TeamVM1

Name: TeamVM2

Name: TeamVM3

Name: TeamVM4

They need to identify which virtual machines can enable Azure Disk Encryption using Vault1.

Which virtual machines would you identify?

- TeamVM3 only
- TeamVM2 and TeamVM3 only
- TeamVM1, TeamVM2, and TeamVM4 only
- TeamVM1, TeamVM2, and TeamVM3 only

*Explanation*

*Correct Answer: TeamVM1, TeamVM2, and TeamVM4 only. Azure Disk Encryption requires that your key vault and VMs reside in the same Azure region and subscription. Because Team\_VM1 is in East US region, you can use Azure Disk Encryption for all virtual machines which are in the same region, which are Team\_VM1, Team\_VM2, and Team\_VM4. You can use Azure Disk Encryption with Windows and Linux virtual machines.*



## Module 12 Manage Workloads in Azure

### Migrate Workloads using Azure Migrate

#### Overview of Azure Migrate Server Migration

Azure Migrate helps you migrate to the Microsoft Azure cloud. The latest version of Azure Migrate provides a central hub to track discovery, assessment and migration of on-premises apps and workloads, and cloud VMs, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.



#### Key features of Azure Migrate

Azure Migrate provides:

**Unified migration platform:** Use a single portal to start, run, and track your migration journey to Azure, with an improved deployment flow and portal experience.

**Range of tools:** Azure Migrate provides native tools, and integrates with other Azure services, as well as with independent software vendor ISV tools. Select the right assessment and migration tools, based on your organizational requirements.

- **Azure Migrate Server Assessment:** Using the Azure Migrate Server Assessment tool, you can assess VMware VMs and Hyper-V VMs for migration to Azure. You can also assess for migration using other Azure services, and ISV tools.
- **Azure Migrate Server Migration:** Using the Azure Migrate Server Migration tool, you can migrate on-premises VMware VMs and Hyper-V VMs to Azure, as well as physical servers, other virtualized servers, and private/public cloud VMs. In addition, you can migrate to Azure using ISV tools.

- **Database assessment/migration:** Assess on-premises databases for migration to Azure, using the Microsoft Data Migration Assistant (DMA). Migrate on-premises databases to Azure using the Azure Database Migration Service (DMS).
- **Azure Migrate appliance:** Azure Migrate deploys a lightweight appliance for discovery and assessment of on-premises VMware VMs and Hyper-V VMs.

This appliance is used by Azure Migrate Server Assessment, and Azure Migrate Server Migration for agentless migration and continuously discovers server metadata and performance data, for the purposes of assessment and migration.

**VMware VM migration:** Azure Migrate Server Migration provides a couple of methods for migrating on-premises VMware VMs to Azure. An agentless migration using the Azure Migrate appliance, and an agent-based migration that uses a replication appliance, and deploys an agent on each VM you want to migrate.

**Database assessment and migration:** From Azure Migrate, you can assess on-premises databases for migration to Azure using the Azure Database Migration Assistant. You can migrate databases using the Azure Database Migration Service.

**Web app migration:** You can assess web apps using a public endpoint URL with the Azure App Service. For migration of internal .NET apps, you can download and run the App Service Migration Assistant.

**Data Box:** Import large amounts offline data into Azure using Azure Data Box in Azure Migrate.

## VMware Migration

VMware VMs can be migrated using Azure Migrate Server Migration with the following two options:

- **Agentless replication:** Migrate VMs without needing to install anything on them.
- **Agent based replication:** Install an agent on the VM for replication.

Although agentless replication is easier from a deployment perspective, it currently has the following limitations:

**Simultaneous replication:** A maximum of 300 VMs can be simultaneously replicated from a vCenter Server. If you have more than 50 VMs for migration, create multiple batches of VMs. Replicating more at a single time will impact performance.

**VM disks:** A VM that you want to migrate must have 60 or fewer disks (Agentless) or 63 or fewer disks (Agent-based).

For more information, go to [Select a VMware migration option<sup>1</sup>](#).

Both agentless and agent-based replication will be discussed in detail in Lessons 2 and 3.

## Deployment Steps Comparison

There are differences between agentless and agent-based deployment tasks in the VMware migration process. Lessons 2 and 3 provide more detail. This is just a high-level summary of the differences.

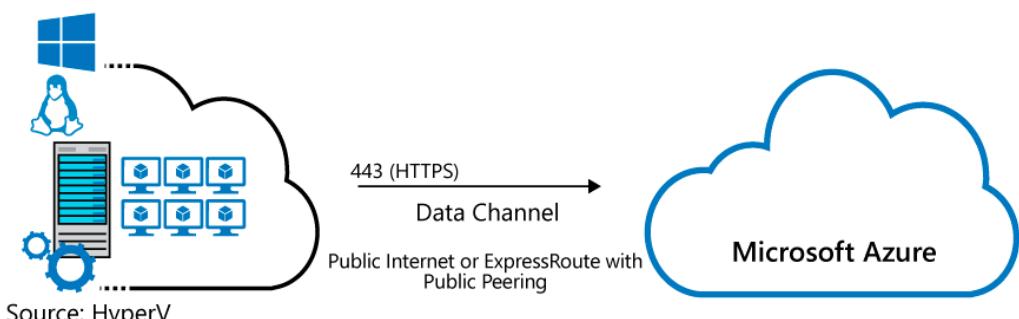
Task	Details	Agentless	Agent-based
<b>Prepare VMware servers and VM for migration</b>	Configure a number of settings on VM servers and VMs	Required	Required

<sup>1</sup> <https://docs.microsoft.com/en-us/azure/migrate/server-migrate-overview#agentless-migration-limitations>

Task	Details	Agentless	Agent-based
<b>Add the Server Migration tool</b>	Add the Azure Migrate Server Migration tool in the Azure Migrate project	Required	Required
<b>Deploy the Azure Migrate appliance</b>	Set up a lightweight appliance on a VMware VM for discovery and assessment	Required	Not required
<b>Install the Mobility service on VMs</b>	Install the Mobility service on each VM you want to replicated	Not required	Required
<b>Deploy the Azure Migrate Server Migration replication appliance</b>	Set up an appliance on a VMware VM to discover VMs and bridge between the Mobility service running on VMs and Azure Migrate Server Migration	Not required	Required
<b>Replicate VMs. Enable VM replication</b>	Configure replication settings and select VMs to replicate	Required	Required
<b>Run a test migration</b>	Run a test migration to make sure everything is working correctly	Required	Required
<b>Run a full migration</b>	Migrate the VMs	Required	Required

## Hyper-V Migration

Azure Migrate Server Migration is a tool for migrating on-premises workloads, and cloud-based VMs, to Azure. Site Recovery is a disaster recovery tool. The tools share some common technology components used for data replication but serve different purposes.



 Microsoft Azure  
Recovery services Agent  
Replicates data to Azure

The Azure Migrate Server Migration tool provides agentless replication for on-premises Hyper-V VMs, using a migration workflow that's optimized for Hyper-V. You install a software agent only on Hyper-V hosts or cluster nodes. Nothing needs to be installed on Hyper-V VMs.

- **Replication provider:** The Microsoft Azure Site Recovery provider is installed on Hyper-V hosts, and registered with Azure Migration Server Migration.

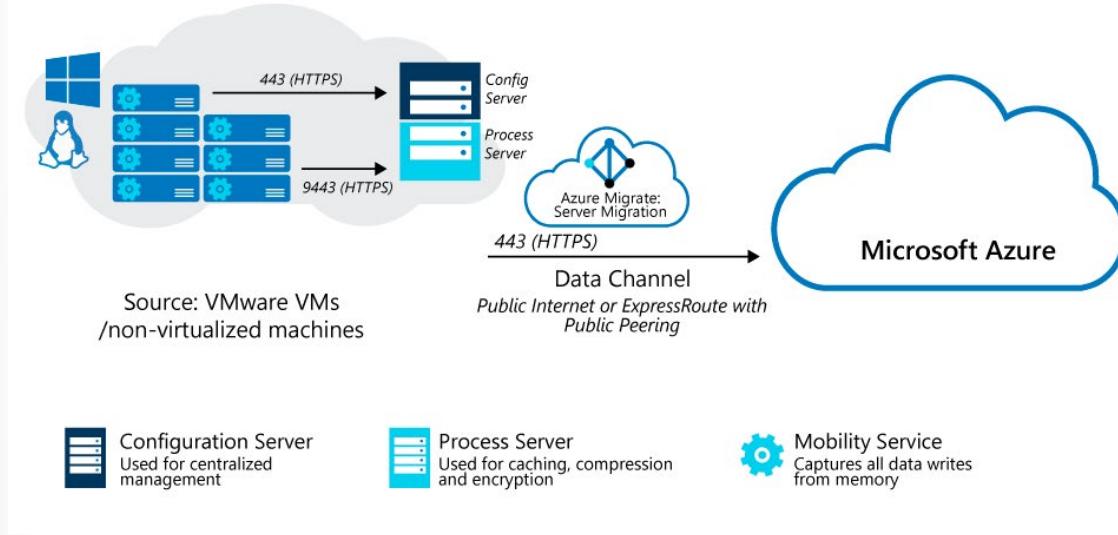
The provider orchestrates replication for Hyper-V VMs.

- **Recovery Services agent:** The Microsoft Azure Recovery Service agent handles data replication. It works with the provider to replicate data from Hyper-V VMs to Azure.

The replicated data is uploaded to a storage account in your Azure subscription. The Server Migration tool processes the replicated data and applies it to replica disks in the subscription. The replica disks are used to create the Azure VMs when you migrate.

## Agent-based Migration Architecture

The architecture for agent-based migration of VMware VMs to Azure is shown in the following diagram.



There are some core requirements for agent-based migration of VMware to Azure migration scenarios.

1. An Azure subscription, Azure Storage account for cache, Managed Disk and Azure network.
2. A Configuration Server VM hosted on VMware. We recommend that you run it as a VMware VM that can be deployed from a downloaded OVF template. The machine runs all on-premises Site Recovery components, which include the configuration server, process server, and master target server.
  - **Configuration server:** Coordinates communications between on-premises and Azure, and manages data replication.
  - **Process server:** Installed by default on the configuration server. It receives replication data; optimizes it with caching, compression, and encryption; and sends it to Azure Storage. The process server also installs Azure Site Recovery Mobility Service on VMs you want to replicate, and performs automatic discovery of on-premises machines. As your deployment grows, you can add additional, separate process servers to handle larger volumes of replication traffic.
3. ESXi and vCenter hosts
  - During Site Recovery deployment, you add VMware servers to the Recovery Services vault.

4. Mobility Service on all VMware VMs to replicate or migrate.
  - We recommend that you allow automatic installation from the process server. Alternatively, you can install the service manually or use an automated deployment method, such as System Center Configuration Manager. An account with permissions to the VMware Hosts.
  - VMs must meet the requirements found listed here: **Replicated machines<sup>2</sup>**
5. Azure Storage – The following are not supported: Cool Storage, Hot Storage, Block Blobs, Import/Export Service, General Purpose v2. For more information, go to **Azure Storage<sup>3</sup>**.

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix#replicated-machines>

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix#azure-storage>

## VMware - Agentless Migration

### Preparation for Agentless VMware Migration

The following sections cover the prerequisites, requirements, and permissions tasks that need to be done prior to an agentless VMWare migration.

1. Review **VMware server requirements**<sup>4</sup> for agentless migration.
2. Set up an account to access the vCenter Server with the **required permissions**<sup>5</sup> for agentless migration.
3. Note the **requirements for VMware VMs**<sup>6</sup> that you want to migrate to Azure using agentless migration.
4. Review **appliance requirements**<sup>7</sup> for agentless migration.
5. Note **appliance URL access**<sup>8</sup> and **port access**<sup>9</sup> requirements for agentless migration.

### Agentless migration-VMware server requirements

This table summarizes assessment support and limitations for VMware visualization servers.

Support	Details
vCenter server	VMware VMs you migrate using an agentless migration must be managed by one or more vCenter Servers running 5.5, 6.0, 6.5, or 6.7.

### Agentless migration-vCenter Server permissions

Permissions	Details
Datastore.Browse	Allow browsing of VM log files to troubleshoot snapshot creation and deletion.
Datastore.LowLevelFileOperations	Allow read/write/delete/rename operations in the datastore browser, to troubleshoot snapshot creation and deletion.
VirtualMachine.Configuration.DiskChangeTracking	Allow enable or disable change tracking of VM disks, to pull changed blocks of data between snapshots.
VirtualMachine.Configuration.DiskLease	Allow disk lease operations for a VM, to read the disk using the VMware vSphere Virtual Disk Development Kit (VDDK).
VirtualMachine.Provisioning.AllowReadOnlyDiskAccess	Allow opening a disk on a VM, to read the disk using the VDDK.

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware#assessment-vmware-server-requirements>

<sup>5</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware#agentless-migration-vcenter-server-permissions>

<sup>6</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware#agentless-migration-vmware-vm-requirements>

<sup>7</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware#assessment-appliance-requirements>

<sup>8</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware#assessment-url-access-requirements>

<sup>9</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware#assessment-port-requirements>

Permissions	Details
VirtualMachine.Provisioning.AllowVirtualMachine-Download	Allows read operations on files associated with a VM, to download the logs and troubleshoot if failure occurs.
VirtualMachine.SnapshotManagement	Allow creation and management of VM snapshots for replication.
Virtual Machine.Interaction.Power Off	Allow the VM to be powered off during migration to Azure.

## Agentless migration-VMware VM requirements

Windows and Linux operating systems are supported by Azure can be migrated using agentless migration. However, some VMs might require changes so that they can run in Azure. Azure Migrate makes these changes automatically for the following operating systems:

- Red Hat Enterprise Linux 6.5+, 7.0+
- CentOS 6.5+, 7.0+
- SUSE Linux Enterprise Server 12 SP1+
- Ubuntu 14.04LTS, 16.04LTS, 18.04LTS
- Debian 7,8

The following table summarizes the remaining agentless migration-VMware requirements, support and limitations.

Support	Details
<b>Linux boot</b>	If /boot is on a dedicated partition, it should reside on the OS disk, and not be spread across multiple disks. If /boot is part of the root (/) partition, then the '/' partition should be on the OS disk, and not span other disks.
<b>UEFI boot</b>	VMs with UEFI boot aren't supported for migration.
<b>Encrypted disks/volumes</b>	VMs with encrypted disks/volumes aren't supported for migration.
<b>RDM/passthrough disks</b>	If VMs have RDM or passthrough disks, these disks won't be replicated to Azure.
<b>NFS</b>	NFS volumes mounted as volumes on the VMs won't be replicated.
<b>Target disk</b>	VMs can only be migrated to managed disks (standard HHD, premium SSD) in Azure.

## Agentless migration-appliance requirements

The following table lists the agentless migration-appliance requirements and prerequisites.

Support	Details
<b>ESXi</b>	The appliance VM must be deployed on an ESXi host running version 5.5 or later.

Support	Details
Azure Migrate project	An appliance can be associated with a single project.
vCenter Server	An appliance can discover up to 10,000 VMware VMs on a vCenter Server. An appliance can connect to one vCenter Server.
VDDK	If you're running an agentless migration with Azure Migrate Server Migration, the VMware vSphere Virtual Disk Development Kit (VDDK) must be installed on the appliance VM.

## Agentless migration-URL access requirements

The Azure Migrate appliance needs internet connectivity to the internet.

- When you deploy the appliance, Azure Migrate does a connectivity check to the URLs summarized in the table below.
- If you're using a URL-based firewall.proxy, allow access to these URLs, making sure that the proxy resolves any CNAME records received while looking up the URLs.

URL	Details
*.portal.azure.com	Navigate to the Azure Migrate in the Azure portal.
*.windows.net	Log into your Azure subscription.
*.microsoftonline.com	Create Active Directory apps for the appliance to communicate with the Azure Migrate service.
management.azure.com	Create Active Directory apps for the appliance to communicate with the Azure Migrate service.
dc.services.visualstudio.com	Upload app logs used for internal monitoring.
*.vault.azure.net	Manage secrets in the Azure Key Vault.
*.servicebus.windows.net	Communication between the appliance and the Azure Migrate service.
*.blob.core.windows.net	Upload data to storage accounts.

Additionally, to connect to Azure Migrate service URLs, you will need to allow access to the following:

- \*.discoverysrv.windowsazure.com
- \*.migration.windowsazure.com
- \*.hypervrecoverymanager.windowsazure.com

## Preparing Azure for Migration

In preparing to migrate, you will need to ensure you have permissions to perform the following tasks in Azure

## Assign permissions to create project

- In the Azure portal, open the subscription, and select **Access control (IAM)**.
- In **Check access**, find the relevant account, and click it to view permissions.

You should have **Contributor** or **Owner** permissions. If you just created a free Azure account, you're the owner of your subscription. If you're not the subscription owner, work with the owner to assign the role.

## Assign permissions to register the appliance

If you're deploying the Azure Migrate appliance to assess or run an agentless migration of VMs, you need to register it. During appliance registration, Azure Migrate creates two Azure Active Directory (Azure AD) apps that uniquely identify the appliance.

- The first app communicates with Azure Migrate service endpoints.
- The second app accesses an Azure Key Vault created during registration to store Azure AD app info and appliance configuration settings.

## Assign permissions to create the Azure AD apps

You can assign permissions for Azure Migrate to create these Azure AD apps using one of the following methods:

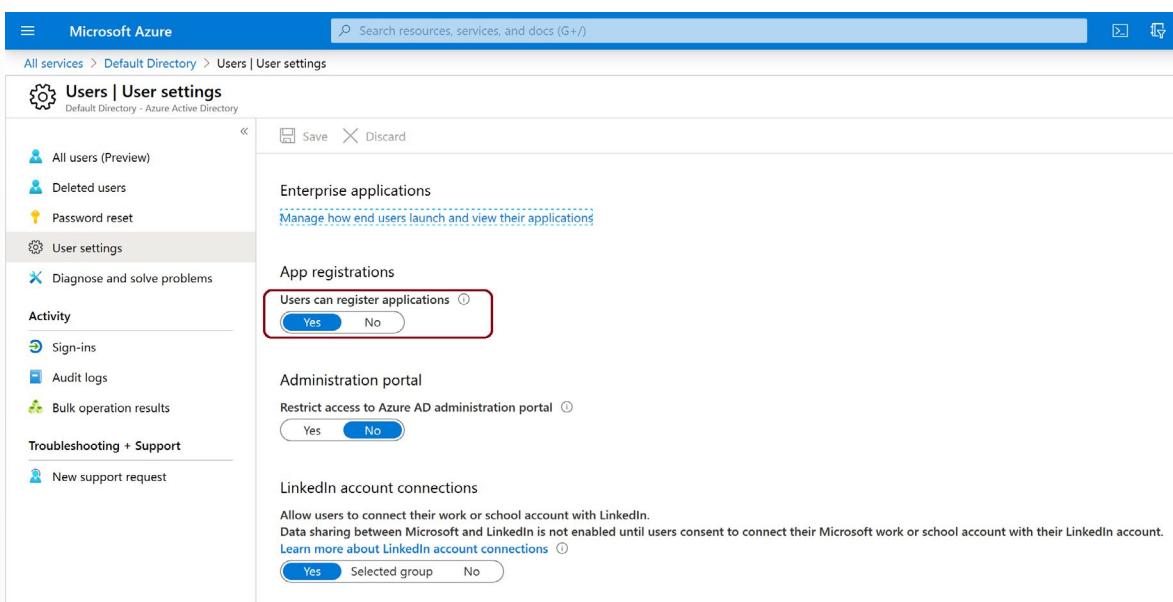
1. A tenant/global admin can grant permissions to users in the tenant, to create and register Azure AD apps.
  2. A tenant/global admin can assign the Application Developer role (that has the permissions) to the account.
- ✓ It's worth noting that the apps don't have any other access permissions on the subscription other than those described above. Additionally, you only need these permissions when you register a new appliance. You can remove the permissions after the appliance is set up.

## Prepare Azure - grant permissions

The tenant/global admin can grant permissions as follows:

In Azure AD, the tenant/global admin should navigate to **Azure Active Directory > Users > User Settings**.

The admin should set App registrations to **Yes**.



The screenshot shows the Microsoft Azure portal interface for managing user settings in a Default Directory - Azure Active Directory. The left sidebar has a tree view with 'User settings' selected. The main content area includes sections for 'Enterprise applications', 'App registrations' (with a 'Users can register applications' toggle set to 'Yes'), 'Administration portal' (with a 'Restrict access to Azure AD administration portal' toggle set to 'No'), and 'LinkedIn account connections' (with a 'Allow users to connect their work or school account with LinkedIn' toggle set to 'Yes' and 'Selected group' selected). There are 'Save' and 'Discard' buttons at the top.

## Assign Application Developer role

The tenant/global admin can assign the Application Developer role to an account.

## Assign permissions to create the Key Vault

Assign role assignment permissions on the resource group in which the Azure Migrate project resides, as follows:

1. In the resource group in the Azure portal, select **Access control (IAM)**.
  2. In **Check access**, find the relevant account, and click it to view permissions. You need **Owner** (or **Contributor and User Access Administrator**) permissions.
- ✓ If you don't have the required permissions, request them from the resource group owner.

## Adding the Azure Migrate Server Migration Tool

Having assigned the required permissions, you next add the Azure Migrate Server Migration tool to the Azure Migrate project.

1. In the Azure Migrate project, click **Overview**.
2. In Discover, assess, and migration servers, click **Assess and migrate servers**.

**Migrate your on-premises datacenter to Azure**

Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or [find an expert](#) to help with your migration. [Learn more](#)

**Windows and Linux servers**

Discover, assess and migrate your on-premises VMware and Hyper-V virtual machines or Physical servers to Azure.

[Assess and migrate servers](#)

**SQL and other databases**

Assess and migrate your on-premises databases to Azure SQL Database Managed Instance or Azure SQL Database.

[Assess and migrate databases](#)

**Explore more scenarios**

Assess and migrate web apps, migrate data and assess virtual desktop infrastructure (VDI). Find guidance on various migration activities

[Explore more](#)

**3. In Migration tools, select [Click here to add a migration tool when you are ready to migrate](#).**

**Assessment tools**

**Azure Migrate: Server Assessment**

[Discover](#) [Assess](#) [Overview](#)

**Quick start**

**1: Discover**  
Click 'Discover' to start discovering your on-premises machines.

**2: Assess**  
Once your on-premises machines are discovered, click "Assess" to create assessments.

Add more assessment tools? [Click here](#).

**Cloudamize**

[Register with Azure Migrate\\*](#)

**Quick start**

**1: Register**  
Procure license for Cloudamize or start with a free trial of Cloudamize. [Learn more](#)

**2: Connect**  
Click on 'Register with Azure Migrate' and follow the listed steps to connect your Cloudamize workspace to Azure Migrate.

You do not have any migration tools yet. [Click here to add a migration tool when you are ready to migrate](#).

**4. In the tools list, select **Azure Migrate: Server Migration > Add tool**.**

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
<b>Azure Migrate: Server Migration</b>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines Physical machines Migration from other public clouds	Supports Windows and Linux Agentless and agent-based migration Cutover in seconds Minimal application downtime	<a href="#">Learn more</a>

Azure Migrate Server Migration runs a lightweight VMware VM appliance. The appliance performs VM discovery and sends VM metadata and performance data to Azure Migrate Server Migration. The same appliance is also used by the Azure Migrate Server Assessment tool.

To do this:

- Download an OVA template file and import it to vCenter Server.
- Create the appliance, and check that it can connect to Azure Migrate Server Assessment.
- Configure the appliance for the first time and register it with the Azure Migrate project.

- ✓ These steps were introduced in Module 1.

## Preparing VMs for Migration

Azure Migrate requires some VM changes to ensure that VMs can be migrated to Azure. For some **operating systems**<sup>10</sup>, Azure Migrate makes these changes automatically. For other operating systems, you need to make adjustments manually before migration. The **migrate tutorial**<sup>11</sup> explains how to do this.

It's important to make these changes before you begin migration. If you migrate the VM before you make the change, the VM might not boot up in Azure.

Configuration changes you make to on-premises VMs are replicated to Azure after replication for the VM is enabled. To ensure that changes are replicated, make sure that the recovery point you migrate to is later than the time at which the configuration changes were made on-premises.

### Windows Server VMs

As you prepare Windows Server VMs for migration, you should first ensure you have done the actions in the following table.

Actions	Details
Ensure that Windows volumes in Azure VM use the same drive letter assignments as the on-premises VM	Configure the SAN policy as Online All
Enable Azure screen access console for the Azure VM	This helps with troubleshooting. You don't need to reboot the VM. The Azure VM will boot using the disk image, and this is equivalent to a reboot for the new VM.
Install Hyper-V Guest Integration	If you're migrating machines running Windows Server 2003, install Hyper-V Integration Services on the VM operating system.
Remote Desktop	Enable Remote Desktop on the VM, and check that the Windows Firewall isn't blocking Remote Desktop access on any network profiles.

To configure the SAN policy:

1. Sign in to the VM with an admin account and open a command window.
2. Type **diskpart** to run the Diskpart utility.
3. Type **SAN POLICY=OnlineAll**
4. Type **Exit** to leave Diskpart, and close the command prompt.

### Linux VMs

Likewise, as you prepare Linux VMs for Migrate, ensure first that you have done the actions in the following table.

<sup>10</sup> <https://docs.microsoft.com/en-us/azure/migrate/server-migrate-overview>

<sup>11</sup> <https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware>

Actions	Details
Install Hyper-V Linux Integration Services	Most new versions of Linux distributions have this included by default.
Rebuild the Linux init image to contain the necessary Hyper-V drivers	This ensures that the VM will boot in Azure, and is only required on some distributions.
Enable Azure serial console logging	This helps with troubleshooting. You don't need to reboot the VM. The Azure VM will reboot using the disk image, and this is equivalent to a reboot for the new VM.
Update device map file	Update the device map file that has the device name to volume associations, to persistent identifiers.
Update fstab entries	Update entries to use persistent volume identifiers.
Remove udev rule	Remove any udev rules that reserve interface names based on mac address, etc.
Update network interfaces	Update network interfaces to receive IP addresses based on DHCP.
Enable ssh	Ensure ssh is enabled and the sshd service is set to start automatically on reboot. Ensure that incoming ssh connection requests are not blocked by the OSS firewall or scriptable rules.

## Replicating VMs

This section walks through the process of setting up replication of VMs in the Azure portal. The instructor may demonstrate this section at this point.

1. In the Azure Migrate project > **Servers, Azure Migrate: Server Migration**, click **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation sidebar with options like Overview, Migration goals (Servers selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area has two sections: 'Assessment tools' and 'Migration tools'. The 'Assessment tools' section contains 'Discover', 'Assess', and 'Overview' tabs, with sub-options for Discovered servers (442), Groups (2), Assessments (2), and Notifications (0). A note says 'Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis'. Below it, there's a link to 'Add more assessment tools? Click here.' The 'Migration tools' section contains 'Discover', 'Replicate' (which is highlighted with a red box), 'Migrate', and 'Overview' tabs, with a 'Discovered servers' count of 442.

2. In **Replicate**, > **Source settings** > **Are your machines virtualized?**, select **Yes, with VMware vSphere**.
3. In **On-premises appliance**, select the name of the Azure Migrate appliance that you set up and click **OK**.

The screenshot shows the 'Replicate' configuration dialog. At the top, there are tabs for 'Source settings' (selected), 'Virtual machines', 'Target settings', 'Compute', 'Disks', and 'Review + Start replication'. Below the tabs, a note says 'The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure.' There are two dropdown menus: one for 'Are your machines virtualized?' containing 'Yes, with VMware vSphere' (selected) and another for 'On-premises appliance' containing '<appliance-name>'.

4. In **Virtual machines**, select the machines you want to replicate.

**Replicate**

Source settings **Virtual machines** Target settings Compute Disks Review + Start replication

Select the virtual machines to be migrated.

\* Import migration settings from an assessment?

Select

Yes, apply migration settings from a Azure Migrate assessment  
No, I'll specify the migration settings manually

- If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. To do this, in **Import migration settings from an Azure Migrate assessment?**, select the **Yes** option.  
If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** option.  
If you selected to use the assessment, select the VM group, and assessment name.
- In **Virtual machines**, search for VMs as needed, and check each VM you want to migrate. Then click **Next: Target settings**.

**Replicate**

Source settings **Virtual machines** Target settings Compute Disks Review + Start replication

Select the virtual machines to be migrated.

\* Import migration settings from an assessment?

\* Virtual machines

Search to filter machines

NAME	IP ADDRESS	OPERATING SYSTEM	BOOT TYPE
ContosoVMwareMigr...	2404.f801:4800:25:c95f5fd3:7347:4f91,1...	Microsoft Windows Server Threshold (64... bios	
ContosoCSASR	2404.f801:4800:25:29:9:2ebd:1ee0:eeb4,...	Microsoft Windows Server 2012 (64-bit) bios	
Contoso-FrontTier3		Microsoft Windows Server Threshold (64... bios	
ContosoWeb1	2404.f801:4800:25:9091:9912:f146:9108,...	Microsoft Windows Server 2008 (32-bit) bios	
Contoso-Configuratio...		Microsoft Windows Server 2012 (64-bit) bios	
Contoso-AzureMigrat...		Microsoft Windows Server 2012 (64-bit) bios	
ContosoWeb3	10.150.13.218,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios
ContosoAppSrv2	2404:f801:4800:25:5de5e919:3448:be33,...	Microsoft Windows Server 2012 (64-bit)	bios
ContosoWeb2	10.150.13.201,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios

Selected items : 9

## Target, Compute, and Disk Settings

This section completes the process of setting up replication of VMs in the Azure portal by showing how to configure target, compute, and disk settings.

### Target settings

- In **Target settings**, select the subscription, and target region to which you'll migrate, and specify the resource group in which the Azure VMs will reside after migration.

2. In **Virtual Network**, select the Azure VNet/subnet to which the Azure VMs will be joined after migration.

3. In **Azure Hybrid Benefit**:

Select **No** if you don't want to apply Azure Hybrid Benefit. Then click **Next**.

Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions, and you want to apply the benefit to the machines you're migrating. Then click **Next**.

The screenshot shows the 'Replicate' dialog box with the 'Target settings' tab selected. It displays fields for selecting a Region (US East US), Subscription (Azure Migrate Program Management Team), Resource group (ContosoDemoRG), Virtual Network (ContosoDemoNW), and Subnet (default). Below these, there's a section for 'Azure Hybrid Benefit' with a note about saving up to 49% on virtual machine costs. A question asks if the user already has an eligible Windows Server license, with 'Yes' and 'No' buttons.

## Compute settings

4. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements<sup>12</sup>](#).
- **VM size:** If you're using assessment recommendations, the VM size dropdown will contain the recommended size. Otherwise Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in **Azure VM size**.
  - **OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
  - **Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.

<sup>12</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware>

**Replicate**

NAME	AZURE VM NAME	SOURCE VM SIZE	AZURE VM SIZE
ContosoVMwareMigration2	ContosoVMwareMigration2	8 Cores, 16384 MB RAM	Automatically select matching configuration
ContosoCSASR	ContosoCSASR	2 Cores, 2048 MB RAM	Automatically select matching configuration
Contoso-FrontTier3	Contoso-FrontTier3	8 Cores, 16384 MB RAM	Automatically select matching configuration
ContosoWeb1	ContosoWeb1	2 Cores, 2048 MB RAM	Automatically select matching configuration
Contoso-ConfigurationServer	Contoso-ConfigurationServer	8 Cores, 16384 MB RAM	Automatically select matching configuration
Contoso-AzureMigrateAppliance	Contoso2	✓ 4 Cores, 8192 MB RAM	Automatically select matching configuration
ContosoWeb3	ContosoWeb3	2 Cores, 2048 MB RAM	Automatically select matching configuration
ContosoAppSrv2	ContosoAppSrv2	2 Cores, 4096 MB RAM	Automatically select matching configuration
ContosoWeb2	ContosoWeb2	2 Cores, 2048 MB RAM	Automatically select matching configuration

## Disk settings

- In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium-managed disks) in Azure. Then click **Next**.  
You can exclude disks from replication.  
If you exclude disks, they won't be present on the Azure VM after migration.

**Replicate**

NAME	DISKS TO REPLICATE	DISK SIZE GB
ContosoVMwareMigration2	All selected	80
	scsi0:0	80
ContosoCSASR	All selected	80
	scsi0:0	80
Contoso-FrontTier3	All selected	80
	scsi0:0	80
ContosoWeb1	All selected	40
	scsi0:0	40

- In **Review and start replication**, review the settings, and click **Replicate** to start the initial replication for the servers.

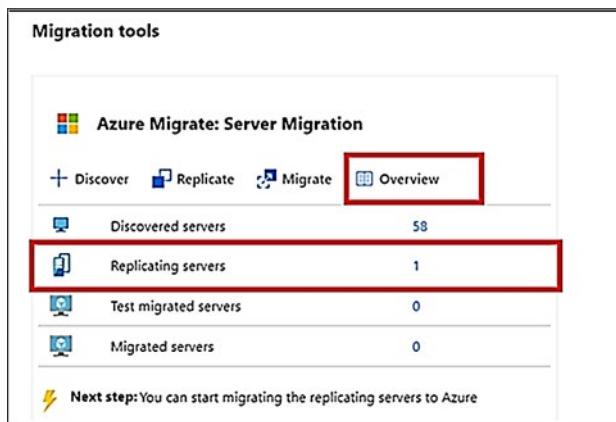
## Tracking and Monitoring Replication

When you click **Replicate** a Start Replication job begins. When the Start Replication job finishes successfully, the machines begin their initial replication to Azure.

During initial replication, a VM snapshot is created. Disk data from the snapshot is replicated to replica managed disks in Azure.

After initial replication finishes, delta replication begins. Incremental changes to on-premises disks are periodically replicated to the replica disks in Azure.

You can track job status in the portal notifications. You can monitor replication status by clicking on **Replicating servers** in **Azure Migrate: Server Migration**.



## Provisioning for the first time

If this is the first VM you're replicating in the Azure Migrate project, Azure Migrate Server Migration automatically provisions these resources in same resource group as the project.

- **Service bus:** Azure Migrate Server Migration uses the service bus to send replication orchestration messages to the appliance.
- **Gateway storage account:** Server Migration uses the gateway storage account to store state information about the VMs being replicated.
- **Log storage account:** The Azure Migrate appliance uploads replication logs for VMs to a log storage account. Azure Migrate applies the replication information to the replica managed disks.
- **Key vault:** The Azure Migrate appliance uses the key vault to manage connection strings for the service bus, and access keys for the storage accounts used in replication. You should have set up the permissions that the key vault needs to access the storage account when you prepared. **Review these permissions<sup>13</sup>.**

## Testing the Migration

When delta replication begins, you can run a test migration for the VMs, before running a full migration to Azure. We highly recommend that you do this at least once for each machine, before you migrate it.

Running a test migration checks that migration will work as expected, without impacting the on-premises machines, which remain operational, and continue replicating. Test migration simulates the migration by creating an Azure VM using replicated data (usually migrating to a non-production VNet in your Azure subscription).

You can use the replicated test Azure VM to validate the migration, perform app testing, and address any issues before full migration.

1. In **Migration goals > Servers > Azure Migrate: Server Migration**, click **Test migrated servers**.

<sup>13</sup> <https://docs.microsoft.com/en-us/azure/migrate/tutorial-prepare-vmware>

The screenshot shows the 'Azure Migrate: Server Migration' dashboard. At the top, there are four navigation links: Discover, Replicate, Migrate, and Overview. Below them is a summary table:

Discovered servers	442
Replicating servers	6
<b>Test migrated servers</b>	1
Migrated servers	1

A note at the bottom says: "Next step: You can start migrating the replicating servers to Azure". The 'Test migrated servers' row is highlighted with a red box.

In **Test Migration**, select the Azure VNet in which the Azure VM will be located after the migration. We recommend you use a non-production VNet. The **Test migration** job starts. Monitor the job in the portal notifications. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.

2. Right-click the VM to test, and click **Test migrate**.

The screenshot shows the 'Replicating machines' list page. On the left is a sidebar with options: Overview, Getting started, Migrate servers to Azure, Manage (selected), Replicating machines, Jobs, Events, Settings, and Properties. The main area lists one machine: Contoso-Win2K8R2SP1, which is in Delta sync status, healthy, and in Test migration pending phase. A context menu is open for this machine, with the 'Clean up test migration' option highlighted with a red box.

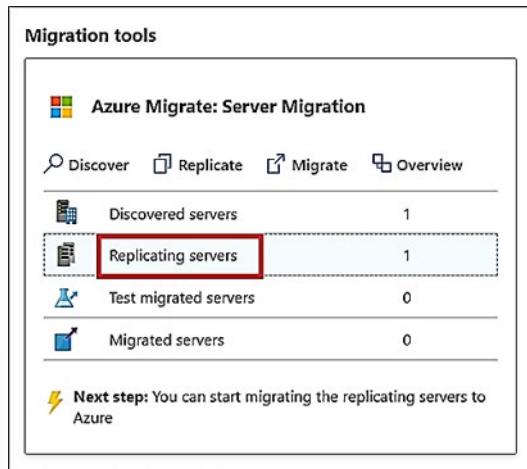
3. After the test is done, right-click the Azure VM in **Replicating machines**, and click **Clean up test migration**.

The screenshot shows the same 'Replicating machines' list page as the previous one. The context menu for the same machine (Contoso-Win2K8R2SP1) is shown again, with the 'Clean up test migration' option highlighted with a red box.

# Migrating Virtual Machines

After you've verified that the test migration works as expected, you can migrate the on-premises machines.

1. In the Azure Migrate project > **Servers** > **Azure Migrate: Server Migration**, click **Replicating servers**.
2. In **Replicating machines**, right-click the VM >**Migrate**.



3. In **Migrate** > **Shut down virtual machines and perform a planned migration with no data loss**, select **Yes** > **OK**.
  - By default Azure Migrate shuts down the on-premises VM and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This ensures no data loss.
  - If you don't want to shut down the VM, select **No**.
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

## Complete the migration

1. After the migration is done, right-click the VM > **Stop migration**. This stops replication for the on-premises machine, and cleans up replication state information for the VM.
2. Install the Azure VM **Windows<sup>14</sup>** or **Linux<sup>15</sup>** agent on the migrated machines.
3. Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
4. Perform final application and migration acceptance testing on the migrated application now running in Azure.
5. Cut over traffic to the migrated Azure VM instance.
6. Remove the on-premises VMs from your local VM inventory.
7. Remove the on-premises VMs from local backups.

<sup>14</sup> <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/agent-windows>

<sup>15</sup> <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/agent-linux>

- 
8. Update any internal documentation to show the new location and IP address of the Azure VMs.

## VMware - Agent-Based Migration

### Preparing Azure for Migration

Just like agentless migration, agent-based migration requires that you prepare Azure and ensure you have the appropriate permissions to perform the following tasks:

- Create an Azure Migrate project
- Register the Azure Migrate replication appliance
- Create a Key Vault

### Assign permissions to create project

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.

You should have **Contributor** or **Owner** permissions. If you just created a free Azure account, you're the owner of your subscription. If you're not the subscription owner, work with the owner to assign the role.

### Assign permissions to register the appliance

If you're deploying the Azure Migrate appliance to assess or run an agentless migration of VMs, you need to register it. During appliance registration, Azure Migrate creates two Azure Active Directory (Azure AD) apps that uniquely identify the appliance.

- The first app communicates with Azure Migrate service endpoints.
- The second app accesses an Azure Key Vault created during registration to store Azure AD app info and appliance configuration settings.

### Assign permissions to create the Azure AD apps

You can assign permissions for Azure Migrate to create these Azure AD apps using one of the following methods:

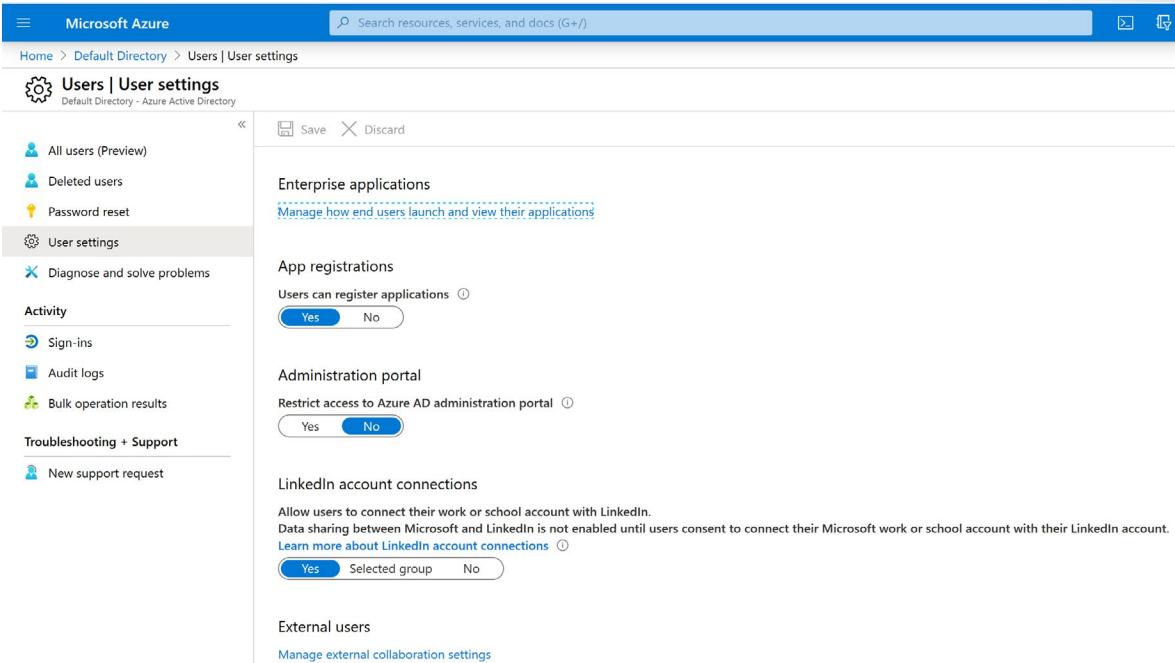
1. A tenant/global admin can grant permissions to users in the tenant, to create and register Azure AD apps.
  2. A tenant/global admin can assign the Application Developer role (that has the permissions) to the account.
- ✓ It's worth noting that the apps don't have any other access permissions on the subscription other than those described above. Additionally, you only need these permissions when you register a new appliance. You can remove the permissions after the appliance is set up.

### Prepare Azure - grant permissions

The tenant/global admin can grant permissions as follows:

In Azure AD, the tenant/global admin should navigate to **Azure Active Directory > Users > User Settings**.

The admin should set App registrations to **Yes**.



## Assign Application Developer role

The tenant/global admin can assign the Application Developer role to an account.

## Assign permissions to create the Key Vault

Assign role assignment permissions on the resource group in which the Azure Migrate project resides, as follows:

1. In the resource group in the Azure portal, select **Access control (IAM)**.
  2. In **Check access**, find the relevant account, and click it to view permissions. You need **Owner** (or **Contributor** and **User Access Administrator**) permissions.
- ✓ If you don't have the required permissions, request them from the resource group owner.

## Preparing the On-premises VMware Environment

As part of the preparation of the VMware environment, you must prepare an account for automatic discovery of the virtual machines on the VMware hosts. Azure Migrate Server Migration needs access to VMware servers to:

- Automatically discover VMs. At least a read-only account is required.
- Orchestrate replication, failover, and fallback.

You need an account that can run operations such as creating and removing disks and powering on VMs. Use a dedicated account, create a role at the vCenter level. In addition, you must install the Mobility service on machines you want to replicate.

## Roles and permissions required for the VMware account

The following lists provide details on roles and permissions for the VMware account:

### VM discovery

- At least a read-only user
  - User assigned at datacenter level, and has access to all the objects in the datacenter.
- Data Center object -> Propagate to Child Object, role=Read-only
  - To restrict access, assign the **No access** role with the **Propagate to child** object, to the child objects (vSphere hosts, datastores, VMs and networks).

### Full replication, failover, fallback

- Create a role (Azure\_Site\_Recovery) with the required permissions, and then assign the role to a VMware user or group
  - User assigned at datacenter level, and has access to all the objects in the datacenter.
- Data Center object -> Propagate to Child Object, role=Azure\_Site\_Recovery
  - To restrict access, assign the **No access** role with the **Propagate to child** object, to the child objects (vSphere hosts, datastores, VMs and networks).
- Datastore -> Allocate space, browse datastore, low-level file operations, remove file, update virtual machine files
- Network -> Network assign
- Resource -> Assign VM to resource pool, migrate powered off VM, migrate powered on VM
- Tasks -> Create task, update task
- Virtual machine -> Configuration
- Virtual machine -> Interact -> answer question, device connection, configure CD media, configure floppy media, power off, power on, VMware tools install
- Virtual machine -> Inventory -> Create, register, unregister
- Virtual machine -> Provisioning -> Allow virtual machine download, allow virtual machine files upload
- Virtual machine -> Snapshots -> Remove snapshots

## Prepare an account for Mobility service installation

The Mobility service must be installed on machines you want to replicate. The Azure Migrate replication appliance can do a push installation of this service when you enable replication for a machine, or you can install it manually, or using installation tools.

- ✓ In this topic, we will look at installing the Mobility service with the push installation.

For this push installation, you need to prepare an account that Azure Migrate Server Migration can use to access the VM.

Prepare the account as follows:

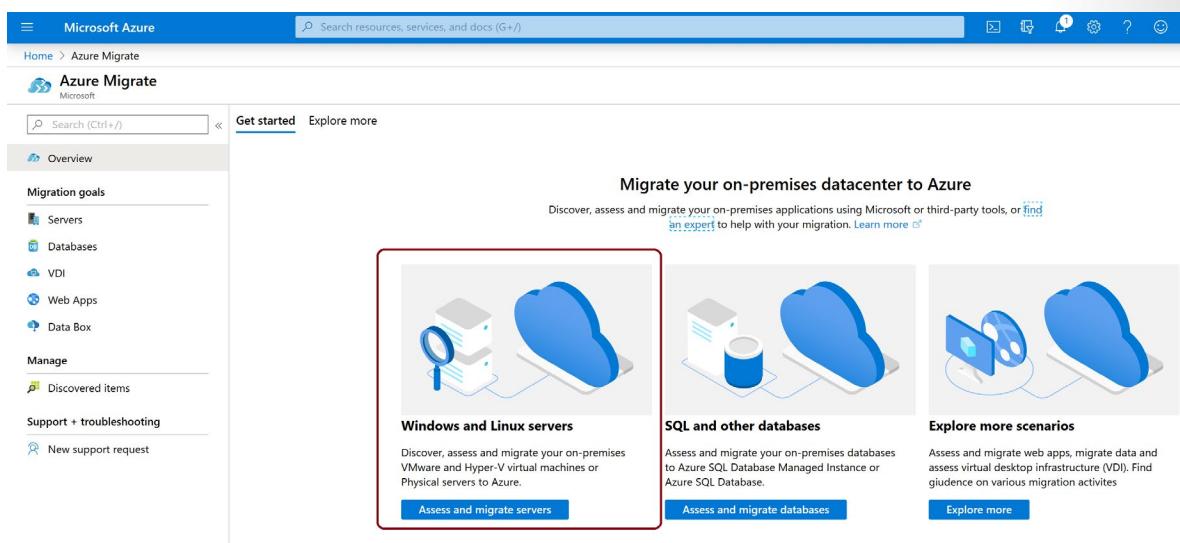
Prepare a domain or local account with permissions to install on the VM.

- **Windows VMs:** To install on Windows VMs if you're not using a domain account, disable Remote User Access control on the local machine. To do this, in the registry > **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**, add the DWORD entry **LocalAccountTokenFilterPolicy**, with a value of 1.
- **Linux VMs:** To install on Linux VMs, prepare a root account on the source Linux server.

## Adding the Azure Migrate Server Migration Tool

As explained in the previous lesson, If you have not yet done so, you need to set up an Azure Migrate project, and then add the Azure Migrate Server Migration tool.

1. In the Azure portal, select **All services**, and search for **Azure Migrate**.
2. Under Services, select **Azure Migrate**.
3. In the Azure Migrate project, click **Overview**.
4. In **Windows and Linux servers**, click **Assess and migrate servers**.



5. In **Discover, assess and migrate servers**, click **Add tools**.
6. In **Migrate project**, select your Azure subscription, and create a resource group if you don't have one.
7. In **Project Details**, specify the project name, and geography in which you want to create the project, and click **Next**.
8. In **Select assessment tool**, select **Skip adding an assessment tool for now > Next**.
9. In **Select migration tool**, select **Azure Migrate: Server Migration > Next**.
10. In **Review + add tools**, review the settings and click **Add tools**.

After adding the tool, it appears in the Azure Migrate project > **Servers > Migration tools**.

The screenshot shows the 'Add a tool' step in the Azure Migrate interface. At the top, there are tabs: 'Migrate project' (selected), 'Select assessment tool', 'Select migration tool', and 'Review + add tool(s)'. Below the tabs, a note says: 'A migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project.' There are dropdown menus for 'Subscription' (set to 'ContosoCorporation') and 'Resource group' (set to 'centraluseup'). Under 'PROJECT DETAILS', there are fields for 'Migrate project' (set to 'Contoso-Project') and 'Geography' (set to 'centraluseup'). At the bottom right is a 'Next' button.

## Replication Appliance

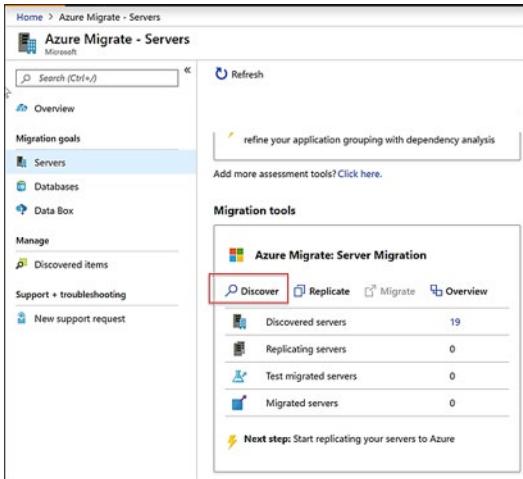
As introduced in the previous lesson, the replication appliance is a single, highly available, on-premises VMware VM that hosts these components:

- **Configuration server:** The configuration server coordinates communications between on-premises and Azure and manages data replication.
- **Process server:** The process server acts as a replication gateway. It receives replication data; optimizes it with caching, compression, and encryption, and sends it to a cache storage account in Azure.

The Process server also installs the Mobility Service agent on VMs you want to replicate and performs automatic discovery of on-premises VMware VMs.

## Download the appliance template

1. In the Azure Migrate project click **Servers** under **Migration Goals**.
2. In **Azure Migrate - Servers > Azure Migrate: Server Migration**, click **Discover**.



3. In **Discover machines > Are your machines virtualized?**, click **Yes, with VMWare vSphere hypervisor**.
4. In **How do you want to migrate?**, select **Using agent-based replication**.
5. In **Target region**, select the Azure region to which you want to migrate the machines.
6. Select **Confirm that the target region for migration is region-name**.
7. Click **Create resources**. This creates an Azure Site Recovery vault in the background.

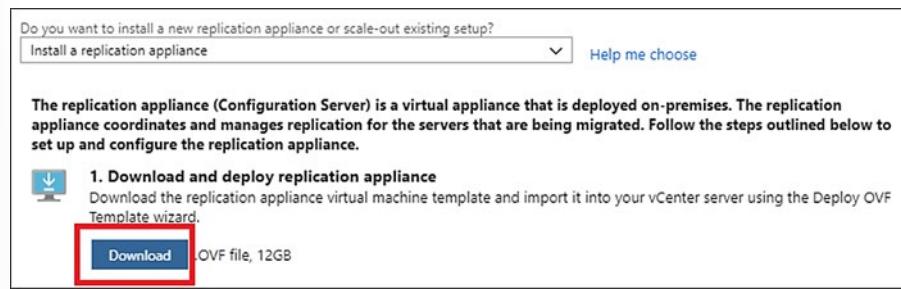
You can't change the target region for this project after clicking this button. All subsequent migrations are to this region.

This is a screenshot of the 'Discover machines' configuration page. It includes the following fields:

- Are your machines virtualized?**: A dropdown menu set to 'Yes, with VMWare vSphere Hypervisor'.
- How do you want to replicate?**: A dropdown menu set to 'Using agent-based replication'.
- Target region**: A dropdown menu set to 'West US'.
- Informational box**: A box containing the text: 'The target region for migration, once confirmed, cannot be changed for the project. After confirmation, the Server Migration tool (in this project) will allow replication and migration only to the selected target region.'
- Checkboxes**: Two checkboxes: one checked with the text 'Confirm that the target region for migration is "West US"' and another unchecked.
- Buttons**: A blue 'Create resources' button at the bottom.

## Download the appliance

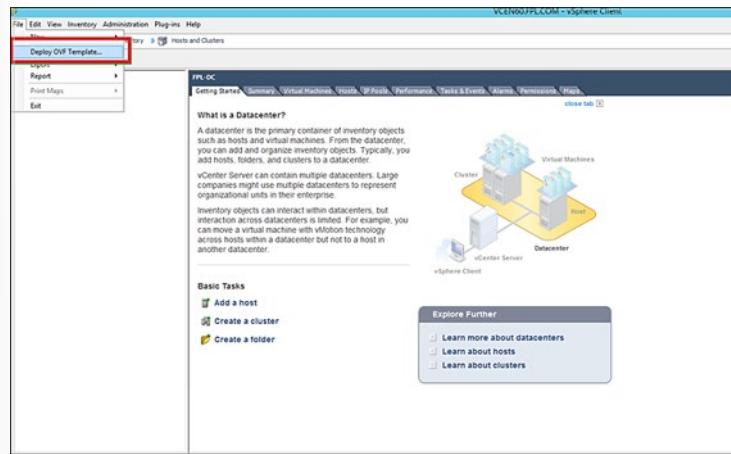
1. In **Do you want to install a new replication appliance?**, select **Install a replication appliance**.
2. Click **Download**, to download the replication appliance. This downloads an OVF template that you use to create a new VMware VM that runs the appliance.
3. Note the name of the resource group and the Recovery Services vault. You need these during appliance deployment.



## Import appliance to VMware

After downloading the OVF template, you import it into VMware to create the replication application on a VMware VM running Windows Server 2016.

1. Sign into the VMware vCenter server or vSphere ESXi host with the VMWare vSphere Client.
2. On the **File** menu, select **Deploy OVF Template** to start the **Deploy OVF Template Wizard**.
3. In **Select source**, enter the location of the downloaded OVF.
4. In **Review details**, select **Next**.
5. In **Select name and folder** and **Select configuration**, accept the default settings.
6. In **Select storage > Select virtual disk format**, for best performance select **Thick Provision Eager Zeroed**.
7. On the rest of the wizard pages, accept the default settings.
8. In **Ready to complete**, to set up the VM with the default settings, select **Power on after deployment > Finish**.



## Appliance Setup and Registration

Having obtained the required permissions to register the replication appliance, continue the appliance set up and register the appliance prior to replicating VMs.

## Replication appliance setup

1. From the VMWare vSphere Client console, turn on the VM.
2. The VM boots up into a Windows Server 2016 installation experience. Accept the license agreement and enter an administrator password.
3. After the installation finishes, sign in to the VM as the administrator, using the admin password.
4. The first time you sign in, the replication appliance setup tool (Azure Site Recovery Configuration Tool) starts within a few seconds.
5. Enter a name to use for registering the appliance with Azure Migrate Server Migration. Then click **Next**.
6. The tool checks that the VM can connect to Azure. After the connection is established, select **Sign in** to sign in to your Azure subscription.
7. Wait for the tool to finish registering an Azure AD app to identify the appliance. The appliance reboots.
8. Sign in to the machine again. In a few seconds, the Configuration Server Management Wizard starts automatically.

## Register the replication appliance

Finish setting up and registering the replication appliance.

1. In the Configuration Server Management Wizard, select **Setup connectivity**.
2. Select the NIC (by default there's only one NIC) that the replication appliance uses for VM discovery, and to do a push installation of the Mobility service on source machines.
3. Select the NIC that the replication appliance uses for connectivity with Azure. Then select **Save**. You cannot change this setting after it's configured.
4. If the appliance is located behind a proxy server, you need to specify proxy settings.  
Specify the proxy name as **http://ip-address**, or **http://FQDN**. HTTPS proxy servers aren't supported.
5. When prompted for the subscription, resource groups, and vault details, add the details that you noted when you downloaded the appliance template.
6. In **Install third-party software**, accept the license agreement. Select **Download and Install** to install MySQL Server.
7. Select **Install VMware PowerCLI**. Make sure all browser windows are closed before you do this. Then select **Continue**.
8. In **Validate appliance configuration**, prerequisites are verified before you continue.
9. In **Configure vCenter Server/vSphere ESXi server**, enter the FQDN or IP address of the vCenter server, or vSphere host, where the VMs you want to replicate are located. Enter the port on which the server is listening. Enter a friendly name to be used for the VMware server in the vault.
10. Enter the credentials for the account you created for **VMware discovery**<sup>16</sup>. Select **Add > Continue**.
11. In **Configure virtual machine credentials**, enter the credentials<sup>17</sup> you created for push installation of the Mobility service, when you enable replication for VMs.

<sup>16</sup> <https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware-agent>

<sup>17</sup> <https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-vmware-agent#register-the-replication-appliance>

For Windows machines, the account needs local administrator privileges on the machines you want to replicate.

For Linux, provide details for the root account.

12. Select **Finalize configuration** to complete registration.

After the replication appliance is registered, Azure Migrate Server Assessment connects to VMware servers using the specified settings and discovers VMs. You can view discovered VMs in **Manage > Discovered items**, in the **Other** tab.

## Replicating VMs

This section walks through the process of setting up replication of VMs in the Azure portal. The instructor may demonstrate this section at this point.

1. In the Azure Migrate project > **Servers**, **Azure Migrate: Server Migration**, click **Replicate**.

The screenshot shows the Azure Migrate - Servers portal. The left sidebar has a 'Migration goals' section with 'Servers' selected. The main area has two sections: 'Assessment tools' and 'Migration tools'. Under 'Assessment tools', there's a summary of 'Discovered servers' (442), 'Groups' (2), 'Assessments' (2), and 'Notifications' (0). A note says 'Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis'. Under 'Migration tools', there's a summary of 'Discovered servers' (442) and buttons for 'Discover', 'Replicate' (which is highlighted with a red box), 'Migrate', and 'Overview'. The 'Replicate' button is the target for step 1.

2. In **Replicate**, > **Source settings** > **Are your machines virtualized?**, select **Yes, with VMware vSphere**.
3. In **On-premises appliance**, select the name of the Azure Migrate appliance that you set up and click **OK**.
4. In **vCenter server**, specify the name of the vCenter server managing the VMs, or the vSphere server on which the VMs are hosted.
5. In **Process Server**, select the name of the replication appliance.
6. In **Guest credentials**, specify the VM admin account that will be used for push installation of the Mobility service. Then click **Next: Virtual machines**.

**Replicate**

Source settings	Virtual machines	Target settings	Compute	Disks	Review + Start replication
The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure.					
* Are your machines virtualized? <span style="color: red;">!</span>					
Yes, with VMware vSphere					
* On-premises appliance <span style="color: red;">!</span>					
WIN-DVHS6VQ9TRQ (Replication Appliance)					
* vCenter server/vSphere host <span style="color: red;">!</span>					
vCenter1					
* Process Server <span style="color: red;">!</span>					
WIN-DVHS6VQ9TRQ					
* Guest credentials <span style="color: red;">!</span>					
VM-admin-account					

- ✓ The next topic *Replication - Selecting the VMs to Replicate* is a continuation of this topic.

## Replication - Selecting the VMs to Replicate

When configuring the Virtual machines settings, you select the machines you want to replicate. If you've already run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. To do this, in **Import migration settings from an Azure Migrate assessment?**, select the **Yes** option. If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** option. Alternatively, if you selected to use the assessment, select the VM group, and assessment name.

- ✓ This topic continues on from the previous topic.

**Replicate**

Source settings	<b>Virtual machines</b>	Target settings	Compute	Disks	Review + Start replication
Select the virtual machines to be migrated.					
* Import migration settings from an assessment? <span style="color: red;">!</span>					
<input checked="" type="checkbox"/> Select Yes, apply migration settings from a Azure Migrate assessment No, I'll specify the migration settings manually					

In **Virtual machines**, search for VMs as needed, and check each VM you want to migrate. Then click **Next: Target settings**.

The screenshot shows the 'Replicate' wizard in the Azure portal. The 'Virtual machines' tab is selected. A dropdown menu shows 'No, I'll specify the migration settings manually'. Below is a table listing nine virtual machines:

NAME	IP ADDRESS	OPERATING SYSTEM	BOOT TYPE
ContosoVMwareMigr...	2404f801:4800:25:c95f5fd3:7347:4f91,1...	Microsoft Windows Server Threshold (64...)	bios
ContosoCSASB...	2404f801:4800:25:29f9:2ebd:fee0eeb4,...	Microsoft Windows Server 2012 (64-bit)	bios
Contoso-FrontTier3		Microsoft Windows Server Threshold (64...)	bios
ContosoWeb1	2404f801:4800:25:9091:9912:5f46:9108,...	Microsoft Windows Server 2008 (32-bit)	bios
Contoso-Configuratio...		Microsoft Windows Server 2012 (64-bit)	bios
Contoso-AzureMigr...		Microsoft Windows Server 2012 (64-bit)	bios
ContosoWeb3	10.150.13.218,2404f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios
ContosoAppSrv2	2404f801:4800:25:5de5e919:3448:be33,...	Microsoft Windows Server 2012 (64-bit)	bios
ContosoWeb2	10.150.13.201,2404f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios

Selected items : 9

## Replication - Target, Compute, and Disk Settings

This section completes the process of setting up replication of VMs in the Azure portal.

It covers how to configure target, compute, and disk settings.

### Target settings

- In **Target settings**, select the subscription, and target region to which you'll migrate, and specify the resource group in which the Azure VMs will reside after migration.
- In **Virtual Network**, select the Azure VNet/subnet to which the Azure VMs will be joined after migration.
- In **Azure Hybrid Benefit**:

Select **No** if you don't want to apply Azure Hybrid Benefit. Then click **Next**.

Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions, and you want to apply the benefit to the machines you're migrating. Then click **Next**.

**Replicate**

---

Source settings Virtual machines **Target settings** Compute Disks Review + Start replication

Select target properties for migration. Migrated machines will be created with the specified properties.

* Region	(US) East US
* Subscription	Azure Migrate Program Management Team
* Resource group	ContosoDemoRG
* Virtual Network	ContosoDemoNW
* Subnet	default

Azure Hybrid Benefit  
Apply Azure Hybrid Benefit and save up to 49% vs. pay-as-you-go virtual machine costs with an eligible Windows Server license.

\* Already have an eligible Windows Server License?

Yes  No

## Compute settings

- In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with **Azure requirements**<sup>18</sup>.
  - VM size:** If you're using assessment recommendations, the VM size dropdown will contain the recommended size. Otherwise Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in **Azure VM size**.
  - OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
  - Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.

**Replicate**

---

Source settings Virtual machines Target settings **Compute** Disks Review + Start replication

Select the Azure VM size and OS disk for the machines that are being migrated. Additionally, select an Availability Set if the migrated machine should be part of one. The OS disk is the disk that contains the operating system.

NAME	AZURE VM NAME	SOURCE VM SIZE	AZURE VM SIZE
ContosoVMwareMigration2	ContosoVMwareMigration2	8 Cores, 16384 MB RAM	Automatically select matching configuration
ContosoCSASR	ContosoCSASR	2 Cores, 2048 MB RAM	Automatically select matching configuration
Contoso-FrontTier3	Contoso-FrontTier3	8 Cores, 16384 MB RAM	Automatically select matching configuration
ContosoWeb1	ContosoWeb1	2 Cores, 2048 MB RAM	Automatically select matching configuration
Contoso-ConfigurationServer	Contoso-ConfigurationServer	8 Cores, 16384 MB RAM	Automatically select matching configuration
Contoso-AzureMigrateAppliance	Contoso2	4 Cores, 8192 MB RAM	Automatically select matching configuration
ContosoWeb3	ContosoWeb3	2 Cores, 2048 MB RAM	Automatically select matching configuration
ContosoAppSrv2	ContosoAppSrv2	2 Cores, 4096 MB RAM	Automatically select matching configuration
ContosoWeb2	ContosoWeb2	2 Cores, 2048 MB RAM	Automatically select matching configuration

## Disk settings

- In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium-managed disks) in Azure. Then click **Next**.

<sup>18</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-vmware>

You can exclude disks from replication.

If you exclude disks, they won't be present on the Azure VM after migration.

The screenshot shows the 'Replicate' dialog box. At the top, there are tabs: Source settings, Virtual machines, Target settings, Compute, Disks, and Review + Start replication. The 'Disks' tab is selected. Below the tabs, a note says: 'Select the managed disk type to use for the disks of the migrated machine. Optionally, you may also choose to exclude certain disks from replication by unselecting those disks from the list of disks to replicate.' A table lists four servers: ContosoVMwareMigration2, ContosoCSASR, ContosoFrontTier3, and ContosoWeb1. For each server, it shows the disk name (scsi0:0) and the 'DISKS TO REPLICATE' dropdown, which is set to 'All selected'. To the right, 'DISK SIZE GB' is listed as 80 for all three servers and 40 for ContosoWeb1. There is a 'Next Step' button at the bottom.

6. In **Review and start replication**, review the settings, and click **Replicate** to start the initial replication for the servers.

## Tracking and Monitoring Replication

When you click **Replicate** a Start Replication job begins. When the Start Replication job finishes successfully, the machines begin their initial replication to Azure.

During initial replication, a VM snapshot is created. Disk data from the snapshot is replicated to replica managed disks in Azure.

After initial replication finishes, delta replication begins. Incremental changes to on-premises disks are periodically replicated to the replica disks in Azure.

You can track job status in the portal notifications. You can monitor replication status by clicking on **Replicating servers** in **Azure Migrate: Server Migration**.

The screenshot shows the 'Migration tools' section of the Azure Migrate: Server Migration interface. It features a navigation bar with 'Discover', 'Replicate', 'Migrate', and 'Overview' (which is highlighted with a red box). Below this, there's a summary table:

Discovered servers	58
Replicating servers	1
Test migrated servers	0
Migrated servers	0

A note at the bottom says: 'Next step: You can start migrating the replicating servers to Azure'. A red box highlights the 'Replicating servers' row.

- ✓ The process of tracking and monitoring is the same whether replicating VMs using agentless migration or agent-based migration.

## Testing the Migration

When delta replication begins, you can run a test migration for the VMs, before running a full migration to Azure. We highly recommend that you do this at least once for each machine, before you migrate it.

Running a test migration checks that migration will work as expected, without impacting the on-premises machines, which remain operational, and continue replicating. Test migration simulates the migration by creating an Azure VM using replicated data (usually migrating to a non-production VNet in your Azure subscription).

You can use the replicated test Azure VM to validate the migration, perform app testing, and address any issues before full migration.

1. In **Migration goals > Servers > Azure Migrate: Server Migration**, click **Test migrated servers**.

The screenshot shows the 'Azure Migrate: Server Migration' dashboard. At the top, there are four navigation tabs: Discover, Replicate, Migrate, and Overview. Below the tabs is a list of categories with counts: Discovered servers (442), Replicating servers (6), Test migrated servers (1, highlighted with a red box), and Migrated servers (1). A note at the bottom says, 'Next step: You can start migrating the replicating servers to Azure.'

In **Test Migration**, select the Azure VNet in which the Azure VM will be located after the migration. We recommend you use a non-production VNet. The **Test migration** job starts. Monitor the job in the portal notifications. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.

2. Right-click the VM to test, and click **Test migrate**.

The screenshot shows the 'Replicating machines' list in the Azure Migrate portal. On the left is a sidebar with options: Overview, Getting started, Migrate servers to Azure, Manage (selected), Replicating machines (highlighted), Jobs, Events, Settings, and Properties. The main area lists a single machine: Contoso-Win2K8R2SP1. The columns are NAME, STATUS, HEALTH, MIGRATION PHASE, LAST SYNC, and TEST MIGRATION STATUS. The STATUS is Delta sync, HEALTH is Healthy, MIGRATION PHASE is Test migration pending, LAST SYNC is 2/17/2019, 12:00:43 AM, and TEST MIGRATION STATUS is Never performed. A context menu is open over the machine name, with 'Test migrate' highlighted with a red box. Other options in the menu are Pin to dashboard, Clean up test migration, and Migrate.

3. After the test is done, right-click the Azure VM in **Replicating machines**, and click **Clean up test migration**.

Last refreshed at: 2/17/2019, 1:02:40 AM

Finished loading data from service.

Filter items...

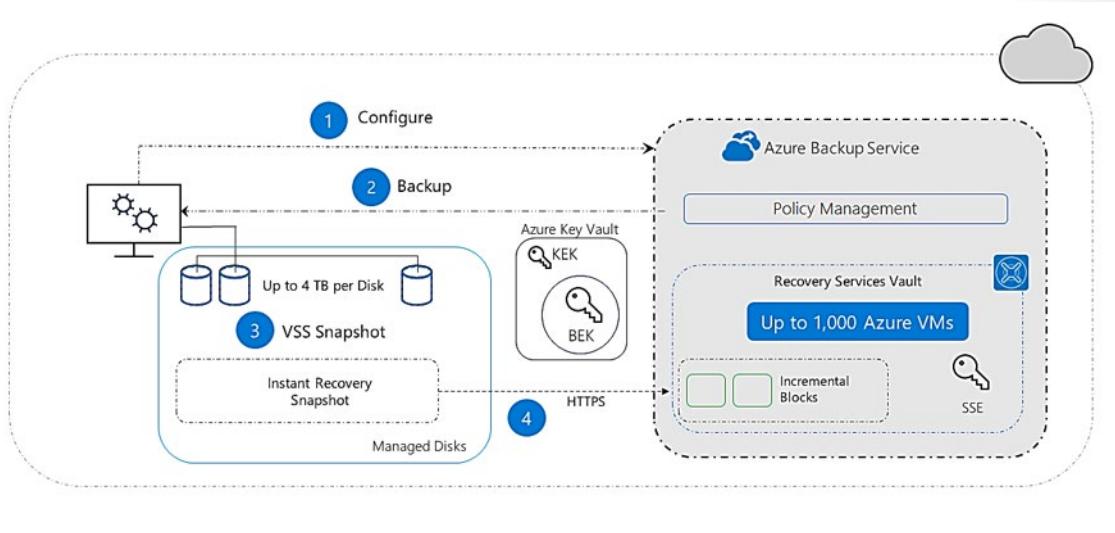
NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC	TEST MIGRATION STATUS
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM	<ul style="list-style-type: none"><li>Pin to dashboard</li><li>Test migrate</li><li><b>Clean up test migration</b></li><li>Migrate</li><li>Error Details</li></ul>

- ✓ The process for testing the migration is the same whether replicating VMs using agentless migration or agent-based migration.

# Implement Azure Backup

## Azure VM Backup Architecture

Let's look at the Azure Virtual Machine Architecture.



- Microsoft has an extension inside of every Azure VM
  - When you configure Backup, it communicates with the Azure Backup Service and associates itself to a policy.
  - It identifies itself to the Azure Backup Service as a VM, and that the service should back it up accordingly.
- When it's time for backup per the backup policy, Microsoft sends a command to the Azure Backup extension and then Azure Backup orchestrates a VSS snapshot.
- Once the snapshot is available it goes to your local VM storage as an instant recovery snapshot which you can quickly recover from as it is in your VM storage.
- In the background, the snapshot is compared to a snapshot of a previous recovery point and moves only the incremental blocks via HTTPs into the recovery services vault.
- The recovery services vault has encryption enabled via server-side encryption (SSE), so the backup is encrypted at rest and is protected while in transit.
- When you secure your data via Azure Disk Encryption you are given keys, key encryption key (KEK) and BitLocker encryption key (BEK), which go to an Azure key vault, and are also backed up via Azure Backup.

This is important because when you recover, you don't have to worry about what keys you had when the backup was taken and the keys are restored for you to apply these keys on the recovered data.

## Microsoft Azure Backup Overview

Microsoft Azure Backup Service offers IT administrators the option to back up and protect critical data in an easily recoverable way from any location.

<b>Reliable offsite data protection</b> <ul style="list-style-type: none"><li>Convenient offsite protection</li><li>Safe data</li><li>Encrypted backups</li></ul>	<b>A simple and integrated solution</b> <ul style="list-style-type: none"><li>Familiar interface</li><li>Azure integration</li></ul>	<b>Efficient backup and recovery</b> <ul style="list-style-type: none"><li>Efficient use of bandwidth and storage</li><li>Flexible configuration</li><li>Cost-effective and metered by usage</li></ul>
---	--	--

The Microsoft Azure Backup Service provides a new way to deliver business continuity benefits to Windows Server 2012 customers by providing a backup solution that requires no upfront hardware cost.

System Center 2012 SP1 Data Protection Manager customers get the added option to select online backup as a short-term recovery goal.

Microsoft Azure Backup is a cloud-hosted backup solution that provides file and folder backup capabilities for Windows Server 2012, Windows Server 2012 R2 and Windows Server 2008 R2 computers.

The Microsoft Azure Backup Agent can back up either files or folders. Customers can use system Center 2012 SP1 Data Protection Manager to back up File/volume, SQL Server and Hyper-V workloads to Azure online storage. Adding Update Rollup 6 to System Center Data Protection Manager will enable customers to do System State backups and Bare Metal Restores.

The fundamental workflow when you backup and restore files and folders to and from Microsoft Azure Backup using the Microsoft Azure Backup Agent are similar workflows that you would experience using any other type of backup.

Much like Windows Server Backup, you identify the items to backup and then the items are copied to a storage where they can be accessed later if they are needed. The difference is that with Azure Backup, the data is compressed and encrypted and the final destination is in the cloud.

## Azure Backup Key Features



Microsoft Azure Backup Service integrates with the familiar Windows Server Backup utility in Windows Server, the Data Protection Manager component in System Center and Windows Server Essentials, in order to provide a seamless backup and recovery experience to a local disk, or to the cloud.

### Block level incremental backups

The Microsoft Azure Backup Agent performs incremental backups by tracking file and block level changes and only transferring the changed blocks, hence reducing the storage and bandwidth utilization. Different

point-in-time versions of the backups use the storage efficiently by only storing the changed blocks between these versions.

#### **Data integrity is verified in the cloud**

In addition to the secure backups, the backed-up data is also automatically checked for integrity once the backup is done. As a result, any corruptions which may arise due to data transfer can be easily identified and are fixed automatically.

#### **Configurable retention policies for storing data in the cloud**

The Microsoft Azure Backup Service accepts and implements retention policies to recycle backups that exceed the desired retention range, thereby meeting business policies and managing backup costs.

## Azure IaaS Backup Components



The Azure portal provides a wizard, which is built into the portal, to help guide through the process of choosing the component to download and deploy. The wizard, which is part of the Recovery Services vault creation, walks through the steps for selecting a backup goal, and choosing the data or application to protect.

Depending on the individual component, Azure Backup components have certain advantages or limitations, and differences in what is protected and where the backups are stored. Consider each component listed below in light of these criteria.

### Azure Backup Server (can be deployed in Azure and on-premises)

#### **Benefits** - App aware snapshots (VSS)

- App aware snapshots (VSS)
- Full flexibility for when to take backups
- Recovery granularity (all)
- Can use Recovery Services vault
- Linux support on Hyper-V and VMware VMs
- Backup and restore VMware VMs
- Does not require a System Center license

#### **Limits**

- Cannot back up Oracle workload
- Always requires live Azure subscription
- No support for tape backup

#### **What is protected?**

- Files

- Folders
- Volumes
- VMs
- Applications
- Workloads
- System State

**Where are backups stored?**

- Recovery Services vault
- Locally attached disk

## Azure IaaS VM Backup

**Benefits**

- Native backups for Windows/Linux
- No specific agent installation required
- Fabric-level backup with no backup infrastructure needed

**Limits**

- Back up VMs once-a-day
- Restore VMs only at disk level
- Cannot back up on-premises

**What is protected?**

- VMs
- All disks (using PowerShell)

**Where are backups stored?**

- Recovery Services vault

## Recovery Services Vault Overview

A 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 screenshot shows the Microsoft Azure portal interface for managing Recovery Services vaults. On the left, there's a sidebar with navigation links like 'Add', 'Edit columns', and 'Filter by name...'. The main content area is titled 'AZ303Test' and includes tabs for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (with 'Properties', 'Locks', and 'Export template'), 'Getting started' (with 'Backup' highlighted in a red box), and 'Protected items' (with 'Backup items' and 'Replicated items'). Below these are 'Manage' sections for 'Backup policies', 'Backup Infrastructure', 'Site Recovery infrastructure', 'Recovery Plans (Site Recovery)', and 'Backup Reports'. The right side features a 'Backup' section with icons for 'Getting started', 'Backup dashboard', 'Backup items', 'Backup policies', 'Backup Reports', and 'Backup Explorer'. It also has a 'Site Recovery' section with similar icons. A 'What's new' section lists several recent updates.

Within an Azure subscription, you can create up to 500 Recovery Services vaults per subscription per region.

## Comparing Recovery Services vaults and Backup vaults

If you still have Backup vaults, they are being auto-upgraded to Recovery Services vaults. By November 2017, all Backup vaults have been upgraded to Recovery Services vaults.

Recovery Services vaults are based on the Azure Resource Manager model of Azure, whereas Backup vaults were based on the Azure Service Manager model. When you upgrade a Backup vault to a Recovery Services vault, the backup data remains intact during and after the upgrade process.

Recovery Services vaults provide features not available for Backup vaults, such as:

- **Enhanced capabilities to help secure backup data:** With Recovery Services vaults, Azure Backup provides security capabilities to protect cloud backups. The security features ensure you can secure your backups, and safely recover data, even if production and backup servers are compromised. [Learn more<sup>19</sup>](#).
- **Central monitoring for your hybrid IT environment:** With Recovery Services vaults, you can monitor not only your [Azure IaaS VMs<sup>20</sup>](#) but also your [on-premises assets<sup>21</sup>](#) from a central portal. [Learn more<sup>22</sup>](#)

<sup>19</sup> <https://docs.microsoft.com/en-us/azure/backup/backup-azure-security-feature>

<sup>20</sup> <https://docs.microsoft.com/en-us/azure/backup/backup-azure-manage-vms>

<sup>21</sup> <https://docs.microsoft.com/en-us/azure/backup/backup-azure-manage-windows-server>

<sup>22</sup> <https://azure.microsoft.com/en-us/blog/alerting-and-monitoring-for-azure-backup/>

- **Role-Based Access Control (RBAC):** RBAC provides fine-grained access management control in Azure. Azure provides various built-in roles<sup>23</sup>, and Azure Backup has three built-in roles to manage recovery points<sup>24</sup>. Recovery Services vaults are compatible with RBAC, which restricts backup and restore access to the defined set of user roles. [Learn more<sup>25</sup>](#)
- **Protect all configurations of Azure Virtual Machines:** Recovery Services vaults protect Resource Manager-based VMs including Premium Disks, Managed Disks, and Encrypted VMs. Upgrading a Backup vault to a Recovery Services vault gives you the opportunity to upgrade your Service Manager-based VMs to Resource Manager-based VMs. While upgrading the vault, you can retain your Service Manager-based VM recovery points and configure protection for the upgraded (Resource Manager-enabled) VMs. [Learn more<sup>26</sup>](#).
- **Instant restore for IaaS VMs:** Using Recovery Services vaults, you can restore files and folders from an IaaS VM without restoring the entire VM, which enables faster restore times. Instant restore for IaaS VMs is available for both Windows and Linux VMs. [Learn more<sup>27</sup>](#).

---

<sup>23</sup> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

<sup>24</sup> <https://docs.microsoft.com/en-us/azure/backup/backup-rbac-rs-vault>

<sup>25</sup> <https://docs.microsoft.com/en-us/azure/backup/backup-azure-security-feature>

<sup>26</sup> <https://azure.microsoft.com/en-us/blog/azure-backup-recovery-services-vault-ga/>

<sup>27</sup> <https://azure.microsoft.com/en-us/blog/instant-file-recovery-from-azure-linux-vm-backup-using-azure-backup-preview/>

## Azure to Azure Site Recovery

### Azure to Azure Site Recovery

With Azure Site to Site recovery, you can replicate Azure VMs to any other Azure location, with no infrastructure to deploy. The process is not tied to the *pairing* of regions encountered with storage, etc.

The ASR Mobility Service extension is automatically deployed to protected machines as part of the protection process.

In this scenario, you can replicate the following:

- VMs
- Virtual Networks
- Availability Sets
- Storage accounts

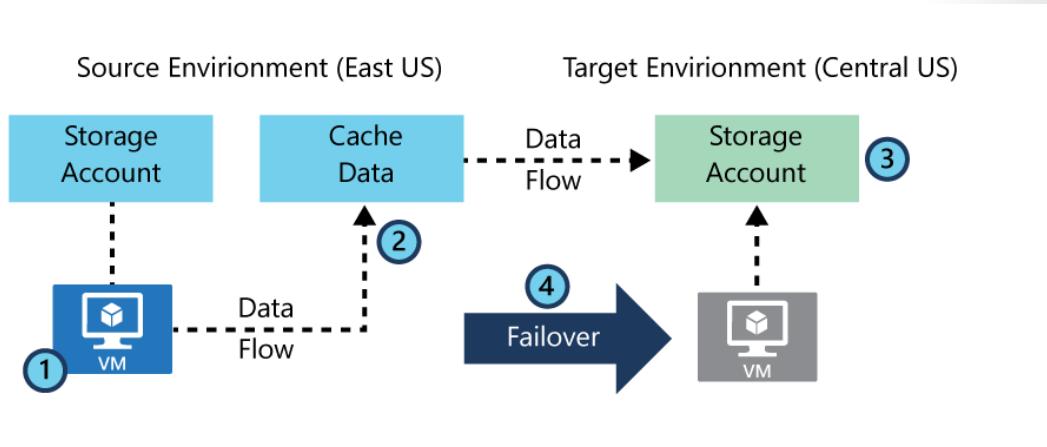
Optionally – you can specify your own VNets, Storage Accounts and Availability Sets

Replication happens on HTTPS channel, port 443 and an Azure egress cost is incurred for outbound traffic from the primary region.

✓ If you are using a URL-based firewall proxy to control outbound connectivity, certain Site Recovery URLs need to be allowed. Also, if you are using an IP-based firewall proxy, or NSG rules to control outbound connectivity, certain IP address ranges need to be allowed. For more information about whitelisted URLs and IP ranges, see **Outbound connectivity for URLs<sup>28</sup>** and **Outbound connectivity for IP address ranges<sup>29</sup>**.

### Azure to Azure Architecture

With disaster recovery set up, Azure VMs continuously replicate from the source to a different target region. If an outage occurs, you can fail over VMs to the secondary region, and access them from there. When everything's running normally again, you can fail back and continue working in the primary location. The process shown in the diagram is as follows:



1. VM is registered with Azure Site Recovery

<sup>28</sup> <https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-about-networking#outbound-connectivity-for-urls>

<sup>29</sup> <https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-about-networking#outbound-connectivity-for-ip-address-ranges>

2. Data is continuously replicated to cache
3. Cache is replicated to the target storage account
4. During failover the virtual machine is added to the target environment

## Architectural components

The components involved in disaster recovery for Azure VMs are summarized in the following table.

Component	Requirement
VMs in source region	One of more Azure VMs in a <b>supported source region</b> ( <a href="https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix#region-support">https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix#region-support</a> ). VMs can be running any <b>supported operating system</b> ( <a href="https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix#replicated-machine-operating-systems">https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix#replicated-machine-operating-systems</a> )
Source VM storage	Azure VMs can be managed, or have non-managed disks spread across storage accounts.
Source VM networks	VMs can be located in one or more subnets in a virtual network (VNet) in the source region.
Cache storage account	You need a cache storage account in the source network. During replication, VM changes are stored in the cache before being sent to target storage. Using a cache ensures minimal impact on production applications that are running on a VM. <b>Learn more</b> ( <a href="https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix#cache-storage">https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix#cache-storage</a> ) about cache storage requirements.
Target resources	Target resources are used during replication, and when a failover occurs. Site Recovery can set up target resource by default, or you can create/ customize them. In the target region, check that you're able to create VMs, and that your subscription has enough resources to support VM sizes that will be needed in the target region.

- ✓ Using a cache ensures minimal impact on production applications that are running on a VM. **Learn more**<sup>30</sup> about cache storage requirements.

## Azure to Azure Site Recovery - Network Traffic

ASR traffic is only **outbound** from protected VMs. If you are using a URL-based firewall proxy to control outbound connectivity, allow these Site Recovery URLs:

URL	Purpose
<b>*.blob.core.windows.net</b>	For storage account writes

<sup>30</sup> <https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix>

URL	Purpose
<b>login.microsoftonline.com</b>	Authorization and authentication to the ASR URLs
<b>*.hypervrecoverymanager.windowsazure.com</b>	ASR service communication channel
<b>*.servicebus.wifondows.net</b>	monitoring and diagnostics

See [this link<sup>31</sup>](#) for a list of all Site Recovery Service and monitoring IP addresses for each Azure location.

The following example shows the Site Recovery service and Site Recovery monitoring IP addresses for the Central US region:

Location	Site Recovery Service IP address	Site Recovery Monitoring IP address
<b>Central US</b>	40.69.144.231	52.165.34.144

## Azure to Azure VM Protection

Establish a recovery services vault in a different location other than where your VMs reside.

The screenshot shows the Microsoft Azure portal interface for creating a Recovery Services vault. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar. Below it, the navigation path is 'Home > Recovery Services vaults > Create Recovery Services vault'. The main section is titled 'Create Recovery Services vault' with a 'Preview' link. There are three tabs at the top: 'Basics \*' (which is selected and highlighted with a dashed border), 'Tags', and 'Review + create'. Under the 'Basics' tab, there are two main sections: 'Project Details' and 'Instance Details'. In 'Project Details', there are fields for 'Subscription \*' (set to 'Azure Pass - Sponsorship') and 'Resource group \*' (a dropdown menu with an empty field and a 'Create new' button). In 'Instance Details', there are fields for 'Vault name \*' (an empty input field with placeholder text 'Enter the name for your vault.') and 'Region \*' (a dropdown menu set to '(US) East US').

## Configuration

Because Azure to Azure ASR is managed as a SaaS-like service, there is no infrastructure to create – and no agents or providers to install. You begin with the first step, which in this case is to replicate the application.

The system will automatically install the ASR Mobility Service on each protected VM in the background.

<sup>31</sup> <https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-about-networking#sample-nsg-configuration>

AZ303Test  
Recovery Services vault

+ Backup + Replicate Delete Refresh

Cross region restore feature is now available in geo-redundant vaults. Learn more.

Overview Backup Site Recovery

What's new

- Azure Backup support for large disks is Generally Available →
- Configure network properties (internal load balancer, public IP and NSG) in the target region, when replicating Azure VMs →
- Enterprise-scale Backup for SQL Server running in Azure VM is Generally Available →
- Protect on-premises VMs by directly replicating to managed disks in Azure →
- Protection of Azure VMs using Storage Spaces Direct is now available →
- Disaster recovery for VMs deployed in Availability Zones to another region →

Backup Site Recovery

## Enable Replication

This procedure assumes that the primary Azure region is East Asia, and the secondary region is South East Asia.

1. In the vault, click **+Replicate**.

Enable replication

Source

Select your source environment

Source: Azure

\* Source location: East US

\* Azure virtual machine deployment model: Resource Manager

\* Source subscription

\* Source resource group: az900Demos

Enable replication

Select virtual machines

NAME	VIRTUAL NETWORK	TAGS
myVM	myVNET	
myVM02	myVNET	
myVM03	myVNET	
myVM06	myVNET	
myVM05	myVNET	
myVM1	myVNET	

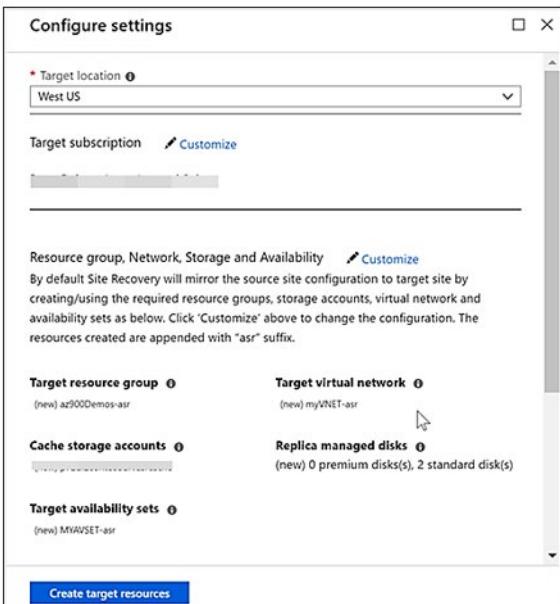
Note the following fields:

- **Source:** The point of origin of the VMs, which in this case is Azure.

- **Source location:** The Azure region from where you want to protect your virtual machines. For this illustration, the source location is *East Asia*
  - **Deployment model:** Azure deployment model of the source machines.
  - **Source subscription:** The subscription to which your source virtual machines belong. This can be any subscription within the same Azure Active Directory tenant where your recovery services vault exists.
  - **Resource Group:** The resource group to which your source virtual machines belong. All the VMs under the selected resource group are listed for protection in the next step.
2. In **Virtual Machines > Select virtual machines**, click and select each VM that you want to replicate. You can only select machines for which replication can be enabled. Then, click **OK**.

## Settings

In Settings, you can optionally configure target site settings:

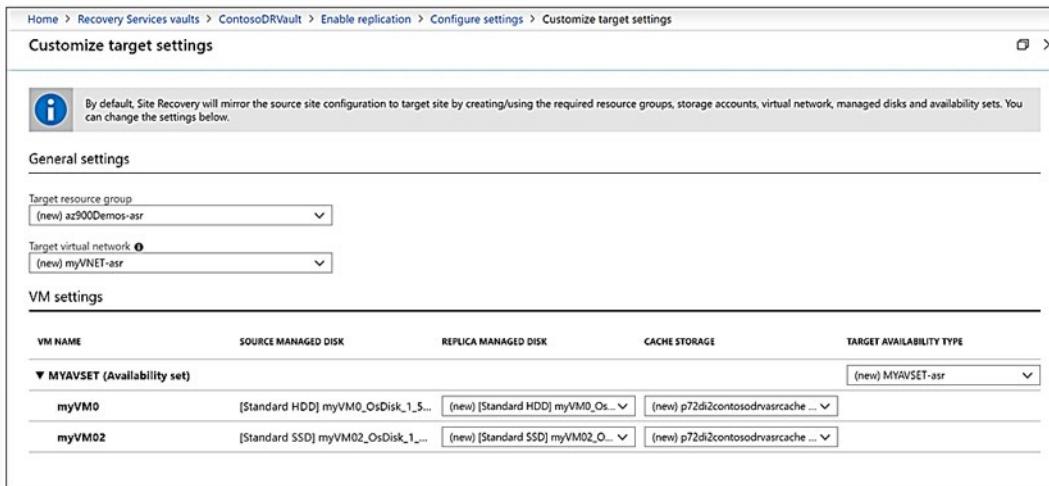


- **Target Location:** The location where your source virtual machine data will be replicated. Depending upon your selected machines location, Site Recovery will provide you the list of suitable target regions. We recommend that you keep the target location the same as the Recovery Services vault location.
- **Target subscription:** The target subscription used for disaster recovery. By default, the target subscription will be same as the source subscription.
- **Target resource group:** The resource group to which all your replicated virtual machines belong. By default Azure Site Recovery creates a new resource group in the target region with name having "asr" suffix. In case resource group created by Azure Site Recovery already exists, it is reused. You can also choose to customize it as shown in the section below. The location of the target resource group can be any Azure region except the region in which the source virtual machines are hosted.
- **Target Virtual Network:** By default, Site Recovery creates a new virtual network in the target region with name having "asr" suffix. This is mapped to your source network, and used for any future protection. Learn more about network mapping.

- **Target Storage accounts (If your source VM does not use managed disks):** By default, Site Recovery creates a new target storage account mimicking your source VM storage configuration. In case storage account already exists, it is reused.
- **Replica managed disks (If your source VM uses managed disks):** Site Recovery creates new replica managed disks in the target region to mirror the source VM's managed disks with the same storage type (Standard or premium) as the source VM's managed disk.
- **Cache Storage accounts:** Site Recovery needs extra storage account called cache storage in the source region. All the changes happening on the source VMs are tracked and sent to cache storage account before replicating those to the target location.
- **Target availability sets:** By default, Azure Site Recovery creates a new availability set in the target region with name having "asr" suffix for the VMs part of an availability set in source region. In case availability set created by Azure Site Recovery already exists, it is reused.
- **Target availability zones:** By default, Site Recovery assigns the same zone number as the source region in target region if the target region supports availability zones.  
If the target region does not support availability zones, the target VMs are configured as single instances by default. If required, you can configure such VMs to be part of availability sets in target region by clicking **Customize**.  
**Note:** You cannot change the availability type - single instance, availability set or availability zone, after you enable replication. You need to disable and enable replication to change the availability type.
- **Replication Policy:** It defines the settings for recovery point retention history and app consistent snapshot frequency. By default, Azure Site Recovery creates a new replication policy with default settings of '24 hours' for recovery point retention and '60 minutes' for app consistent snapshot frequency.

## Customize Target Resources

You can modify the default target settings used by Site Recovery.



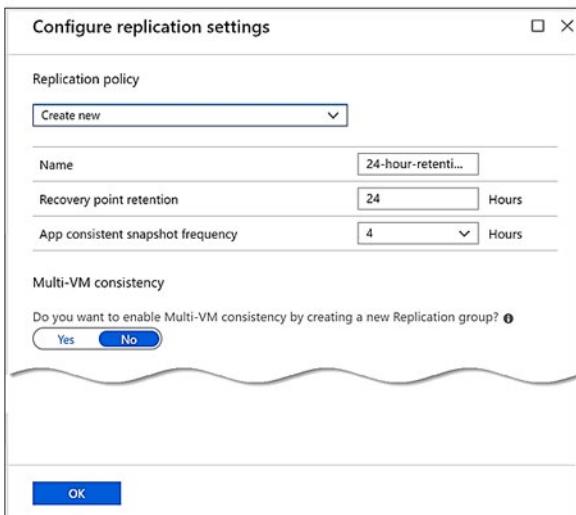
The screenshot shows the 'Customize target settings' dialog box. At the top, there is a breadcrumb navigation: Home > Recovery Services vaults > ContosoDRVault > Enable replication > Configure settings > Customize target settings. Below the title 'Customize target settings' is a note: 'By default, Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network, managed disks and availability sets. You can change the settings below.' The dialog is divided into sections: 'General settings' (Target resource group: (new) a2900Demos-asr, Target virtual network: (new) myVNET-asr) and 'VM settings'. The 'VM settings' section contains a table with columns: VM NAME, SOURCE MANAGED DISK, REPLICA MANAGED DISK, CACHE STORAGE, and TARGET AVAILABILITY TYPE. There are two rows for VMs 'myVM0' and 'myVM02'. For 'myVM0', the source disk is '[Standard HDD] myVM0\_OsDisk\_1.5...' and the replica disk is '(new) [Standard HDD] myVM0\_Os...'. For 'myVM02', the source disk is '[Standard SSD] myVM02\_OsDisk\_1...' and the replica disk is '(new) [Standard SSD] myVM02\_O...'. The 'TARGET AVAILABILITY TYPE' dropdown is set to '(new) MYAVSET-asr'.

1. Click **Customize**: next to 'Target subscription' to modify the default target subscription. Select the subscription from the list of all the subscriptions available in the same Azure Active Directory (AAD) tenant.
2. Click **Customize**: to modify default settings:

3. In **Target resource group**, select the resource group from the list of all the resource groups in the target location of the subscription.
4. In **Target virtual network**, select the network from a list of all the virtual network in the target location.
5. In **Availability set**, you can add availability set settings to the VM, if they're part of an availability set in the source region.
6. In **Target Storage accounts**, select the account you want to use.

## Replication Settings

1. Click **Customize**: to modify replication settings.



2. In **Multi-VM consistency**, select the VMs which you want to replicate together
  - All the machines in a replication group will have shared crash consistent and app-consistent recovery points when failed over. Enabling multi-VM consistency can impact workload performance (as it is CPU intensive) and should be used only if machines are running the same workload and you need consistency across multiple machines.
  - For example, if an application has 2 sql virtual machines and 2 web servers then you should add only sql virtual machines as a part of replication group.
  - You can choose to have at max 16 virtual machines in a replication group.
  - If you enable multi-VM consistency, machines in the replication group communicate with each other over port 20004. Ensure that there is no firewall appliance blocking the internal communication between the VMs over port 20004. If you want Linux VMs to be part of a replication group, ensure the outbound traffic on port 20004 is manually opened as per the guidance of the specific Linux version.
3. Click **Create target resource > Enable Replication**.
4. After the VMs are enabled for replication, you can check the status of VM health under **Replicated items**.

## Recovery Plans

A recovery plan helps you to define a systematic recovery process, by creating small independent units that you can fail over. A unit typically represents an app in your environment. A recovery plan defines how machines fail over, and the sequence in which they start after failover.

The screenshot shows the 'DR-Drill-RecoveryPlan' recovery plan interface. At the top, there are buttons for 'Group', 'Save', 'Discard', and 'Change group'. Below this, a message states 'This recovery plan contains 5 machine(s.)'. The main area displays a table of stages:

STAGE NAME	DETAILS	...
All groups shut down	5 machines in 4 groups.	...
▶ All groups failover		...
▶ Group 1: Start	1 Machine	...
▼ Group 2: Start	1 Machine	...
ContosoSQLSrv1	Machine	...
▼ Group 3: Start	2 Machines	...
ContosoAppSrv1	Machine	...
ContosoAppSrv2	Machine	...
▼ Group 4: Start	1 Machine	...
ContosoWeb1	Machine	...
▶ Group 4: Post-steps	1 Step	...

Use recovery plans to:

- Model an app around its dependencies.
- Automate recovery tasks to reduce RTO.
- Verify that you're prepared for migration or disaster recovery by ensuring that your apps are part of a recovery plan.
- Run test failover on recovery plans, to ensure disaster recovery or migration is working as expected.

## Model apps

You can plan and create a recovery group to capture app-specific properties. As an example, let's consider a typical three-tier application with a SQL server backend, middleware, and a web frontend. Typically, you customize the recovery plan so that machines in each tier start in the correct order after failover.

- The SQL backend should start first, the middleware next, and finally the web frontend.
- This start order ensures that the app is working by the time the last machine starts.
- This order ensures that when the middleware starts and tries to connect to the SQL Server tier, the SQL Server tier is already running.
- This order also helps ensure that the front-end server starts last, so that end users don't connect to the app URL before all the components are up and running, and the app is ready to accept requests.

To create this order, you add groups to the recovery group, and add machines into the groups. Where order is specified, sequencing is used. Actions run in parallel where appropriate, to improve application

recovery RTO.

Machines in a single group fail over in parallel, while machines in different groups fail over in group order, so that Group 2 machines start their failover only after all the machines in Group 1 have failed over and started.

With this customization in place, here's what happens when you run a failover on the recovery plan:

- A shutdown step attempts to turn off the on-premises machines. The exception is if you run a test failover, in which case the primary site continues to run.
- The shutdown triggers a parallel failover of all the machines in the recovery plan.
- The failover prepares virtual machine disks using replicated data.
- The startup groups run in order and start the machines in each group. First, Group 1 runs, then Group 2, and finally, Group 3. If there's more than one machine in any group, then all the machines start in parallel.

## Automate tasks

Recovering large applications can be a complex task. Manual steps make the process prone to error, and the person running the failover might not be aware of all app intricacies. You can use a recovery plan to impose order, and automate the actions needed at each step, using Azure Automation runbooks for failover to Azure, or scripts. For tasks that can't be automated, you can insert pauses for manual actions into recovery plans. There are a couple of types of tasks you can configure:

- **Tasks on the Azure VM after failover:** When you're failing over to Azure, you typically need to perform actions so that you can connect to the VM after failover. For example:
  - Create a public IP address on the Azure VM.
  - Assign a network security group to the network adapter of the Azure VM.
  - Add a load balancer to an availability set.
- **Tasks inside the VM after failover:** These tasks typically reconfigure the app running on the machine, so that it continues to work correctly in the new environment. For example:
  - Modify the database connection string inside the machine.
  - Change the web server configuration or rules.

## Test Failover

You can use a recovery plan to trigger a test failover. Use the following best practices:

- Always complete a test failover on an app, before running a full failover. Test failovers help you to check whether the app comes up on the recovery site.
- If you find you've missed something, trigger a clean-up, and then rerun the test failover.
- Run a test failover multiple times, until you're sure that the app recovers smoothly.
- Because each app is unique, you need to build recovery plans that are customized for each application and run a test failover on each.

- Apps and their dependencies change frequently. To ensure recovery plans are up-to-date, run a test failover for each app every quarter.

The screenshot shows the 'ContosoEUS - Recovery Plans (Site Recovery)' page in the Azure portal. The left sidebar has 'Manage' and 'Monitoring' sections. Under 'Manage', 'Recovery Plans (Site Recovery)' is selected. The main area lists a single plan: 'DR-Drill-Recover...' with 'South Central US' as the source and 'East US' as the target. The 'CURRENT JOB' status is 'Test failover cleanup'. A context menu is open over this plan, with the 'Test failover' option highlighted in red. Other options in the menu include 'Pin to dashboard', 'Customize', 'Cleanup test failover', 'Failover', 'Re-protect', 'Commit', and 'Delete'.

# Lab

## Lab: Protecting Hyper-V VMs by using Azure Site Recovery

✓ **Important:** To download the most recent version of this lab, please visit the AZ-303 [GitHub repository](#)<sup>32</sup>.

Direct link to the [Lab: Protecting Hyper-V VMs by using Azure Site Recovery](#)<sup>33</sup>.

### Lab scenario



While Adatum Corporation has, over the years, implemented a number of high availability provisions for their on-premises workloads, its disaster recovery capabilities are still insufficient to address the Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) demanded by its business. Maintaining the existing secondary on-premises site requires an extensive effort and incurs significant costs. The failover and fallback procedures are, for the most part, manual and are poorly documented.

To address these shortcomings, the Adatum Enterprise Architecture team decided to explore capabilities of Azure Site Recovery, with Azure taking on the role of the hoster of the secondary site. Azure Site Recovery automatically and continuously replicates workloads running on physical and virtual machines from the primary to the secondary site. Site Recovery uses storage-based replication mechanism, without intercepting application data. With Azure as the secondary site, data is stored in Azure Storage, with built-in resilience and low cost. The target Azure VMs are hydrated following a failover by using the replicated data. The Recovery Time Objectives (RTO) and Recovery Point objectives are minimized since Site Recovery provides continuous replication for VMware VMs and replication frequency as low as 30 seconds for Hyper-V VMs. In addition, Azure Site Recovery also handles orchestration of failover and fallback processes, which, to large extent, can be automated. It is also possible to use Azure Site Recovery for migrations to Azure, although the recommended approach relies on Azure Migrate instead.

The Adatum Enterprise Architecture team wants to evaluate the use of Azure Site Recovery for protecting on-premises Hyper-V virtual machines to Azure VM.

### Objectives

After completing this lab, you will be able to:

- Configure Azure Site Recovery
- Perform test failover
- Perform planned failover
- Perform unplanned failover

<sup>32</sup> <https://github.com/MicrosoftLearning/AZ-303-Microsoft-Azure-Architect-Technologies>

<sup>33</sup> [https://aka.ms/303\\_Module\\_12\\_Lab](https://aka.ms/303_Module_12_Lab)

## Lab Environment

Windows Server admin credentials

- User Name: **Student**
- Password: **Pa55w.rd1234**

Estimated Time: 120 minutes

## Lab Files (Located in the GitHub repository listed above)

- \\AZ303\AllFiles\Labs\07\azuredeploy30307suba.json

### Exercise 0: Prepare the lab environment

The main tasks for this exercise are as follows:

1. Deploy an Azure VM by using an Azure Resource Manager QuickStart template
2. Configure nested virtualization in the Azure VM

### Exercise 1: Create and configure an Azure Site Recovery vault

The main tasks for this exercise are as follows:

1. Create an Azure Site Recovery vault
2. Configure the Azure Site Recovery vault

### Exercise 2: Implement Hyper-V protection by using Azure Site Recovery vault

The main tasks for this exercise are as follows:

1. Implement the target Azure environment
2. Implement protection of a Hyper-V virtual machine
3. Perform a failover of the Hyper-V virtual machine
4. Remove Azure resources deployed in the lab

## Module 12 Review Questions

### Module 12 Review Questions



#### Review Question 1

*Your organization needs a way to create application aware snapshots, and backup Linux virtual machines and VMware virtual machines. You have files, folders, volumes, and workloads to protect. You recommend which of the following solutions? Select one.*

- Azure Backup (MARS) agent
- Azure Backup Server
- Enable disk snapshots
- Enable backup for individual Azure VMs

#### Review Question 2

*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 3

*You have several Azure VMs that are currently running production workloads. You have a mix of Windows Server and Linux servers and you need to implement a backup strategy for your production workloads. Which feature should you use in this case? Select one.*

- Managed snapshots.
- Azure Backup.
- Azure Site Recovery.
- Azure Migrate.

## Review Question 4

You 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

# Answers

## Review Question 1

Your organization needs a way to create application aware snapshots, and backup Linux virtual machines and VMware virtual machines. You have files, folders, volumes, and workloads to protect. You recommend which of the following solutions? Select one.

- Azure Backup (MARS) agent
- Azure Backup Server
- Enable disk snapshots
- Enable backup for individual Azure VMs

*Explanation*

Azure backup server provides app aware snapshots, support for Linux virtual machines and VMware virtual machines. Backup server can protect files, folders, volumes, and workloads.

## Review Question 2

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 3

You have several Azure VMs that are currently running production workloads. You have a mix of Windows Server and Linux servers and you need to implement a backup strategy for your production workloads. Which feature should you use in this case? Select one.

- Managed snapshots.
- Azure Backup.
- Azure Site Recovery.
- Azure Migrate.

*Explanation*

For backing up Azure virtual machines running production workloads, use Azure Backup. Azure Backup supports application-consistent backups for both Windows and Linux virtual machines. Azure Site Recovery coordinates virtual-machine and physical-server replication, failover, and fallback, but Azure Backup will protect and restore data at a more granular level. Managed snapshots provide a read-only full copy of a managed disk, and is an ideal solution in development and test environments, but Azure Backup is the better option for your production workloads.

**Review Question 4**

You 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.*

## Module 13 Implement Container-Based Applications

### Configure Azure Kubernetes Service

#### Azure Kubernetes Service

Azure Kubernetes Service (AKS) manages your hosted Kubernetes environment and makes it simple to deploy and manage containerized applications in Azure. Your AKS environment is enabled with features such as automated updates, self-healing, and easy scaling. The Kubernetes cluster master is managed by Azure and is free. You manage the agent nodes in the cluster and only pay for the VMs on which your nodes run.

You can either create your cluster in the Azure portal or use the Azure CLI. When you create the cluster, you can use Resource Manager templates to automate cluster creation. With these templates, you specify features such as advanced networking, Azure Active Directory (AD) integration, and monitoring. This information is then used to automate the cluster deployment on your behalf.

At its core, an AKS cluster is a cloud hosted Kubernetes cluster. Unlike a custom Kubernetes installation, AKS streamlines the installation process and takes care of most of the underlying cluster management tasks.

You have two options when you create an AKS cluster. You either use the Azure portal or Azure CLI.

#### How workloads are developed and deployed to AKS

AKS supports the Docker image format that means that you can use any development environment to create a workload, package the workload as a container and deploy the container as a Kubernetes pod.

Here you use the standard Kubernetes command-line tools or the Azure CLI to manage your deployments. The support for the standard Kubernetes tools ensures that you don't need to change your current workflow to support an existing Kubernetes migration to AKS.

AKS also supports all the popular development and management tools such as Helm, Draft, Kubernetes extension for Visual Studio Code and Visual Studio Kubernetes Tools.

## Deployment Center

Deployment center simplifies setting up a DevOps pipeline for your application. You can use this configured DevOps pipeline to set up a continuous integration (CI) and continuous delivery (CD) pipeline to your AKS Kubernetes cluster.

With Azure DevOps Projects you can:

- Automatically create Azure resources, such as an AKS cluster
- Create an Azure Application Insights resource for monitoring an AKS cluster
- Enable Azure Monitor for containers to monitor performance for the container workloads on an AKS cluster

## Azure Service Integration

AKS allows us to integrate any Azure service offering and use it as part of an AKS cluster solution.

## Demonstration - Deploy Kubernetes with AKS

In this demonstration, you will:

- Create a new resource group.
- Configure cluster networking.
- Create an Azure Kubernetes Service cluster.
- Connect to the Kubernetes cluster by using kubectl.
- Create a Kubernetes namespace.

### Create a new resource group

You'll first need to create a resource group for your resources to deploy into.

1. Sign in to Azure Cloud Shell with your Azure account. Select the Bash version of Cloud Shell.

#### Azure Cloud Shell<sup>1</sup>

2. You need to choose a region where you want to create a resource group, for example, **East US**. If you select a different value, remember it for the rest of the exercises in this module. You may need to redefine the value between Cloud Shell sessions. Run the following commands to record these values in Bash variables.

```
REGION_NAME=eastus
RESOURCE_GROUP=aksworkshop
SUBNET_NAME=aks-subnet
VNET_NAME=aks-vnet
```

You can check each value using the echo command, for example, echo \$REGION\_NAME.

3. Create a new resource group with the name \*\*aksworkshop. Deploy all resources created in these exercises in this resource group. A single resource group makes it easier to clean up the resources after you finish the module.

---

<sup>1</sup> <https://shell.azure.com/>

```
az group create \
--name $RESOURCE_GROUP \
--location $REGION_NAME
```

## Configure networking

We have two network models to choose from when deploying an AKS cluster. The first model is *Kubenet networking*, and the second is *Azure Container Networking Interface (CNI) networking*.

### Kubenet networking

Kubenet networking is the default networking model in Kubernetes. With Kubenet networking, nodes get assigned an IP address from the Azure virtual network subnet. Pods receive an IP address from a logically different address space to the Azure virtual network subnet of the nodes.

Network address translation (NAT) is then configured so that the pods can reach resources on the Azure virtual network. The source IP address of the traffic is translated to the node's primary IP address and then configured on the nodes. Note, that pods receive an IP address that's "hidden" behind the node IP.

### Azure Container Networking Interface (CNI) networking

With Azure Container Networking Interface (CNI), the AKS cluster is connected to existing virtual network resources and configurations. In this networking model, every pod gets an IP address from the subnet and can be accessed directly. These IP addresses must be unique across your network space and calculated in advance.

Some of the features you'll use require you to deploy the AKS cluster by using the *Azure Container Networking Interface networking* configuration.

Below we create the virtual network for your AKS cluster. We will use this virtual network and specify the networking model when we deploy the cluster.

1. First, create a virtual network and subnet. Pods deployed in your cluster will be assigned an IP from this subnet. Run the following command to create the virtual network.

```
az network vnet create \
--resource-group $RESOURCE_GROUP \
--location $REGION_NAME \
--name $VNET_NAME \
--address-prefixes 10.0.0.0/8 \
--subnet-name $SUBNET_NAME \
--subnet-prefix 10.240.0.0/16
```

2. Next, retrieve, and store the subnet ID in a Bash variable by running the command below.

```
SUBNET_ID=$(az network vnet subnet show \
--resource-group $RESOURCE_GROUP \
--vnet-name $VNET_NAME \
--name $SUBNET_NAME \
--query id -o tsv)
```

## Create the AKS cluster

With the new virtual network in place, you can go ahead and create your new cluster. There are two values you need to know before running the `az aks create` command. The first is the version of the latest, non-preview, Kubernetes version available in your selected region, and the second is a unique name for your cluster.

1. To get the latest, non-preview, Kubernetes version you use the `az aks get-versions` command. Store the value that returns from the command in a Bash variable named `VERSION`. Run the command below the retrieve and store the version number.

```
SUBNET_ID=$(az network vnet subnet show \
    --resource-group $RESOURCE_GROUP \
    --vnet-name $VNET_NAME \
    --name $SUBNET_NAME \
    --query id -o tsv)
```

2. The AKS cluster name must be unique. Run the following command to create a Bash variable that holds a unique name.

```
AKS_CLUSTER_NAME=aksworkshop-$RANDOM
```

3. Run the following command to output the value stored in `$AKS_CLUSTER_NAME`. Note this for later use. You'll need it to reconfigure the variable in the future, if necessary.

```
echo $AKS_CLUSTER_NAME
```

4. Run the following `az aks create` command to create the AKS cluster running the latest Kubernetes version. This command can take a few minutes to complete.

```
az aks create \
    --resource-group $RESOURCE_GROUP \
    --name $AKS_CLUSTER_NAME \
    --vm-set-type VirtualMachineScaleSets \
    --load-balancer-sku standard \
    --location $REGION_NAME \
    --kubernetes-version $VERSION \
    --network-plugin azure \
    --vnet-subnet-id $SUBNET_ID \
    --service-cidr 10.2.0.0/24 \
    --dns-service-ip 10.2.0.10 \
    --docker-bridge-address 172.17.0.1/16 \
    --generate-ssh-keys
```

## Test cluster connectivity by using kubectl

`kubectl` is the main Kubernetes command-line client you use to interact with your cluster and is available in Cloud Shell. A cluster context is required to allow `kubectl` to connect to a cluster. The context contains the cluster's address, a user, and a namespace. Use the `az aks get-credentials` command to configure your instance of `kubectl`.

1. Retrieve the cluster credentials by running the command below.

```
az aks get-credentials \
--resource-group $RESOURCE_GROUP \
--name $AKS_CLUSTER_NAME
```

2. Let's take a look at what was deployed by listing all the nodes in your cluster. Use the `kubectl get nodes` command to list all the nodes.

```
kubectl get nodes
```

You'll see a list of your cluster's nodes. Here's an example.

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-24503160-vmss000000	Ready	agent	1m	v1.15.7
aks-nodepool1-24503160-vmss000001	Ready	agent	1m	v1.15.7
aks-nodepool1-24503160-vmss000002	Ready	agent	1m	v1.15.7

## Create a Kubernetes namespace for the application

A namespace in Kubernetes creates a logical isolation boundary. Names of resources must be unique within a namespace but not across namespaces. If you don't specify the namespace when you work with Kubernetes resources, the default namespace is implied.

Let's create a namespace for your ratings application.

1. List the current namespaces in the cluster.

```
kubectl get namespace
```

You'll see a list of namespaces similar to this output.

NAME	STATUS	AGE
default	Active	1h
kube-node-lease	Active	1h
kube-public	Active	1h
kube-system	Active	1h

2. Use the `kubectl create namespace` command to create a namespace for the application called **ratingsapp**.

```
kubectl create namespace ratingsapp
```

You'll see a confirmation that the namespace was created.

```
namespace/ratingsapp created
```

# Azure Container Instances

## Azure Container Instances

Azure Container Instances offers the fastest and simplest way to run a container in Azure, without having to manage any virtual machines and without having to adopt a higher-level service.

Azure Container Instances is a great solution for any scenario that can operate in isolated containers, including simple applications, task automation, and build jobs.

### Fast startup times

Containers offer significant startup benefits over virtual machines (VMs). Azure Container Instances can start containers in Azure in seconds, without the need to provision and manage VMs.

### Container access

Azure Container Instances enables exposing your container groups directly to the internet with an IP address and a fully qualified domain name (FQDN). When you create a container instance, you can specify a custom DNS name label so your application is reachable at `customlabel.azureregion.azurecontainer.io`.

Azure Container Instances also supports executing a command in a running container by providing an interactive shell to help with application development and troubleshooting. Access takes places over HTTPS, using TLS to secure client connections.

### Hypervisor-level security

Historically, containers have offered application dependency isolation and resource governance but have not been considered sufficiently hardened for hostile multi-tenant usage. Azure Container Instances guarantees your application is as isolated in a container as it would be in a VM.

### Custom sizes

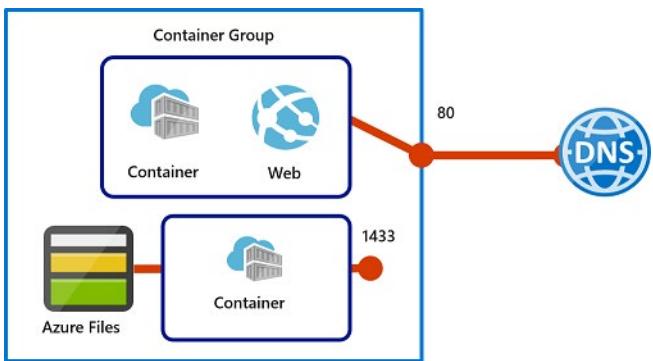
Containers are typically optimized to run just a single application, but the exact needs of those applications can differ greatly. Azure Container Instances provides optimum utilization by allowing exact specifications of CPU cores and memory. You pay based on what you need and get billed by the second, so you can fine-tune your spending based on actual need.

### Linux and Windows containers

Azure Container Instances can schedule both Windows and Linux containers with the same API. Simply specify the OS type when you create your container groups.

## Container Groups

The top-level resource in Azure Container Instances is the container group. A container group is a collection of containers that get scheduled on the same host machine. The containers in a container group share a lifecycle, resources, local network, and storage volumes. It's similar in concept to a pod in Kubernetes.



An example container group:

- Is scheduled on a single host machine.
- Is assigned a DNS name label.
- Exposes a single public IP address, with one exposed port.
- Consists of two containers. One container listens on port 80, while the other listens on port 1433.
- Includes two Azure file shares as volume mounts, and each container mounts one of the shares locally.

## Deployment options

Here are two common ways to deploy a multi-container group: use a Resource Manager template or a YAML file. A Resource Manager template is recommended when you need to deploy additional Azure service resources (for example, an Azure Files share) when you deploy the container instances. Due to the YAML format's more concise nature, a YAML file is recommended when your deployment includes only container instances.

## Resource allocation

Azure Container Instances allocates resources such as CPUs, memory, and optionally GPUs to a multi-container group by adding the resource requests of the instances in the group. Taking CPU resources as an example, if you create a container group with two container instances, each requesting 1 CPU, then the container group is allocated 2 CPUs.

## Networking

Container groups can share an external-facing IP address, one or more ports on that IP address, and a DNS label with a fully qualified domain name (FQDN). To enable external clients to reach a container within the group, you must expose the port on the IP address and from the container. Because containers within the group share a port namespace, port mapping isn't supported. A container group's IP address and FQDN will be released when the container group is deleted.

## Common scenarios

Multi-container groups are useful in cases where you want to divide a single functional task into a small number of container images. These images can then be delivered by different teams and have separate resource requirements. Example usage could include:

- A container serving a web application and a container pulling the latest content from source control.

- An application container and a logging container. The logging container collects the logs and metrics output by the main application and writes them to long-term storage.
- An application container and a monitoring container. The monitoring container periodically makes a request to the application to ensure that it's running and responding correctly, and raises an alert if it's not.
- A front-end container and a back-end container. The front end might serve a web application, with the back end running a service to retrieve data.

## Demonstration - Run Azure Container Instances

In this demonstration you create a container in Azure and expose it to the Internet with a fully qualified domain name (FQDN).

Azure Container Instances is useful for scenarios that can operate in isolated containers, including simple applications, task automation, and build jobs. Here are some of the benefits:

- **Fast startup:** Launch containers in seconds.
- **Per second billing:** Incur costs only while the container is running.
- **Hypervisor-level security:** Isolate your application as completely as it would be in a VM.
- **Custom sizes:** Specify exact values for CPU cores and memory.
- Persistent storage: Mount Azure Files shares directly to a container to retrieve and persist state.
- Linux and Windows: Schedule both Windows and Linux containers using the same API.

For scenarios where you need full container orchestration, including service discovery across multiple containers, automatic scaling, and coordinated application upgrades, we recommend Azure Kubernetes Service (AKS).

### Create a container

1. Sign into the [Azure portal](#)<sup>2</sup> with your Azure subscription.
2. Open the Azure Cloud Shell from the Azure portal using the Cloud Shell icon.



3. Create a new resource group with the name **learn-deploy-aci-rg** so that it will be easier to clean up these resources when you are finished with the module. If you choose a different resource group name, remember it for the rest of the exercises in this module. You also need to choose a region in which you want to create the resource group, for example **East US**.

```
az group create --name learn-deploy-aci-rg --location eastus
```

You create a container by providing a name, a Docker image, and an Azure resource group to the `az container create` command. You can optionally expose the container to the Internet by specifying a DNS name label. In this example, you deploy a container that hosts a small web app. You can also select

<sup>2</sup> <https://portal.azure.com/>

the location to place the image - you'll use the **East US** region, but you can change it to a location close to you.

4. You provide a DNS name to expose your container to the Internet. Your DNS name must be unique. For learning purposes, run this command from Cloud Shell to create a Bash variable that holds a unique name.

```
DNS_NAME_LABEL=aci-demo-$RANDOM
```

5. Run the following az container create command to start a container instance.

```
az container create \
--resource-group learn-deploy-aci-rg \
--name mycontainer \
--image microsoft/aci-helloworld \
--ports 80 \
--dns-name-label $DNS_NAME_LABEL \
--location eastus
```

\$DNS\_NAME\_LABEL specifies your DNS name. The image name, **microsoft/aci-helloworld**, refers to a Docker image hosted on Docker Hub that runs a basic Node.js web application.

6. When the az container create command completes, run az container show to check its status.

```
az container show \
--resource-group learn-deploy-aci-rg \
--name mycontainer \
--query "{FQDN:ipAddress.fqdn, ProvisioningState:provisioningState}" \
--out table
```

You see your container's fully qualified domain name (FQDN) and its provisioning state. Here's an example.

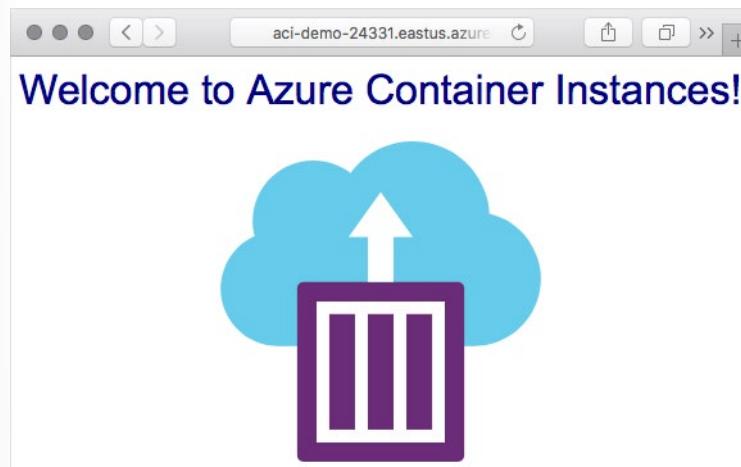
```
FQDN ProvisioningState
```

```
-----
```

```
aci-demo.eastus.azurecontainer.io Succeeded
```

If your container is in the **Creating** state, wait a few moments and run the command again until you see the **Succeeded** state.

7. From a browser, navigate to your container's FQDN to see it running. You see this.



## Module 13 Review Questions

### Module 13 Review Questions



#### Review Question 1

*You decide to move all your services to Azure Kubernetes service. Which of the following components will contribute to your monthly Azure charge? Select one.*

- Master node
- Pods
- Node virtual machines
- Tables

#### Review Question 2

*Which of the following is not true about container groups? Select one.*

- Is scheduled on a multiple host machines.
- Is assigned a DNS name label.
- Exposes a single public IP address, with one exposed port.
- Consists of two containers.
- Includes two Azure file shares as volume mounts.

#### Review Question 3

*Which of the following is the Kubernetes agent that processes the orchestration requests from the cluster master, and schedules running the requested containers? Select one.*

- controller master
- container runtime
- kube-proxy
- kubelet

## Review Question 4

You are configuring networking for the Azure Kubernetes service. Which of the following maps incoming direct traffic to the pods? Select one.

- AKS node
- ClusterIP
- Load Balancer
- NodePort

# Answers

## Review Question 1

You decide to move all your services to Azure Kubernetes service. Which of the following components will contribute to your monthly Azure charge? Select one.

- Master node
- Pods
- Node virtual machines
- Tables

*Explanation*

*Node virtual machines. You only pay for the virtual machines instances, storage, and networking resources consumed by your Kubernetes cluster.*

## Review Question 2

Which of the following is not true about container groups? Select one.

- Is scheduled on a multiple host machines.
- Is assigned a DNS name label.
- Exposes a single public IP address, with one exposed port.
- Consists of two containers.
- Includes two Azure file shares as volume mounts.

*Explanation*

*Is scheduled on a multiple host machines. A container group is scheduled on a single host machine.*

## Review Question 3

Which of the following is the Kubernetes agent that processes the orchestration requests from the cluster master, and schedules running the requested containers? Select one.

- controller master
- container runtime
- kube-proxy
- kubelet

*Explanation*

*kubelet. The kubelet process the orchestration requests from the cluster master, and schedules the running the requested containers.*

**Review Question 4**

You are configuring networking for the Azure Kubernetes service. Which of the following maps incoming direct traffic to the pods? Select one.

- AKS node
- ClusterIP
- Load Balancer
- NodePort

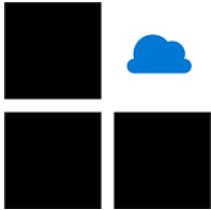
*Explanation*

*NodePort. NodePort maps incoming direct traffic to the pods.*

## Module 14 Implement an Application Infrastructure

### Create and Configure Azure App Service

#### Azure App Service Overview



Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. You can develop in your favorite language, be it .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. Applications run and scale with ease on both Windows and Linux-based environments.

App Service not only adds the power of Microsoft Azure to your application, such as security, load balancing, autoscaling, and automated management. You can also take advantage of its DevOps capabilities, such as continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domain, and TLS/SSL certificates.

With App Service, you pay for the Azure compute resources you use. The compute resources you use is determined by the App Service plan that you run your apps on.

#### Deployment slots

Using the Azure portal, you can easily add **deployment slots** to an App Service web app. For instance, you can create a **staging** deployment slot where you can push your code to test on Azure. Once you are happy with your code, you can easily **swap** the staging deployment slot with the production slot. You do all this with a few simple mouse clicks in the Azure portal.

The screenshot shows the Microsoft Azure portal interface for the ContosoSalesApp - Deployment slots. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Deployment (Quickstart and Deployment slots selected), and Deployment Center. The main content area has a heading 'Deployment Slots' with a sub-section 'Deployment Slots'. It says 'You haven't added any deployment slots. Click here to get started.' Below this is a table with columns NAME, STATUS, APP SERVICE PLAN, and TRAFFIC %. A single row is shown for 'contososalesapp' which is 'Running' under the 'PRODUCTION' slot, with an 'ASP-' plan and 100% traffic.

## Continuous integration/deployment support

The Azure portal provides out-of-the-box continuous integration and deployment with Azure DevOps, GitHub, Bitbucket, FTP, or a local Git repository on your development machine. Connect your web app with any of the above sources and App Service will do the rest for you by automatically syncing your code and any future changes on the code into the web app.

The screenshot shows the Azure App Service Deployment Center. At the top, it says 'Deployment Center' and 'App Service Deployment Center enables you to choose the location of your code as well as options for build and deployment to the cloud. [Learn more](#)'. Below this is a flow diagram with three steps: 1 SOURCE CONTROL, 2 BUILD PROVIDER, and 3 CONFIGURE. Under SOURCE CONTROL, there are five options: Azure Repos (Configure continuous integration with an Azure Repo, part of Azure DevOps Services (formerly known as VSTS)), GitHub (Configure continuous integration with a GitHub repo, associated with user 'nickwalkmsft'), Bitbucket (Configure continuous integration with a Bitbucket repo, status 'Not Authorized'), Local Git (Deploy from a local Git repo), and FTP (Use an FTP connection to access and copy app files).

## Creating a web app

When you're ready to run a web app on Azure, you visit the Azure portal and create a **Web App** resource. Creating a web app allocates a set of hosting resources in App Service, which you can use to host any web-based application that is supported by Azure, whether it be ASP.NET Core, Node.js, Java, Python, etc.

The Azure portal provides a wizard to create a web app. This wizard requires the following fields:

Field	Description
Subscription	A valid and active Azure subscription.
Resource group	A valid resource group.
App name	The name of the web app. This name becomes part of the app's URL, so it must be unique among all Azure App Service web apps.
Publish	You can deploy your application to App Service as code or as a ready-to-run Docker image. Selecting Docker image will activate the Docker tab of the wizard, where you provide information about the Docker registry from which App Service will retrieve your image.
Runtime stack	If you choose to deploy your application as code, App Service needs to know what runtime your application uses (examples include Node.js, Python, Java, and .NET). If you deploy your application as a Docker image, you will not need to choose a runtime stack, since your image will include it.
Operating system	App Service can host applications on Windows or Linux servers. See below for additional information.
Region	The Azure region from which your application will be served.
App Service Plan	See below for information about App Service plans.

## App Service plans

An App Service plan is a set of virtual server resources that run App Service apps. A plan's size (sometimes referred to as its sku or pricing tier) determines the performance characteristics of the virtual servers that run the apps assigned to the plan and the App Service features that those apps have access to. Every App Service web app you create must be assigned to a single App Service plan that runs it.

A single App Service plan can host multiple App Service web apps. In most cases, the number of apps you can run on a single plan will be limited by the performance characteristics of the apps and the resource limitations of the plan.

App Service plans are the unit of billing for App Service. The size of each App Service plan in your subscription, in addition to the bandwidth resources used by the apps deployed to those plans, determines the price that you pay. The number of web apps deployed to your App Service plans has no effect on your bill.

# Demonstration - Azure App Service

In this demonstration, you will use the Azure portal to create a web app and an Azure App Service.

Sign into the [Azure portal](#) <sup>1</sup>.

1. On the Azure portal menu or from the **Home** page, select **App Services**.

The screenshot shows the Microsoft Azure portal's Home page. At the top, there is a search bar labeled "Search resources, services, and docs (G+/-)". Below the search bar, there is a "Create a resource" button (blue plus icon) and an "App Services" button (blue app icon), which is highlighted with a red box. Other service icons include Azure Active Directory, Recovery Services vaults, Activity log, Log Analytics workspaces, and Virtual machine scale sets. Below these sections, there is a "Recent resources" table:

Name	Type
AZ303Test	Recovery Services vault
az303303	Log Analytics workspace
AZ303VM	Virtual machine

Below the recent resources is a "Navigate" section with links for Subscriptions, Resource groups, and All resources. At the bottom, there is a "Tools" section with links for Microsoft Learn, Azure Monitor, and Security Center.

2. From the **App Services** page, select **Create app service**.

<sup>1</sup> <https://portal.azure.com/learn.docs.microsoft.com>

The screenshot shows the Microsoft Azure portal's App Services blade. At the top, there are navigation links for Home > App Services and a search bar. Below the header are several buttons: Add, Manage view, Refresh, Export to CSV, Assign tags, Start, Restart, Stop, Delete, Feedback, and Leave preview. There are also filters for Subscription (all), Resource group (all), and Location (all). A message at the top says 'Showing 0 to 0 of 0 records.' Below this, there is a table header with columns for Name, Status, Location, Pricing T..., App Ser..., and more. In the center, there is a large blue circular icon with a network-like pattern. Below the icon, the text 'No app services to display' is shown. A descriptive paragraph follows: 'Create, build, deploy, and manage powerful web, mobile, and API apps for employees or customers using a single back-end. Build standards-based web apps and APIs using .NET, Java, Node.js, PHP and Python.' A link 'Learn more about App Service' is provided, and a prominent blue button with the text 'Create app service' is highlighted with a red border.

3. From the **Web App**, complete the following values:

Field	Value	Details
Subscription	Select your subscription	The web app you are creating must belong to a resource group. Here, you select the Azure subscription to which the resource group belongs (or will belong, if you are creating it within the wizard).
Resource Group	Select from the menu	The resource group to which the web app will belong. All Azure resources must belong to a resource group.
Name	Enter a unique name	The name of your web app. This name will be part of the app's URL: appname.azurewebsites.net. The name you choose must be unique among all Azure web apps.
Publish	Code	The method you will use to publish your application. When publishing your application as code, you also must configure Runtime stack to prepare your App Service resources to run your app.

Field	Value	Details
Runtime stack	.NET Core 3.1 (LTS)	The platform on which your application runs. Your choice may affect whether you have a choice of operating system - for some runtime stacks, App Service supports only one operating system.
Operating System	Linux	The operating system used on the virtual servers that run your app.
Region	Central US	The geographical region from which your app will be hosted.
Linux Plan	Leave default	The name of the App Service plan that will power your app. By default, the wizard will create a new plan in the same region as the web app.
Sku and size	Default	The pricing tier of the plan being created. This determines the performance characteristics of the virtual servers that power your app, and the features it has access to. To select the F1 tier, select Change size to open the Spec Picker wizard. On the Dev / Test tab, select F1 from the list, then select Apply.

**Project Details**

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

Subscription *	Azure Pass - Sponsorship
Resource Group *	(New) AZ-303RG
	<a href="#">Create new</a>

**Instance Details**

Name *	Web App name. .azurewebsites.net
Publish *	Code Docker Container
Runtime stack *	.NET Core 3.1 (LTS)
Operating System *	Linux Windows
Region *	Central US <small>Not finding your App Service Plan? Try a different region.</small>

**App Service Plan**

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app.  
[Learn more](#)

Linux Plan (Central US) *	(New) <a href="#">Create new</a>
Sku and size *	<b>Premium V2 P1v2</b> 210 total ACU, 3.5 GB memory <a href="#">Change size</a>

**Review + create**    < Previous    Next : Monitoring >

4. Select **Review and Create** to navigate to the review page, then select **Create** to create the web app.

Microsoft Azure

Home > App Services > Web App

## Web App

Basics Monitoring Tags **Review + create**

### Summary

 **Web App**  
by Microsoft

### Details

Subscription	3d4abc70-49fd-4424-a3e2-d84e1e68443d
Resource Group	AZ303RG
Name	AZ303AppSvc
Publish	Code
Runtime stack	.NET Core 3.1 (LTS)

### App Service Plan (New)

Name	ASP-AZ303RG-aa58
Operating System	Windows
Region	Central US
SKU	Standard
Size	Small
ACU	100 total ACU
Memory	1.75 GB memory

### Monitoring (New)

Application Insights	Enabled
Name	AZ303AppSvc
Region	Central US

**Create** < Previous Next > Download a template for automation

It can take a few seconds to get your web app created and ready for your use.

The portal will display the deployment page, where you can view the status of your deployment. Once the app is ready, navigate to the new app in the Azure portal:

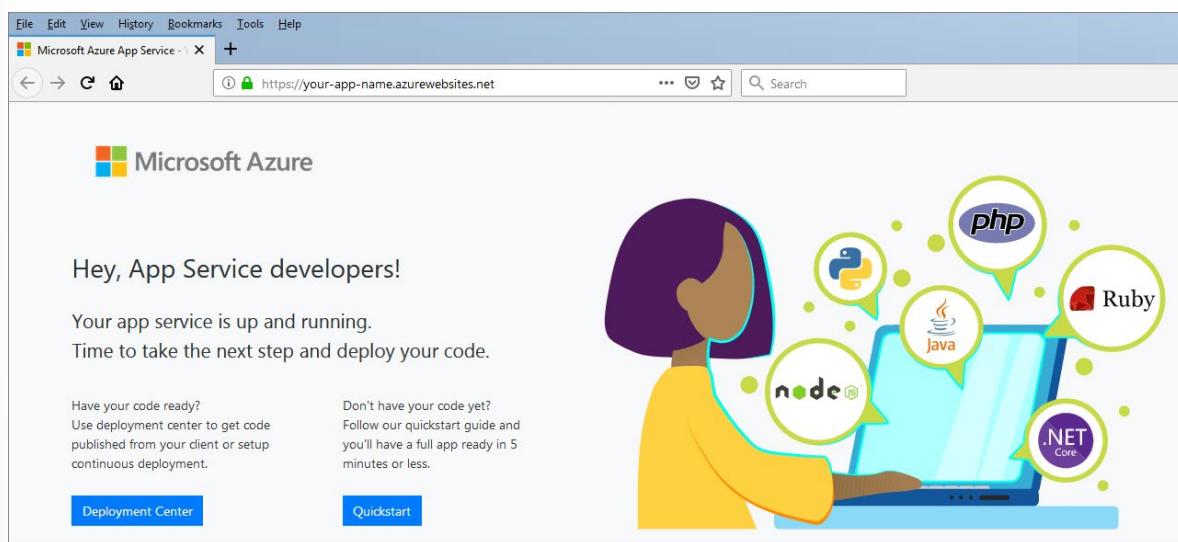
1. On the Azure portal menu or from the **Home page**, select **All resources**.
2. Select the App Service for your web app from the list. Make sure to select the App Service, and not the App Service plan.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar. Below the header, the URL 'Home > App Services' is visible. The main content area is titled 'App Services' with a 'Default Directory' link. There are several filter and search options at the top: 'Filter by name...', 'Subscription == all', 'Resource group == all', 'Location == all', and a 'Add filter' button. Below these filters, it says 'Showing 1 to 1 of 1 records.' A table lists one item: 'AZ303AppSvc' with a small icon, 'Running' status, and 'Central US' location. The entire row for 'AZ303AppSvc' is highlighted with a red border.

The portal displays the **App Services** overview page.

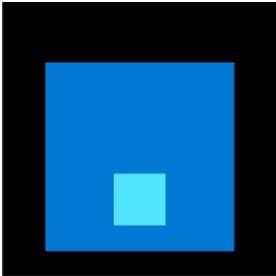
This screenshot shows the detailed overview page for the 'AZ303AppSvc' App Service. The left sidebar has a tree view with nodes like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Deployment', 'Quickstart', 'Deployment slots', 'Deployment Center', 'Settings', 'Configuration', 'Authentication / Authorizat...', 'Application Insights', 'Identity', 'Backups', 'Custom domains', 'TLS/SSL settings', 'Networking', 'Scale up (App Service plan)', 'Scale out (App Service plan)', 'Webhooks', 'Push', and 'MySQL In App'. The main content area has a purple banner with a link to a quickstart guide. It shows resource details: Resource group (AZ303RG), Status (Running), Location (Central US), Subscription (Azure Pass - Sponsorship), Subscription ID, and Tags. Below this are three cards: 'Diagnose and solve problems' (with a link to help identify and resolve issues), 'Application Insights' (with a link to detect and diagnose quality issues), and 'App Service Advisor' (with a link to insights for improving app experience). At the bottom, there are three charts: 'Http 5xx' (0 errors), 'Data In' (19.91 MB), and 'Data Out' (13.96 MB).

To preview your new web app's default content, select its URL at the top right. The placeholder page that loads indicates that your web app is up and running and ready to receive deployment of your app's code.



# Create an App Service Web App for Containers

## Azure Container Registry



Azure Container Registry enables you to store Docker images in the cloud, in an Azure storage account.

Container Registry is an Azure service that you can use to create your own private Docker registries. Like Docker Hub, Container Registry is organized around repositories that contain one or more images. Container Registry also lets you automate tasks such as redeploying an app when an image is rebuilt.

Security is an important reason to choose Container Registry instead of Docker Hub:

- You have much more control over who can see and use your images.
- You can sign images to increase trust and reduce the chances of an image becoming accidentally (or intentionally) corrupted or otherwise infected.
- All images stored in a container registry are encrypted at rest.

## Using Container Registry

You create a registry by using either the Azure portal or the Azure CLI **acr create** command. In the following code example, the name of the new registry is myregistry:

```
az acr create --name myregistry --resource-group mygroup --sku standard  
--admin-enabled true
```

In addition to storing and hosting images, you can also use Container Registry to build images. Instead of building an image yourself and pushing it to Container Registry, use the CLI to upload the Docker file and other files that make up your image. Container Registry will then build the image for you. Use the **acr build** command to run a build:

```
az acr build --file Dockerfile --registry myregistry --image myimage .
```

## Build an Image using Azure Container Registry

Azure Container Registry provides storage for Docker images in the cloud.

In this topic, you'll use the Azure portal to create a new registry in Azure Container Registry. You'll build a Docker image from the source code for a web app and upload it to a repository in your registry.

## Create a registry in Azure Container Registry

1. Sign in to the [Azure portal](#)<sup>2</sup> with your Azure subscription.
2. Choose **Create a resource**, select **Containers**, and then select **Container Registry**.

The screenshot shows the Azure Marketplace interface. On the left, there's a sidebar with categories like Get started, Recently created, AI + Machine Learning, Analytics, Blockchain, Compute, Containers (which is highlighted with a blue border), Databases, Developer Tools, DevOps, and Identity. On the right, there are several service cards: Container Instances (Quickstart tutorial), Container Registry (Quickstart tutorial, which is highlighted with a red box), Kubernetes Service (Quickstart tutorial), Red Hat OpenShift Container Platform (Self-Managed (preview), Learn more, PREVIEW), and DC/OS on Azure (Quickstart tutorial, PREVIEW).

3. Specify the values in the following table for each of the properties:

Property	Value
Registry name	Enter a unique name and make a note of it for later.
Subscription	Select your default Azure subscription in which you are allowed to create and manage resources.
Resource Group	Create a new resource group with the name <b>learn-deploy-container-acr-rg</b> so that it will be easier to clean up these resources when you're finished with the module. If you choose a different resource group name, remember it for the rest of the exercises in this module.
Location	Select a location that is close to you.
Admin user	<b>Enable</b>
SKU	<b>Standard</b>

4. Click **Create**. Wait until the container registry has been created before you continue.

Build a Docker image and upload it to Azure Container Registry

1. In the Azure Cloud Shell in the portal, run the following command to download the source code for the sample web app. This web app is simple. It presents a single page that contains static text and a carousel control that rotates through a series of images.

```
git clone https://github.com/MicrosoftDocs/mslearn-deploy-run-container-app-service.git
```

<sup>2</sup> <https://portal.azure.com/learn/docs.microsoft.com>

2. Move to the source folder:

```
cd mslearn-deploy-run-container-app-service/dotnet
```

3. Run the following command. This command sends the folder's contents to Azure Container Registry, which uses the instructions in the Docker file to build the image and store it. Replace <container\_registry\_name> with the name of the registry you created earlier. Take care not to leave out the . character at the end of the command.

```
az acr build --registry <container_registry_name> --image webimage .
```

The Docker file contains the step-by-step instructions for building a Docker image from the source code for the web app. Azure Container Registry runs these steps to build the image, and as each step completes a message is generated. The build process should finish after a couple of minutes without any errors or warnings.

## Examine the container registry

- 1.In the **Azure portal** <sup>3</sup>, navigate to the Overview page for your container registry.
- 2.Under **Services**, select **Repositories**. You'll see a repository named `webimage`.
- 3.Select the `webimage` repository. It contains an image with the `latest` tag. This is the Docker image for the sample web app.

<sup>3</sup> <https://portal.azure.com/learn.docs.microsoft.com>

The screenshot shows the Azure Container Registry interface. On the left, a sidebar menu includes: Overview, Activity log, Access control (IAM), Tags, Quick start, Events, Settings (with Access keys, Locks, Automation script), Services (Repositories selected), Webhooks, Replications, Policies (Content trust (Preview)), Monitoring (Metrics (Preview)), Support + troubleshooting (New support request), and New support request. The main area has a Refresh button and a search bar for repositories. It lists a repository named 'webimage' with a '...' button next to it. Below the repository list is a search bar for tags and a section for tags with 'latest' listed. At the top right are Refresh and Delete buttons.

The Docker image that contains your web app is now available in your registry for deployment to App Service.

## Deploy a Web App from a Docker Image

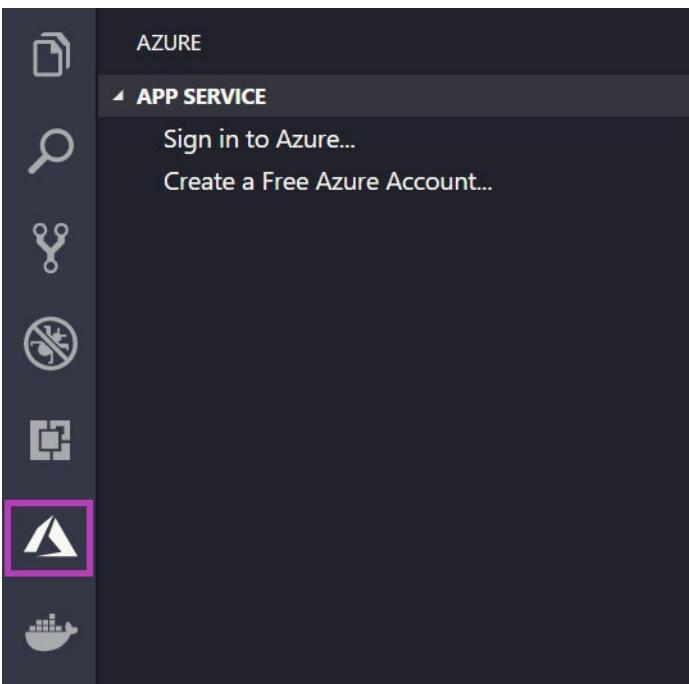
Azure App Service provides the hosting environment for an Azure-based web app. You can configure App Service to retrieve the image for the web app from a repository in Azure Container Registry.

In this topic, you'll see how to create a new web app by using the Docker image stored in Azure Container Registry. You'll use App Service with a predefined App Service plan to host the web app.

Create a web app

1. Sign in to the [Azure portal](#) <sup>4</sup>.
2. Select **Create a resource > Web > Web App**.

<sup>4</sup> <https://portal.azure.com/learn.docs.microsoft.com>



3. Specify these settings for each of the properties:

Property	Value
Subscription	Select your default Azure subscription in which you are allowed to create and manage resources.
Resource Group	Reuse the existing resource group learn-deploy-container-acr-rg.
Name	Enter a unique name and make a note of it for later.
Publish	<b>Docker Image</b>
OS	<b>Linux</b>
App Service plan	Use the default.

4. Click **Next: Docker >**.

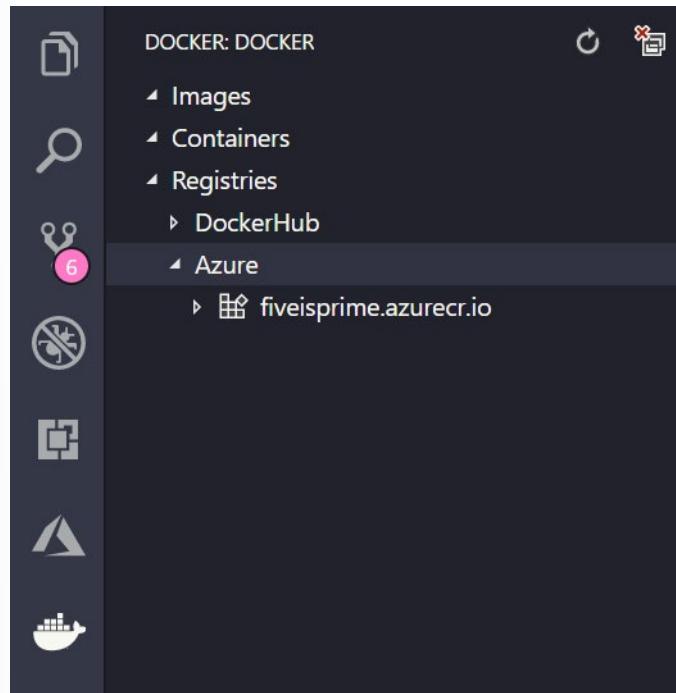
5. In the **Docker** tab, specify these settings for each of the properties:

Property	Value
Options	<b>Single Container</b>
Image Source	<b>Azure Container Registry</b>
Registry	Select your registry.
Image	webimage
Tag	latest
Startup Command	Leave this empty.

6. Select **Review and create**, and then click **Create**. Wait until the web app has been deployed before you continue.

## Test the web app

1. Use the **All resources** view in the Azure portal to go to the **Overview** page of the web app you just created.
2. Select the **Browse** button to open the site in a new browser tab.
3. After the cold-start delay while your app's Docker image loads and starts, you'll see a page like this:



App Service is now hosting the app from your Docker image.

# Create and Configure an App Service Plan

## Azure App Service Plans

In App Service, an app runs in an App Service plan. An App Service plan defines a set of compute resources for a web app to run. These compute resources are analogous to the server farm in conventional web hosting. One or more apps can be configured to run on the same computing resources (or in the same App Service plan).

When you create an App Service plan in a certain region (for example, West Europe), a set of compute resources is created for that plan in that region. Whatever apps you put into this App Service plan run on these compute resources as defined by your App Service plan. Each App Service plan defines:

- **Region** (West US, East US, etc.)
- **Number of VM instances**
- **Size of VM instances** (Small, Medium, Large)

## How the app runs and scales

In the Free and Shared tiers, an app receives CPU minutes on a shared VM instance and cannot scale out. In other tiers, an app runs and scales as follows.

When you create an app in App Service, it is put into an App Service plan. When the app runs, it runs on all the VM instances configured in the App Service plan. If multiple apps are in the same App Service plan, they all share the same VM instances. If you have multiple deployment slots for an app, all deployment slots also run on the same VM instances. If you enable diagnostic logs, perform backups, or run WebJobs, they also use CPU cycles and memory on these VM instances.

## Considerations

Since you pay for the computing resources your App Service plan allocates, you can potentially save money by putting multiple apps into one App Service plan. You can continue to add apps to an existing plan as long as the plan has enough resources to handle the load. However, keep in mind that apps in the same App Service plan all share the same compute resources. To determine whether the new app has the necessary resources, you need to understand the capacity of the existing App Service plan, and the expected load for the new app. Overloading an App Service plan can potentially cause downtime for your new and existing apps. Isolate your app into a new App Service plan when:

- The app is resource-intensive.
- You want to scale the app independently from the other apps in the existing plan.
- The app needs resource in a different geographical region.

## App Service Plan Pricing Tiers

	Free Try for free	Shared Environment for dev/test	Basic Dedicated environment for dev/test	Standard Run produc- tion work- loads	Premium Enhanced performance and scale	Isolated High-Per- formance, Security and Isolation
Web, mobile, or API apps	10	100	Unlimited	Unlimited	Unlimited	Unlimited
Disk space	1 GB	1 GB	10 GB	50 GB	250 GB	1 TB
Maximum instances	–	–	Up to 3	Up to 10	Up to 30*	Up to 100
Custom domain	–	Supported	Supported	Supported	Supported	Supported
Auto Scale	–	–	–	Supported	Supported	Supported
Hybrid Connectivity	–	–	Supported	Supported	Supported	Supported
Virtual Network Connectivity	–	–	–	Supported	Supported	Supported
Private Endpoints	–	–	–	–	Supported	Supported
Compute Type	Shared	Shared	Dedicated	Dedicated	Dedicated	Isolated
Price	Free	\$0.013/hour	\$0.075/hour	\$0.10/hour	\$0.20/hour	\$0.40/hour

The pricing tier of an App Service plan determines what App Service features you get and how much you pay for the plan. There are a few categories of pricing tiers:

- **Free and Shared.** The Free and Shared service plans are base tiers that run on the same Azure VMs as other apps. Some apps may belong to other customers. These tiers are intended to be used only for development and testing purposes. There is no SLA provided for Free and Shared service plans. Free and Shared plans are metered on a per App basis.
- **Basic.** The Basic service plan is designed for apps that have lower traffic requirements, and don't need advanced auto scale and traffic management features. Pricing is based on the size and number of instances you run. Built-in network load balancing support automatically distributes traffic across instances.
- **Standard.** The Standard service plan is designed for running production workloads. Pricing is based on the size and number of instances you run. Built-in network load balancing support automatically distributes traffic across instances. The Standard plan includes auto scale that can automatically adjust the number of virtual machine instances running to match your traffic needs.
- **Premium.** The Premium service plan is designed to provide enhanced performance for production apps. The upgraded Premium plan, Premium v2, features Dv2-series VMs with faster processors, SSD storage, and double memory-to-core ratio compared to Standard.
- **Isolated.** The Isolated service plan is designed to run mission critical workloads, that are required to run in a virtual network. The Isolated plan allows customers to run their apps in a private, dedicated environment in an Azure datacenter using Dv2-series VMs with faster processors, SSD storage, and double the memory-to-core ratio compared to Standard.

# App Service Plan Scaling

There are two workflows for Web App scaling, **scale up** and **scale out**. Apps can be scaled manually or automatically (autoscale).

Choose how to scale your resource



## Manual scale

Maintain a fixed instance count



## Custom autoscale

Scale on any schedule, based on any metrics

**Scale up.** Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more. You scale up by changing the pricing tier of the App Service plan that your app belongs to.

**Scale out:** Increase the number of VM instances that run your app. You can scale out to as many as 30 instances, depending on your pricing tier. App Service Environments in Isolated tier further increases your scale-out count to 100 instances. The scale instance count can be configured manually or automatically (autoscale). Autoscale is based on predefined rules and schedules.

## Changing your App Service plan (scale up)

Your App Service plan can be scaled up and down at any time. It is as simple as changing the pricing tier of the plan. You can choose a lower pricing tier at first and scale up later when you need more App Service features.

For example, you can start testing your web app in a Free App Service plan and pay nothing. When you want to add your custom DNS name to the web app, just scale your plan up to the Shared tier. Later, when you want to create an SSL binding, scale your plan up to Basic tier. When you want to have staging environments, scale up to Standard tier. When you need more cores, memory, or storage, scale up to a bigger VM size in the same tier.

The same works in the reverse. When you feel you no longer need the capabilities or features of a higher tier, you can scale down to a lower tier, which saves you money.

## Other considerations

- The scale settings take only seconds to apply and affect all apps in your App Service plan. They don't require you to change your code or redeploy your application.
- If your app depends on other services, such as Azure SQL Database or Azure Storage, you can scale up these resources separately. These resources aren't managed by the App Service plan.

## Demonstration - Create an App Service Plan

In this demonstration, we will create and work with Azure App Service plans.

### Create an App Service Plan

1. Sign-in to the **Azure portal**<sup>5</sup>.
2. Search for and select **App Service Plans**.
3. Click **+ Add** to create a new App Service plan.

Setting	Value
Subscription	<b>Choose your subscription</b>
Resource Group	<b>myRGAppServices</b> (create new)
Name	<b>AppServicePlan1</b>
Operating System	<b>Windows</b>
Region	<b>East US</b>

4. Click **Review + Create** and then **Create**.
5. Wait for your new App Service plan to deploy.

### Review Pricing Tiers

1. Locate your new App Service plan.
2. Under **Settings**, click **Scale up (App Service Plan)**.
3. Notice there are three tiers: **Dev/Test**, **Production**, and **Isolated**.
4. Click each tier and review the included features and included hardware.
5. How do the tiers compare?

### Review autoscaling

1. Under **Settings** click **Scale out (App Service Plan)**.
2. Notice the default is **Manual scale**.
3. Notice you can specify an **instance count** depending on your App Service plan selection.
4. Click **Custom autoscale**.
5. Notice two scale modes: **Scale based on a metric** and **Scale to a specific instance count**.
6. Click **Add a rule**.

✓ **Note:** This rule will add an instance when the CPU percentages is greater than 80% for 10 minutes.

Setting	Value
Time aggregation	<b>Average</b>
Metric name	<b>CPU percentage</b>
Operator	<b>Greater than</b>
Threshold	<b>80</b>
Duration	<b>10 minutes</b>
Operation	<b>Increase count by</b>
Instance count	<b>1</b>
Cool down	<b>5 minutes</b>

7. **Add** your rule changes.
8. Review the **Instance limits: Minimum, Maximum, and Default**.

<sup>5</sup> <http://portal.azure.com/>

9. Notice that you can add a **Schedule** and **Specify start/end dates** and **Repeat specific days**.
10. Do you see how you can create different App Service plans for your apps?

# Configure Networking for an App Service

## Integrate an App with an Azure Virtual Network

This lesson describes the Azure App Service VNet Integration feature and how to set it up with apps in Azure App Service. With Azure Virtual Network (VNets), you can place multiple Azure resources in a non-internet-routable network. VNet Integration enables apps to access resources in or through a VNet.

Azure App Service has two variations on Net Integration:

- The multitenant systems that support the full range of pricing plans except Isolated.
- The App Service Environment, which deploys into your VNet and supports Isolated pricing plan apps.

The VNet Integration feature is used in multitenant apps. If apps are in App Service Environment, then it's already in a VNet and doesn't require use of the VNet Integration feature to reach resources in the same VNet.

VNet Integration gives your app access to resources in a VNet, but it doesn't grant inbound private access to your app from the VNet. Private site access refers to making an app accessible only from a private network, such as from within an Azure virtual network. VNet Integration is used only to make outbound calls from your app into your VNet. The VNet Integration feature behaves differently when it's used with VNet in the same region and with VNet in other regions. The VNet Integration feature has two variations:

- **Regional VNet Integration:** When you connect to Azure Resource Manager virtual networks in the same region, you must have a dedicated subnet in the VNet you're integrating with.
- **Gateway-required VNet Integration:** When you connect to VNet in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway provisioned in the target VNet.

The VNet Integration features:

- Require a Standard, Premium, PremiumV2, PremiumV3, or Elastic Premium pricing plan.
- Support TCP and UDP.
- Work with Azure App Service apps and function apps.

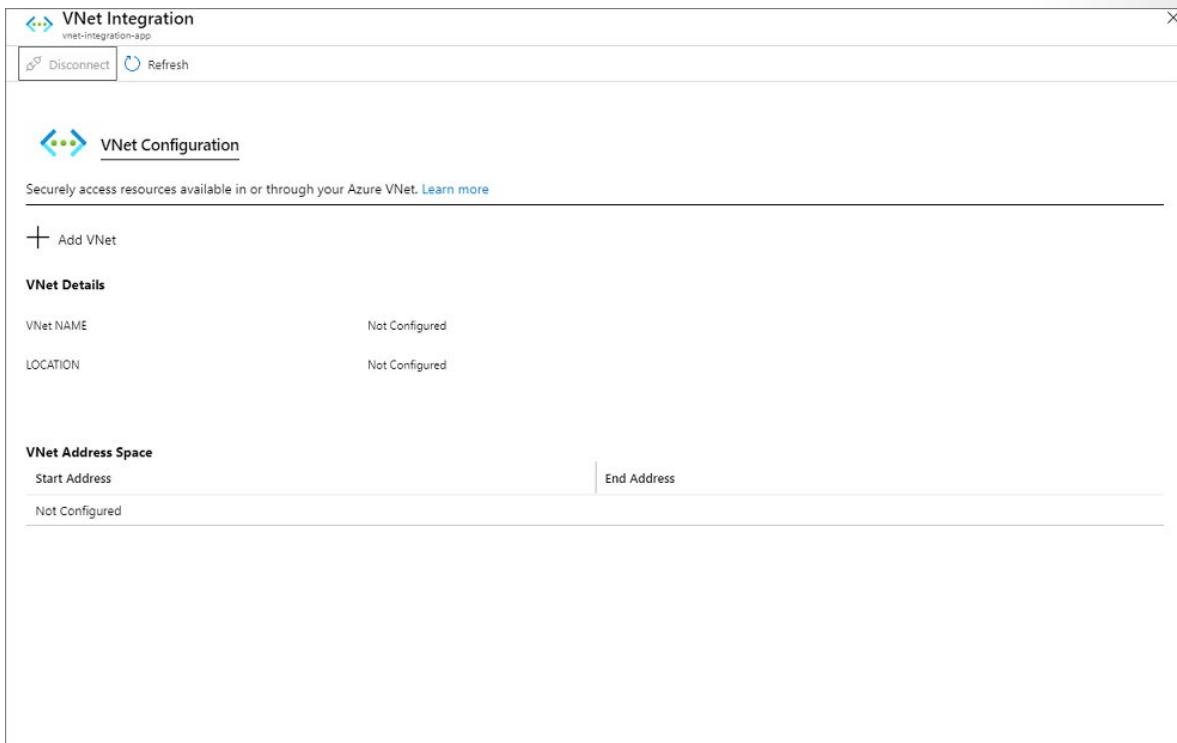
There are some things that VNet Integration doesn't support, like:

- Mounting a drive.
- Active Directory integration.
- NetBIOS.

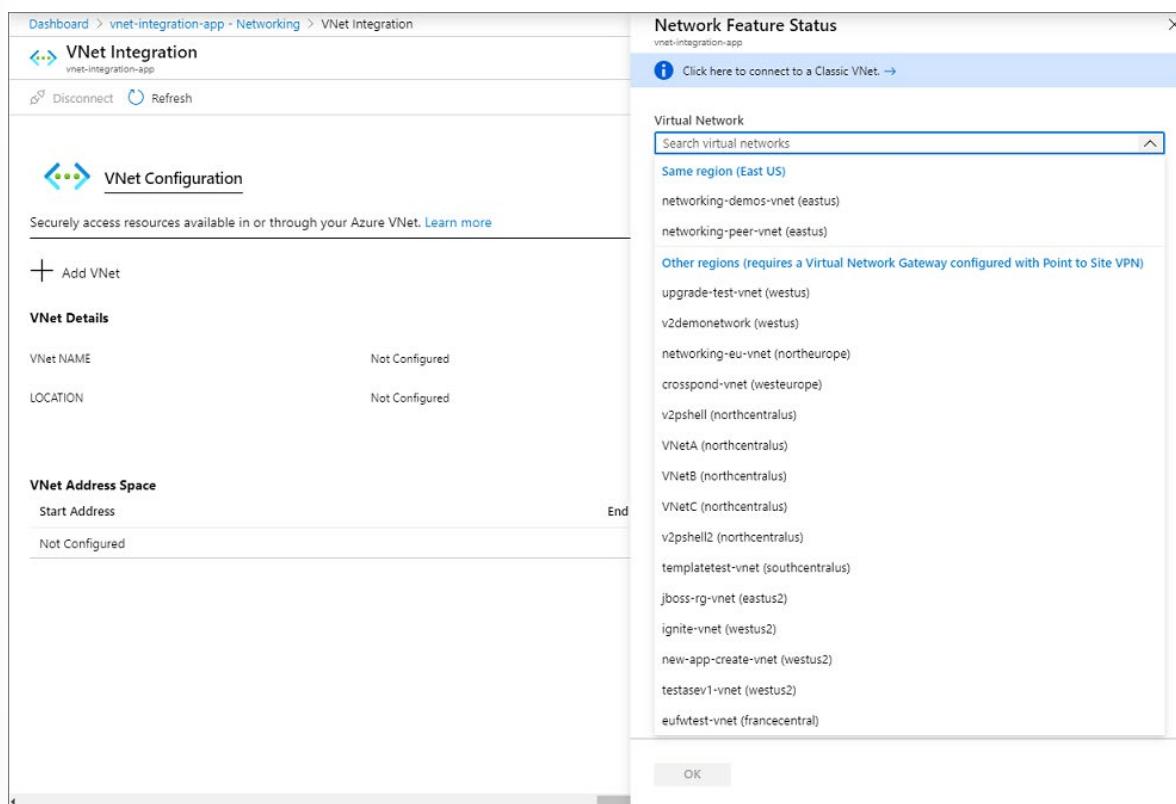
Gateway-required VNet Integration provides access to resources only in the target VNet or in networks connected to the target VNet with peering or VPNs.

## Enable VNet Integration

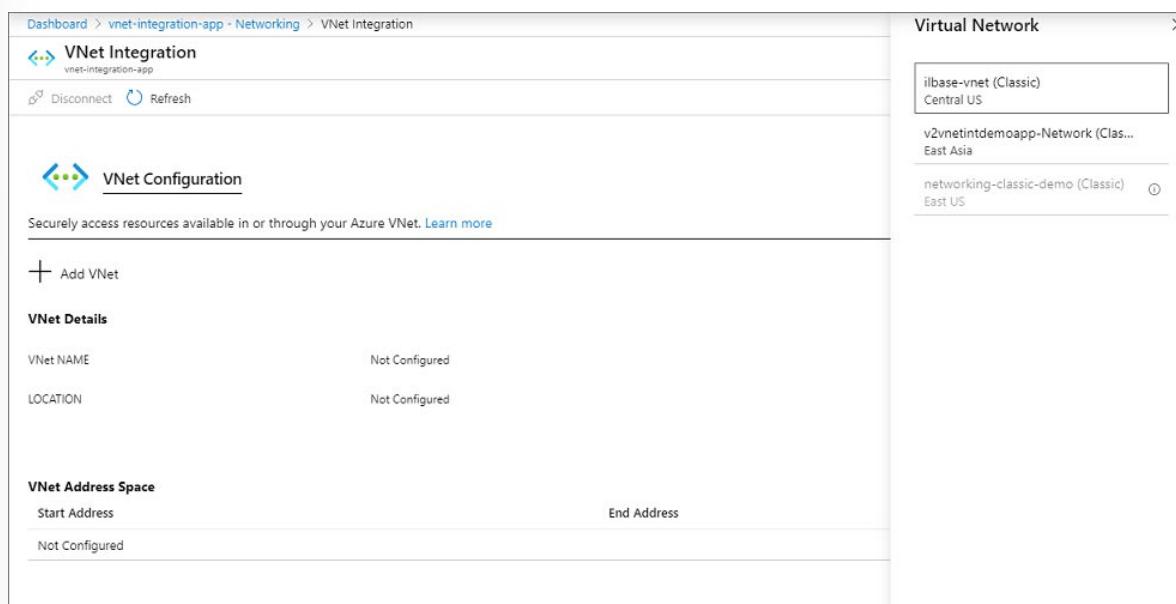
1. Go to the Networking UI in the App Service portal. Under **VNet Integration**, select **Click here** to configure.
2. Select **Add VNet**.



3. The drop-down list contains all of the Azure Resource Manager virtual networks in your subscription in the same region. Underneath that is a list of the Resource Manager virtual networks in all other regions. Select the VNet you want to integrate with.



- If the VNet is in the same region, either create a new subnet or select an empty preexisting subnet.
- To select a VNet in another region, you must have a VNet gateway provisioned with point to site enabled.
- To integrate with a classic VNet, instead of selecting the Virtual Network drop-down list, select Click here to connect to a Classic VNet. Select the classic virtual network you want. The target VNet must already have a Virtual Network gateway provisioned with point-to-site enabled.



During the integration, the app is restarted. When integration is finished, you'll see details on the VNet you're integrated with.

## Regional VNet Integration

Using regional VNet Integration enables your app to access:

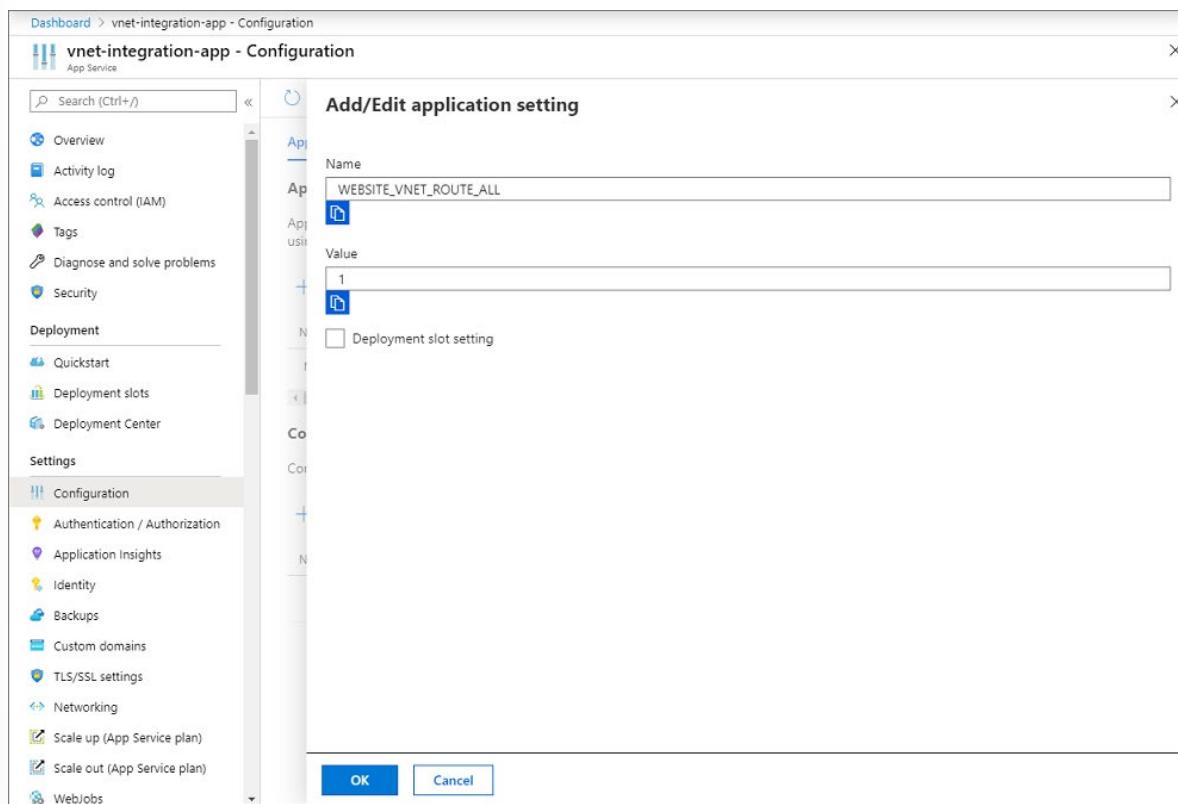
- Resources in a VNet in the same region as your app.
- Resources in VNets peered to the VNet your app is integrated with.
- Service endpoint secured services.
- Resources across Azure ExpressRoute connections.
- Resources in the VNet you're integrated with.
- Resources across peered connections, which includes Azure ExpressRoute connections.
- Private endpoints

When you use VNet Integration with VNets in the same region, you can use the following Azure networking features:

- Network security groups (NSGs): You can block outbound traffic with an NSG that's placed on your integration subnet. The inbound rules don't apply because you can't use VNet Integration to provide inbound access to your app.
- Route tables (UDRs): You can place a route table on the integration subnet to send outbound traffic where you want.

By default, your app routes only RFC1918 traffic into your VNet. If you want to route all of your outbound traffic into your VNet, apply the app setting WEBSITE\_VNET\_ROUTE\_ALL to your app. To configure the app setting:

1. Go to the Configuration UI in your app portal. Select **New application** setting.
2. Enter WEBSITE\_VNET\_ROUTE\_ALL in the **Name** box, and enter **1** in the **Value** box.



3. Select **OK**.
4. Select **Save**.

# Create and Manage Deployment Slots

## Deployment Slots



Within a single Azure App Service web app, you can create multiple deployment slots. Each slot is a separate instance of that web app, and it has a separate host name. You can deploy a different version of your web app into each slot.

One slot is the production slot. This slot is the web app that users see when they connect. Make sure that the app deployed to this slot is stable and well tested.

Use additional slots to host new versions of your web app. Against these instances, you can run tests such as integration tests, acceptance tests, and capacity tests. Fix any problems before you move the code to the production slot. Additional slots behave like their own App Service instances, so you can have confidence that your tests show how the app will run in production.

When you use more than one deployment slot for a web app, those slots are treated as separate instances of that web app. For example, they're listed separately on the **All resources** page in the Azure portal. They each have their own URL. However, each slot shares the resources of the App Service plan, including virtual machine memory and CPU as well as disk space.

## Slots and Tiers

Deployment slots are available only when your web app uses an App Service plan in the Standard, Premium, or Isolated tier. The following table shows the maximum number of slots you can create:

Tier	Maximum staging slots
Free	0
Shared	0
Basic	0
Standard	5
Premium	20
Isolated	20

## Avoid a cold start during swaps

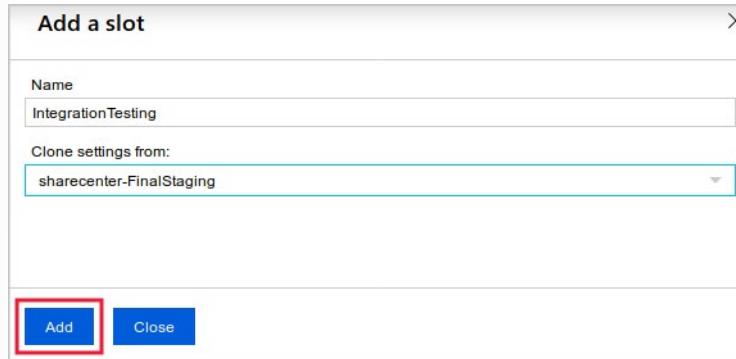
Many of the technologies that developers use to create web apps require final compilation and other actions on the server before they deliver a page to a user. Many of these tasks are completed when the app starts up and receives a request. For example, if you use ASP.NET to build your app, code is compiled and views are completed when the first user requests a page. Subsequent requests for that page receive a faster response because the code is already compiled.

The initial delay is called a cold start. You can avoid a cold start by using slot swaps to deploy to production. When you swap a slot into production, you "warm up" the app because your action sends a request to the root of the site. The warm-up request ensures that all compilation and caching tasks finish. After the swap, the site responds as fast as if it had been deployed for days.

## Create a Deployment Slot

Before you create a slot, make sure your web app is running in the Standard, Premium, or Isolated tier:

1. Open your web app in the Azure portal.
2. Select the **Deployment Slots** page.
3. Select **Add Slot**.
4. Name the slot.
5. Choose whether to clone settings from another slot. If you choose to clone, settings are copied to your new slot from the slot you specify.



Select **Add** to create the new slot. You now see the new slot in the list on the **Deployment Slots** page. Select the slot to view its management page.

The screenshot shows the 'Deployment Slots' page. It includes a description of deployment slots and a table listing three slots: 'sharecenter' (Production, Running, ShareCenterASP, 100%), 'sharecenter-FinalStaging' (Running, ShareCenterASP, 0%), and 'sharecenter-IntegrationTesting' (Running, ShareCenterASP, 0%).

NAME	STATUS	APP SERVICE PLAN	TRAFFIC %
sharecenter <span style="background-color: green; border: 1px solid black; padding: 2px;">PRODUCTION</span>	Running	ShareCenterASP	<div style="width: 100%;">100</div>
sharecenter-FinalStaging	Running	ShareCenterASP	<div style="width: 0%;">0</div>
sharecenter-IntegrationTesting	Running	ShareCenterASP	<div style="width: 0%;">0</div>

## Access a Deployment Slot

The new slot's host name is derived from the web app name and the name of the slot. You see this host name when you select the slot on the **Deployment Slots** page:

The screenshot shows the Azure portal's 'Overview' page for a web application named 'IntegrationTesting'. The URL 'https://sharecenter-integrationtesting.azurewebsites.net' is highlighted with a red box. Other visible details include the Resource group ('sharecenterrrg'), Status ('Running'), Location ('Central US'), Subscription ('Pay-As-You-Go'), Subscription ID ('ce698c92-57c9-43df-b269-2e10273a0425'), and Tags.

You can deploy your code to the new slot the same way you deploy it for the production slot. Just substitute the new slot's name or URL in the configuration of the deployment tool you use. If you use FTP to deploy, you'll see the FTP host name and username just under the slot's URL.

The new slot is effectively a separate web app with a different host name. That's why anyone on the internet can access it if they know that host name. Unless you register the slot with a search engine or link to it from a crawled page, the slot won't appear in search engine indexes. It will remain obscure to the general internet user.

You can control access to a slot by using IP address restrictions. Create a list of IP address ranges that you'll allow to access the slot or a list of ranges that you'll deny access to the slot. These lists are like the allow ranges and deny ranges that you can set up on a firewall. Use this list to permit access only to computers that belong to your company or development team.

# Implement Azure Functions

## Azure Functions

Azure Functions allows you to run small pieces of code (called “functions”) without worrying about application infrastructure. With Azure Functions, the cloud infrastructure provides all the up-to-date servers you need to keep your application running at scale.

A function is “triggered” by a specific type of event. Supported triggers include responding to changes in data, responding to messages, running on a schedule, or as the result of an HTTP request.

While you can always code directly against a myriad of services, integrating with other services is streamlined by using bindings. Bindings give you declarative access to a wide variety of Azure and third-party services.

## Features

Some key features of Azure Functions include:

- **Serverless applications:** Functions allow you to develop **serverless<sup>6</sup>** applications on Microsoft Azure.
- **Choice of language:** Write functions using your choice of **C#, Java, JavaScript, Python, and PowerShell<sup>7</sup>**.
- **Pay-per-use pricing model:** Pay only for the time spent running your code. See the Consumption hosting plan option in the **pricing section<sup>8</sup>**.
- **Bring your own dependencies:** Functions supports NuGet and NPM, giving you access to your favorite libraries.
- **Integrated security:** Protect HTTP-triggered functions with OAuth providers such as Azure Active Directory, Facebook, Google, Twitter, and Microsoft Account.
- **Simplified integration:** Easily integrate with Azure services and software-as-a-service (SaaS) offerings.
- **Flexible development:** Set up continuous integration and deploy your code through **GitHub<sup>9</sup>, Azure DevOps Services<sup>10</sup>, and other supported development tools<sup>11</sup>**.
- **Stateful serverless architecture:** Orchestrate serverless applications with **Durable Functions<sup>12</sup>**.
- **Open-source:** The Functions runtime is open-source and **available on GitHub<sup>13</sup>**.

## What Azure Functions Do?

Functions is a great solution for processing bulk data, integrating systems, working with the internet-of-things (IoT), and building simple APIs and micro-services.

---

<sup>6</sup> <https://azure.microsoft.com/solutions/serverless/>

<sup>7</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/supported-languages>

<sup>8</sup> [https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview?WT.mc\\_id=thomasmaurer-blog-thmaure](https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview?WT.mc_id=thomasmaurer-blog-thmaure)

<sup>9</sup> <https://docs.microsoft.com/en-us/azure/app-service/scripts/cli-continuous-deployment-github>

<sup>10</sup> <https://docs.microsoft.com/en-us/azure/app-service/scripts/cli-continuous-deployment-vsts>

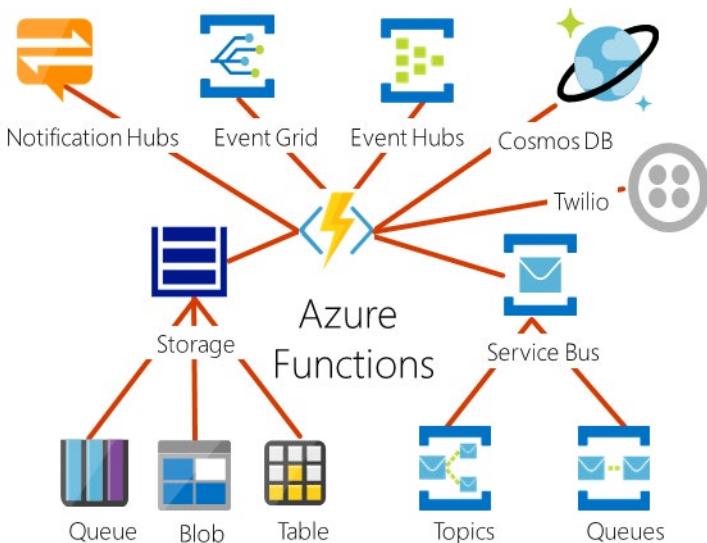
<sup>11</sup> <https://docs.microsoft.com/en-us/azure/app-service/deploy-local-git>

<sup>12</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/durable/durable-functions-overview>

<sup>13</sup> <https://github.com/azure/azure-webjobs-sdk-script>

A series of templates is available to get you started with key scenarios including:

- **HTTP:** Run code based on **HTTP requests**<sup>14</sup>
- **Timer:** Schedule code to **run at predefined times**<sup>15</sup>
- **Azure Cosmos DB:** Process **new and modified Azure Cosmos DB documents**<sup>16</sup>
- **Blob storage:** Process **new and modified Azure Storage blobs**<sup>17</sup>
- **Queue storage:** Respond to **Azure Storage queue messages**<sup>18</sup>
- **Event Grid:** Respond to **Azure Event Grid events via subscriptions and filters**<sup>19</sup>
- **Event Hub:** Respond to **high-volumes of Azure Event Hub events**<sup>20</sup>
- **Service Bus Queue:** Connect to other Azure or on-premises services by **responding Service Bus queue messages**<sup>21</sup>
- **Service Bus Topic:** Connect other Azure services or on-premises services by **responding to Service Bus topic messages**<sup>22</sup>



## Demonstration - Create a Function App

Functions are hosted in an execution context called a function app. You define function apps to logically group and structure your functions and a compute resource in Azure.

<sup>14</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-first-azure-function>

<sup>15</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-scheduled-function>

<sup>16</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-cosmos-db-triggered-function>

<sup>17</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-storage-blob-triggered-function>

<sup>18</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-storage-queue-triggered-function>

<sup>19</sup> <https://docs.microsoft.com/en-us/azure/event-grid/resize-images-on-storage-blob-upload-event>

<sup>20</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-event-hubs>

<sup>21</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-service-bus>

<sup>22</sup> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-service-bus>

## Create a function app

Do the following to create a function app in the Azure portal.

1. Sign into the **Azure portal** <sup>23</sup>.
2. From the portal menu, select **Create a resource**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the text "Microsoft Azure" and a search bar labeled "Search resources, services, and docs (G+/-)". Below the header, there's a section titled "Azure services" featuring a large button with a plus sign and the text "Create a resource", which is highlighted with a red box. To the right of this button are icons for "App Services", "Azure Active Directory", "Recovery Services vaults", "Activity log", "Log Analytics workspaces", "Virtual machine scale sets", and "Service Health". Below this section is a "Recent resources" table with four entries:

Name	Type
AZ303AppSvd	App Service
AZ303Test	Recovery Services vault
az303303	Log Analytics workspace
AZ303VM	Virtual machine

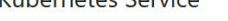
3. Select **Compute > Function App**.

<sup>23</sup> <https://portal.azure.com/learn/docs.microsoft.com>

Microsoft Azure Search resources, services, and docs (G+)

Home > New

## New

Azure Marketplace	See all	Featured	See all
Get started		 Virtual machine	
Recently created		 SQL Server 2017 Enterprise Windows Server 2016	
AI + Machine Learning		 Analytics	 Learn more
Analytics			
Blockchain			
<b>Compute</b>	 Compute	 Reserved VM Instances	 Quickstarts + tutorials
Containers			
Databases		 Kubernetes Service	 Quickstarts + tutorials
Developer Tools			
DevOps		 Service Fabric Cluster	 Quickstarts + tutorials
Identity			
Integration		 Web App for Containers	 Quickstarts + tutorials
Internet of Things			
Media		 Function App	 Quickstarts + tutorials
Mixed Reality			
IT & Management Tools		 Batch Service	
Networking		 Quickstarts + tutorials	
Software as a Service (SaaS)			
Security		 Debian 9 "Stretch" with backports kernel	
Storage		 Ubuntu Server 16.04 LTS	 Quickstarts + tutorials
Web			

4. Select an Azure subscription.
5. Select a resource group or create a new one.

6. Type an app name.
7. Select **Code**.
8. For **Runtime stack**, select **.NET Core**.
9. For **Version** select **3.1**.
10. Select **Review + create**.

The screenshot shows the Microsoft Azure portal interface for creating a new Function App. The top navigation bar includes the Microsoft Azure logo, a search bar, and links for Home, New, and Function App. The main title is 'Function App'. Below the title, there are tabs for Basics, Hosting, Monitoring, Tags, and Review + create. The Basics tab is selected. A descriptive text explains what a function app is: 'Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.' The 'Project Details' section contains fields for Subscription (set to 'Azure Pass - Sponsorship'), Resource Group (set to 'AZ303RG'), and a 'Create new' link. The 'Instance Details' section includes fields for Function App name ('AZ-303FunctionApp'), Publish (radio buttons for 'Code' and 'Docker Container' with 'Code' selected), Runtime stack ('.NET Core'), Version ('3.1'), and Region ('Central US'). At the bottom, there are navigation buttons: 'Review + create' (highlighted with a red box), '< Previous', 'Next : Hosting >', and 'Review and create'.

11. Review the **Function App** details and select **Create**.

The screenshot shows the Microsoft Azure portal interface for creating a new Function App. The app is named 'AZ-303FunctionApp' and is configured with a Consumption (Serverless) plan, Windows operating system, and Central US region. The 'Review + create' step is currently selected. The portal includes a search bar, navigation menu, and a taskbar at the bottom.

## Verify your Azure function app

- After the deployment is complete, select **Your deployment is complete**.

The screenshot shows the Microsoft Azure portal's 'Deployment' blade for a function app. It displays deployment details: Deployment name: Microsoft.Web-FunctionApp-Portal-b3cb210f-8621, Subscription: Azure Pass - Sponsorship, Resource group: AZ303RG, Start time: 5/7/2020, 12:34:16 PM, and Correlation ID: 96fa2f1f-6681-4bca-a7e2-cfd777422605. The 'Your deployment is complete' message is shown with a green checkmark. Under 'Next steps', there is a 'Go to resource' button, which is highlighted with a red box.

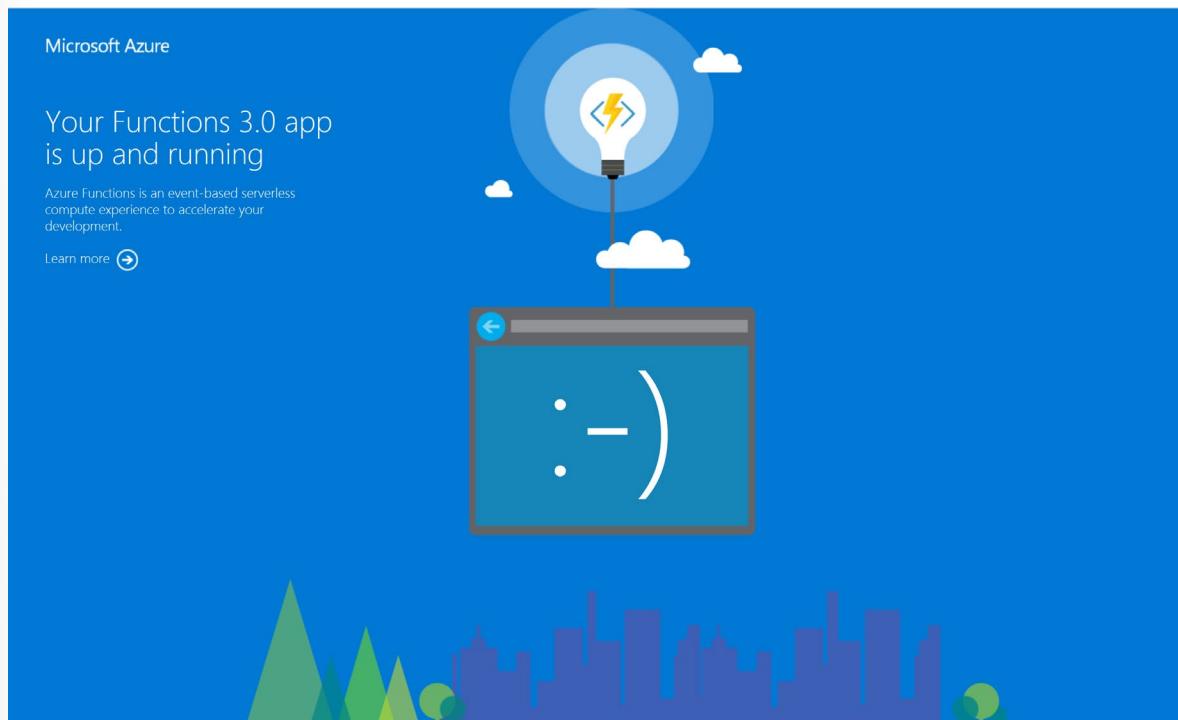
- From the information page for your function app, underneath **URL**, click the link for your function app.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar with the placeholder "Search resources, services, and docs (G+)." Below the search bar, the title "AZ-303FunctionApp" is displayed under the "Function Apps" category. On the left sidebar, there are sections for "Functions", "Proxies", and "Slots". The main content area is titled "Overview" and contains the following details:

Status	Subscription	Resource group	URL
Running	Azure Pass - Sponsorship	AZ303RG	(Redacted)
	Subscription ID 3d4abc70-49fd-4424-a3e2-d84e1e68443d	Location Central US	App Service plan / pricing tier ASP-AZ303RG-9886 (Consumption)

Below the overview, there's a section titled "Configured features" with icons for "Function app settings", "Configuration", and "Application Insights". To the right, there's a blue cloud icon with a lightning bolt. Text on the right says "You have created a function app! Now it is time to add your code..." and a blue button labeled "+ New function".

The item with the lightning bolt Function icon, listed as an App Service, is your new function app. You can click on it to open the details about the new function - it has a public URL assigned to it, if you open that in a browser, you should get a default web page that indicates your Function App is running.



# Implement Logic Apps

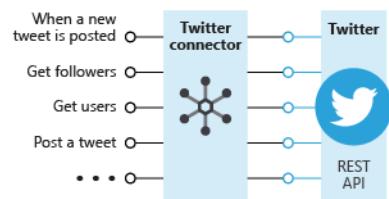
## Logic Apps

This topic helps to decide whether Logic Apps will work for you without any customization. In cases where you do need to create custom components, you'll be able to determine how difficult it will be.

### Connector

A *connector* is a component that provides an interface to an external service. For example, the Twitter connector allows you to send and retrieve tweets, while the Office 365 Outlook connector lets you manage your email, calendar, and contacts. Logic Apps provides hundreds of pre-built connectors that you can use to create your apps.

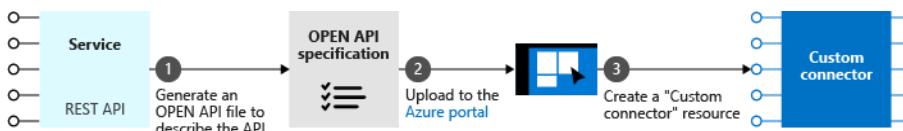
A connector uses the external service's REST or SOAP API to do its work. When you use a connector in your Logic App, the connector calls the service's underlying API for you. The following illustration shows the Twitter connector and its use of the Twitter REST API.



### Custom connectors

You can write custom connectors to access services that don't have pre-built connectors. The services must have a REST or SOAP API. The requirement that the services provide an API shouldn't be too surprising since connectors are essentially wrappers around that underlying API.

To create a custom connector, you first generate an OpenAPI or Postman description of the API. You then use that API description to create a Custom Connector resource in the Azure portal. You can give your connector a name, an icon, and a description for each operation. The following illustration shows an example of the process. Notice that there's no coding involved.

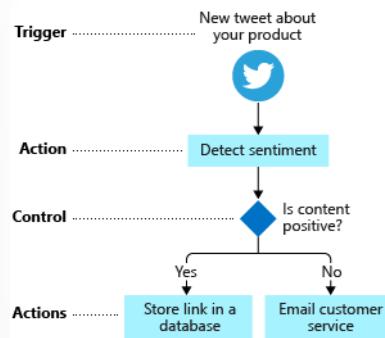


You can use your new connector in your own apps and share it with other people in your organization. You can also submit your connector to Microsoft for certification. Once your connector is certified, it will be included in the set of connectors available to all users.

### Triggers and Actions

Workflows are built from different types of tasks. For example, in our social-media monitor scenario we start the workflow when a new tweet is posted, perform work like detect the sentiment, and decide based on the sentiment score. Logic Apps uses the terms *trigger*, *action*, and *control action* for these concepts.

These operations are the building blocks of Logic Apps. The following illustration shows how we use each type of step in the social-media monitor app.

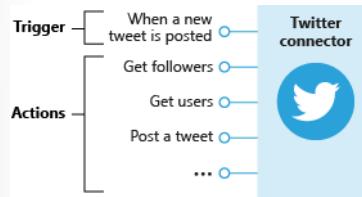


Let's be more specific about the definitions for trigger and action:

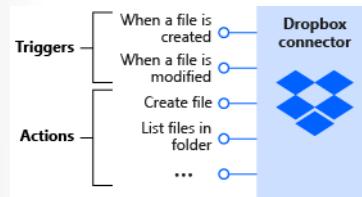
- A *trigger* is an event that occurs when a specific set of conditions is satisfied. Triggers activate automatically when conditions are met. For example, when a timer expires or data becomes available.
- An *action* is an operation that executes a task in your business process. Actions run when a trigger activates or another action completes.

A connector is a container for related triggers and actions. Let's look at a few examples.

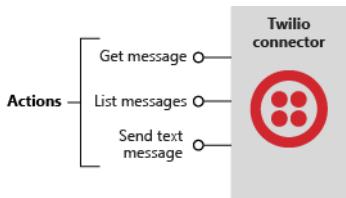
The Twitter connector lets your Logic App interact with Twitter. The social-media monitor app would use a trigger from the Twitter connector to determine when new relevant tweets are available. The following illustration shows the Twitter connector with its trigger and actions.



Next, we have the Dropbox connector. Suppose you were working with a small team on a project that stored its shared data in Dropbox. You could build a workflow that detects when someone modifies any of your files and sends a notification to the other team members. The following illustration shows the Dropbox connector with its triggers and actions.

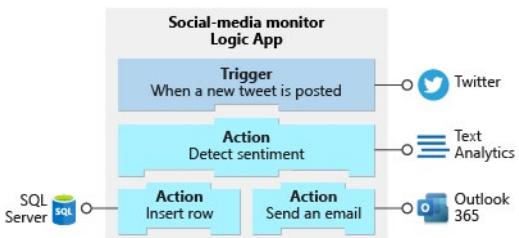


Finally, let's look at the Twilio connector. Most connectors offer both triggers and actions, but this one only has actions. The Twilio connector is great whenever you want to send text messages for notifications. For example, you could use it in the Dropbox scenario to let team members know that a shared file had changed. The following illustration shows the Twilio connector and its actions.



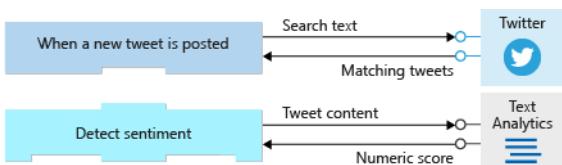
## Build Logic Apps from Triggers and Actions

You build a Logic App from triggers and actions. An app must begin with a trigger. After the trigger, you include as many actions as you need to implement your workflow. The following illustration shows the trigger and actions used in the social-media monitor app.

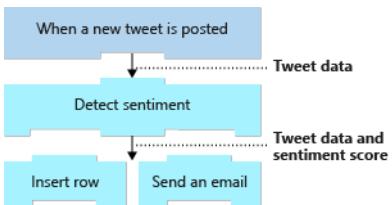


## Triggers and Actions Working Together

Triggers and actions are essentially function calls to an underlying API operation. Each operation has inputs and outputs. For example, the "When a new tweet is posted" Twitter trigger takes in a search string and returns the tweets that contain that string. The "Detect sentiment" action takes a string as input and returns the sentiment score as a floating-point number. The following illustration shows these two operations.

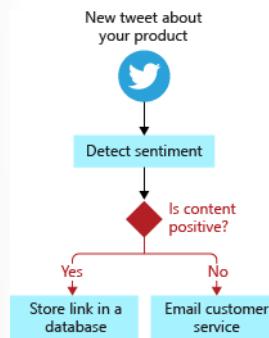


Logic Apps automatically makes the return values available throughout the rest of the operations. This feature lets you pass the results from one operation as input to the next operation. The following illustration shows the data flow for the first two operations in the social-media monitor app. Notice that the results from an operation are available in all of the following steps.



## Control Actions

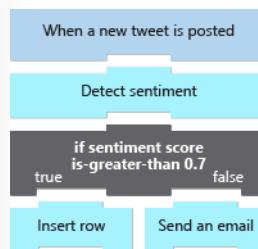
Most workflows need to do different actions based on the data being processed. For example, an expense report might be routed to a different manager based on the amount. In the social-media monitor app, we need to branch based on the sentiment score of the tweet. The following illustration shows the flowchart for the social-media monitor app with the control logic highlighted.



Control actions are special actions built-in to Logic Apps that provides these control constructs:

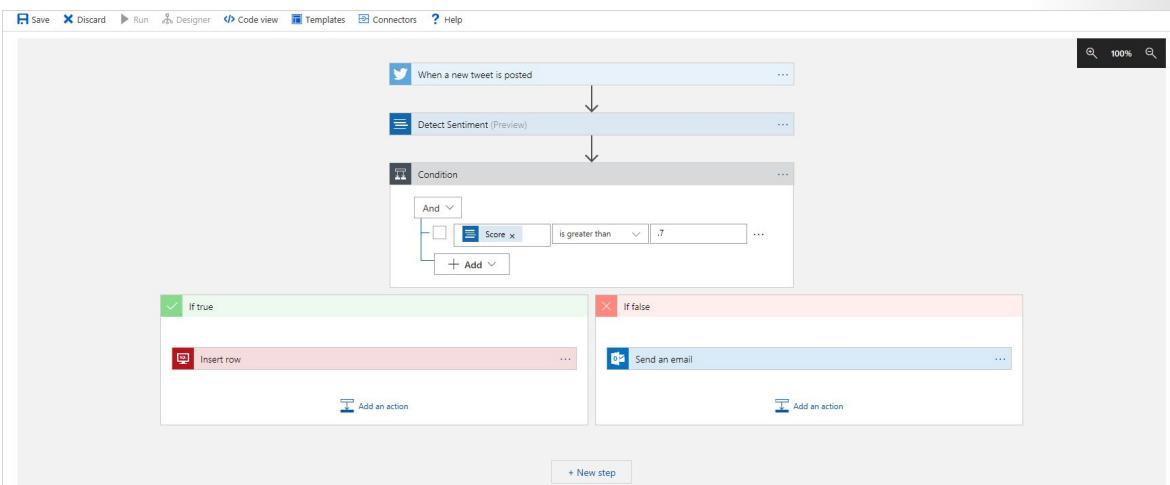
- *Condition* statements controlled by a Boolean expression
- *Switch* statements
- *For each* and *Until* loops
- Unconditional *Branch* instructions.

The following illustration shows the use of a \*Condition\* statement in the social-media monitoring application.



## Logic Apps Designer

The Logic Apps Designer is a graphical tool for creating your workflows. It gives you a design canvas that you use to add a trigger and actions to your app. For example, the social-media monitor app uses the *When a new tweet is posted* trigger, a *Condition* to branch, and the *Detect Sentiment*, *Insert row*, and *Send an email* actions. The following screenshot shows the social-media monitor Logic App displayed in the Designer.



## Demonstration - Create a Workflow using Azure Logic Apps

In this demonstration, you build a logic app that regularly checks a website's RSS feed for new items. If new items exist, the logic app sends an email for each item. When you're done, your logic app looks like this workflow at a high level:



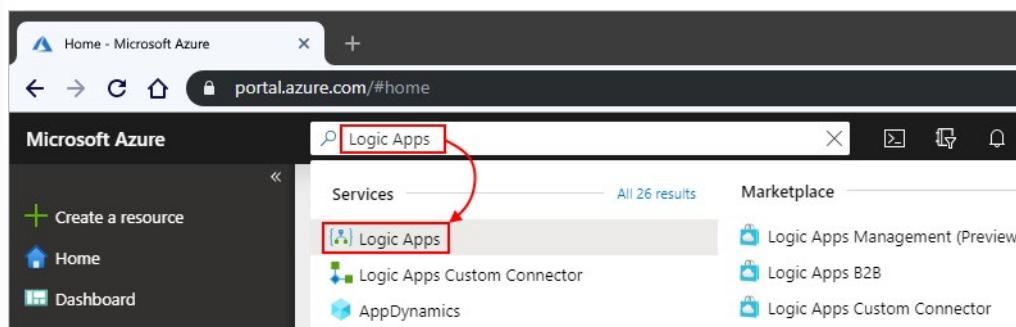
For this scenario, you need an Azure and an email account from a service that's supported by Azure Logic Apps, such as, Outlook.com, or Gmail.

### Create your logic app

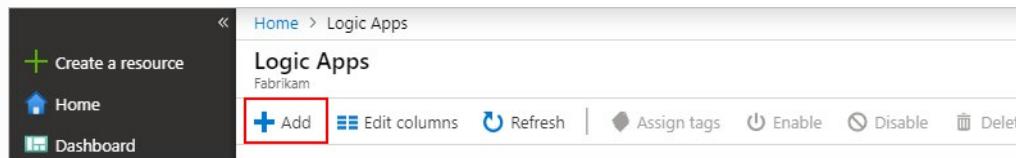
Sign in to the [Azure portal<sup>24</sup>](#) with your Azure account credentials.

- From the Azure home page, in the search box, find and select **Logic Apps**.

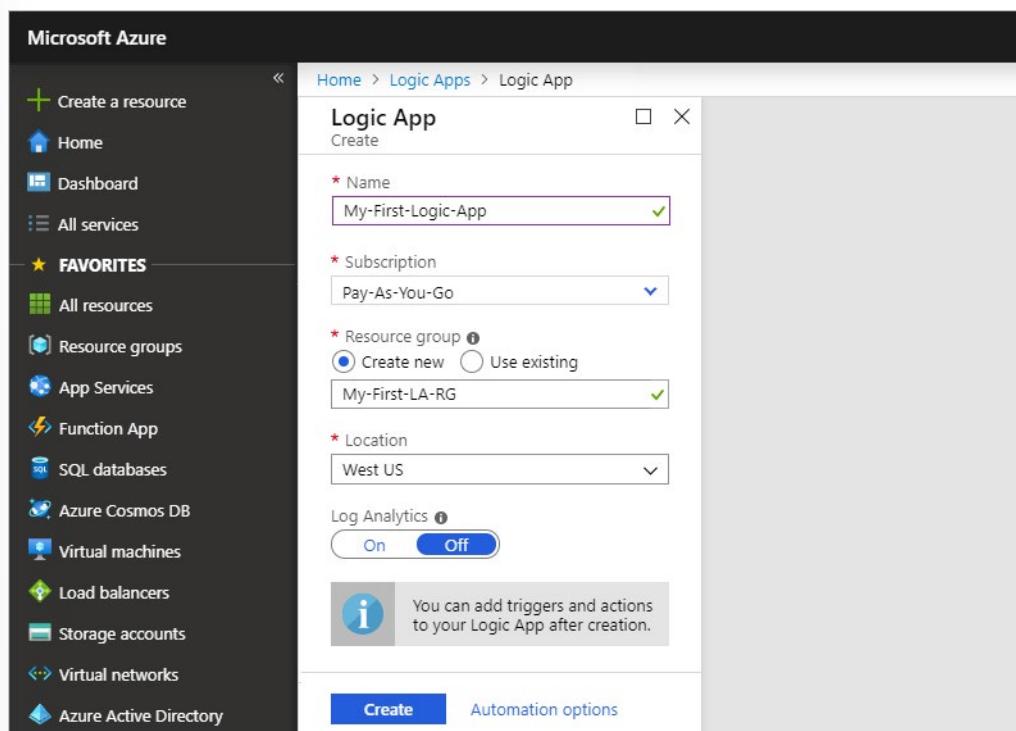
<sup>24</sup> <https://portal.azure.com/>



2. On the **Logic Apps** page, select **Add**.



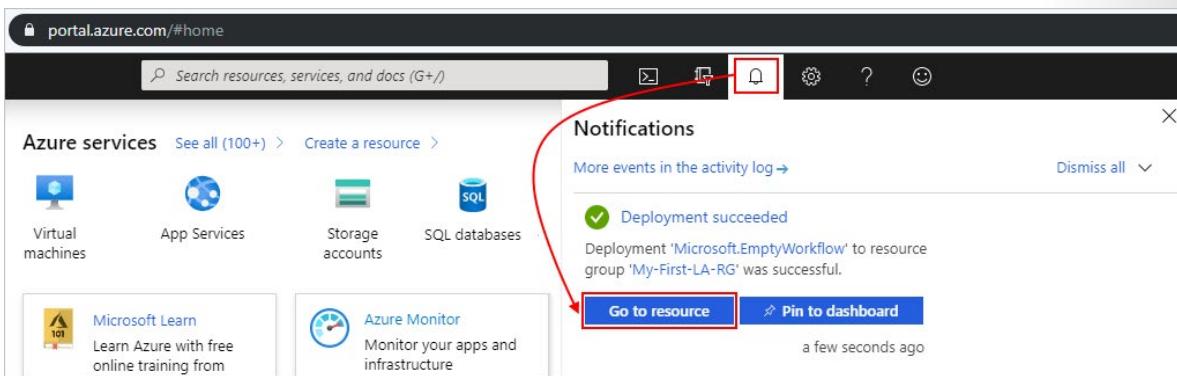
3. On the **Logic App** pane, provide details about your logic app as shown below. After you're done, select **Create**.



Property	Value	Description
<b>Name</b>	<i>logic-app-name</i>	Your logic app name, which can contain only letters, numbers, hyphens (-), underscores (_), parentheses ((, )), and periods (.). This example uses "My-First-Logic-App".

Property	Value	Description
<b>Subscription</b>	<i>Azure-subscription-name</i>	Your Azure subscription name
<b>Resource group</b>	<i>Azure-resource-group-name</i>	The name for the Azure resource group used to organize related resources. This example uses "My-First-LA-RG".
<b>Location</b>	<i>Azure-region</i>	The region where to store your logic app information. This example uses "West US".
<b>Log Analytics</b>	<b>Off</b>	Keep the Off setting for diagnostic logging.

4. After Azure deploys your app, on the Azure toolbar, select **Notifications > Go to resource** for your deployed logic app.



The Logic Apps Designer opens and shows a page with an introduction video and commonly used triggers. Under **Templates**, select **Blank Logic App**.

The screenshot shows the Logic Apps Designer in the Azure portal. At the top, there's a video thumbnail titled "Introducing Azure Logic Apps" with a play button. To the right of the video, there's a descriptive text block about Logic Apps, followed by a bulleted list of features:

- Create business processes and workflows visually
- Integrate with SaaS and enterprise applications
- Unlock value from on-premises and cloud applications

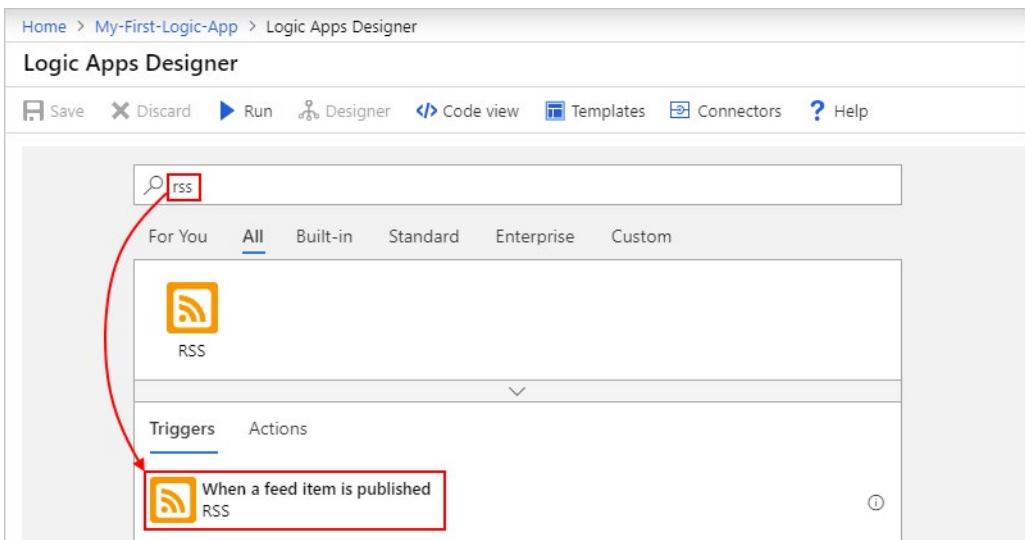
Below the video, there's a section titled "Start with a common trigger" with the sub-instruction "Pick from one of the most commonly used triggers, then orchestrate any number of actions using the rich collection of connectors". A grid of trigger icons is shown:

When a message is received in a Service Bus queue	When a HTTP request is received	When a new tweet is posted	When a Event Grid event occurs
Recurrence	When a new email is received in Outlook.com	When a new file is created on OneDrive	When a file is added to FTP server

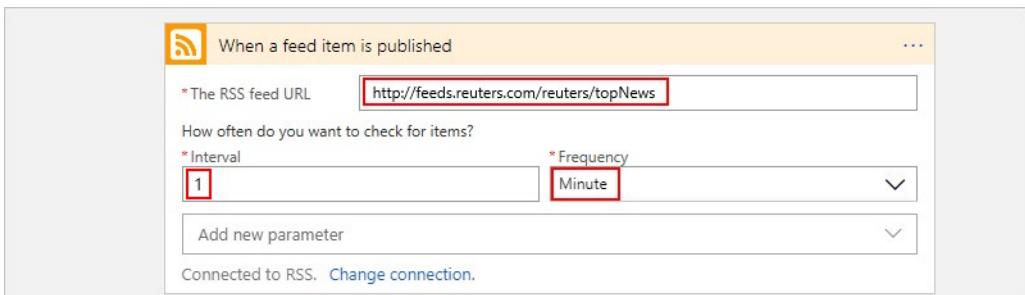
Below the triggers, there's a "Templates" section with a "Blank Logic App" button highlighted with a red border and a plus sign. To the right, there are two cards: "Azure Monitor - Metrics Alert Handler" and a card for a scheduled action with a purple bar at the bottom. At the bottom right, there are filters for "Category: All" and "Sort by: Popularity".

## Add the RSS trigger

1. In the **Logic App Designer**, under the search box, select **All**.
2. In the search box, enter **rss** to find the RSS connector. From the triggers list, select the **When a feed item is published** trigger.



- Provide this information for your trigger as shown and described here:



Property	Value	Description
<b>The RSS feed URL</b>	<a href="http://feeds.reuters.com/reuters/topNews">http://feeds.reuters.com/reuters/topNews</a>	The link for the RSS feed that you want to monitor
<b>Interval</b>	1	The number of intervals to wait between checks
<b>Frequency</b>	Minute	The unit of time for each interval between checks

Together, the interval and frequency define the schedule for your logic app's trigger. This logic app checks the feed every minute.

- To collapse the trigger details for now, click inside the trigger's title bar.

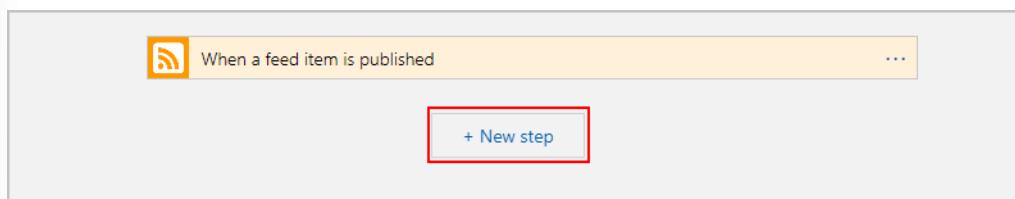


- Save your logic app. On the designer toolbar, select **Save**.

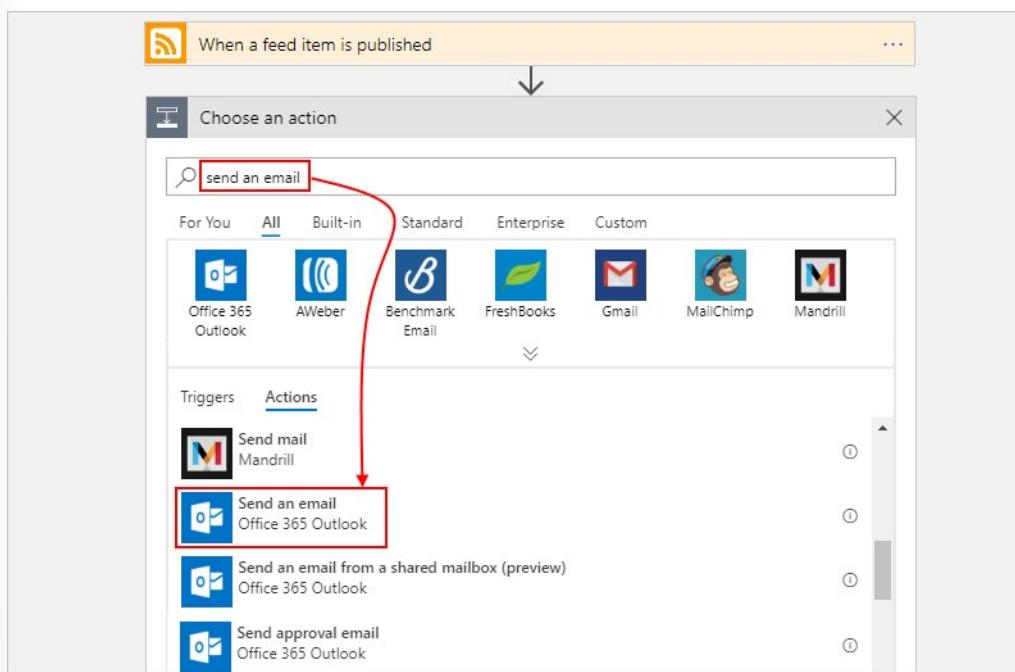
## Add the send email action

Now add an action that sends an email when a new item appears in the RSS feed.

- Under the **When a feed item is published** trigger, select **New step**.



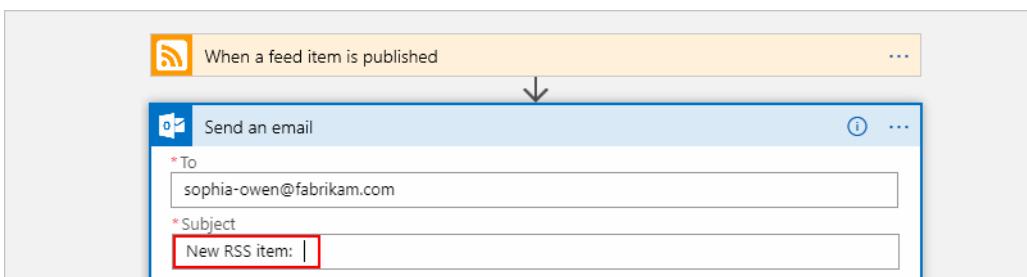
- Under **Choose an action** and the search box, select **All**.
- In the search box, enter **send an email** to find connectors that offer this action. From the actions list, select the "send an email" action for the email service that you want to use. This example uses the Office 365 Outlook connector, which has the **Send an email** action.



To filter the actions list to a specific app or service, you can select that app or service first:

- For Azure work or school accounts, select Office 365 Outlook.
  - For personal Microsoft accounts, select Outlook.com.
- If your selected email connector prompts you to authenticate your identity, complete that step now to create a connection between your logic app and your email service.
  - In the **Send an email** action, specify the data that you want the email to include.
    - In the **To** box, enter the recipient's email address. For testing purposes, you can use your email address.
      - For now, ignore the **Add dynamic content** list that appears. When you click inside some edit boxes, this list appears and shows any available parameters from the previous step that you can include as inputs in your workflow.

- In the **Subject** box, enter this text with a trailing blank space: New RSS item:



- From the Add dynamic content list, select Feed title to include the RSS item title.

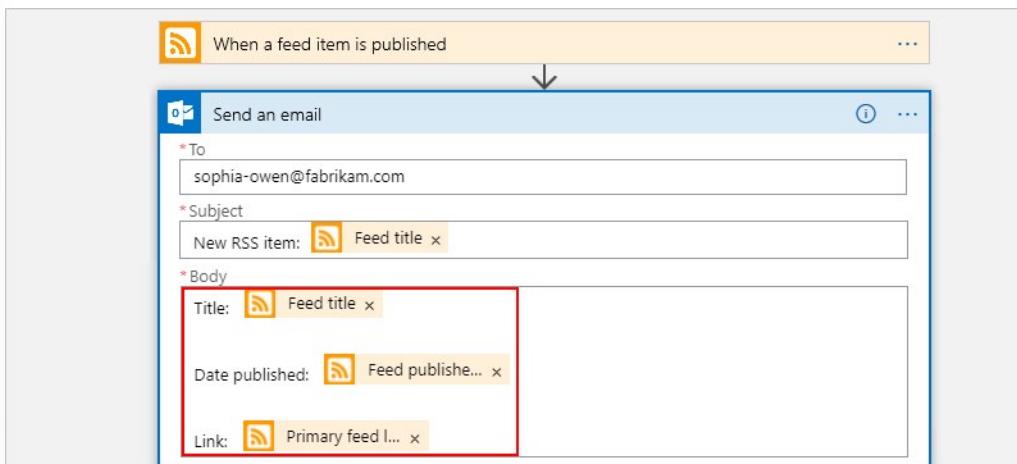
The screenshot shows the Logic App designer with a red arrow pointing from the 'Subject' field in the 'Send an email' step to the 'Feed title' option in the 'Add dynamic content' list. The 'Feed title' option is highlighted with a red box.

When you're done, the email subject looks like this example:



If a "For each" loop appears on the designer, then you selected a token for an array, for example, the **categories-Item** token. For these kinds of tokens, the designer automatically adds this loop around the action that references that token. That way, your logic app performs the same action on each array item. To remove the loop, select the Vellipses (...)V on the loop's title bar, then select **Delete**.

In the **Body** box, enter this text, and select these tokens for the email body. To add blank lines in an edit box, press Shift + Enter.



Property	Description
<b>Feed title</b>	The item's title
<b>Feed published on</b>	The item's publishing date and time
<b>Primary feed link</b>	The URL for the item

6. Save your logic app.

## Run the logic app

To manually start your logic app, on the designer toolbar bar, select **Run**. Or, wait for your logic app to check the RSS feed based on your specified schedule (every minute). If the RSS feed has new items, your logic app sends an email for each new item. Otherwise, your logic app waits until the next interval before checking again. If you don't get any emails, check your junk email folder.

For example, here is a sample email that this logic app sends.



## Labs

# Lab: Implementing an Azure App Service Web App with a Staging Slot

✓ **Important:** To download the most recent version of this lab, please visit the AZ-303 [GitHub repository<sup>25</sup>](#).

Direct link to the [Lab: Implementing an Azure App Service Web App with a Staging Slot<sup>26</sup>](#).

## Lab scenario



Adatum Corporation has a number of web apps that are updated on relatively frequent basis. While Adatum has not yet fully embraced DevOps principles, it relies on Git as its version control and is exploring the options to streamline the app updates. As Adatum is transitioning some of its workloads to Azure, the Adatum Enterprise Architecture team decided to evaluate the use of Azure App Service and its deployment slots to accomplish this objective.

Deployment slots are live apps with their own host names. App content and configurations elements can be swapped between two deployment slots, including the production slot. Deploying apps to a non-production slot has the following benefits:

- It is possible to validate app changes in a staging deployment slot before swapping it with the production slot.
- Deploying an app to a slot first and swapping it into production makes sure that all instances of the slot are warmed up before being swapped into production. This eliminates downtime when during app deployment. The traffic redirection is seamless, and no requests are dropped because of swap operations. This workflow can be automated by configuring auto swap when pre-swap validation is not needed.
- After a swap, the slot with previously staged app has the previous production app. If the changes swapped into the production slot need to be reversed, this simply involves another swap immediately to return to the last known good state.

Deployment slots facilitate two common deployment patterns: blue/green and A/B testing. Blue-green deployment involves deploying an update into a production environment that is separate from the live application. After the deployment is validated, traffic routing is switched to the updated version. A/B testing involves gradually routing some of the traffic to a staging site in order to test a new version of an app.

The Adatum Architecture team wants to use Azure App Service web apps with deployment slots in order to test these two deployment patterns:

- Blue/Green deployments
- A/B testing

<sup>25</sup> <https://github.com/MicrosoftLearning/AZ-303-Microsoft-Azure-Architect-Technologies>

<sup>26</sup> [https://aka.ms/303\\_Module\\_14a\\_Lab](https://aka.ms/303_Module_14a_Lab)

## Objectives

After completing this lab, you will be able to:

- Implement Blue/Green deployment pattern by using deployment slots of Azure App Service web apps
- Perform A/B testing by using deployment slots of Azure App Service web apps

## Lab Environment

Estimated Time: 60 minutes

## Lab Files

None

### Exercise 1: Implement an Azure App Service web app

1. Deploy an Azure App Service web app
2. Create an App Service web app deployment slot

### Exercise 2: Manage App Service web app deployment slots

The main tasks for this exercise are as follows:

1. Deploy web content to an App Service web app staging slot
2. Swap App Service web app staging slots
3. Configure A/B testing
4. Remove Azure resources deployed in the lab

## Lab: Configuring a Message-Based Integration Architecture

✓ **Important:** To download the most recent version of this lab, please visit the AZ-303 [GitHub repository<sup>27</sup>](#).

Direct link to the [Lab: Configuring a Message-Based Integration Architecture<sup>28</sup>](#).

## Lab scenario



Adatum Corporation has several web applications that process files uploaded in regular intervals to their on-premises file servers. File sizes vary, but they can reach up to 100 MB. Adatum is considering migrat-

---

<sup>27</sup> <https://github.com/MicrosoftLearning/AZ-303-Microsoft-Azure-Architect-Technologies>

<sup>28</sup> [https://aka.ms/303\\_Module\\_14b\\_Lab](https://aka.ms/303_Module_14b_Lab)

ing the applications to Azure App Service or Azure Functions-based apps and using Azure Storage to host uploaded files. You plan to test two scenarios:

- using Azure Functions to automatically process new blobs uploaded to an Azure Storage container.
- using Event Grid to generate Azure Storage queue messages that will reference new blobs uploaded to an Azure Storage container.

These scenarios are intended to address a challenge common to a messaging-based architecture, when sending, receiving, and manipulating large messages. Sending large messages to a message queue directly is not recommended as they would require more resources to be used, result in more bandwidth to be consumed, and negatively impact the processing speed, since messaging platforms are usually fine-tuned to handle high volumes of small messages. In addition, messaging platforms usually limit the maximum message size they can process.

One potential solution is to store the message payload into an external service, like Azure Blob Store, Azure SQL or Azure Cosmos DB, get the reference to the stored payload and then send to the message bus only that reference. This architectural pattern is known as "claim check". The clients interested in processing that specific message can use the obtained reference to retrieve the payload, if needed.

On Azure this pattern can be implemented in several ways and with different technologies, but it typically it relies on events to either automate the claim check generation and to push it into the message bus to be used by clients or to trigger payload processing directly. One of the common components included in such implementations is Event Grid, which is an event routing service responsible for delivery of events within a configurable period (up to 24 hours). After that, events are either discarded or dead lettered. If archival of event contents or replayability of event stream are needed, it is possible to facilitate this requirement by setting up an Event Grid subscription to the Event Hub or a queue in Azure Storage where messages can be retained for longer periods and archival of messages is supported.

In this lab, you will use Azure Storage Blob service to store files to be processed. A client just needs to drop the files to be shared into a designated Azure Blob container. In the first exercise, the files will be consumed directly by an Azure Function, leveraging its serverless nature. You will also take advantage of the Application Insights to provide instrumentation, facilitating monitoring and analyzing file processing. In the second exercise, you will use Event Grid to automatically generate a claim check message and send it to an Azure Storage queue. This allows a client application to poll the queue, get the message and then use the stored reference data to download the payload directly from Azure Blob Storage.

It is worth noting that the Azure Function in the first exercise relies on the Blob Storage trigger. You should opt for Event Grid trigger instead of the Blob storage trigger when dealing with the following requirements:

- blob-only storage accounts: blob storage accounts are supported for blob input and output bindings but not for blob triggers. Blob storage triggers require a general-purpose storage account.
- high scale: high scale can be loosely defined as containers that have more than 100,000 blobs in them or storage accounts that have more than 100 blob updates per second.
- reduced latency: if your function app is on the Consumption plan, there can be up to a 10-minute delay in processing new blobs if a function app has gone idle. To avoid this latency, you can use an Event Grid trigger or switch to an App Service plan with the Always On setting enabled.
- processing of blob delete events: blob delete events are not supported by blob storage triggers.

## Objectives

After completing this lab, you will be able to:

- Configure and validate an Azure Function App Storage Blob trigger

- Configure and validate an Azure Event Grid subscription-based queue messaging

## Lab Environment

Estimated Time: 60 minutes

## Lab Files

None

### Exercise 1: Configure and validate an Azure Function App Storage Blob trigger

The main tasks for this exercise are as follows:

1. Configure an Azure Function App Storage Blob trigger
2. Validate an Azure Function App Storage Blob trigger

### Exercise 2: Configure and validate an Azure Event Grid subscription-based queue messaging

The main tasks for this exercise are as follows:

1. Configure an Azure Event Grid subscription-based queue messaging
2. Validate an Azure Event Grid subscription-based queue messaging
3. Remove Azure resources deployed in the lab

# Module 14 Review Questions

## Module 14 Review Questions



### Review Question 1

You are administering a production web app. The app requires scaling to five instances, 40GB of storage, and a custom domain name. Which App Service Plan should you select? Select one.

- Free
- Shared
- Basic
- Standard
- Premium

### Review Question 2

You are backing up your App Service. Which of the following is included in the backup? Select two.

- App configuration
- Azure database for MySQL
- Files and database content totalling 15GB
- Firewall enabled-storage account
- SSL enabled Azure Database for MySQL

### Review Question 3

What method does Microsoft Azure App Service use to obtain credentials for users attempting to access an app? Select one.

- credentials that are stored in the browser
- pass-through authentication
- redirection to a provider endpoint
- synchronization of accounts across providers

## Review Question 4

You have multiple apps running in a single App Service plan. True or False: Each app in the service plan can have different scaling rules.

- True
- False

## Review Question 5

You are backing up your App Service. Which of the following is included in the backup? Select two.

- App configuration
- Azure database for MySQL
- Files and database content totalling 15GB
- Firewall enabled-storage account
- SSL enabled Azure Database for MySQL

## Review Question 6

Your organization has a Basic App Service plan named OEM\_Plan\_1 that hosts an Azure App Service named OEM\_AppSvc\_1.

- You are asked to configure a custom domain and enable backups for OEM\_AppSvc\_1.

What do you recommend be done first?

- Scale out OEM\_Plan\_1
- Scale up OEM\_Plan\_1
- Configure the application settings for OEM\_AppSvc\_1
- Create an separate Azure App Service for OEM\_Plan\_1

# Answers

## Review Question 1

You are administering a production web app. The app requires scaling to five instances, 40GB of storage, and a custom domain name. Which App Service Plan should you select? Select one.

- Free
- Shared
- Basic
- Standard
- Premium

*Explanation*

*Standard. The Standard App Service Plan meets the requirements at the least cost.*

## Review Question 2

You are backing up your App Service. Which of the following is included in the backup? Select two.

- App configuration
- Azure database for MySQL
- Files and database content totalling 15GB
- Firewall enabled-storage account
- SSL enabled Azure Database for MySQL

*Explanation*

*App configuration and Azure database for MySQL. App Service can back up: app configuration, file content, and a database connected to your app (SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, MySQL in-app). Backups can be up to 10 GB of app and database content. Using a firewall enabled storage account as the destination for your backups is not supported. SSL enabled Azure Database for MySQL does not get backed up.*

## Review Question 3

What method does Microsoft Azure App Service use to obtain credentials for users attempting to access an app? Select one.

- credentials that are stored in the browser
- pass-through authentication
- redirection to a provider endpoint
- synchronization of accounts across providers

*Explanation*

*Redirection to a provider endpoint. Microsoft Azure App Service apps redirect requests to an endpoint that signs in users for that provider. The App Service can automatically direct all unauthenticated users to the endpoint that signs in users. Course: Module 4*

**Review Question 4**

You have multiple apps running in a single App Service plan. True or False: Each app in the service plan can have different scaling rules.

- True
- False

*Explanation*

*False. The App Service plan is the scale unit of the App Service apps. If the plan is configured to run five VM instances, then all apps in the plan run on all five instances. If the plan is configured for autoscaling, then all apps in the plan are scaled out together based on the autoscale settings.*

**Review Question 5**

You are backing up your App Service. Which of the following is included in the backup? Select two.

- App configuration
- Azure database for MySQL
- Files and database content totalling 15GB
- Firewall enabled-storage account
- SSL enabled Azure Database for MySQL

*Explanation*

*App configuration and Azure database for MySQL. App Service can back up: app configuration, file content, and a database connected to your app (SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, MySQL in-app). Backups can be up to 10 GB of app and database content. Using a firewall enabled storage account as the destination for your backups is not supported. SSL enabled Azure Database for MySQL does not get backed up.*

**Review Question 6**

Your organization has a Basic App Service plan named OEM\_Plan\_1 that hosts an Azure App Service named OEM\_AppSvc\_1.

What do you recommend be done first?

- Scale out OEM\_Plan\_1
- Scale up OEM\_Plan\_1
- Configure the application settings for OEM\_AppSvc\_1
- Create an separate Azure App Service for OEM\_Plan\_1

*Explanation*

*Correct Answer: Scale up OEM\_Plan\_1. Scaling up is similar to switching to a Production plan that will enable the required features.*

## Module 15 Implement Cloud Infrastructure Monitoring

### Azure Infrastructure Security Monitoring

#### Azure Infrastructure Monitoring

##### **Configuration and Change Management**

Azure reviews and updates configuration settings and baseline configurations of hardware, software, and network devices annually. Changes are developed, tested, and approved prior to entering the production environment from a development and/or test environment.

The baseline configurations that are required for Azure-based services are reviewed by the Azure security and compliance team and by service teams. A service team review is part of the testing that occurs before the deployment of their production service.

##### **Vulnerability Management**

Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure is also able to draw on the resources of the Microsoft Security Response Center (MSRC). The MSRC identifies, monitors, responds to, and resolves security incidents and cloud vulnerabilities around the clock, every day of the year.

##### **Vulnerability Scanning**

Vulnerability scanning is performed on server operating systems, databases, and network devices. The vulnerability scans are performed on a quarterly basis at minimum. Azure contracts with independent assessors to perform penetration testing of the Azure boundary. Red-team exercises are also routinely performed and the results are used to make security improvements.

##### **Protective Monitoring**

Azure security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include the Microsoft Monitoring Agent (MMA) and System Center Operations Manager. These tools are configured to provide time alerts to Azure security personnel in situations that require immediate action.

### Incident Management

Microsoft implements a security incident management process to facilitate a coordinated response to incidents, should one occur.

If Microsoft becomes aware of unauthorized access to customer data that's stored on its equipment or in its facilities, or it becomes aware of unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of customer data, Microsoft takes the following actions:

- Promptly notifies the customer of the security incident.
- Promptly investigates the security incident and provides customers detailed information about the security incident.
- Takes reasonable and prompt steps to mitigate the effects and minimize any damage resulting from the security incident.

An incident management framework has been established that defines roles and allocates responsibilities. The Azure security incident management team is responsible for managing security incidents, including escalation, and ensuring the involvement of specialist teams when necessary. Azure operations managers are responsible for overseeing the investigation and resolution of security and privacy incidents.

## Security Posture

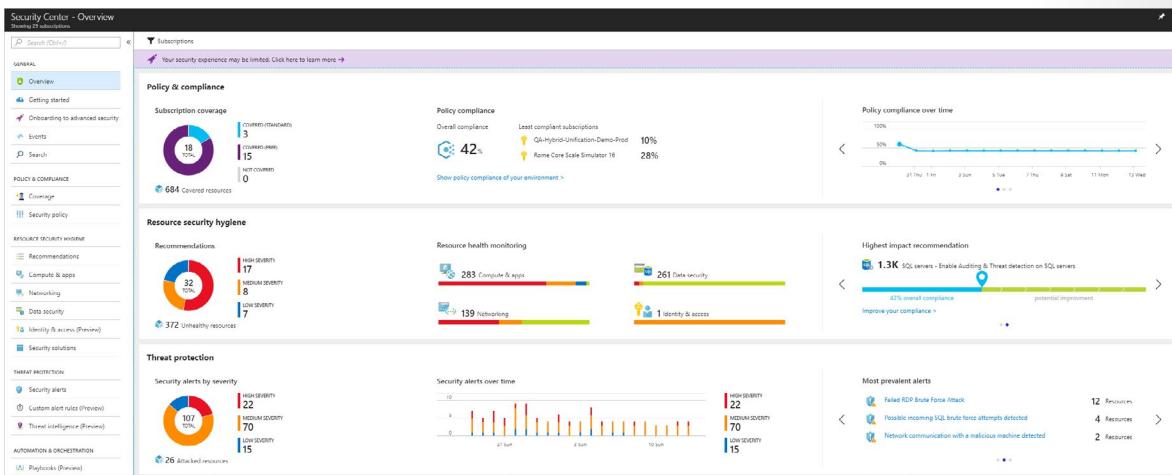
We often think of monitoring as watching and waiting for an event to occur so that we can react to the situation. Strengthening your security posture refers to having a proactive strategy that audits your resources to identify systems that do not meet organizational standards or best practices.

Azure Security Center enables you to strengthen your security posture. This means it helps you identify and perform the hardening tasks recommended as security best practices and implement them across your machines, data services, and apps. This includes managing and enforcing your security policies, and making sure your Azure virtual machines, non-Azure servers, and Azure PaaS services are compliant. Security Center provides you with the tools you need to have a bird's eye view on your workloads, with focused visibility on your network security estate.

You can view the security state of your resources and any issues per resource type:

- To monitor the health of your computer resources and your apps and receive recommendations for improving their security.
- To monitor your network resources, such as virtual machines, network security groups and endpoints, and receive recommendations for improving their security.
- To monitor your data and storage resources, such as SQL servers and storage accounts, and receive recommendations for improving their security.
- To monitor your identity and access resources, including MFA and account permissions, and receive recommendations for improving their security.
- To monitor just-in-time access to your resources.

You can monitor capabilities in Azure Security Center to make sure your resource security is as tight as possible and monitor compliance with policies.



## Azure Security Center

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud, and at the same time, when you move to IaaS (infrastructure as a service) there is more customer responsibility than there was in PaaS (platform as a service), and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services and make sure you're on top of your security posture.

### Azure Security Center addresses the three most urgent security challenges:

- Rapidly changing workloads – It's both a strength and a challenge of the cloud. On the one hand, end users are empowered to do more. On the other, how do you make sure that the ever-changing services people are using and creating are up to your security standards and follow security best practices?
- Increasingly sophisticated attacks - Wherever you run your workloads, the attacks keep getting more sophisticated. You have to secure your public cloud workloads, which are, in effect, an Internet facing workload that can leave you even more vulnerable if you don't follow security best practices.
- Security skills are in short supply - The number of security alerts and alerting systems far outnumbers the number of administrators with the necessary background and experience to make sure your environments are protected. Staying up-to-date with the latest attacks is a constant challenge, making it impossible to stay in place while the world of security is an ever-changing front.

### To help you protect yourself against these challenges, Security Center provides you with the tools to:

- Strengthen security posture: Security Center assesses your environment and enables you to understand the status of your resources, and whether they are secure.
- Protect against threats: Security Center assesses your workloads and raises threat prevention recommendations and security alerts.

- Get secure faster: In Security Center, everything is done in cloud speed. Because it is natively integrated, deployment of Security Center is easy, providing you with autoprovisioning and protection with Azure services.

### **Architecture**

Because Security Center is natively part of Azure, PaaS services in Azure - including Service Fabric, SQL databases, and storage accounts - are monitored and protected by Security Center without necessitating any deployment.

In addition, Security Center protects non-Azure servers and virtual machines in the cloud or on premises, for both Windows and Linux servers, by installing the Log Analytics agent on them. Azure virtual machines are auto-provisioned in Security Center.

The events collected from the agents and from Azure are correlated in the security analytics engine to provide you tailored recommendations (hardening tasks), that you should follow to make sure your workloads are secure, and security alerts. You should investigate such alerts as soon as possible to make sure malicious attacks aren't taking place on your workloads.

When you enable Security Center, the security policy built-in to Security Center is reflected in Azure Policy as a built in initiative under Security Center category. The built-in initiative is automatically assigned to all Security Center registered subscriptions (Free or Standard tiers). The built-in initiative contains only Audit policies.

You'll provide information on how to protect resources and respond to threats by using Azure Security Center.

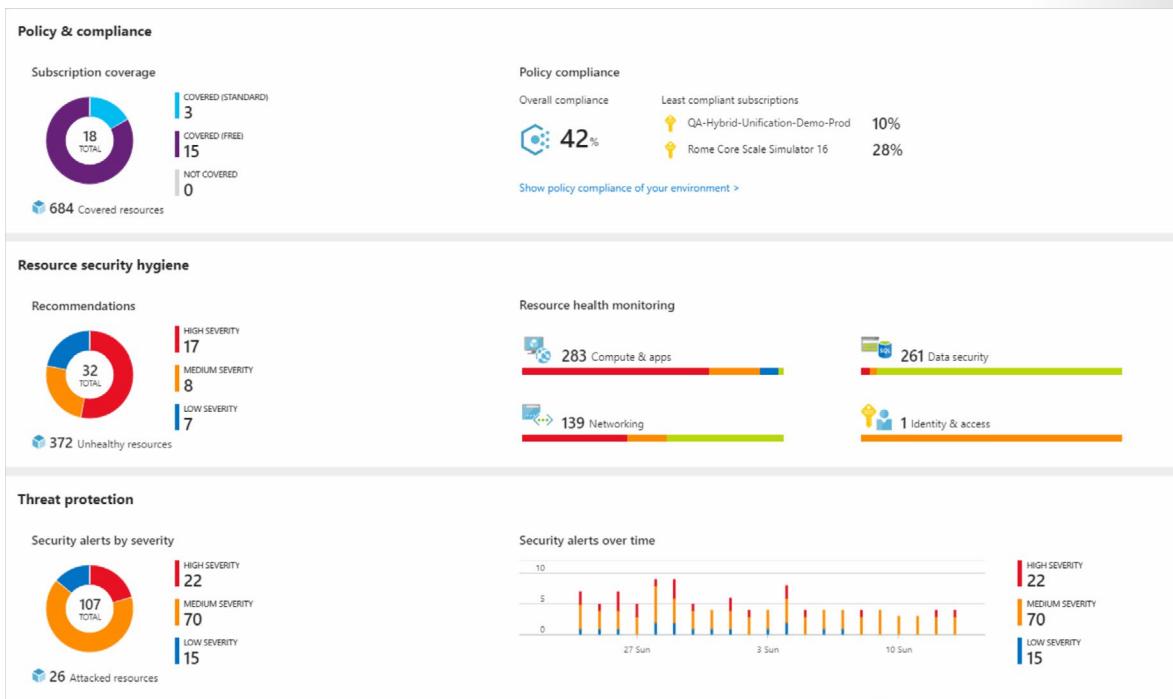
### **Criteria for assessing Azure Security Center**

You use Security Center if:

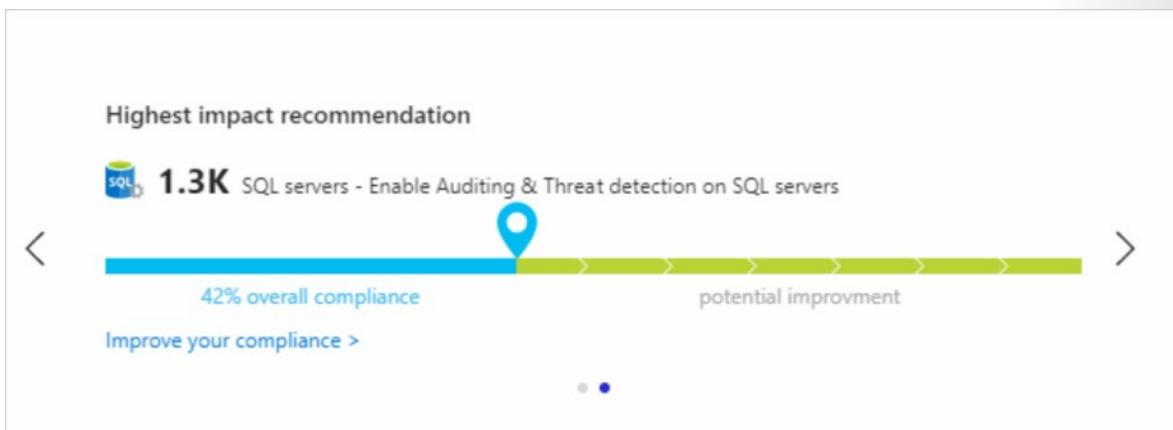
- You want to identify and address risks and threats to your infrastructure.
- You don't have the traditional in-house skills and capital needed to secure a complex infrastructure.
- You want to secure an infrastructure that consists of on-premises and cloud resources.

### **Understand the security posture of your architecture**

Security Center gives detailed analyses of different components of your environment. These components include data security, network security, identity and access, and application security. This way, Security Center helps you understand the security of your architecture. You can then build and maintain better infrastructures.



Security Center recommends how to address the issues and risks that it has uncovered. You use recommendations like the following one to improve the security and compliance of your architecture.



## Strengthened Security Posture

It's good to make sure your workloads are secure, and it starts with having tailored security policies in place. Because all the policies in Security Center are built on top of Azure policy controls, you're getting the full range and flexibility of a world-class policy solution. In Security Center, you can set your policies to run on management groups, across subscriptions, and even for a whole tenant.

 Policy Management

Manage the security policies by choosing a subscription or management group from the list below. In order to define additional policies, manage exclusions and advanced settings, go to Azure policies > Click here to learn more >

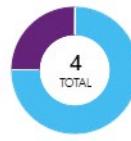
7 MANAGEMENT GROUPS 4 SUBSCRIPTIONS 20 WORKSPACES

NAME	POLICY INITIATIVE ASSIGNMENT(S)	COMPLIANCE	COVERAGE	SETTINGS
Rome ILDC - Detection Prod Test 1	ASC Default (subscription: 845d028d-fc71-4c45-b41d-a47b)	32%	Standard	<a href="#">Edit settings &gt;</a>
Visual Studio Enterprise		---	Free	<a href="#">Edit settings &gt;</a>
72f988bf-86f1-41af-91ab-2d7cd011db47 (2 of 8 subscriptions)	⚠ Limited permissions	---	<a href="#">Edit settings &gt;</a>	
BenKligerMG (1 of 1 subscriptions)	⚠ Limited permissions	---	<a href="#">Edit settings &gt;</a>	
ASC DEMO	[Preview]: Enable Monitoring in Azure Security Center	27%	Standard	<a href="#">Edit settings &gt;</a>
Contoso (1 of 7 subscriptions)	⚠ Limited permissions	---	<a href="#">Edit settings &gt;</a>	
Applications (0 of 5 subscriptions)	⚠ Limited permissions	---	<a href="#">Edit settings &gt;</a>	
IT (1 of 2 subscriptions)	⚠ Limited permissions	---	<a href="#">Edit settings &gt;</a>	
Application Team (1 of 1 subscriptions)	⚠ Limited permissions	---	<a href="#">Edit settings &gt;</a>	
Contoso IT - demo	[Preview]: Enable Monitoring in Azure Security Center	13%	Standard	<a href="#">Edit settings &gt;</a>
Infrastructure Team (0 of 1 subscriptions)	⚠ Limited permissions	---	<a href="#">Edit settings &gt;</a>	

Security Center helps you **identify Shadow IT subscriptions**. By looking at subscriptions labeled **not covered** in your dashboard, you can know immediately when there are newly created subscriptions and make sure they are covered by your policies, and protected by Azure Security Center.

**Policy & compliance**

**Subscription coverage**



Covered (standard)	3
Covered (free)	1
Not covered	0

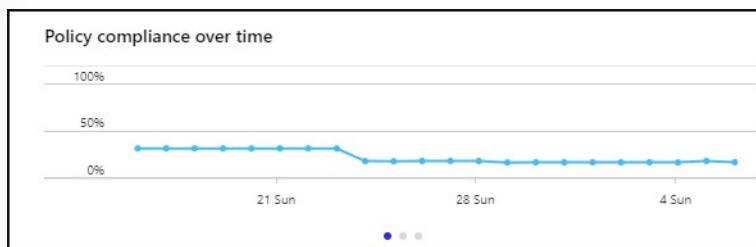
394 Covered resources

**Policy compliance**

Overall compliance	17%	Least compliant subscriptions
	Contoso IT - demo	13%
	ASC DEMO	27%

[Show policy compliance of your environment >](#)

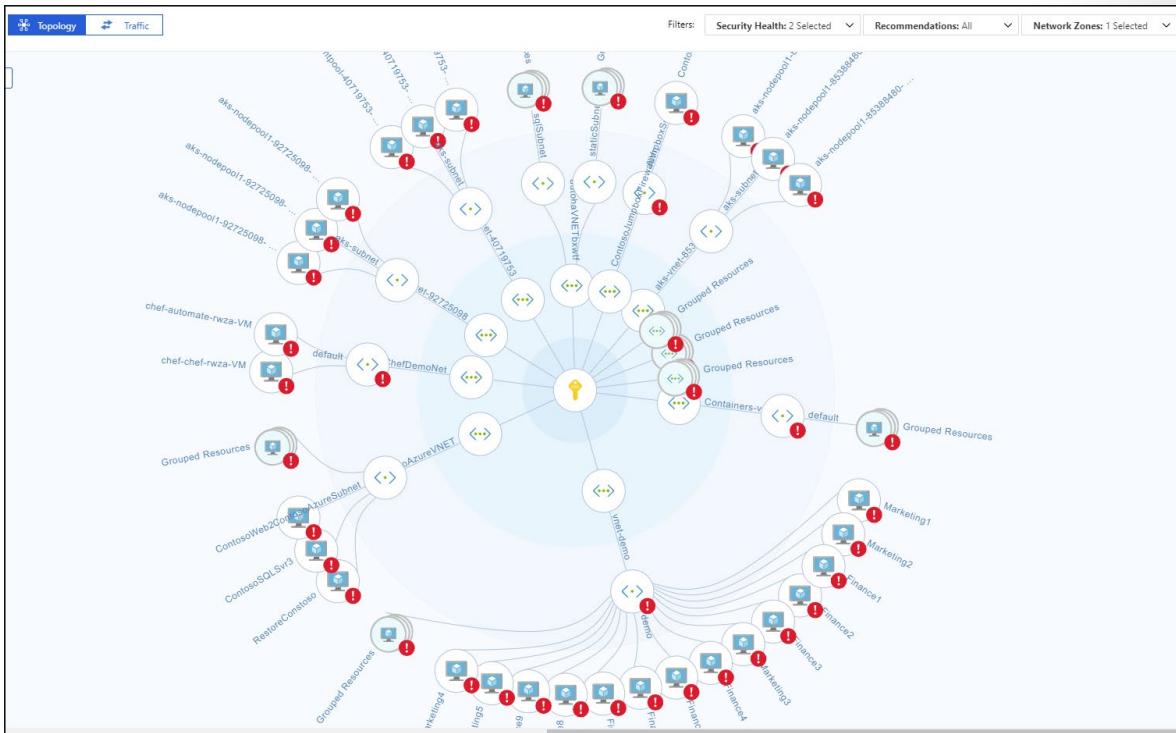
The advanced monitoring capabilities in Security Center also let you **track and manage compliance and governance over time**. The **overall compliance** provides you with a measure of how much your subscriptions are compliant with policies associated with your workload.



### Continuous assessments

Security Center continuously discovers new resources that are being deployed across your workloads and assesses whether they are configured according to security best practices, if not, they're flagged and you get a prioritized list of recommendations for what you need to fix in order to protect your machines.

One of the most powerful tools Security Center provides for continuously monitoring the security status of your network is the **Network map**. The map enables you to see the topology of your workloads, so you can see if each node is properly configured. You can see how your nodes are connected, which helps you block unwanted connections that could potentially make it easier for an attacker to creep along your network.



Security Center makes mitigating your security alerts one step easier, by adding a **Secure Score**. The Secure Scores are now associated with each recommendation you receive to help you understand how important each recommendation is to your overall security posture. This is crucial in enabling you to **prioritize your security work**.



# Protect Against Threats with Azure Security Center

You have the responsibility to dismiss alerts if no action is required, such as if there are false positives. You also need to act to address known attacks and block, for example, known malicious IP addresses. Also, you must decide which alerts require more investigation.

Security Center gives a centralized view of all your security alerts. Security Center ranks security alerts based on their severity. Security Center also combines related alerts as much as possible into a single security incident.

The screenshot shows the Azure Security Center - Overview page. A specific incident is highlighted:

**Security incident detected**  
Incident Detected

Description: The incident which started on 2019-08-09 01:01:00Z and most recently detected on 2019-08-10 10:01:00Z indicate that an attacker has attacked other resources from your virtual machine vm1.

Activity time: Saturday, August 10, 2019, 1:01:00 PM

Severity: ● High

State: Active

Attacked Resource: vm1

Subscription: ASC DEMO

Detected by: Microsoft

Action Taken: Detected

Environment: Azure

Remediation Steps: 1. Escalate the alert to the information security team.  
2. Review the remediation steps of each one of the alerts

Alerts included in this incident:

DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY
SQL injection blocked	4	08/09/19, 04:01 AM	vm1	<span style="color: blue;">●</span> Low
Failed RDP Brute Force Attack	4	08/09/19, 05:01 AM	vm1	<span style="color: blue;">●</span> Low
Successful RDP brute force attack	4	08/10/19, 05:01 AM	vm1	<span style="color: red;">●</span> High
Suspicious SVCHOST process executed	4	08/10/19, 06:01 AM	vm1	<span style="color: blue;">●</span> Low
Multiple Domain Accounts Queried	4	08/10/19, 07:01 AM	vm1	<span style="color: blue;">●</span> Low
Network communication with a malicious machine detected	4	08/10/19, 08:01 AM	vm1	<span style="color: orange;">⚠</span> Medium

Security Center helps you respond to threats faster, and in an automated way, through playbooks. Playbooks are automated procedures that you run against alerts. You configure a playbook in the Playbooks pane of the Azure Security Center menu. You create a playbook by configuring a logic app.

The screenshot shows the Azure Security Center Playbooks (Preview) interface. On the left, there's a sidebar with icons for different services like Security Center, Log Analytics, and Azure Monitor. The main area displays a list of playbooks under the heading "Security Playbooks". It shows 0 runs with 0 succeeded, 0 failed, and 0 running. A search bar at the bottom of this list is set to "Search playbooks". To the right, a modal window titled "Logic App" is open, showing a configuration form. The "Name" field is set to "ProcessExecuted" with a green checkmark. The "Subscription" field is set to "Your-subscription" with a red exclamation mark. The "Resource group" section has "Create new" selected and "resource-group" entered. The "Location" is set to "Central US". Under "Log Analytics", the "On" button is selected. A note says "You can add triggers and actions to your Logic App after creation." At the bottom of the modal are "Create" and "Automation options" buttons.

Your created playbook appears in a list.

Home > Security Center - Playbooks (Preview)

## Security Center - Playbooks (Preview)

Showing subscription 'Technologists\_A'

Search (Ctrl+ /)

Add Playbook Refresh Filter Enable Disable Delete

IoT Hubs & resources  
Data & storage  
Identity & access  
Security solutions

ADVANCED CLOUD DEFENSE

Adaptive application controls  
Just in time VM access  
Adaptive network hardening  
File Integrity Monitoring

THREAT PROTECTION

Security alerts  
Security alerts map (Preview)

AUTOMATION & ORCHESTRATION

Playbooks (Preview)

Security Playbooks      Runs      Run Summary

1      0      Succeeded: 0  
Failed: 0  
Running: 0

Playbooks

Search playbooks

NAME	STATUS	TO...	RU...	SU...	FA...
ProcessExecuted	Enabled	0	0	0	0

Edit your playbook by selecting it and using the Azure Logic Apps Designer that appears.

Choose a template below to create your Logic App.

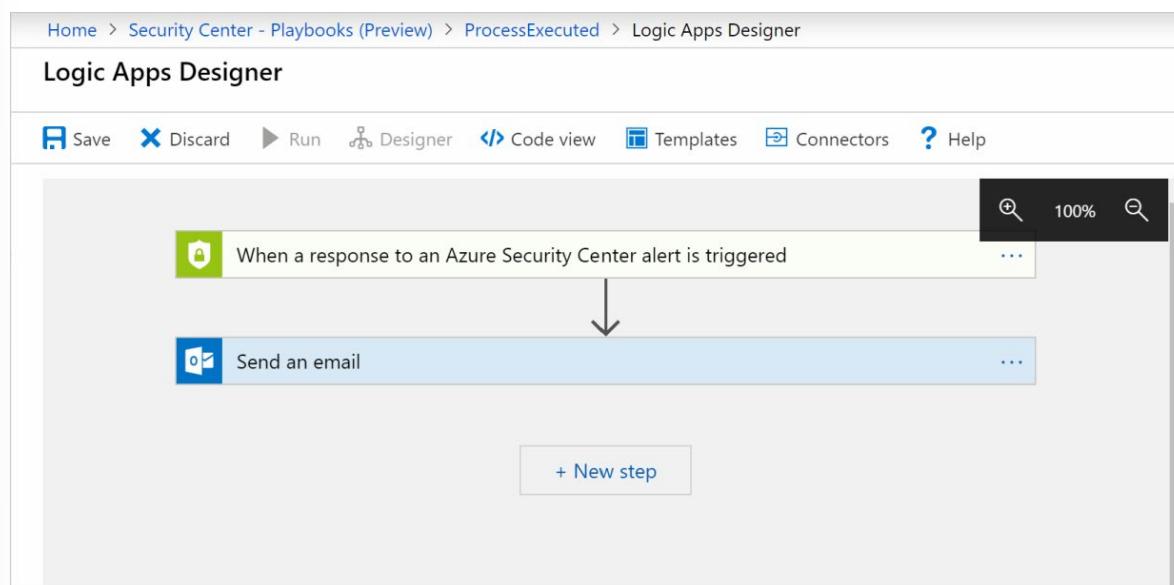
Category : Security Sort by : Popularity

The screenshot shows a grid of logic app templates. The first template is 'Blank Logic App' with a large blue plus sign icon. The second and third templates are both titled 'Get a notification email when Security Center creates a recommendation' and 'Get a notification email when Security Center detects a threat', each featuring a shield and mail icon. The fourth template is 'Post message in Slack', with a shield and hash tag icon. The fifth template is 'Post message to Teams channel and send email notification', with a shield and Microsoft Teams icon. The sixth template is 'Send notification email', with a shield and mail icon.

After you create a new blank logic app, you can use the designer to search for Security Center connectors and triggers for your playbook. For example, look for Azure Security Center and see all the triggers you can use. You then choose a trigger that details what should happen when the playbook is triggered.

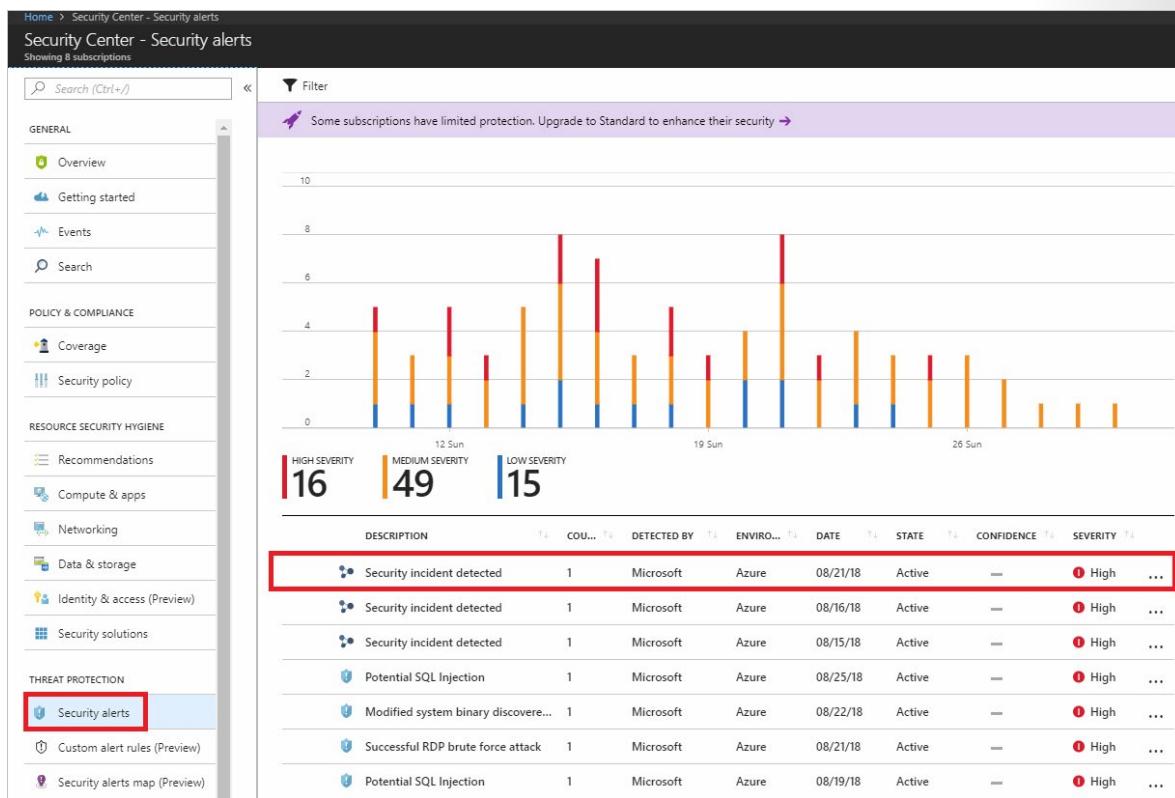
The screenshot shows the Azure Logic Apps designer interface with a search bar at the top containing 'azure security center'. Below the search bar, there are two sections: 'Connectors' and 'Triggers (1) Actions (0)'. Under 'Connectors', there is one item: 'Request'. Under 'Triggers (1)', there is one item: 'Request - When a response to an Azure Security Center alert is triggered'. At the bottom of the screen, there are two feedback options: 'TELL US WHAT YOU NEED' and 'Help us decide which connectors and triggers to add next with UserVoice'.

You then define actions that should be taken and which conditions must be met for these actions. Your actions can specify that an email should be sent when an alert is triggered.



Home > Security Center - Overview > Security alerts > Security incident detected																																				
<b>Security incident detected</b> Incident Detected																																				
Description	The incident which started on 2019-08-09 01:01:00Z and most recently detected on 2019-08-10 10:01:00Z indicate that an attacker has attacked other resources from your virtual machine vm1																																			
Activity time	Saturday, August 10, 2019, 1:01:00 PM																																			
Severity	High																																			
State	Active																																			
Attacked Resource	vm1																																			
Subscription	ASC DEMO																																			
Detected by	Microsoft																																			
Action Taken	Detected																																			
Environment	Azure																																			
Remediation Steps	1. Escalate the alert to the information security team. 2. Review the remediation steps of each one of the alerts																																			
Alerts included in this incident																																				
<table border="1"><thead><tr><th>DESCRIPTION</th><th>COUNT</th><th>ACTIVITY TIME</th><th>ATTACKED RESOURCE</th><th>SEVERITY</th></tr></thead><tbody><tr><td>SQL injection blocked</td><td>4</td><td>08/09/19, 04:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Failed RDP Bruteforce Attack</td><td>4</td><td>08/09/19, 05:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Successful RDP bruteforce attack</td><td>4</td><td>08/10/19, 05:01 AM</td><td>vm1</td><td>High</td></tr><tr><td>Suspicious SVCHOST process executed</td><td>4</td><td>08/10/19, 06:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Multiple Domain Accounts Queried</td><td>4</td><td>08/10/19, 07:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Network communication with a malicious machine detected</td><td>4</td><td>08/10/19, 08:01 AM</td><td>vm1</td><td>Medium</td></tr></tbody></table>		DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY	SQL injection blocked	4	08/09/19, 04:01 AM	vm1	Low	Failed RDP Bruteforce Attack	4	08/09/19, 05:01 AM	vm1	Low	Successful RDP bruteforce attack	4	08/10/19, 05:01 AM	vm1	High	Suspicious SVCHOST process executed	4	08/10/19, 06:01 AM	vm1	Low	Multiple Domain Accounts Queried	4	08/10/19, 07:01 AM	vm1	Low	Network communication with a malicious machine detected	4	08/10/19, 08:01 AM	vm1	Medium
DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY																																
SQL injection blocked	4	08/09/19, 04:01 AM	vm1	Low																																
Failed RDP Bruteforce Attack	4	08/09/19, 05:01 AM	vm1	Low																																
Successful RDP bruteforce attack	4	08/10/19, 05:01 AM	vm1	High																																
Suspicious SVCHOST process executed	4	08/10/19, 06:01 AM	vm1	Low																																
Multiple Domain Accounts Queried	4	08/10/19, 07:01 AM	vm1	Low																																
Network communication with a malicious machine detected	4	08/10/19, 08:01 AM	vm1	Medium																																

View your security alerts through the **Security alerts** pane under the **Security** section on the main menu.



You drill down into specific security incidents by selecting an incident.

Security incident detected

Incident Detected

DESCRIPTION The incident which started on 2018-01-01T12:00:00.000Z and most recently detected on 2018-01-02T19:00:00.000Z indicate that an attacker has attacked other resources from your virtual machine ContosoWebFE1

DETECTION TIME Thursday, January 4, 2018, 3:02:00 AM

SEVERITY ! High

STATE Active

ATTACKED RESOURCE ContosoWebFE1

SUBSCRIPTION <Subscription ID>

DETECTED BY Microsoft

ENVIRONMENT Azure

REMEDIATION STEPS

1. Escalate the alert to the information security team.
2. Review the remediation steps of each one of the alerts

Alerts included in this incident

DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
Successful RDP brute force attack	1	01/04/18, 4:20 AM	ContosoWebFE1	<span style="color: red;">!</span> High
Suspicious SVCHOST process executed	1	01/04/18, 5:19 AM	ContosoWebFE1	<span style="color: blue;">i</span> Low
Multiple Domain Accounts Queried	1	01/04/18, 5:21 AM	ContosoWebFE1	<span style="color: blue;">i</span> Low

[Continue investigation](#)

From here, you can see the list of alerts that the incident holds. You request more information about a specific alert by selecting one.

**Successful RDP brute force attack**  
ContosoWebFE1

[Learn more](#)

### General information

Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.

DESCRIPTION	Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.
DETECTION TIME	Thursday, January 4, 2018, 4:20:00 AM
SEVERITY	<span style="color: red;">!</span> High
STATE	Active
ATTACKED RESOURCE	ContosoWebFE1
SUBSCRIPTION	<Subscription ID>
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
TIMEGENERATEDOFFSETMIN	30
SOURCE	FreeRDP (96.81.218.10)
SUCCESSFUL LOGINS	1
ATTACK DURATION	30 minutes
FAILED ATTEMPTS	60
NON-EXISTENT USERS	20
EXISTING USERS	1
REPORTS	<a href="#">Report: RDP Brute Forcing</a>
END TIME UTC	1/4/2018 1:21:00 PM

### Remediation steps

[Continue investigation](#) [Run playbooks](#)

You can then choose to run your configured playbooks against your alert.

You can further investigate the alert by using the **Continue investigation** option. An investigation map shows all of the entities that are related to this alert.

The screenshot shows the Investigation Dashboard (Preview) interface. On the left, there's a navigation bar with icons for Home, Dashboards, Reports, and Help. Below it is a search bar with placeholder text 'Search' and a date range selector '10/13/2017 4:57 PM — 11/6/2017 3:57 PM (24 days)'. A sidebar on the right contains links for Entities, Search, Exploration, Playbooks, Comments, and Audit.

The main area displays an investigation path starting with 'Security incident detected'. This leads to 'Successful RDP brute force ...' and then 'Multiple Domain Accounts Qu...'. A zoomed-in view of the central node shows three associated entities: 'Suspicious SVCHOST process', 'Successful RDP brute force ...', and 'Multiple Domain Accounts Qu...'. Each entity has a small circular icon with a red exclamation mark.

On the right side, there's a detailed panel for the 'Security incident detected' entity. It includes sections for 'General Information' (Description: 'The alert has no log data in this time interval', Alert ID: '2518942547722139231\_77a4630c-bebe-4957-ada1-5920e3a3f1b8', Time Generated: '10/15/2017 2:25:41:000 AM'), 'Remediation Steps' (empty), and 'Unrelated TO INCIDENT' (High PRIORITY).

You request more information about a specific entity in the map by selecting it. Entities include devices or even users. The map expands with new entities, and properties for the selected entity are displayed on the right. Use this information to better understand a particular path that an attack might have taken.

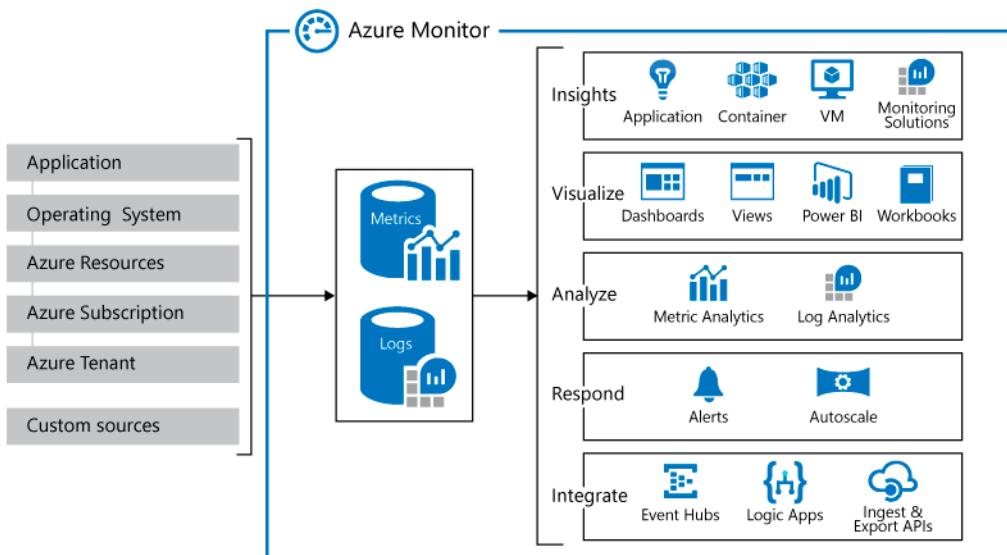
# Azure Monitor

## 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.



## Key Capabilities

- **Monitor and visualize metrics.** Metrics are numerical values available from Azure resources helping you understand the health, operation and performance of your system.
- **Query and analyze logs.** Logs are activity logs, diagnostic logs, and telemetry from monitoring solutions; analytics queries help with troubleshooting and visualizations.
- **Setup alerts and actions.** Alerts notify you of critical conditions and potentially take automated corrective actions based on triggers from metrics or logs.

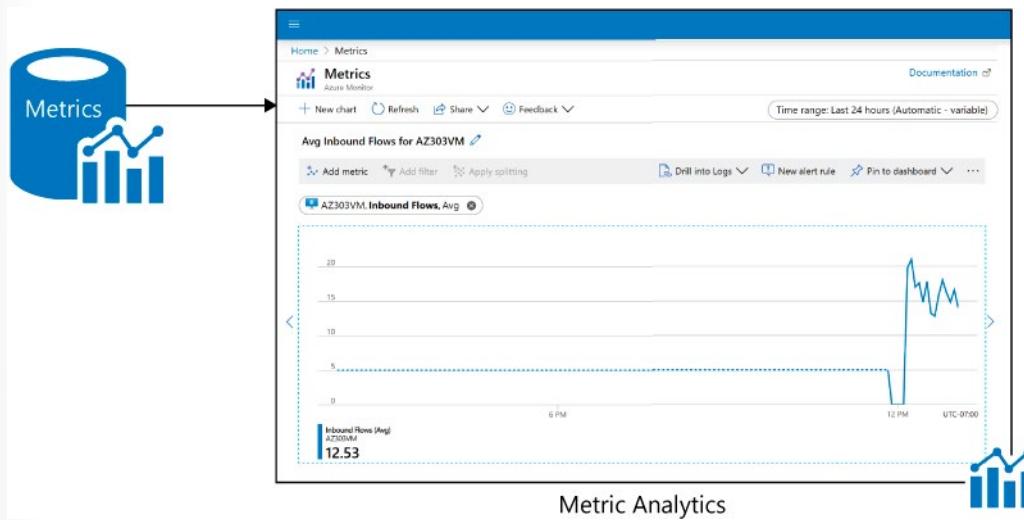


## Monitoring Data Platform

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

- **Metrics** are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios.
- **Logs** contain different kinds of data organized into records with different sets of properties for each type. 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**<sup>2</sup> to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using the Log

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

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

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<sup>3</sup>** query language that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics. You can quickly learn the query language using multiple lessons. Particular guidance is provided to users who are already familiar with SQL and Splunk.

Operation name	Status	Time	Time stamp	Subscription
> Create Deployment	Succeeded	2 minutes a...	Fri May 01 2...	Azure Pass - Sponsorship
> Validate Deployment	Succeeded	3 minutes a...	Fri May 01 2...	Azure Pass - Sponsorship
> RegisterSubscription	Succeeded	3 minutes a...	Fri May 01 2...	Azure Pass - Sponsorship
> Validate Deployment	Succeeded	3 minutes a...	Fri May 01 2...	Azure Pass - Sponsorship
> RegisterSubscription	Succeeded	3 minutes a...	Fri May 01 2...	Azure Pass - Sponsorship
> Create Vault	Succeeded	37 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship
> Validate Features	Succeeded	47 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship
> Validate Features	Succeeded	47 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship
> Export template for deployment	Succeeded	47 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship
> Validate Deployment	Succeeded	48 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship
> Check Resource Name Availability Action	Succeeded	48 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship
> Check Resource Name Availability Action	Succeeded	48 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship
> Register Subscription for Migrate	Succeeded	53 minutes ...	Fri May 01 2...	Azure Pass - Sponsorship

Log analytics

## 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.

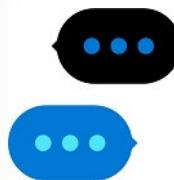
As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data. Activity Logs record when resources are created or modified. Metrics tell you how the resource is performing and the resources that it's consuming.

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.

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/kusto/query/>

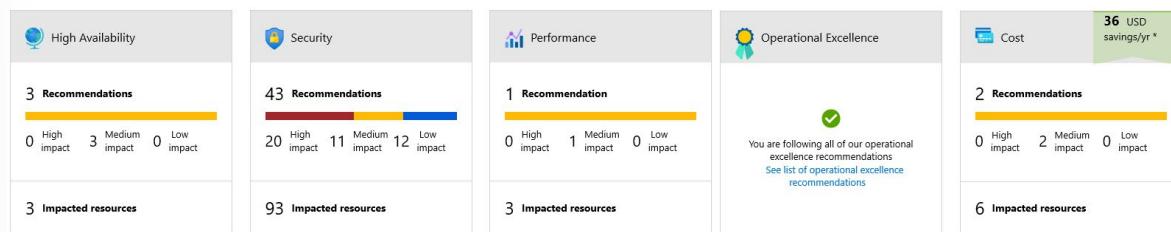
- ✓ Azure Monitor can collect log data from any REST client using the Data Collector API. This allows you to create custom monitoring scenarios and extend monitoring to resources that don't expose telemetry through other sources.

## Azure Advisor



Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.

The Advisor cost recommendations page helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources.



Select the recommended action for a recommendation to implement the recommendation. A simple interface will open that enables you to implement the recommendation or refer you to documentation that assists you with implementation.

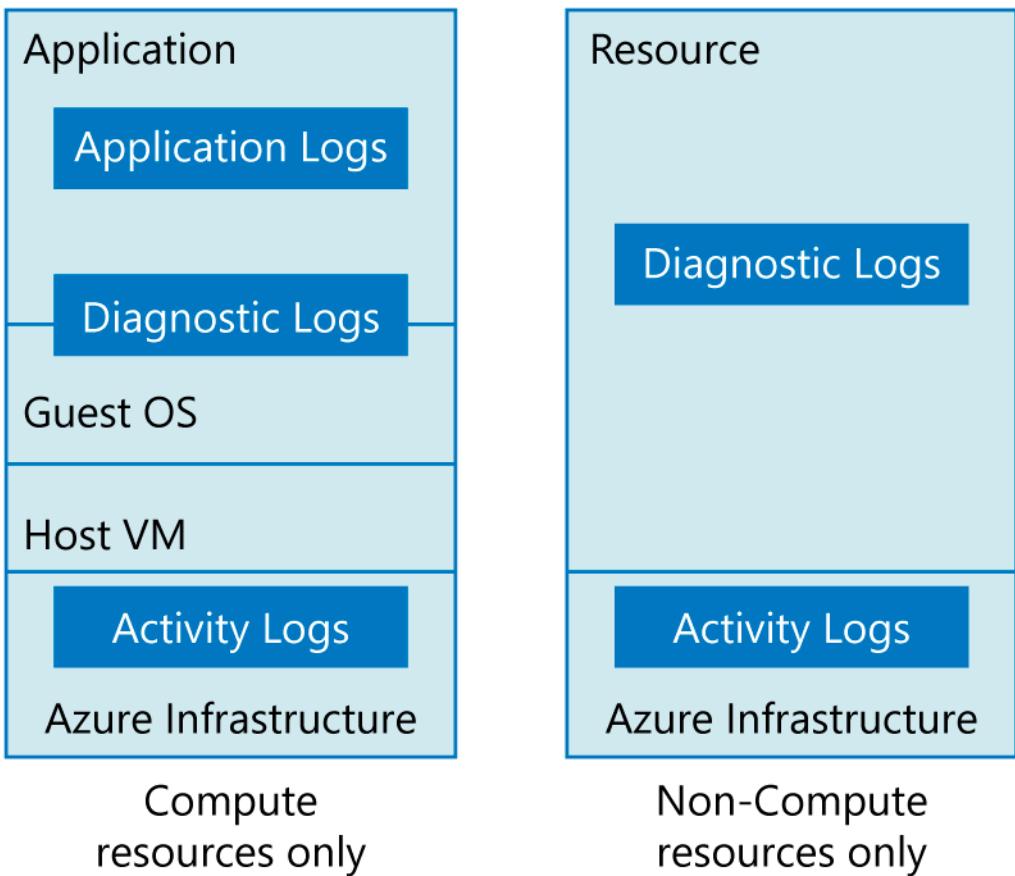
- ✓ Advisor provides recommendations for virtual machines, availability sets, application gateways, App Services, SQL servers, and Redis Cache.

## Activity Log

The Azure Activity Log is a subscription log that provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.

With the Activity Log, you can determine the 'what, who, and when' for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. You can also understand the status of the operation and other relevant properties. Through activity logs, you can determine:

- What operations were taken on the resources in your subscription.
- Who started the operation.
- When the operation occurred.
- The status of the operation.
- The values of other properties that might help you research the operation.



- ✓ Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past. You can retrieve events from your Activity Log using the Azure portal, CLI, PowerShell cmdlets, and Azure Monitor REST API.

## Query the Activity Log

The screenshot shows the Microsoft Azure Activity log interface. At the top, there's a navigation bar with "Microsoft Azure" and a search bar. Below it, the page title is "Activity log". A toolbar includes "Edit columns", "Refresh", "Diagnostics settings", "Download as CSV", "Logs", "Pin current filters", and "Reset filters". At the bottom, there are filters for "Subscription", "Timespan", "Event severity", and a "Add Filter" button.

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

- **Subscription.** One or more Azure subscription names.
- **Timespan.** The start and end time for events.
- **Event Severity.** The severity level of the event (Informational, Warning, Error, Critical).
- **Resource group.** One or more resource groups within those subscriptions.
- **Resource (name).** The name of a specific resource.

- **Resource type.** The type of resource, for example, Microsoft.Compute/virtualmachines.
- **Operation name.** The name of an Azure Resource Manager operation, for example, Microsoft.SQL/servers/Write.
- **Event initiated by.** The 'caller,' or user who performed the operation.
- **Search.** This is an open text search box that searches for that string across all fields in all events.

## Event categories

- **Administrative.** This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would observe in this category include "create virtual machine" and "delete network security group". The Administrative category also includes any changes to role-based access control in a subscription.
  - **Service Health.** This category contains the record of any service health incidents that have occurred in Azure. An example of the type of event you would observe in this category is "SQL Azure in East US is experiencing downtime." Service health events come in five varieties: Action Required, Assisted Recovery, Incident, Maintenance, Information, or Security.
  - **Resource Health.** This category contains the record of any resource health events that have occurred to your Azure resources. An example of the type of event you would see in this category is "Virtual Machine health status changed to unavailable." Resource health events can represent one of four health statuses: Available, Unavailable, Degraded, and Unknown.
  - **Alert.** This category contains the record of all activations of Azure alerts. An example of the type of event you would observe in this category is "CPU % on myVM has been over 80 for the past 5 minutes."
  - **Autoscale.** This category contains the record of any events related to the operation of the autoscale engine based on any autoscale settings you have defined in your subscription. An example of the type of event you would observe in this category is "Autoscale scale up action failed."
  - **Recommendation.** This category contains recommendation events from certain resource types, such as web sites and SQL servers. These events offer recommendations for how to better utilize your resources.
  - **Security.** This category contains the record of any alerts generated by Azure Security Center. An example of the type of event you would observe in this category is "Suspicious double extension file executed."
  - **Policy.** This category contains records of all effect action operations performed by Azure Policy. Examples of the types of events you would see in this category include Audit and Deny.
- ✓ Once you have defined a set of filters, you can pin the filtered state to the dashboard or download the search results as a CSV file.

# Azure Alerts

## Azure Monitor Alerts

### Alerts

The screenshot shows the Azure Monitor Alerts dashboard. At the top, there are links for 'New alert rule', 'Manage alert rules', 'Manage actions', 'View classic alerts', 'Refresh', and 'Provide feedback'. Below this, key metrics are displayed: Total alerts (1179), Smart groups (3), Total alert rules (9), and Action rules (0). A chart shows a 99.75% reduction in alerts since 2/11/2020. A table below details alert counts by severity: Sev 0 (0), Sev 1 (0), Sev 2 (0), Sev 3 (1178), and Sev 4 (1).

Severity	Total Alerts	New	Acknowledged	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0
Sev 2	0	0	0	0
Sev 3	1178	1178	0	0
Sev 4	1	1	0	0

The Monitor Alerts experience has many benefits.

- **Better notification system.** All newer alerts use action groups, which are named groups of notifications and actions that can be reused in multiple alerts.
- **A unified authoring experience.** All alert creation for metrics, logs and activity log across Azure Monitor, Log Analytics, and Application Insights is in one place.
- **View Log Analytics alerts in Azure portal.** You can now also observe Log Analytics alerts in your subscription. Previously these were in a separate portal.
- **Separation of Fired Alerts and Alert Rules.** Alert Rules (the definition of the condition that triggers an alert), and Fired Alerts (an instance of the alert rule firing) are differentiated, so the operational and configuration views are separated.
- **Better workflow.** The new alerts authoring experience guides the user along the process of configuring an alert rule, which makes it simpler to discover the right things to get alerted on.

## Managing Alerts

You can alert on metrics and logs as described in monitoring data sources. These include but are not limited to:

- Metric values
- Log search queries
- Activity Log events
- Health of the underlying Azure platform
- Tests for web site availability

## Alert states

You can set the state of an alert to specify where it is in the resolution process. When the criteria specified in the alert rule is met, an alert is created or fired, it has a status of **New**. You can change the status when you acknowledge an alert and when you close it. All state changes are stored in the history of the alert. The following alert states are supported.

State	Description
<b>New</b>	The issue has just been detected and has not yet been reviewed.
<b>Acknowledged</b>	An administrator has reviewed the alert and started working on it.
<b>Closed</b>	The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state.

✓ 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.

For more information, [The new alerts experience in Azure Monitor](#)<sup>4</sup>

## Creating Alert Rules

Alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues before the users of your system notice them. Alerts consists of alert rules, action groups, and monitor conditions.

Create rule

Rules management

**\* RESOURCE**

Select the target(s) that you wish to monitor

Select

**\* CONDITION**

No condition defined, click on 'Add condition' to select a signal and define its logic

Add condition

**ACTION GROUPS**

Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more [here](#)

ACTION GROUP NAME	ACTION GROUP TYPE
No action group selected	

Select existing      Create New

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-unified-alerts>

Alert rules are separated from alerts and the actions that are taken when an alert fires. The alert rule captures the target and criteria for alerting. The alert rule can be in an enabled or a disabled state. Alerts only fire when enabled. The key attributes of an alert rule are:

- **Target Resource** – Defines the scope and signals available for alerting. A target can be any Azure resource. Example targets: a virtual machine, a storage account, a virtual machine scale set, a Log Analytics workspace, or an Application Insights resource. For certain resources (like Virtual Machines), you can specify multiple resources as the target of the alert rule.
- **Signal** – Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.
- **Criteria** – Criteria is a combination of Signal and Logic applied on a Target resource. Examples: \* Percentage CPU > 70%; Server Response Time > 4 ms; and Result count of a log query > 100.
- **Alert Name** – A specific name for the alert rule configured by the user.
- **Alert Description** – A description for the alert rule configured by the user.
- **Severity** – The severity of the alert once the criteria specified in the alert rule is met. Severity can range from 0 to 4.
- **Action** – A specific action taken when the alert is fired. Tje Action Groups topic is coming up.

## Action Groups

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered. Various alerts may use the same action group or different action groups depending on the user's requirements.

When an action is configured to notify a person by email or SMS the person will receive a confirmation indicating they have been added to the action group.

Add action group

Action group name \* ⓘ  
Sample action group

Short name \* ⓘ  
SampleAG

Subscription \* ⓘ  
Visual Studio Enterprise

Resource group \* ⓘ  
Default-ActivityLogAlerts (to be created)

Actions

Action name \* Action Type \*

Unique name for the action Select an action type ^

- Automation Runbook
- Azure Function
- Email Azure Resource Manager Role
- Email/SMS/Push/Voice
- ITSM
- LogicApp
- Secure Webhook
- Webhook

- **Automation runbook** - An automation runbook is the ability to define, build, orchestrate, manage, and report on workflows that support system and network operational processes. A runbook workflow can potentially interact with all types of infrastructure elements, such as applications, databases, and hardware.
  - **Azure Function** – Azure functions is a serverless compute service that lets you run event-triggered code without having to explicitly provision or manage infrastructure.
  - **Email Azure Resource Manager role** – Send email to the members of the subscription's role. Email will only be sent to Azure AD user members of the role. Email will not be sent to Azure AD groups or service principals.
  - **Email/SMS/Push/Voice** - Specify any email, SMS, push, or voice actions.
  - **ITSM** – Connect Azure and a supported IT Service Management (ITSM) product/service. This requires an ITSM Connection.
  - **Logic App** – Logic apps connect your business-critical apps and services by automating your workflows.
  - **Webhook** – A webhook is a HTTP endpoint that allows external applications to communicate with your system.
- ✓ Always check the documentation for the number of actions you can create.

## Demonstration - Alerts

In this demonstration, we will create an alert rule.

### Create an alert rule

1. In Azure portal, click on **Monitor**. The Monitor blade consolidates all your monitoring settings and data in one view.

2. Click **Alerts** then click **+ New alert rule**. As most resource blades also have Alerts in their resource menu under Monitoring, you could create alerts from there as well.

#### Explore alert targets

1. Click **Select** under Target, to select a target resource that you want to alert on. Use **Subscription** and **Resource type** drop-downs to find the resource you want to monitor. You can also use the search bar to find your resource.
2. If the selected resource has metrics you can create alerts on, Available signals on the bottom right will include metrics. You can view the full list of resource types supported for metric alerts in this article.
3. Click **Done** when you have made your selection.

#### Explore alert conditions

1. Once you have selected a target resource, click on **Add condition**.
2. You will observe a list of signals supported for the resource, select the metric you want to create an alert on.
3. Optionally, refine the metric by adjusting Period and Aggregation. If the metric has dimensions, the Dimensions table will be presented.
4. Observe a chart for the metric for the last 6 hours. Adjust the **Show history** drop-down.
5. Define the **Alert logic**. This will determine the logic which the metric alert rule will evaluate.
6. If you are using a static threshold, the metric chart can help determine what might be a reasonable threshold. If you are using a Dynamic Thresholds, the metric chart will display the calculated thresholds based on recent data.
7. Click **Done**.
8. Optionally, add another criteria if you want to monitor a complex alert rule.

#### Explore alert details

1. Fill in Alert details like **Alert Rule Name**, **Description** and **Severity**.
2. Add an action group to the alert either by selecting an existing action group or creating a new action group.
3. Click **Done** to save the metric alert rule.

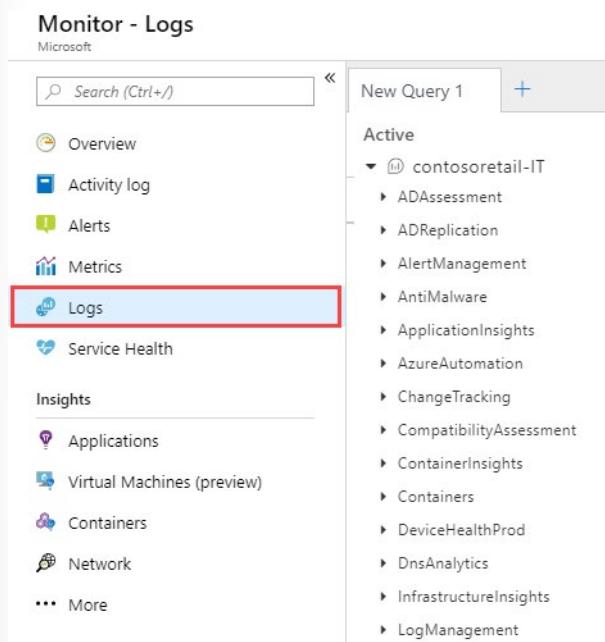
## Log Analytics

### Log Analytics

Log Analytics is a service in that helps you collect and analyze data generated by resources in your cloud and on-premises environments.

Log queries helps you to fully leverage the value of the data collected in Azure Monitor Logs. A powerful query language allows you to join data from multiple tables, aggregate large sets of data, and perform complex operations with minimal code. Virtually any question can be answered and analysis performed as long as the supporting data has been collected, and you understand how to construct the right query.

Some features in Azure Monitor such as insights and solutions process log data without exposing you to the underlying queries. To fully leverage other features of Azure Monitor, you should understand how queries are constructed and how you can use them to interactively analyze data in Azure Monitor Logs.



The screenshot shows the Azure Monitor - Logs interface. On the left, there's a navigation sidebar with icons for Overview, Activity log, Alerts, Metrics, and Logs (which is highlighted with a red box). Below that are sections for Insights, Applications, Virtual Machines (preview), Containers, Network, and More. The main area is titled 'New Query 1' and shows a tree view of log sources under 'Active'. One source, 'contosoretail-IT', is expanded, showing its sub-components: ADAssessment, ADReplication, AlertManagement, AntiMalware, ApplicationInsights, AzureAutomation, ChangeTracking, CompatibilityAssessment, ContainerInsights, Containers, DeviceHealthProd, DnsAnalytics, InfrastructureInsights, and LogManagement.

### Example 1 - Assessing updates

An important part of the daily routine for any IT administrator is assessing systems update requirements and planning patches. Accurate scheduling is critical, as it directly relates to SLAs to the business and can seriously impact business functions. In the past, you had to schedule an update with only limited knowledge of how long the patching would take. Operations Management Suite collects data from all customers performing patches and uses that data to provide an average patching time for specific missing updates. This use of "crowd-sourced" data is unique to cloud systems, and is a great example of how Log Analytics can help meet strict SLAs.

### Example 2 - Change tracking

Troubleshooting an operational incident is a complex process, requiring access to multiple data streams. With Operations Management Suite, you can easily perform analysis from multiple angles, using data from a wide variety of sources through a single interface for correlation of information. By tracking changes throughout the environment, Log Analytics helps to easily identify things like abnormal behavior

from a specific account, users installing unapproved software, unexpected system reboots or shutdowns, evidence of security breaches, or specific problems in loosely coupled applications.

## Create a Workspace

To get started with Log Analytics you need to add a workspace.

**Log Analytics workspace**  
Create new or link existing workspace

---

Create New  Link Existing

Log Analytics Workspace \* ⓘ  
enter workspace name

Subscription \*  
Azure Pass - Sponsorship

Resource group \*  
Select existing...  
Create new

Location \*  
West US

- Provide a name for the new Log Analytics workspace.
- Select a Subscription from the drop-down list.
- For Resource Group, select an existing resource group that contains one or more Azure virtual machines.
- Select the Location your VMs are deployed to.
- The workspace will automatically use the Per GB pricing plan.

## Connected Sources

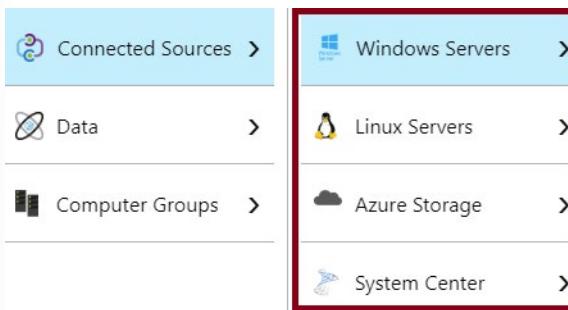
Connected Sources are the computers and other resources that generate data collected by Log Analytics. This can include agents installed on **Windows<sup>5</sup>** and **Linux<sup>6</sup>** computers that connect directly or agents in connected **System Center Operations Manager management group<sup>7</sup>**. Log Analytics can also collect data from **Azure storage<sup>8</sup>**.

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

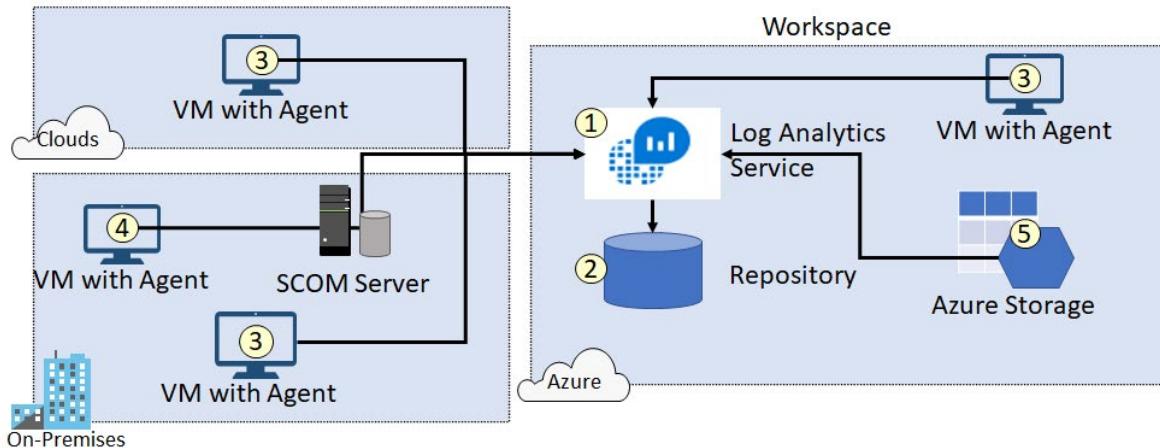
<sup>6</sup> <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-linux-agents>

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

<sup>8</sup> <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.

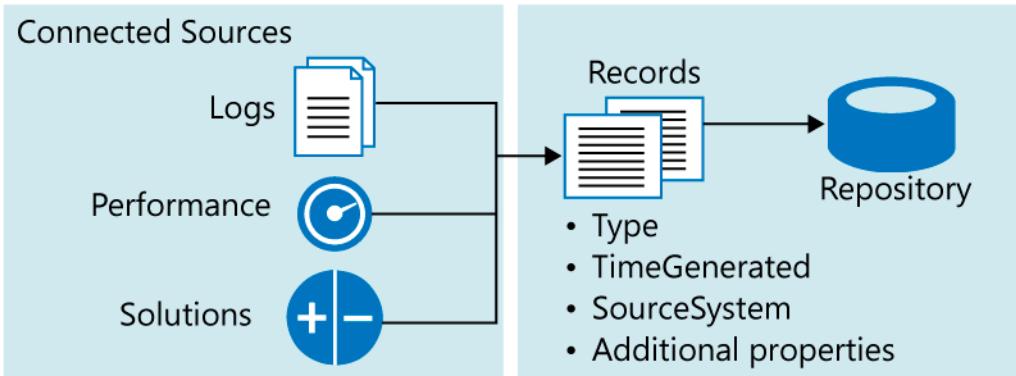


Ensure you can locate each of the following.

- The Log Analytics service (1) collects data and stores it in the repository (2). The repository is hosted in Azure. Connected Sources provide information to the Log Analytics service.
- Computer agents (3) generate data to the Log Analytics service. These agents can run on Windows or Linux computers, virtual or physical computers, on-premises or cloud computers, and Azure or other cloud providers.
- A System Center Operations Manager (SCOM) management group can be connected to Log Analytics. SCOM agents (4) communicate with management servers which forward events and performance data to Log Analytics.
- An Azure storage account (5) can also collect Azure Diagnostics data from a worker role, web role, or virtual machine in Azure. This information can be sent to the Log Analytics service.

## Data Sources

Data sources are the different kinds of data collected from each connected source. These can include events and performance data from Windows and Linux agents, in addition to sources such as IIS logs and custom text logs. You configure each data source that you want to collect, and the configuration is automatically delivered to each connected source.



When you configure the Log Analytics settings the available data sources are shown. Data sources include: Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog. Each data source has additional configuration options. For example, the Windows Event Log can be configured to forward Error, Warning, or Informational messages.

Overview > Settings

### Data Sources

- Solutions
- Connected Sources
- Data**
- Computer Groups
- Accounts
- Alerts
- Preview Features

Collect events from the following event logs

LOG NAME	ERROR	WARNING	INFORMATION	Remove
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Remove
Operations Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Remove
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Remove

## Log Analytics Querying

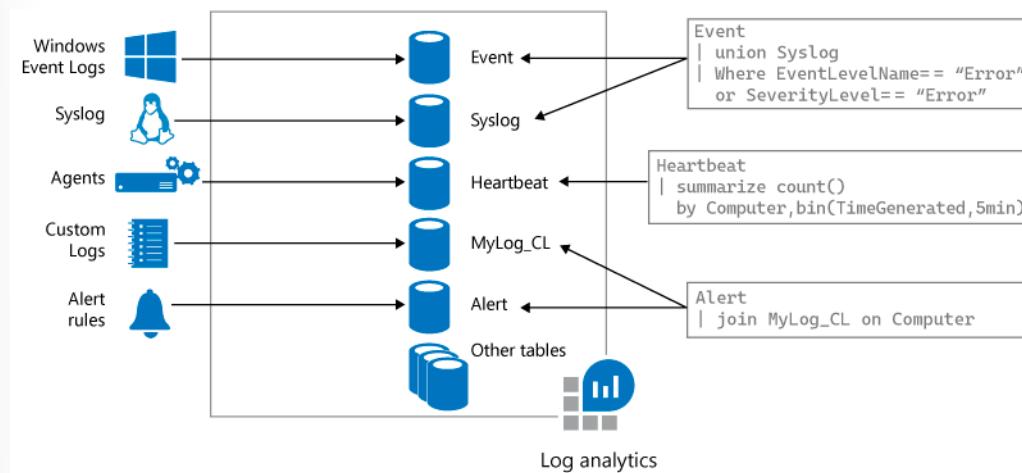
Log Analytics provides a query syntax to quickly retrieve and consolidate data in the repository. You can create and save Log Searches to directly analyze data in the portal or have log searches run automatically to create an alert if the results of the query indicate an important condition.



To give a quick graphical view of the health of your overall environment, you can add visualizations for saved log searches to your dashboard. To analyze data outside of Log Analytics, you can export the data from the repository into tools such as Power BI or Excel. You can also leverage the Log Search API to build custom solutions that leverage Log Analytics data or to integrate with other systems.

## Query Language Syntax

When you build a query, you start by determining which tables have the data that you're looking for. Each data source and solution stores its data in dedicated tables in the Log Analytics workspace. Documentation for each data source and solution includes the name of the data type that it creates and a description of each of its properties. Many queries will only require data from a single table, but others may use a variety of options to include data from multiple tables.



Some common query tables are: Event, Syslog, Heartbeat, and Alert.

The basic structure of a query is a source table followed by a series of operators separated by a pipe character |. You can chain together multiple operators to refine the data and perform advanced functions. For example, this query returns a count of the top 10 errors in the Event log during the last day. The results are in descending order.

```
Event
| where (EventLevelName == "Error")
| where (TimeGenerated > ago(1days))
| summarize ErrorCount = count() by Computer
| top 10 by ErrorCount desc
```

Some common operators are:

- **count** - Returns the number of records in the input record set.

```
StormEvents | count
```

- **limit** - Return up to the specified number of rows.

```
T | limit 5
```

- **summarize** - Produces a table that aggregates the content of the input table.

```
T | summarize count(), avg(price) by fruit, supplier
```

- **top** - Returns the first N records sorted by the specified columns.

```
T | top 5 by Name desc nulls last
```

- **where** - Filters a table to the subset of rows that satisfy a predicate.

```
T | where fruit=="apple"
```

For more information, [Azure Monitor log queries<sup>9</sup>](#)

<sup>9</sup> <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/query-language>

# Network Watcher

## Network Watcher

**Network Watcher** provides tools to **monitor**, **diagnose**, view **metrics**, and enable or disable **logs** for resources in an Azure virtual network. Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level.

- **Automate remote network monitoring with packet capture.** Monitor and diagnose networking issues without logging in to your virtual machines (VMs) using Network Watcher. Trigger packet capture by setting alerts, and gain access to real-time performance information at the packet level. When you observe an issue, you can investigate in detail for better diagnoses.
- **Gain insight into your network traffic using flow logs.** Build a deeper understanding of your network traffic pattern using Network Security Group flow logs. Information provided by flow logs helps you gather data for compliance, auditing and monitoring your network security profile.
- **Diagnose VPN connectivity issues.** Network Watcher provides you the ability to diagnose your most common VPN Gateway and Connections issues. Allowing you, not only, to identify the issue but also to use the detailed logs created to help further investigate.

### Connection monitor

Connection monitor is a feature of Network Watcher that can monitor communication between a virtual machine and an endpoint. The connection monitor capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint.

For example, you might have a web server VM that communicates with a database server VM. Someone in your organization may, unknown to you, apply a custom route or network security rule to the web server or database server VM or subnet.

If an endpoint becomes unreachable, connection troubleshoot informs you of the reason. Potential reasons might be DNS name resolution problem, the CPU, memory, or firewall within the operating system of a VM, or the hop type of a custom route, or security rule for the VM or subnet of the outbound connection. Connection monitor also provides the minimum, average, and maximum latency observed over time.

## Network performance monitor

Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute. Network performance monitor detects network issues like traffic blackholing, routing errors, and issues that conventional network monitoring methods aren't able to detect. The solution generates alerts and notifies you when a threshold is breached for a network link. It also ensures timely detection of network performance issues and localizes the source of the problem to a particular network segment or device.

- ✓ To use Network Watcher capabilities, the account you log into Azure with, must be assigned to the Owner, Contributor, or Network contributor built-in roles, or assigned to a custom role. A custom role can be given permissions to read, write, and delete the Network Watcher.

For more information, **Network Watcher**<sup>10</sup>

<sup>10</sup> <https://azure.microsoft.com/en-us/services/network-watcher/>

# Network Watcher Diagnostics

≡ Microsoft Azure

Home > Network Watcher

## Network Watcher

Microsoft

Search (Ctrl+/)

Overview

### Monitoring

- Topology
- Connection monitor
- Connection monitor (Preview)
- Network Performance Monitor

### Network diagnostic tools

- IP flow verify
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

### Metrics

- Usage + quotas

### Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

**Verify IP Flow:** Quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment. For example, confirming if a security rule is blocking ingress or egress traffic to or from a virtual machine. IP flow verify is ideal for making sure security rules are being correctly applied. When used for troubleshooting, if IP flow verify doesn't show a problem, you will need to explore other areas such as firewall restrictions.

**Next Hop:** To determine if traffic is being directed to the intended destination by showing the next hop. This will help determine if networking routing is correctly configured. Next hop also returns the route table associated with the next hop. If the route is defined as a user-defined route, that route is returned. Otherwise, next hop returns System Route. Depending on your situation the next hop could be Internet, Virtual Appliance, Virtual Network Gateway, VNet Local, VNet Peering, or None. None lets you know that while there may be a valid system route to the destination, there is no next hop to route the traffic to the destination. When you create a virtual network, Azure creates several default outbound routes for network traffic. The outbound traffic from all resources, such as VMs, deployed in a virtual network, are routed based on Azure's default routes. You might override Azure's default routes or create additional routes.

**VPN Diagnostics:** Troubleshoot gateways and connections. VPN Diagnostics returns a wealth of information. Summary information is available in the portal and more detailed information is provided in log files. The log files are stored in a storage account and include things like connection statistics, CPU and memory information, IKE security errors, packet drops, and buffers and events.

**NSG Flow Logs:** NSG Flow Logs maps IP traffic through a network security group. These capabilities can be used in security compliance and auditing. You can define a prescriptive set of security rules as a model for security governance in your organization. A periodic compliance audit can be implemented in a programmatic way by comparing the prescriptive rules with the effective rules for each of the VMs in your network.

**Connection Troubleshoot.** Azure Network Watcher Connection Troubleshoot is a more recent addition to the Network Watcher suite of networking tools and capabilities. Connection Troubleshoot enables you to troubleshoot network performance and connectivity issues in Azure.

## Diagnostics - IP Flow Verify

**Verify IP Flow Purpose:** Quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment. For example, confirming if a security rule is blocking ingress or egress traffic to or from a virtual machine.

### Example

When you deploy a VM, Azure applies several default security rules to the VM that allow or deny traffic to or from the VM. You might override Azure's default rules or create additional rules. At some point, a VM may become unable to communicate with other resources, because of a security rule.

The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which security rule allowed or denied the communication, so that you can resolve the problem.

The screenshot shows the Azure Network Watcher interface for IP flow verify. On the left, there's a sidebar with various diagnostic tools like IP flow verify, Next hop, Effective security rules, VPN troubleshoot, Packet capture, Connection troubleshoot, Metrics, Usage + quotas, Logs, NSG flow logs, Diagnostic logs, and Traffic Analytics. The 'IP flow verify' option is currently selected. The main panel is titled 'Packet details' and contains fields for 'Protocol' (set to TCP), 'Direction' (set to Inbound), 'Local IP address' (10.1.1.4), 'Local port' (3389), 'Remote IP address' (13.24.35.46), and 'Remote port' (3389). A 'Check' button is at the bottom. The results section shows a red 'Access denied' message with a note about the security rule 'DenyAllInBound'.

- ✓ IP flow verify is ideal for making sure security rules are being correctly applied. When used for troubleshooting, if IP flow verify doesn't show a problem, you will need to explore other areas such as firewall restrictions.

## Diagnostics - Next Hop

**Next Hop Purpose:** To determine if traffic is being directed to the intended destination by showing the next hop. This will help determine if networking routing is correctly configured.

When you create a virtual network, Azure creates several default outbound routes for network traffic. The outbound traffic from all resources, such as VMs, deployed in a virtual network, are routed based on Azure's default routes. You might override Azure's default routes or create additional routes.

### Example

You may find that a VM can no longer communicate with other resources because of a specific route. The next hop capability enables you to specify a source and destination IPv4 address. Next hop then tests the communication and informs you what type of next hop is used to route the traffic. You can then remove, change, or add a route, to resolve a routing problem.

Subscription \* ⓘ  
MSDN Platforms Subscription

Resource group \* ⓘ  
Demo

Virtual machine \* ⓘ  
vm01

Network interface \*

Source IP address \* ⓘ  
10.1.1.4

Destination IP address \* ⓘ  
13.24.35.46

**Next hop**

Result  
Next hop type  
**None**

IP address  
**10.1.1.100**

Route table ID  
</subscriptions/2301e3a0-8420-...>

Next hop also returns the route table associated with the next hop. If the route is defined as a user-defined route, that route is returned. Otherwise, next hop returns System Route. Depending on your situation the next hop could be Internet, Virtual Appliance, Virtual Network Gateway, VNet Local, VNet Peering, or None. None lets you know that while there may be a valid system route to the destination, there is no next hop to route the traffic to the destination.

## Diagnostics - Effective Security Rules

If you have several NSGs and are not sure which security rules are being applied, you can examine the Effective security rules.

nsg01												
Inbound rules												
Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access ↑↓
RDP_Inbound	100			13.23.34.45/32	0-65535		0.0.0.0/0	3389-3389		TCP	Allow	
AllowVnetInBound	65000			Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All	Allow	
AllowAzureLoadBalancerInBound	65001			Azure load balancer (2 prefixes)	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All	Allow	
DenyAllInBound	65500			0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All	Deny	
Outbound rules												
Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access ↑↓
AllowVnetOutBound	65000			Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All	Allow	
AllowInternetOutBound	65001			0.0.0.0/0,0.0.0.0/0	0-65535		Internet (216 prefixes)	0-65535		All	Allow	
DenyAllOutBound	65500			0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All	Deny	

- Priority.** A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

- **Source.** Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group. Specifying a range, a service tag, or application security group, enables you to create fewer security rules.
- **Protocol.** TCP, UDP, ICMP or Any.
- **Action.** Allow or deny.

## Diagnostics - VPN Troubleshoot

**VPN Troubleshoot Purpose:** Troubleshoot gateways and connections.

### Example

Virtual Network Gateways provide connectivity between on-premises resources and other virtual networks within Azure. Monitoring gateways and their connections are critical to ensuring communication is working as expected. VPN diagnostics can troubleshoot the health of the gateway, or connection, and provide detailed logging. The request is a long running transaction and results are returned once the diagnosis is complete.

Name	Troubleshooting s...	Resource status	Resource Group	Location
vng01	Running	Succeeded	Demo	East US
cn01	-	Succeeded	Demo	East US

VPN Troubleshoot returns a wealth of information. Summary information is available in the portal and more detailed information is provided in log files. The log files are stored in a storage account and include things like connection statistics, CPU and memory information, IKE security errors, packet drops, and buffers and events.

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

## Diagnostics - Packet Capture

Add packet capture

Subscription \*

MSDN Platforms Subscription

Resource group \*

Demo

Target virtual machine \*

vm01

Packet capture name \*

capture01

Capture configuration

The packet capture output file (.cap) can be stored in a storage account and/or on the target VM.

Storage account  File  Both

Storage accounts \*

samcteusvmdiagnostic

Maximum bytes per packet ⓘ

default: 0 (entire packet)

Maximum bytes per session ⓘ

default: 1073741824

Time limit (seconds) ⓘ

default: 18000

+ Add filter

Network Watcher packet capture allows you to create capture sessions to track traffic to and from a virtual machine. Filters are provided for the capture session to ensure you capture only the traffic you want. Packet capture helps to diagnose network anomalies, both reactively, and proactively. Other uses include gathering network statistics, gaining information on network intrusions, to debug client-server communication, and much more. Being able to remotely trigger packet captures, eases the burden of running a packet capture manually on a desired virtual machine, which saves valuable time.

## Diagnostics - Connection Troubleshoot

The connection troubleshoot feature of Network Watcher provides the capability to check a direct TCP connection from a virtual machine to a virtual machine (VM), fully qualified domain name (FQDN), URI, or IPv4 address. Network scenarios are complex, they are implemented using network security groups, firewalls, user-defined routes, and resources provided by Azure. Complex configurations make troubleshooting connectivity issues challenging. Network Watcher helps reduce the amount of time to find and detect connectivity issues. The results returned can provide insights into whether a connectivity issue is due to a platform or a user configuration issue.

Source  
Subscription \*  MSDN Platforms Subscription  
Resource group \*  Demo  
Source type \*  Virtual machine  
\*Virtual machine  vm01  
Destination  
 Select a virtual machine  Specify manually  
URI, FQDN or IPv4 \*  13.24.35.46  
Probe Settings  
Protocol  TCP  ICMP  
Destination port \*  3389  
Advanced settings  
Source port  3389  
Check

Further examples of different supported network troubleshooting scenarios include:

- Checking the connectivity and latency to a remote endpoint, such as for websites and storage endpoints.
- Connectivity between an Azure VM and an Azure resource like Azure SQL server, where all Azure traffic is tunneled through an on-premises network.
- Connectivity between VMs in different VNets connected using VNet peering.

## Logs - NSG Flow Logs

NSG flow logs allows you to view information about ingress and egress IP traffic through an NSG. Flow logs are written in JSON format and show outbound and inbound flows on a per rule basis. The JSON format can be visually displayed in Power BI or third-party tools like Kibana.

Metrics	Name	Resource type	Resource group	Status	Location
Usage + quotas	nsg01	Network security gro...	Demo	Enabled	East US
Logs	nsg02	Network security gro...	Demo	Enabled	East US
NSG flow logs	nsg03	Network security gro...	Demo	Enabled	East US
Diagnostic logs					

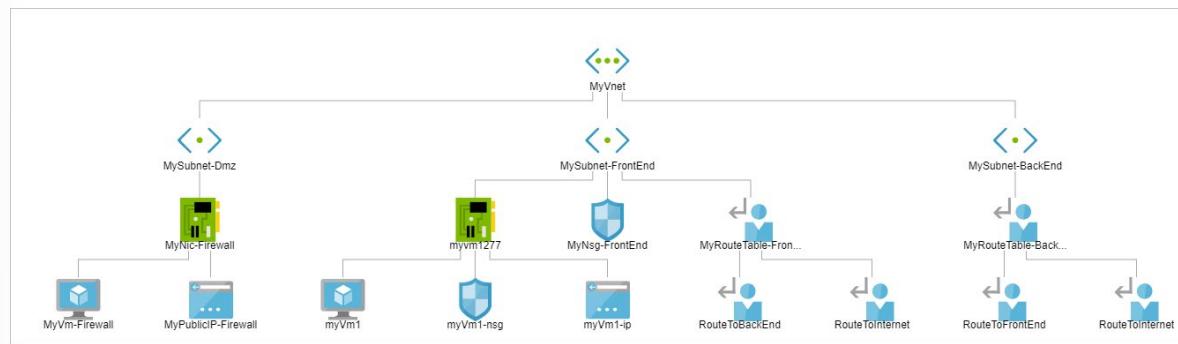
- ✓ This feature now supports (January 2020) firewalled storage accounts and service endpoints for storage.

## Monitoring - Topology

Suppose you have to troubleshoot a virtual network created by your colleagues. Unless you were involved in the creation process of the network, you might not know about all the aspects of the infrastruc-

ture. You can use the topology tool to visualize and understand the infrastructure you're dealing with before you start troubleshooting.

Network Watcher's Topology capability enables you to generate a visual diagram of the resources in a virtual network, and the relationships between the resources. The following picture shows an example topology diagram for a virtual network that has three subnets, two VMs, network interfaces, public IP addresses, network security groups, route tables, and the relationships between the resources:



The topology tool generates a graphical display of your Azure virtual network, its resources, its interconnections, and their relationships with each other.

- ✓ To generate the topology, you need a Network Watcher instance in the same region as the virtual network.

# Azure Service Health

## Azure Service Health



Azure offers a suite of experiences to keep you informed about the health of your cloud resources. This information includes current and upcoming issues such as service impacting events, planned maintenance, and other changes that may affect your availability.

Azure Service Health is a combination of three separate smaller services.

**Azure status** informs you of service outages in Azure on the Azure Status page. The page is a global view of the health of all Azure services across all Azure regions. The status page is a good reference for incidents with widespread impact, but we strongly recommend that current Azure users leverage Azure service health to stay informed about Azure incidents and maintenance.

**Azure service health** provides a personalized view of the health of the Azure services and regions you're using. This is the best place to look for service impacting communications about outages, planned maintenance activities, and other health advisories because the authenticated Azure Service Health experience knows which services and resources you currently use. The best way to use Service Health is to set up Service Health alerts to notify you via your preferred communication channels when service issues, planned maintenance, or other changes may affect the Azure services and regions you use.

**Azure resource health** provides information about the health of your individual cloud resources such as a specific virtual machine instance. Using Azure Monitor, you can also configure alerts to notify you of availability changes to your cloud resources. Azure Resource Health along with Azure Monitor notifications will help you stay better informed about the availability of your resources minute by minute and quickly assess whether an issue is due to a problem on your side or related to an Azure platform event.

Together, these experiences provide you with a comprehensive view into the health of Azure, at the granularity that is most relevant to you.

**Note:**

This service supports **Azure delegated resource management**<sup>11</sup>, which lets service providers sign in to their own tenant to manage subscriptions and resource groups that customers have delegated.

## Azure Status Page

Azure status provides you with a global view of the health of Azure services and regions. With Azure status, you can get information on service availability. Azure status is available to everyone to view all services that report their service health, as well as incidents with wide-ranging impact. If you're a current Azure user, however, we strongly encourage you to use the personalized experience in Azure Service Health. Azure Service Health includes all outages, upcoming planned maintenance activities, and service advisories.

<sup>11</sup> <https://docs.microsoft.com/en-us/azure/lighthouse/concepts/azure-delegated-resource-management>

Azure status

Last updated 55 seconds ago

Services are operating normally.

Status history >

Get a personalized view of the health of your Azure services

Go to your personalized dashboard >

Refresh every 2 minutes

Good Warning Error Information

Products and Services	Non-Regional*	East US	East US 2	Central US	North Central US	South Central US	West Central US	West US	West US 2	Canada East	Canada Central	Brazil South
Compute												
Virtual Machines		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SAP HANA on Azure Large Instances		✓						✓				
Cloud Services		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Machine Scale Sets		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Functions		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓

### Azure status updates

The Azure status page gets updated in real time as the health of Azure services change. If you leave the Azure status page open, you can control the rate at which the page refreshes with new data. At the top, you can see the last time the page was updated.

### Azure status history

While the Azure status page always shows the latest health information, you can view older events using the Azure status history page.

## Service Health Walkthrough



Service Health provides you with a customizable dashboard which tracks the health of your Azure services in the regions where you use them. In this dashboard, you can track active events like ongoing service issues, upcoming planned maintenance, or relevant health advisories. When events become inactive, they get placed in your health history for up to 90 days. Finally, you can use the Service Health dashboard to create and manage service health alerts which proactively notify you when service issues are affecting you.

### Service Health Events

Service Health tracks four types of health events that may impact your resources:

- Service issues** - Problems in the Azure services that affect you right now.
- Planned maintenance** - Upcoming maintenance that can affect the availability of your services in the future.
- Health advisories** - Changes in Azure services that require your attention. Examples include deprecation of Azure features or upgrade requirements (e.g upgrade to a supported PHP framework).
- Security advisories** - Security related notifications that may affect the availability of your Azure services.

**✓ Note:**

To view Service Health events, users must be granted the Reader role on a subscription.

### Get started with Service Health

To launch your Service Health dashboard, select the Service Health tile on your portal dashboard. If you have previously removed the tile or you're using custom dashboard, search for Service Health service in "More services" (bottom left on your dashboard).

### See current issues which impact your services

The Service issues view shows any ongoing problems in Azure services that are impacting your resources. You can understand when the issue began, and what services and regions are impacted. You can also read the most recent update to understand what Azure is doing to resolve the issue.

The screenshot shows the Azure Service Health - Service Issues dashboard. On the left, there's a sidebar with navigation links: ACTIVE EVENTS (Service issues, Planned maintenance, Health advisories), HISTORY (Health history), RESOURCE HEALTH (Resource health), and ALERTS (Health alerts). The main area displays a table of active issues. One row is highlighted with a red box:

ISSUE NAME	TRAC...	SERV...	REGIO...	START TIME	UPDATED
Virtual Machines - West US	H97W-2J0	Virtual M...	West US	20:16 UTC, 03/16/2018 (5 h ago)	5 h ago

Below the table, there's a world map with red dots indicating impacted regions. To the right, there's a callout for "Virtual Machines located at West US". At the bottom of the main content area, there's a summary section with a red box around the last paragraph:

Last update (5 h ago)  
Starting at 20:16 UTC on 16 Mar 2018 you have been identified as a customer using Virtual Machines in West US who may intermittently experience higher than expected latency or degraded performance when trying to access or use a subset of Virtual Machines hosted in this region. Engineers are aware of this issue and are actively investigating.  
[See all updates](#)

On the right side of the dashboard, there are several action buttons:

- Download the issue summary as a PDF.
- Track this issue on mobile.
- Quickly connect with our problem-solving experts.
- Contact Azure Support if you need additional help with this issue.

A "Was this helpful?" button is at the bottom right.

Choose the Potential impact tab to see the specific list of resources you own that might be impacted by the issue. You can download a CSV list of these resources to share with your team.

The screenshot shows the Azure Service Health - Service issues page. On the left, there's a sidebar with various monitoring categories like Active Events, History, Resource Health, and Alerts. The main area displays a single service issue for "Virtual Machines - West US" with tracking ID H97W-2J0. The issue was reported at 20:16 UTC on 03/16/2018 and last updated 5 hours ago. A world map indicates the issue is located in West US. A red box highlights the "Issue updates" tab, which shows the resource name "Operations-Splunk-03", resource type "Virtual Machines", resource group "Splunk", and subscription "4970d23e-de7u-rb00-9c19-02a1d...".

### Get links and downloadable explanations

You can get a link for the issue to use in your problem management system. You can download PDF and sometimes CSV files to share with people who don't have access to the Azure portal.

This screenshot shows the same Service Health page as above, but with additional sharing options. A red box highlights the "Issue updates" tab, which now includes a "Tracking Id" field containing "H97W-2J0" and a "Share the below link with your team or use it for reference in your problem management system" button. Another red box highlights a "Download the issue summary as a PDF" button. To the right, there are links for "Track this issue on mobile" (with a QR code), "Quickly connect with our problem-solving experts" (via Twitter @AzureSupport), and "Contact Azure Support if you need additional help with this issue" (with a "Create a support request" link). A "Was this helpful?" button is at the bottom right.

### Get support from Microsoft

Contact support if your resource is left in a bad state even after the issue is resolved. Use the support links on the right of the page.

### Pin a personalized health map to your dashboard

Filter Service Health to show your business-critical subscriptions, regions, and resource types. Save the filter and pin a personalized health world map to your portal dashboard.

The screenshot shows the Azure Service Health - Service issues page. At the top, there is a search bar and a filter bar with dropdowns for Subscription (4 selected), Region (8 selected), and Service (114 selected). A red box highlights the "Pin filtered world map to dashboard" button. Below the filter bar, there is a table with columns: ISSUE NAME, TRAC..., SERVI..., REGIO..., START TIME, and UPDATED. One row is visible: Virtual Machines - West US, H97W-2J0, Virtual M..., West US, 20:16 UTC, 03/16/2018 (5 h ago), 5 h ago. To the right of the table is a world map with a red dot over the West US region, labeled "Virtual Machines located at West US". Below the map, there is a summary section with tabs for Summary, Potential impact, and Issue updates. The Potential impact tab shows "1 Virtual Machines in 1 subscription(s)". On the right side of the page, there are several support links: "Download the issue summary as a PDF.", "Track this issue on mobile.", "Quickly connect with our problem-solving experts. Tweet @AzureSupport.", and "Contact Azure Support if you need additional help with this issue. Create a support request.". At the bottom right, there is a "Was this helpful?" button.

The screenshot shows the Microsoft Azure Dashboard. In the center, there is a pinned card for "Service Health - Service issues OPERATIONS". The card displays a world map with a red dot over the West US region, labeled "West US - Virtual Machines". The card also includes the title "Service Health - Service issues OPERATIONS" and a link to "Windows Virtual Machines". On the left side of the dashboard, there is a sidebar with various service icons and a "Service Health" button. The main dashboard area shows a list of resources under "All resources ALL SUBSCRIPTIONS", including "Operations-01-DB-02" (SQL database) and several storage accounts. There are also sections for "Quickstart tutorials" (Windows Virtual Machines, Linux Virtual Machines, App Service, Functions, SQL Database) and "Help + support".

### Configure service health alerts

Service Health integrates with Azure Monitor to alert you via emails, text messages, and webhook notifications when your business-critical resources are impacted. Set up an activity log alert for the

appropriate service health event. Route that alert to the appropriate people in your organization using Action Groups.

## Resource Health Overview

Azure Resource Health helps you diagnose and get support for service problems that affect your Azure resources. It reports on the current and past health of your resources.

Azure status reports on service problems that affect a broad set of Azure customers. Resource Health gives you a personalized dashboard of the health of your resources. Resource Health shows all the times that your resources have been unavailable because of Azure service problems. This data makes it easy for you to see if an SLA was violated.

### Resource definition and health assessment

A resource is a specific instance of an Azure service, such as a virtual machine, web app, or SQL database. Resource Health relies on signals from different Azure services to assess whether a resource is healthy. If a resource is unhealthy, Resource Health analyzes additional information to determine the source of the problem. It also reports on actions that Microsoft is taking to fix the problem and identifies things that you can do to address it.

### Health status

The health of a resource is displayed as one of the following statuses.

#### Available

Available means that there are no events detected that affect the health of the resource. In cases where the resource recovered from unplanned downtime during the last 24 hours, you'll see a "Recently resolved" notification.

The screenshot shows the Azure Resource Health dashboard for a virtual machine named 'rijia'. The top navigation bar has 'Resource health' and a user profile icon. Below the header, there's a 'Refresh' button with a circular arrow icon. A message states: 'Resource health watches your resource and tells you if it's running as expected.' A green checkmark indicates the resource is 'Available'. The last update was '12/6/2016, 10:12:26 AM'. A note says, 'There aren't any known Azure platform problems affecting this virtual machine.' A blue link 'Report incorrect health status' is present. A red box highlights a 'Recently resolved' message: 'Recently resolved at 3/19/2017, 12:25:36 PM. A problem with your Virtual machine has been resolved.' At the bottom, a section titled 'What actions can you take?' lists two items: '1. If you're having problems, use the [Troubleshoot tool](#) to get recommended solutions' and '2. If you are experiencing problems you believe are caused by Azure, [contact support](#)'.

#### Unavailable

Unavailable means that the service detected an ongoing platform or non-platform event that affects the health of the resource.

## Platform events

Platform events are triggered by multiple components of the Azure infrastructure. They include both scheduled actions (for example, planned maintenance) and unexpected incidents (for example, an unplanned host reboot or degraded host hardware that is predicted to fail after a specified time window).

Resource Health provides additional details about the event and the recovery process. It also enables you to contact Microsoft Support even if you don't have an active support agreement.

The screenshot shows the 'Resource health' blade for a resource named 'rij'a. At the top, there's a 'Refresh' button. Below it, a message states: 'Resource health watches your resource and tells you if it's running as expected. [Learn more](#)'. A critical event is listed: 'Unavailable' (indicated by a red exclamation mark), last updated at 12/6/2016, 10:12:26 AM. The message says: 'We're sorry, your virtual machine isn't available because of a problem in the Azure compute infrastructure'. There's a link to 'Report incorrect health status'. Below this, instructions say: 'Please take the following actions' with two steps: 'Redeploy this virtual machine to a different host' and 'To get help recovering your virtual machine, [contact support](#)'.

## Non-platform events

Non-platform events are triggered by user actions. Examples include stopping a virtual machine or reaching the maximum number of connections to Azure Cache for Redis.

The screenshot shows the 'Resource health' blade for a resource. At the top, there's a 'Refresh' button. Below it, a message states: 'Resource health watches your resource and tells you if it's running as expected. [Learn more](#)'. A non-platform event is listed: 'Unavailable' (indicated by a blue information icon), last updated at 12/6/2016, 10:12:26 AM. The message says: 'This virtual machine has been shut down'. There's a link to 'Report incorrect health status'. Below this, a section titled 'What actions can you take?' lists two steps: 'To start this virtual machine, open the [resource blade](#) and click Start' and 'If you are experiencing problems you believe are caused by Azure, [contact support](#)'.

### Unknown

Unknown means that Resource Health hasn't received information about the resource for more than 10 minutes. Although this status isn't a definitive indication of the state of the resource, it's an important data point for troubleshooting.

If the resource is running as expected, the status of the resource will change to Available after a few minutes.

If you experience problems with the resource, the Unknown health status might mean that an event in the platform is affecting the resource.

The screenshot shows a web-based interface for monitoring resource health. At the top, there's a dark header bar with the title "Resource health" and a user name "rija". On the right side of the header are two small icons: a square with a minus sign and a close button (X). Below the header is a light-colored main area. On the left, there's a sidebar with a "Refresh" button featuring a circular arrow icon. The main content area contains the following text:  
"Resource health watches your resource and tells you if it's running as expected. [Learn more](#)"  
Below this, there's a section for a specific resource:  
"Unknown" (with a question mark icon) and "Last updated: 12/6/2016, 10:12:26 AM" (with a refresh icon).  
The message states: "We are currently unable to determine the health of this virtual machine".  
There is also a link "[Report incorrect health status](#)".  
At the bottom of the main content area, under the heading "What actions can you take?", there is a numbered list of five items:

1. Check back here for status updates
2. If you're having problems, use the [Troubleshoot tool](#) to get recommended solutions
3. Review your virtual machine's [console screenshot](#) to correct boot problems
4. [Redeploy this virtual machine](#) to a different host
5. If you are experiencing problems you believe are caused by Azure, [contact support](#)

### Degraded

Degraded means that your resource detected a loss in performance, although it's still available for use.

Different resources have their own criteria for when they report that they are degraded.

Resource health  
deturb

Refresh

Resource health watches your resource and tells you if it's running as expected. [Learn more](#)

**Degraded** Last updated: 2/15/2018 3:53:44 PM ⓘ

This Storage Account is degraded.

[Report incorrect health status](#)

What actions can you take?

1. Ensure that storage service implementation follow [Azure Storage retry guidelines](#) ⓘ
1. Follow [Partition Naming Convention](#) ⓘ to optimize load-balancing system
2. To get help recovering your storage accounts, [contact support](#)

### Reporting an incorrect status

If you think that the current health status is incorrect, you can tell us by selecting Report incorrect health status. In cases where an Azure problem is affecting you, we encourage you to contact Support from Resource Health.

Available Last updated: 3/16/2018 7:03:37 PM ⓘ

There aren't any known Azure platform problems affecting this virtual machine

[Report incorrect health status](#)

If you need help from an Azure support engineer, [contact support](#)

Tell us why this status is incorrect. Make sure you don't provide contact information

[Submit](#)

[Cancel](#)

### History information

You can access up to 30 days of history in the Health history section of Resource Health.

Home > Service Health - Resource health > Resource health

Resource health

deturb

Refresh

What actions can you take?

1. If you're having problems, use the [Troubleshoot tool](#) to get recommended solutions.
2. If you are experiencing problems you believe are caused by Azure, [contact support](#)

---

Health history

Resource health events over the last 2 weeks

TIMESTAMP	DESCRIPTION
3/16/2018	Available
3/15/2018	Available
3/14/2018	Available
3/13/2018	Available
3/12/2018	Available
3/11/2018	Available
3/10/2018	Available
3/9/2018	Available
▼ 3/8/2018	1 health event(s), 1 health annotation(s)
3/8/2018 11:34:35 ...	>Your virtual machine is unavailable.
3/8/2018 11:34:34 ...	This virtual machine is rebooting as requested by an authorized user or process. It will be back online after the reboot completes.
3/7/2018	Available

# Azure Workbooks

## Azure Workbooks Overview

Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure and combine them into unified interactive experiences.

### Data sources

Workbooks can query data from multiple sources within Azure. Authors of workbooks can transform this data to provide insights into the availability, performance, usage, and overall health of the underlying components. For instance, analyzing performance logs from virtual machines to identify high CPU or low memory instances and displaying the results as a grid in an interactive report.

But the real power of workbooks is the ability to combine data from disparate sources within a single report. This allows for the creation of composite resource views or joins across resources enabling richer data and insights that would otherwise be impossible.

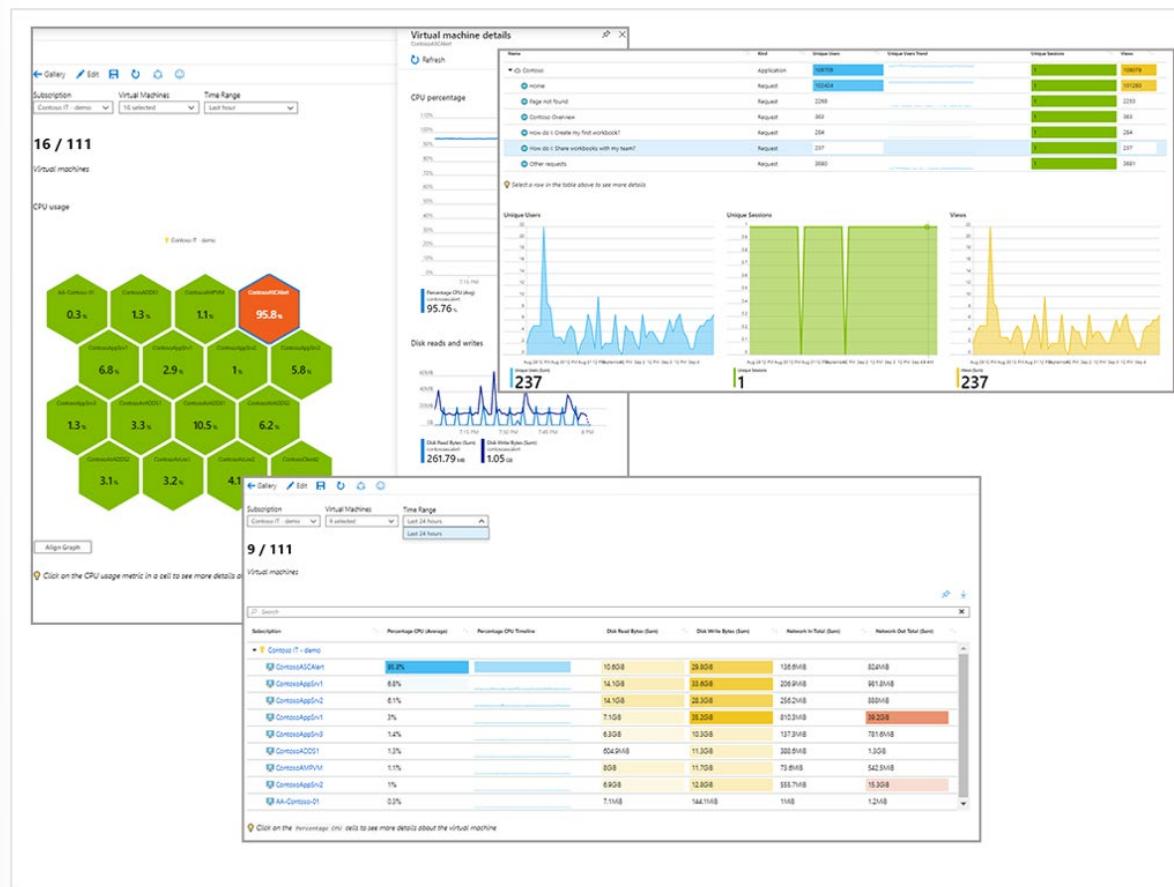
Workbooks are currently compatible with the following data sources:

- Logs
- Metrics
- Azure Resource Graph
- Alerts (Preview)
- Workload Health (Preview)
- Azure Resource Health (Preview)
- Azure Data Explorer (Preview)

### Visualizations

Workbooks provide a rich set of capabilities for visualizing your data. For detailed examples of each visualization type you can consult the example links below:

- Text
- Charts
- Grids
- Tiles
- Trees
- Graphs



## Using Azure Workbooks

To explore the workbooks experience, first navigate to the Azure Monitor service. This can be done by typing **Monitor** into the search box in the Azure portal.

Then select **Workbooks**.

The screenshot shows the Microsoft Azure Monitor | Overview page. At the top, there's a search bar with the placeholder "Search resources, services, and". Below the search bar, the breadcrumb navigation shows "Home > Monitor | Overview". The main title is "Monitor | Overview" with a Microsoft logo. A navigation bar below the title includes a search input ("Search (Ctrl+/)"), "What's new", "Get started" (which is underlined), and "Tutorials & Demos". On the left, a sidebar menu lists several options: "Overview" (selected), "Activity log", "Alerts", "Metrics", "Logs", "Service Health", and "Workbooks" (which is highlighted with a red border). Below the sidebar, the "Insights" section lists "Applications", "Virtual Machines", "Storage Accounts (preview)", "Containers", "Networks (preview)", "Cosmos DB (preview)", and a "More" option.

## Gallery

This takes you to the workbooks gallery:

To get started, choose a report or template below, or use 'Open' to open an existing report.

## Workbooks versus workbook templates

You can see a *workbook* in green and a number of *workbook templates* in purple. Templates serve as curated reports that are designed for flexible reuse by multiple users and teams. Opening a template creates a transient workbook populated with the content of the template.

You can adjust the template-based workbook's parameters and perform analysis without fear of breaking the future reporting experience for colleagues. If you open a template, make some adjustments, and then select the save icon you will be saving the template as a workbook which would then show in green leaving the original template untouched.

Under the hood, templates also differ from saved workbooks. Saving a workbook creates an associated Azure Resource Manager resource, whereas the transient workbook created when just opening a template has no unique resource associated with it.

### Exploring a workbook template

Select **Application Failure Analysis** to see one of the default application workbook templates.

As stated previously, opening the template creates a temporary workbook for you to be able to interact with. By default, the workbook opens in reading mode which displays only the information for the intended analysis experience that was created by the original template author.

In the case of this particular workbook, the experience is interactive. You can adjust the subscription, targeted apps, and the time range of the data you want to display. Once you have made those selections the grid of HTTP Requests is also interactive whereby selecting an individual row will change what data is rendered in the two charts at the bottom of the report.

## Editing mode

To understand how this workbook template is put together you need to swap to editing mode by selecting **Edit**.



Once you have switched to editing mode you will notice a number of Edit boxes appear to the right corresponding with each individual aspect of your workbook.

Name	Kind	Failed Requests	Failed Request Trend	All Requests	Success Rate	Users
GET Customers/Details	Request	82		82	0%	82
GET Home/Index	Request	1		310	99.68%	298
GET robots.txt/Index	Request	1		1	0%	1
GET /Content/fonts/segoewp-webfont.ttf	Request	0		1	100%	1
GET ServiceTickets/GetLogEntries	Request	0		1	100%	1
Other Requests	Request	0		81	100%	15

If we select the edit button immediately under the grid of request data we can see that this part of our workbook consists of a Kusto query against data from an Application Insights resource.

The screenshot shows the Azure Monitor Workbook Editor interface. At the top, there's a toolbar with various icons for navigation and editing. Below the toolbar is a header bar with tabs for 'Run Query' (which is selected), 'Samples', 'Time Range' (set to 'TimeRange'), 'Visualization' (set to 'Set by query'), 'Size' (set to 'Medium'), and 'Column Settings'. To the right of the header is a 'Query help' link and a download icon.

The main area contains two sections: a code editor and a chart visualization. The code editor displays a complex Kusto query for Application Insights Logs:

```
let appCount = 5;
let requestCount = 5;
let selectedApps = range i from 1 to 1 step 1
| extend x = '{Apps:name}'
| extend x = split(x, ',')
| mvexpand x to typeof(string) limit 100
| project appName = x;
let topItems = requests
| top-nested appCount of appName by AppMetric = countif(success == false) desc, top-nested requestCount of name by RequestMetric = countif(success == false) desc;
let topApps = topItems | summarize by appName;
let topRequests = topItems | summarize by strcat(appName, '::', name);
let rawData = requests
| extend name = iff(strcat(appName, '::', name) in (topRequests), name, 'Other Requests'), appName = iff(appName in (topApps), appName, 'Other Apps');
let apps = rawData
| summarize FailedRequests = countif(success == false), AllRequests = count(), Users = dcount(user_Id) by appName
| project Id = appName, ParentId = '', Name = strcat('△ ', appName), Kind = 'Application', FailedRequests, AllRequests, Users
| join kind = inner (
    rawData
    | make-series Trend = countif(success == false) default = 0 on timestamp from {TimeRange:start} to {TimeRange:end} step {TimeRange:grain} by Id = appName
) on Id
| project-away Id1, timestamp
| join kind = fullouter (selectedApps) on $left.Id == $right.appName
```

Below the code editor is a search bar labeled 'Search'.

The chart visualization is a horizontal bar chart with the following data:

Name	Type	Failed Requests	Failed Request Trend	All Requests	Success Rate	Users
GET Customers/Details	Request	82		82	0%	82
GET Home/Index	Request	1		310	99.68%	298
GET robots.txt/Index	Request	1		1	0%	1
GET /Content/fonts/segoewp-webfont.ttf	Request	0		1	100%	1
GET ServiceTickets/GetLogEntries	Request	0		1	100%	1
Other Requests	Request	0		81	100%	15

Clicking the other **Edit** buttons on the right will reveal a number of the core components that make up workbooks like markdown-based text boxes, parameter selection UI elements, and other chart/visualization types.

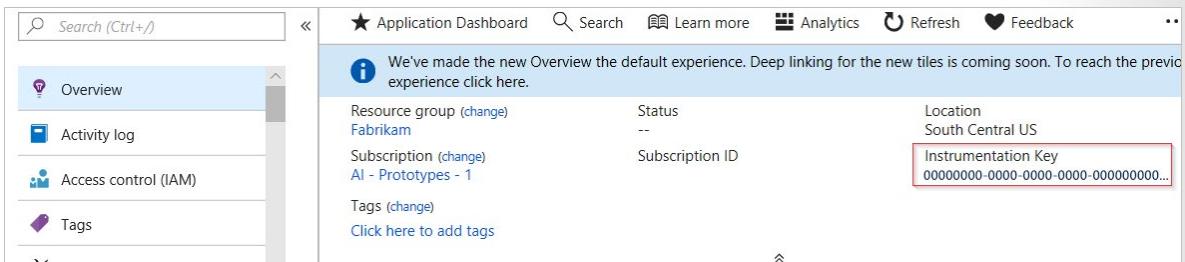
Exploring the pre-built templates in edit-mode and then modifying them to fit your needs and save your own custom workbook is an excellent way to start to learn about what is possible with Azure Monitor workbooks.

# Azure Application Insights

## Integrate Application Insight

To integrate Application Insights with your applications, you set up an Application Insights resource in the Azure portal. You also install an instrumentation package in your application. The package will monitor your application and send log data to the Log Analytics workspace.

For example, in your JavaScript web applications, you use a Node.js SDK as the instrumentation package. You need the Application Insights resource's instrumentation key from the Azure portal. You're going to use the key in your application's code.



The screenshot shows the Azure Application Insights Overview page. On the left, there's a sidebar with links for Overview, Activity log, Access control (IAM), and Tags. The main content area has a message: "We've made the new Overview the default experience. Deep linking for the new tiles is coming soon. To reach the previous experience click here." Below this, it shows Resource group (Fabrikam), Status (not specified), Subscription (AI - Prototypes - 1), Subscription ID, Location (South Central US), and the Instrumentation Key (00000000-0000-0000-0000-000000000000...). The instrumentation key is highlighted with a red border.

You then need to add the Node.js library via the package.json file as a dependency, by using npm.

```
npm install applicationinsights --save
```

Your code needs to load the library. You load it before everything else, including other require statements. You need to add the following code to your top-level .js file:

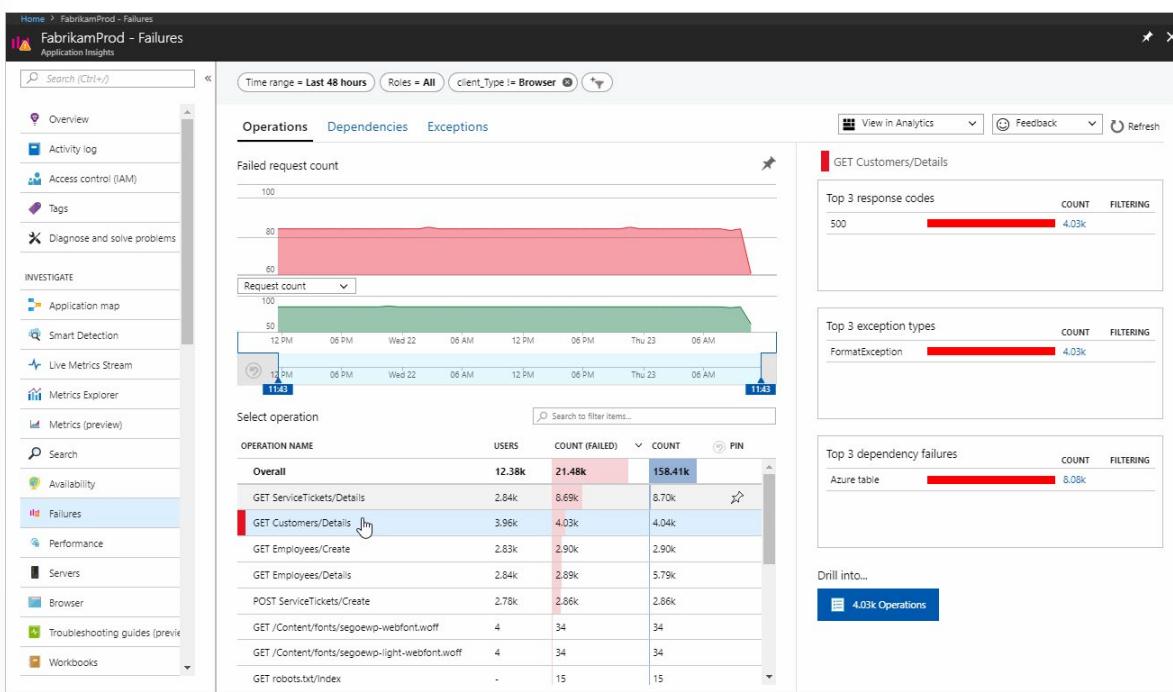
```
const appInsights = require("applicationinsights");

appInsights.setup("<your-instrumentation_key>");

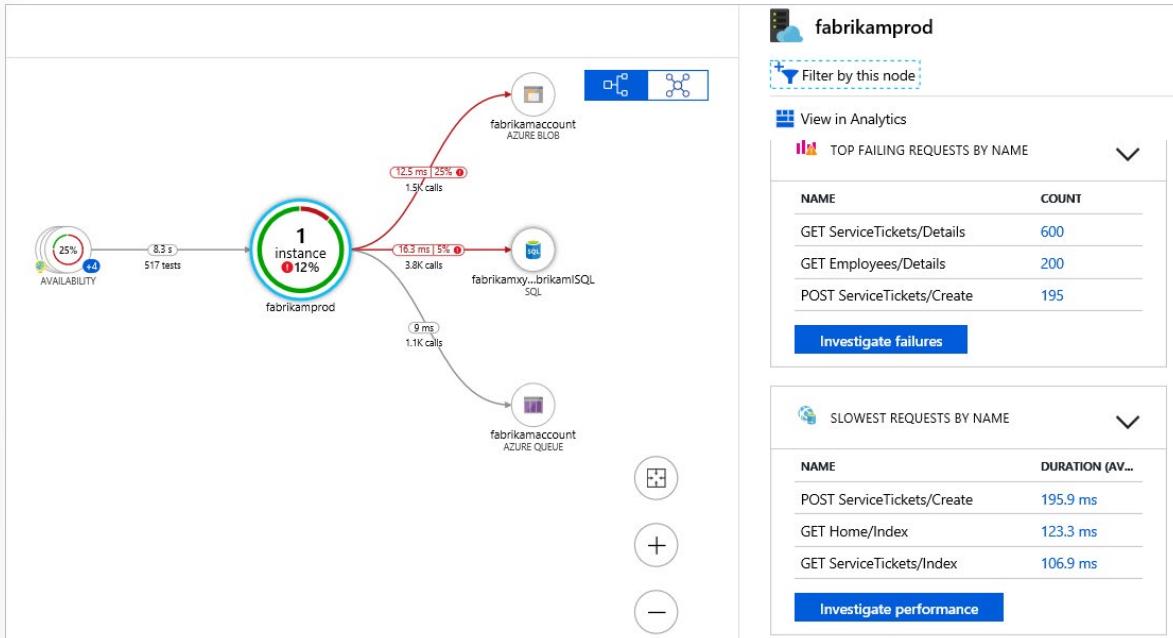
appInsights.start();
```

You also use the environment variable APPINSIGHTS\_INSTRUMENTATIONKEY to hold your key. The environment variable helps keep the key invisible in commits when you're using version control.

The SDK automatically gathers data about your Node.js runtime as you use your application. You can view this data in the Application Insights dashboard, in the Azure portal. From there you can, for example, get a list of all failures that have been collected and drill down into each one.

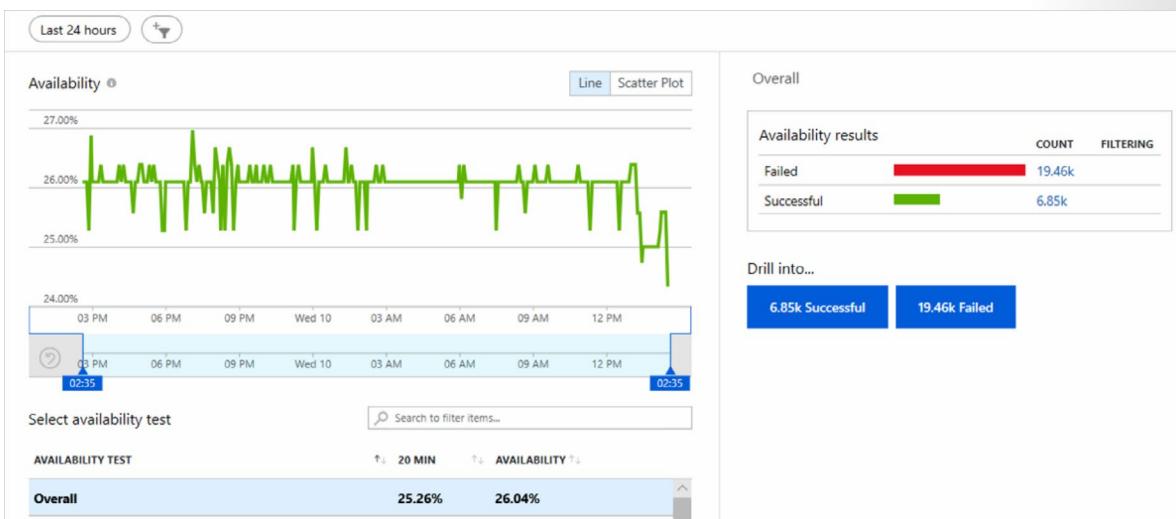


The SDK also analyzes your application for a typology. You see this typology through the Application map option. View more details of each component in the map by selecting it. You can, among other things, view the slowest requests for an instance and investigate performance further. These detailed analytics help you understand the application better and respond to its needs.



## Monitor Applications Continuously

Application Insights can send alerts for issues like failures or unavailability of your application. You can create availability tests to monitor the health of your applications continuously. Availability tests allow you to check the health of your application from different geographic locations.



You can create an availability test in the Azure portal. You need to specify details like the frequency, the URL of your application, and locations from which to test it.

### Create test

**Basic Information**

**\* Test name**  
Give your test a name  
[Learn more about configuring tests against applications hosted behind a firewall](#)

**Test type**  
URL ping test

**\* URL**

**Parse dependent requests** ?

**Enable retries for availability test failures.** ?

**Test frequency** ?  
5 minutes

**Test locations**  
5 location(s) configured

**Success criteria**  
HTTP response: 200, Test Timeout: 120 seconds

**Alerts**  
Enabled

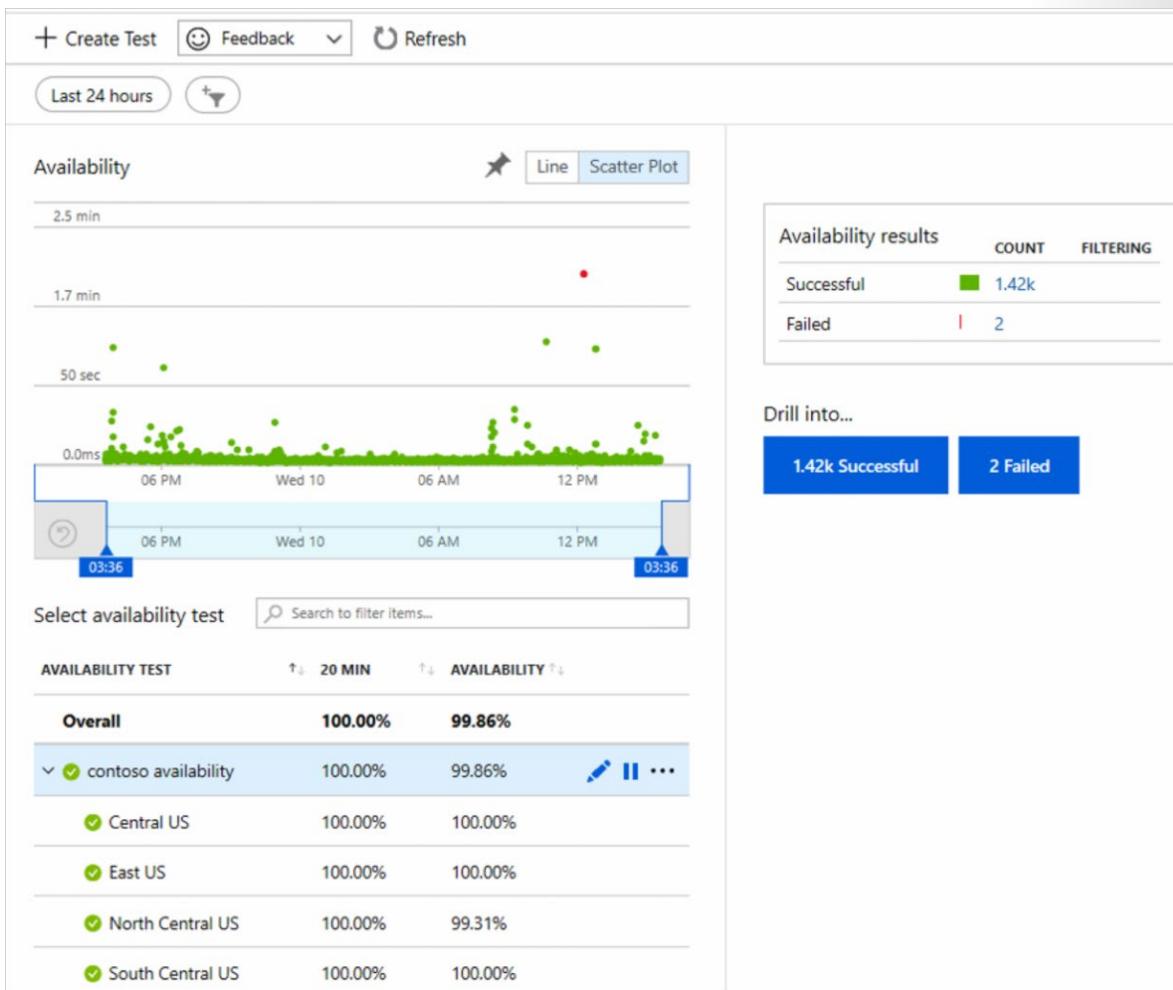
**Create**

The preceding example shows the configuration of a test that will send a request to an application every five minutes. The test is done from five geographic locations.

You also need to configure an alert rule for your availability test. Use alert rules to dictate how alerts should be handled for your tests.

The screenshot shows the 'contoso availability alerts-contoso' alert configuration page. At the top, there are buttons for Save, Discard, Enable, and Delete. The 'RESOURCE' section shows the alert name and its hierarchy under 'Visual Studio Enterprise > Contoso'. A note says '[Go to webtest for more details]'. The 'CONDITION' section contains a checked condition: 'Whenever the Failed locations is Greater than or equal to 3 count'. A note below it states: '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'. The 'ACTION GROUPS' section shows one group named 'Contoso' associated with '1 Email'. Buttons for 'Select existing' and 'Create New' are available. The 'ALERT DETAILS' section includes fields for 'Alert rule name' (set to 'Specify alert rule name. Sample: "Percentage CPU greater than 70"'), 'Description' (set to 'Automatically created alert rule for availability test " availability alerts-contoso"'), and 'Severity' (set to 'Sev 1'). A note at the bottom says: 'It can take up to 10 minutes for a metric alert rule to become active.'

You specify the conditions that should trigger an alert. For example, Application Insights can send an alert if a certain number of locations are unavailable. And you specify who should be notified. Send notifications through email or text message. Or use runbooks and webhooks to respond to alerts in an automated way.



When you've created your availability test, you'll see how your application is doing across different locations. Each dot in the preceding example represents a test that was run. A red dot means that a test failed. You can find more information about a failed test when you select a dot.

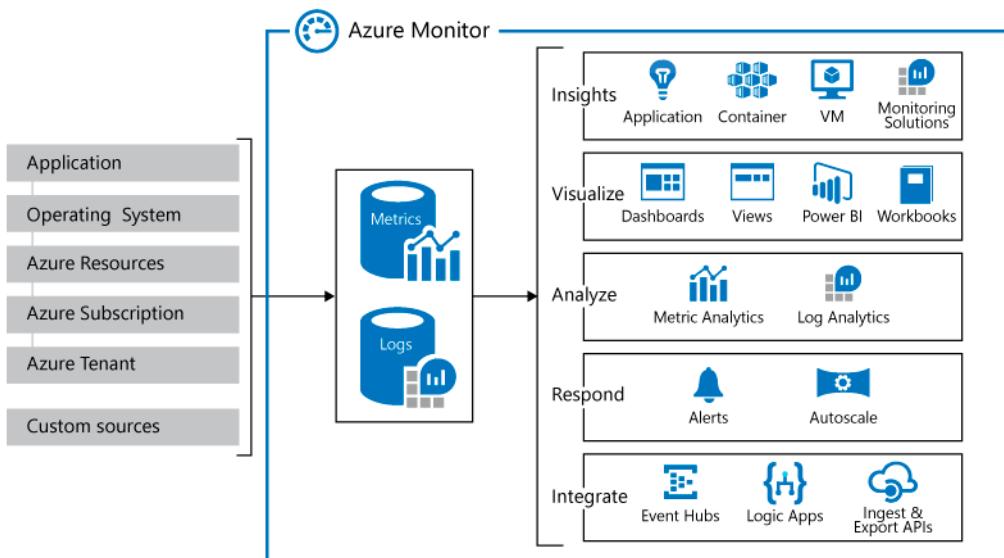
The screenshot shows the Azure Application Insights interface for 'End-to-end transaction details'. On the left, there's a search sidebar with filters like 'customDimensions.FullTestResultAvailable == true' and 'name == contoso avail...'. The main area displays an 'End-to-end transaction' timeline from 4/10/2019, 10:53 AM to 12:17 PM. The timeline shows a red bar for 'contoso availability' and a blue bar for 'https://www.contoso.com/'. A specific event at 12:17:52 PM is highlighted as 'Failed' with a duration of 0. To the right, the 'Availability Test Step Properties' pane shows details for 'contoso availability' in 'North Central US': Event time 4/10/2019, 12:17:52 PM, Test name 'contoso availability', Test location 'North Central US', Test success 'false', and Test duration '0'. Below this, the 'Exceptions' pane lists 'System.Exception: Failure' with the note '\*\*\*\* NOTE: This is not a real web request \*\*\*\* Web Test exceeded the configured timeout (00:02:00) and was aborted.'

You'll then see a detailed breakdown of the test failure, including information on what might have caused it. Use the information to respond appropriately.

# Unified Monitoring in Azure

## Unified Metrics and Logs

Azure Monitor centralizes and combines your metrics and log data from different sources. In the following diagram, the left side shows the sources that Azure Monitor supports. The right side shows what Azure Monitor lets you do with the data collected from those sources. You can analyze data, respond to alerts, and visualize by using different tools.



Additionally, you can run a single query over the logs collected from your services. You can then analyze log data collected from several sources, and have a unified understanding of all of your data.

Azure Monitor requires little to no configuration to get started. For example, Azure Monitor automatically makes log data available to you from your virtual machines. That's because the Log Analytics Agent in Azure Security Center automatically collects all the data into a workspace for Azure Monitor. The agent is enabled and deployed on all your virtual machines through a switch on the portal.

## Integration with Azure Security Center

Azure Security Center collects data from resources such as virtual machines by using the Log Analytics Agent. The agent gathers security-related information from resources like virtual machines and puts it into a workspace that you can use for analysis. Information such as operating system logs and running processes are copied to the workspace, along with any crash dump files. Your workspace consists of multiple tables, each of which stores data from a specific source.

The Log Analytics Agent can be installed automatically on all virtual machines. You'll need to set automatic provisioning to On in Azure Security Center under Settings - Data Collection.

**Settings - Data Collection**

Security Center collects security data and events from your resources and services to help you prevent, detect, and respond to threats. [Learn more >](#)

**Auto Provisioning**

This enables the automatic installation of the Microsoft Monitoring Agent on all the VMs in your subscription. If enabled, any new or existing VM without an installed Microsoft Monitoring agent (MMA) extension, will have it provisioned. [Learn more >](#)

**On** **Off**

**Workspace configuration**

Data collected by Security Center is stored in Log Analytics workspace(s). You can select to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. [Learn more >](#)

**Use workspace(s) created by Security Center (default)**  
Connect Azure VMs to report to workspaces created by Security Center

**Use another workspace**  
Connect Azure VMs to report to selected user workspace  
**Choose a workspace**

From that point, your data will be stored in a Log Analytics workspace. A workspace is created for you, or you choose an existing one.

A workspace can be used with multiple subscriptions. You can gather data from machines across multiple subscriptions and analyze it together from one central location.

You can analyze log data in workspaces by using Log Analytics. Log Analytics is an interactive tool in Azure that you use to write and test queries for your logs, and analyze results.

**Monitor - Logs**

**Logs** (selected)

New Query 1 +

contosoretail-IT

Run Time range: Last 24 hours

Save Copy link Export New alert rule Pin

Schema Filter (preview)

Type your query here...

Filter by name or type...

Active

- contosoretail-IT
  - ADAssessment
  - ADReplication
  - AlertManagement
  - AntiMalware
  - ApplicationInsights
  - AzureAutomation
  - ChangeTracking
  - CompatibilityAssessment
  - ContainerInsights
  - Containers
  - DeviceHealthProd
  - DnsAnalytics
  - InfrastructureInsights
  - LogManagement
  - NetworkMonitoring
  - Office365
  - SQLAssessment

**Select queries**

Heartbeat Performance Usage

Chart the number of reporting computers each hour  
Heartbeat | summarize dcountr(ComputerIP) by bin(TimeGenerated, 1h) | render timechart

List all computer heartbeats from the last hour  
Heartbeat | where TimeGenerated > ago(1h)

Last heartbeat of each computer  
Heartbeat | summarize arg\_max(TimeGenerated, \*) by Computer

Computers that stopped sending a heartbeat in the last 5 hours  
Heartbeat | summarize LastHeartbeat=max(TimeGenerated) by Computer | where LastHeartbeat < ago(5h)

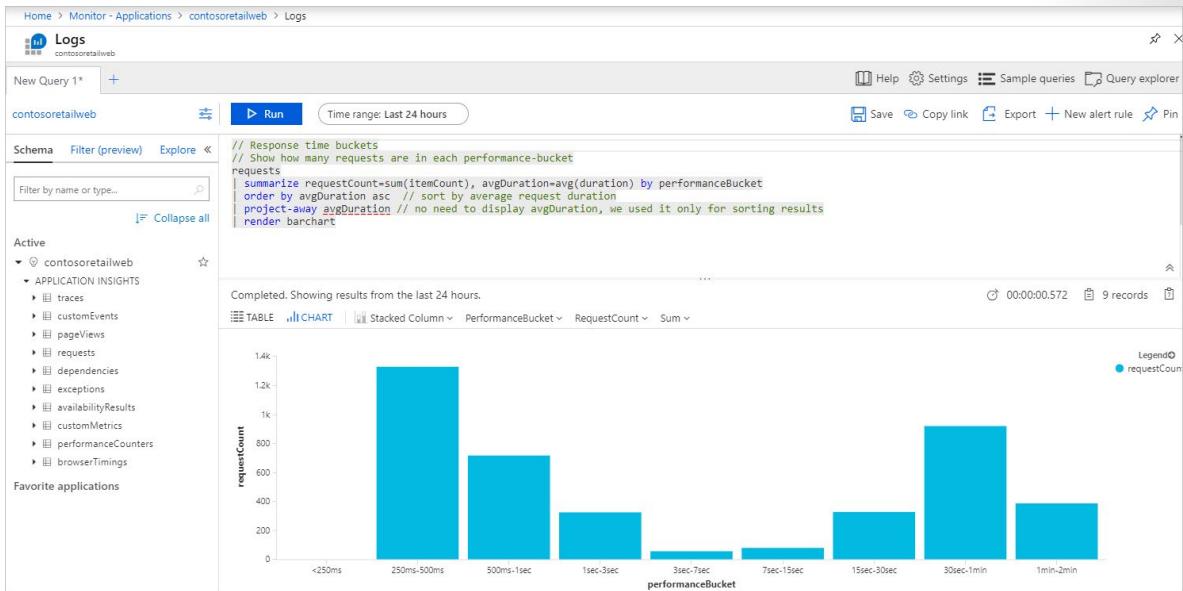
Calculate availability rate for connected computers

**Learn more**

- Documentation
- Online course
- Query language
- Community
- What's new

# Integration with Application Insights

Azure Application Insights and Azure Monitor come integrated. Your Application Insights data is collected and stored in logs that you can view and analyze by using Log Analytics. You can open Log Analytics from Application Insights by selecting **Analytics** from the **Overview** pane of your application.



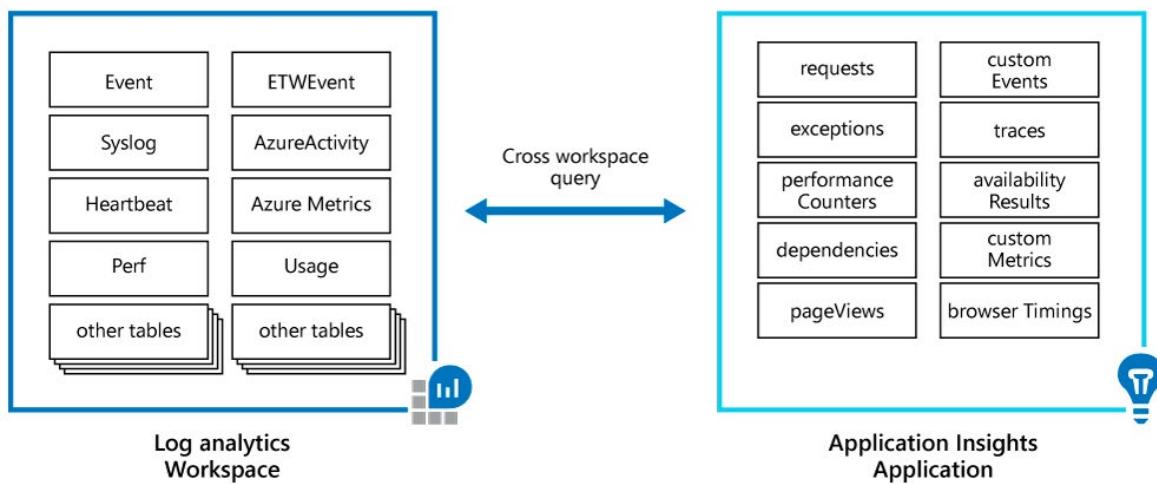
From here, you create and run queries on your logs and view results.

Queries for logs are written in the Kusto query language (KQL). A KQL query might look like this:

```
SecurityEvent
| where TimeGenerated > ago(7d)
| where EventID == 12345
| summarize count() by Computer, bin(TimeGenerated, 1h)
| render timechart
```

This query filters for specific records based on how long ago an event was generated and renders the summarized result to a time chart.

You can use a cross-resource query to analyze the log data collected from other sources such as Security Center, together with your Application Insights data. Use a cross-resource query to gain a deeper understanding of your applications and environment.



Your cross-resource query might look like this:

```
union Update, workspace("contosofinance-it").Update, workspace("c65g7445-  
914x-4h7j-6nbv-w876499056").Update  
  
| where TimeGenerated >= ago(24h)  
  
| where UpdateState == "Needed"  
  
| summarize dcount(Computer) by Classification
```

You reference workspaces by using `workspace()`.

Cross-resource querying can result in complex queries. Saving your query as a function in Log Analytics will help you reduce the complexity of your query structure.

The following query checks workspaces from multiple applications for requests. The query is saved as a function.

The screenshot shows the Azure Log Analytics workspace interface. On the left, there is a code editor window containing a Log Search query:

```
union withsource= SourceApp
app('app1').requests,
app('pp2').requests,
app('app3').requests,
app('app4').requests,
app('app5').requests
```

Below the code editor, the status "Canceled" is displayed. To the right, a "Save" dialog box is open:

- Name:** applicationsFunction
- Save as:** Function
- Function Alias:** applicationsFunction
- Save this query as a computer group:** (unchecked)
- Category:** cross-resource

At the bottom right of the dialog are "Save" and "Cancel" buttons.

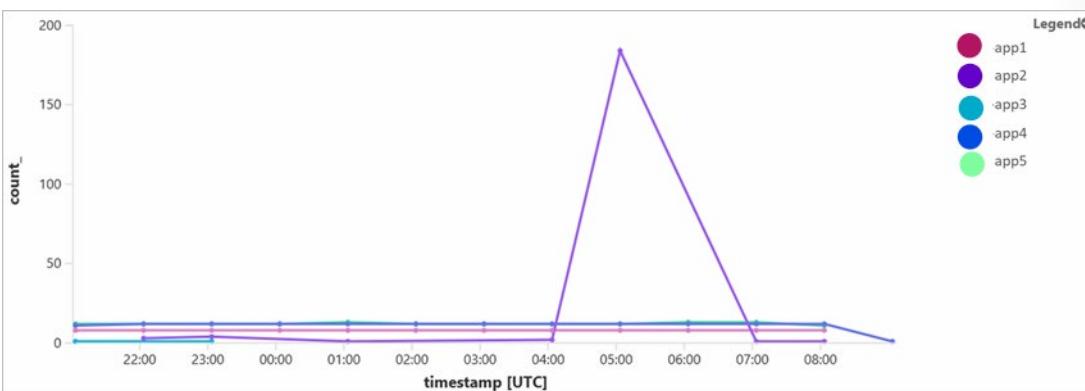
From this point on, we can use this function for cross-resource querying. In the following cross-resource query, the returned result for applicationsFunction is further filtered by the new query for any requests that have failed.

The screenshot shows the Azure Log Analytics workspace interface. The code editor window now contains a modified query:

```
applicationsFunction
| where timestamp > ago(12h)
| where success == 'False'
| parse SourceApp with * `(` applicationName `)`
| summarize count() by applicationName, bin(timestamp, 1h)
| render timechart
```

The "Time range" dropdown at the top is set to "Last 24 hours". To the right, there are buttons for "Save", "Copy", "Export", and "New alert rule".

The query renders its results to a time chart.



# Azure Security Center

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud, and at the same time, when you move to IaaS (infrastructure as a service) there is more customer responsibility than there was in PaaS (platform as a service), and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services and make sure you're on top of your security posture.

## **Azure Security Center addresses the three most urgent security challenges:**

- Rapidly changing workloads – It's both a strength and a challenge of the cloud. On the one hand, end users are empowered to do more. On the other, how do you make sure that the ever-changing services people are using and creating are up to your security standards and follow security best practices?
- Increasingly sophisticated attacks - Wherever you run your workloads, the attacks keep getting more sophisticated. You have to secure your public cloud workloads, which are, in effect, an Internet facing workload that can leave you even more vulnerable if you don't follow security best practices.
- Security skills are in short supply - The number of security alerts and alerting systems far outnumbers the number of administrators with the necessary background and experience to make sure your environments are protected. Staying up-to-date with the latest attacks is a constant challenge, making it impossible to stay in place while the world of security is an ever-changing front.

## **To help you protect yourself against these challenges, Security Center provides you with the tools to:**

- Strengthen security posture: Security Center assesses your environment and enables you to understand the status of your resources, and whether they are secure.
- Protect against threats: Security Center assesses your workloads and raises threat prevention recommendations and security alerts.
- Get secure faster: In Security Center, everything is done in cloud speed. Because it is natively integrated, deployment of Security Center is easy, providing you with autoprovisioning and protection with Azure services.

## **Architecture**

Because Security Center is natively part of Azure, PaaS services in Azure - including Service Fabric, SQL databases, and storage accounts - are monitored and protected by Security Center without necessitating any deployment.

In addition, Security Center protects non-Azure servers and virtual machines in the cloud or on premises, for both Windows and Linux servers, by installing the Log Analytics agent on them. Azure virtual machines are auto-provisioned in Security Center.

The events collected from the agents and from Azure are correlated in the security analytics engine to provide you tailored recommendations (hardening tasks), that you should follow to make sure your workloads are secure, and security alerts. You should investigate such alerts as soon as possible to make sure malicious attacks aren't taking place on your workloads.

When you enable Security Center, the security policy built-in to Security Center is reflected in Azure Policy as a built in initiative under Security Center category. The built-in initiative is automatically assigned to all

Security Center registered subscriptions (Free or Standard tiers). The built-in initiative contains only Audit policies.

You'll provide information on how to protect resources and respond to threats by using Azure Security Center.

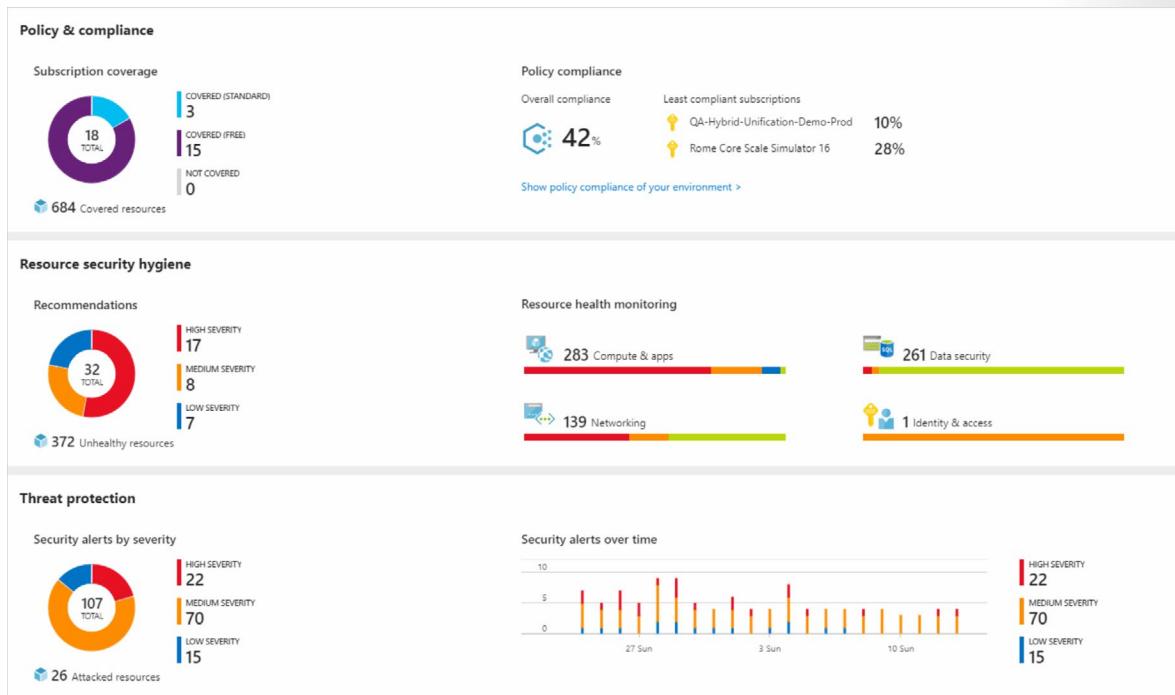
### Criteria for assessing Azure Security Center

You use Security Center if:

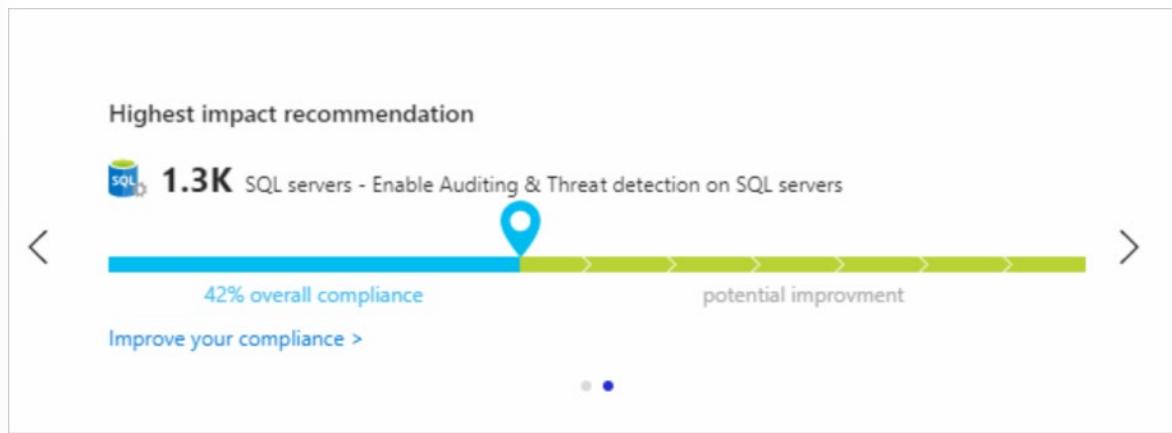
- You want to identify and address risks and threats to your infrastructure.
- You don't have the traditional in-house skills and capital needed to secure a complex infrastructure.
- You want to secure an infrastructure that consists of on-premises and cloud resources.

### Understand the security posture of your architecture

Security Center gives detailed analyses of different components of your environment. These components include data security, network security, identity and access, and application security. This way, Security Center helps you understand the security of your architecture. You can then build and maintain better infrastructures.



Security Center recommends how to address the issues and risks that it has uncovered. You use recommendations like the following one to improve the security and compliance of your architecture.



## Protect Against Threats with Azure Security Center

You have the responsibility to dismiss alerts if no action is required, such as if there are false positives. You also need to act to address known attacks and block, for example, known malicious IP addresses. Also, you must decide which alerts require more investigation.

Security Center gives a centralized view of all your security alerts. Security Center ranks security alerts based on their severity. Security Center also combines related alerts as much as possible into a single security incident.

The figure shows a screenshot of the Azure Security Center - Overview page. The main heading is "Security incident detected". Below it, a detailed view of a specific incident is shown:

Description	The incident which started on 2019-08-09 01:01:00Z and most recently detected on 2019-08-10 10:01:00Z indicate that an attacker has attacked other resources from your virtual machine vm1																																			
Activity time	Saturday, August 10, 2019, 1:01:00 PM																																			
Severity	High																																			
State	Active																																			
Attacked Resource	vm1																																			
Subscription	ASC DEMO																																			
Detected by	Microsoft																																			
Action Taken	Detected																																			
Environment	Azure																																			
Remediation Steps	1. Escalate the alert to the information security team. 2. Review the remediation steps of each one of the alerts																																			
Alerts included in this incident	<table border="1"><thead><tr><th>DESCRIPTION</th><th>COUNT</th><th>ACTIVITY TIME</th><th>ATTACKED RESOURCE</th><th>SEVERITY</th></tr></thead><tbody><tr><td>SQL injection blocked</td><td>4</td><td>08/09/19, 04:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Failed RDP Brute Force Attack</td><td>4</td><td>08/09/19, 05:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Successful RDP brute force attack</td><td>4</td><td>08/10/19, 05:01 AM</td><td>vm1</td><td>High</td></tr><tr><td>Suspicious SVCHOST process executed</td><td>4</td><td>08/10/19, 06:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Multiple Domain Accounts Queried</td><td>4</td><td>08/10/19, 07:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Network communication with a malicious machine detected</td><td>4</td><td>08/10/19, 08:01 AM</td><td>vm1</td><td>Medium</td></tr></tbody></table>	DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY	SQL injection blocked	4	08/09/19, 04:01 AM	vm1	Low	Failed RDP Brute Force Attack	4	08/09/19, 05:01 AM	vm1	Low	Successful RDP brute force attack	4	08/10/19, 05:01 AM	vm1	High	Suspicious SVCHOST process executed	4	08/10/19, 06:01 AM	vm1	Low	Multiple Domain Accounts Queried	4	08/10/19, 07:01 AM	vm1	Low	Network communication with a malicious machine detected	4	08/10/19, 08:01 AM	vm1	Medium
DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY																																
SQL injection blocked	4	08/09/19, 04:01 AM	vm1	Low																																
Failed RDP Brute Force Attack	4	08/09/19, 05:01 AM	vm1	Low																																
Successful RDP brute force attack	4	08/10/19, 05:01 AM	vm1	High																																
Suspicious SVCHOST process executed	4	08/10/19, 06:01 AM	vm1	Low																																
Multiple Domain Accounts Queried	4	08/10/19, 07:01 AM	vm1	Low																																
Network communication with a malicious machine detected	4	08/10/19, 08:01 AM	vm1	Medium																																

Security Center helps you respond to threats faster, and in an automated way, through playbooks. Playbooks are automated procedures that you run against alerts. You configure a playbook in the Playbooks pane of the Azure Security Center menu. You create a playbook by configuring a logic app.

The screenshot shows the Azure Security Center - Playbooks (Preview) interface. On the left, there's a sidebar with icons for various services like Log Analytics, Metrics, and Security Center. The main area displays a summary of security playbooks: 0 runs, 0 succeeded, 0 failed, and 0 running. A search bar for 'Search playbooks' is present. On the right, a 'Logic App' creation dialog is open. It includes fields for Name (ProcessExecuted), Subscription (Your-subscription), Resource group (resource-group), Location (Central US), and Log Analytics (Off). A note says, 'You can add triggers and actions to your Logic App after creation.' At the bottom are 'Create' and 'Automation options' buttons.

Your created playbook appears in a list.

Home > Security Center - Playbooks (Preview)

## Security Center - Playbooks (Preview)

Showing subscription 'Technologists\_A'

Search (Ctrl+ /)

Add Playbook Refresh Filter Enable Disable Delete

IoT Hubs & resources  
Data & storage  
Identity & access  
Security solutions

ADVANCED CLOUD DEFENSE

Adaptive application controls  
Just in time VM access  
Adaptive network hardening  
File Integrity Monitoring

THREAT PROTECTION

Security alerts  
Security alerts map (Preview)

AUTOMATION & ORCHESTRATION

Playbooks (Preview)

NAME	STATUS	TO...	RU...	SU...	FA...
ProcessExecuted	Enabled	0	0	0	0

Edit your playbook by selecting it and using the Azure Logic Apps Designer that appears.

Choose a template below to create your Logic App.

Category : Security Sort by : Popularity

The screenshot shows a grid of logic app templates under the 'Security' category, sorted by popularity. The templates include:

- Blank Logic App**: A simple template with a large blue plus sign icon.
- Get a notification email when Security Center creates a recommendation**: Triggers via Azure Security Center and sends an email.
- Get a notification email when Security Center detects a threat**: Triggers via Azure Security Center and sends an email.
- Post message in Slack**: Triggers via Azure Security Center and posts to Slack.
- Post message to Teams channel and send email notification**: Triggers via Azure Security Center and posts to Teams and sends an email.
- Send notification email**: Triggers via Azure Security Center and sends an email.

After you create a new blank logic app, you can use the designer to search for Security Center connectors and triggers for your playbook. For example, look for Azure Security Center and see all the triggers you can use. You then choose a trigger that details what should happen when the playbook is triggered.

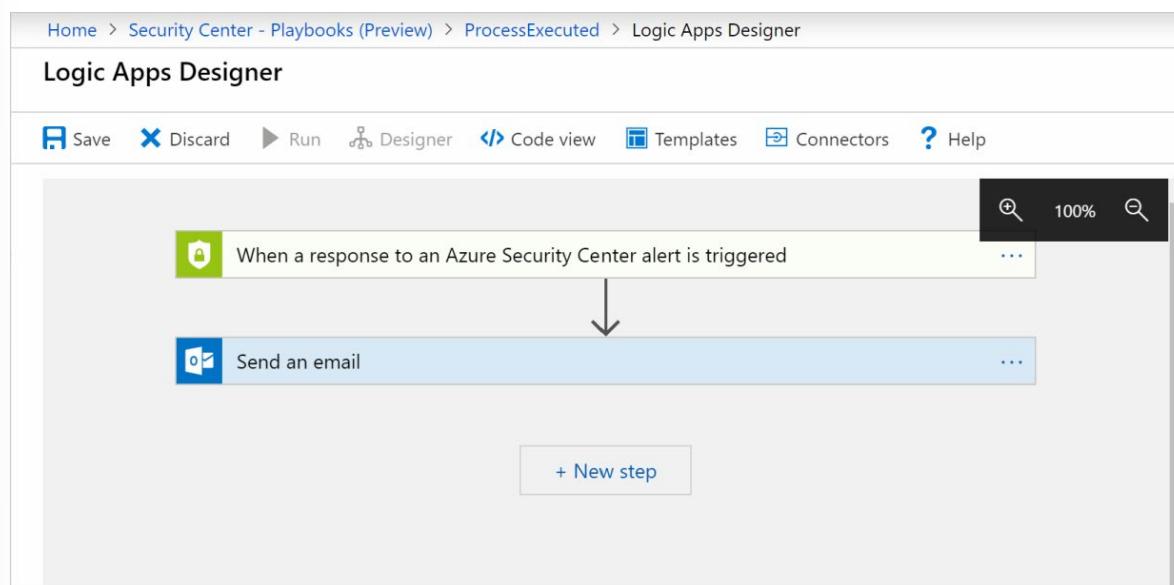
The screenshot shows the Azure Logic Apps designer interface with a search bar at the top containing 'azure security center'. Below the search bar, there are two sections:

- Connectors**: Shows one connector named 'Request' with a small icon.
- Triggers (1) Actions (0)**: Shows one trigger named 'Request - When a response to an Azure Security Center alert is triggered' with a small icon.

At the bottom of the screen, there are two feedback options:

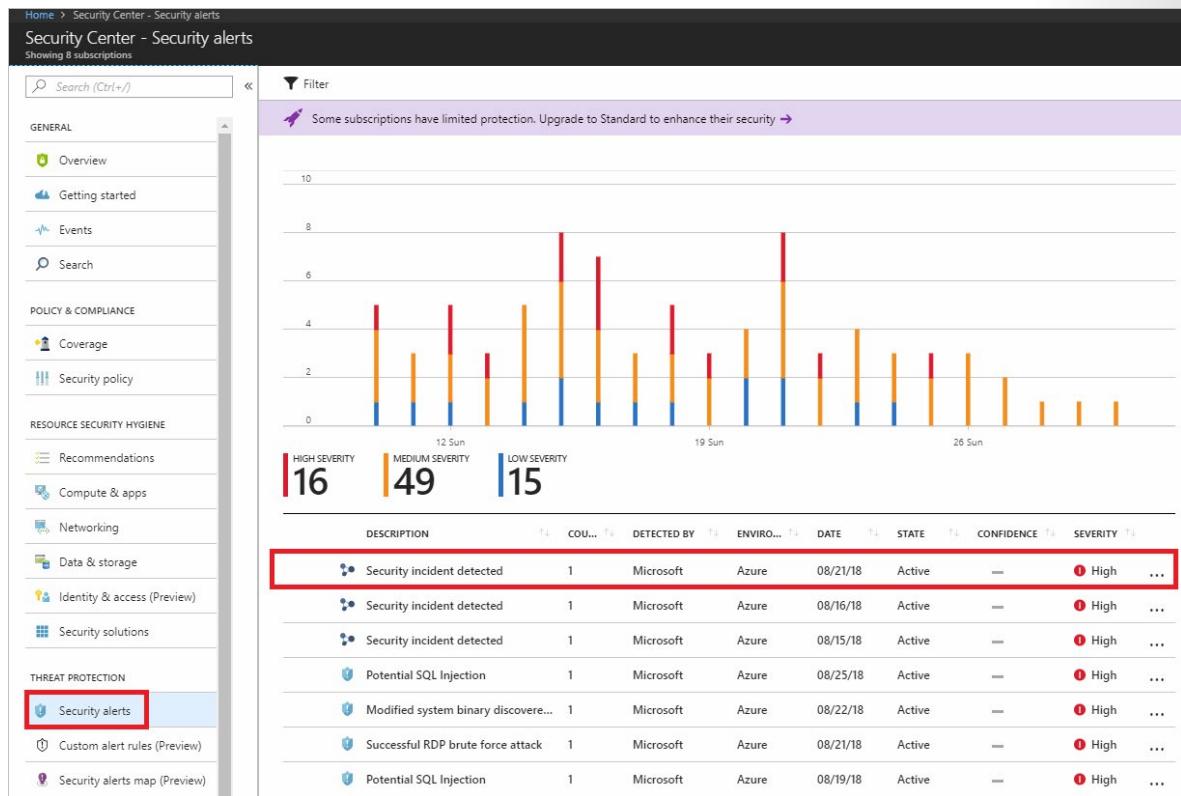
- TELL US WHAT YOU NEED**
- Help us decide which connectors and triggers to add next with UserVoice**

You then define actions that should be taken and which conditions must be met for these actions. Your actions can specify that an email should be sent when an alert is triggered.



Home > Security Center - Overview > Security alerts > Security incident detected																																				
<b>Security incident detected</b> Incident Detected																																				
Description	The incident which started on 2019-08-09 01:01:00Z and most recently detected on 2019-08-10 10:01:00Z indicate that an attacker has attacked other resources from your virtual machine vm1																																			
Activity time	Saturday, August 10, 2019, 1:01:00 PM																																			
Severity	High																																			
State	Active																																			
Attacked Resource	vm1																																			
Subscription	ASC DEMO																																			
Detected by	Microsoft																																			
Action Taken	Detected																																			
Environment	Azure																																			
Remediation Steps	1. Escalate the alert to the information security team. 2. Review the remediation steps of each one of the alerts																																			
Alerts included in this incident																																				
<table border="1"><thead><tr><th>DESCRIPTION</th><th>COUNT</th><th>ACTIVITY TIME</th><th>ATTACKED RESOURCE</th><th>SEVERITY</th></tr></thead><tbody><tr><td>SQL injection blocked</td><td>4</td><td>08/09/19, 04:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Failed RDP Bruteforce Attack</td><td>4</td><td>08/09/19, 05:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Successful RDP bruteforce attack</td><td>4</td><td>08/10/19, 05:01 AM</td><td>vm1</td><td>High</td></tr><tr><td>Suspicious SVCHOST process executed</td><td>4</td><td>08/10/19, 06:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Multiple Domain Accounts Queried</td><td>4</td><td>08/10/19, 07:01 AM</td><td>vm1</td><td>Low</td></tr><tr><td>Network communication with a malicious machine detected</td><td>4</td><td>08/10/19, 08:01 AM</td><td>vm1</td><td>Medium</td></tr></tbody></table>		DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY	SQL injection blocked	4	08/09/19, 04:01 AM	vm1	Low	Failed RDP Bruteforce Attack	4	08/09/19, 05:01 AM	vm1	Low	Successful RDP bruteforce attack	4	08/10/19, 05:01 AM	vm1	High	Suspicious SVCHOST process executed	4	08/10/19, 06:01 AM	vm1	Low	Multiple Domain Accounts Queried	4	08/10/19, 07:01 AM	vm1	Low	Network communication with a malicious machine detected	4	08/10/19, 08:01 AM	vm1	Medium
DESCRIPTION	COUNT	ACTIVITY TIME	ATTACKED RESOURCE	SEVERITY																																
SQL injection blocked	4	08/09/19, 04:01 AM	vm1	Low																																
Failed RDP Bruteforce Attack	4	08/09/19, 05:01 AM	vm1	Low																																
Successful RDP bruteforce attack	4	08/10/19, 05:01 AM	vm1	High																																
Suspicious SVCHOST process executed	4	08/10/19, 06:01 AM	vm1	Low																																
Multiple Domain Accounts Queried	4	08/10/19, 07:01 AM	vm1	Low																																
Network communication with a malicious machine detected	4	08/10/19, 08:01 AM	vm1	Medium																																

View your security alerts through the **Security alerts** pane under the **Security** section on the main menu.



You drill down into specific security incidents by selecting an incident.

Security incident detected

Incident Detected

DESCRIPTION The incident which started on 2018-01-01T12:00:00.000Z and most recently detected on 2018-01-02T19:00:00.000Z indicate that an attacker has attacked other resources from your virtual machine ContosoWebFE1

DETECTION TIME Thursday, January 4, 2018, 3:02:00 AM

SEVERITY ! High

STATE Active

ATTACKED RESOURCE ContosoWebFE1

SUBSCRIPTION <Subscription ID>

DETECTED BY Microsoft

ENVIRONMENT Azure

REMEDIATION STEPS

1. Escalate the alert to the information security team.
2. Review the remediation steps of each one of the alerts

Alerts included in this incident

DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
Successful RDP brute force attack	1	01/04/18, 4:20 AM	ContosoWebFE1	<span style="color: red;">!</span> High
Suspicious SVCHOST process executed	1	01/04/18, 5:19 AM	ContosoWebFE1	<span style="color: blue;">i</span> Low
Multiple Domain Accounts Queried	1	01/04/18, 5:21 AM	ContosoWebFE1	<span style="color: blue;">i</span> Low

[Continue investigation](#)

From here, you can see the list of alerts that the incident holds. You request more information about a specific alert by selecting one.

**Successful RDP brute force attack**  
ContosoWebFE1

[Learn more](#)

### General information

Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.

DESCRIPTION	Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.
DETECTION TIME	Thursday, January 4, 2018, 4:20:00 AM
SEVERITY	<span style="color: red;">!</span> High
STATE	Active
ATTACKED RESOURCE	ContosoWebFE1
SUBSCRIPTION	<Subscription ID>
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
TIMEGENERATEDOFFSETMIN	30
SOURCE	FreeRDP (96.81.218.10)
SUCCESSFUL LOGINS	1
ATTACK DURATION	30 minutes
FAILED ATTEMPTS	60
NON-EXISTENT USERS	20
EXISTING USERS	1
REPORTS	<a href="#">Report: RDP Brute Forcing</a>
END TIME UTC	1/4/2018 1:21:00 PM

### Remediation steps

[Continue investigation](#) [Run playbooks](#)

You can then choose to run your configured playbooks against your alert.

You can further investigate the alert by using the **Continue investigation** option. An investigation map shows all of the entities that are related to this alert.

The screenshot shows the Investigation Dashboard (Preview) interface. On the left, there's a navigation bar with icons for Home, Dashboards, Reports, and Help. Below it is a search bar with placeholder text 'Search' and a date range selector '10/13/2017 4:57 PM — 11/6/2017 3:57 PM (24 days)'. The main area displays an investigation path starting with 'Security incident detected' (highlighted in blue), followed by 'Successful RDP brute force ...' and 'Multiple Domain Accounts Qu...'. A timeline at the bottom shows 'Suspicious SVCHOST process', 'Successful RDP brute force ...', and 'Multiple Domain Accounts Qu...'. On the right, a detailed view of the first incident is shown with sections for 'General Information' (Description: 'The alert has no log data in this time interval', Alert ID: '2518942547722139231\_77a4630c-bebe-4957-ada1-5920e3a3f1b8', Time Generated: '10/15/2017 2:25:41:000 AM'), 'Remediation Steps' (empty), and a sidebar with links for Entities, Search, Exploration, Playbooks, Comments, and Audit.

You request more information about a specific entity in the map by selecting it. Entities include devices or even users. The map expands with new entities, and properties for the selected entity are displayed on the right. Use this information to better understand a particular path that an attack might have taken.

# Monitor Azure Costs

## Monitoring Azure Costs

Cost monitoring is about establishing controls and business processes for reviewing your cloud spend to avoid any misuse and take advantage of new opportunities through flexibility provided by the cloud. Effective ongoing cost management includes informed cost reviews with key stakeholders. Reviews should be scheduled on a regular cadence. You may also need to have reactive cost reviews, for example when a budget limit causes an alert.

### Identify stakeholders

Which of your regular financial stakeholders need visibility and input for your cloud costs? Do they understand cloud billing, capabilities, and business benefits to enable them to understand both the financial metrics and the impact of their decisions? Consider what additional knowledge or training they may need to help them understand cloud cost metering and cloud architectures.

Which additional stakeholders also need to be present? This could include key application owners, systems administrators who monitor and back-up cloud systems, and business unit representatives.

Which other stakeholders may be required but only when necessary? Are your resources appropriately tagged so you can easily identify owners of systems or applications that are contributing to cost noise? Are they aware that their participation in cost reviews may be required and what is expected of them?

### Determine frequency

You may have regular business reviews where it would make sense to also review, or you may wish to schedule an additional meeting. Cloud costs can be reviewed:

- During the billing period for an awareness of the estimated pending billing.
- After the billing period to review actual spend with activity that occurred that month
- On an ad-hoc basis – usually triggered by a **budget alert**<sup>12</sup> or Azure Advisor recommendation.

Web Direct (pay as you go) and CSP billing occurs monthly. While Enterprise Agreement (EA) billing occurs annually, costs should still be reviewed monthly.

### Responding to cost alerts

Check the current consumption data first. Budget alerts do not fire in real time and there may be a delay (up to 8 hrs) between this alert and your current actual cost. Check for any significant difference between when the alert happened and your current costs.

Are the costs due to unnecessary or expensive resources? Do you need to implement additional Azure Policy controls to prevent this in the future? Do you need to add **budget automation**<sup>13</sup> to trigger resource scaling or shutdowns?

### Define budgets

After you identify and analyze your spending patterns, you can set budget limits for applications or business units. You will want to assign access to view or manage each budget to the appropriate groups. Setting several alert thresholds for each budget can help track your burn down rate.

### Gather information

<sup>12</sup> <https://docs.microsoft.com/azure/cost-management/cost-mgt-alerts-monitor-usage-spending>

<sup>13</sup> <https://docs.microsoft.com/azure/billing/billing-cost-management-budget-scenario>

It's natural to reach for the invoice as the sole basis for your costs. Stakeholders should review this information in relation to other data and events. Identify the business data that's relevant to your cost conversation to ensure that all factors are considered.

In addition to usage details on your invoice, Azure provides tools that can make recommendations on cost savings. It's important to consider building custom solutions to maximize cost savings where it makes sense for your business.

### Azure Cost Management – Cost Analysis

Cost Analysis allows you to view aggregated costs to understand your spending trends. Spending can be viewed by time period against your budgets. You can also view costs at different scopes, such as for a resource group or specific resource tag. Cost Analysis provides built-in charts as well as custom views. You can also download your cost data in CSV format to analyze with other tools. For more information, see: [quick acm cost analysis<sup>14</sup>](#)

### Azure Cost Management - Advisor

Advisor cost management recommendations highlight over provisioned services and steps you can take to realize cost savings. This includes virtual machines which could be resized to a lower SKU, unprovisioned ExpressRoute circuits and idle virtual network gateways. You can act on these recommendations, postpone them or download them as a CSV or PDF file. To get started visit [Advisor cost management recommendations<sup>15</sup>](#).

**✓ Note:** There are several different ways of purchasing Azure services and not all of them are supported by Azure Cost Management. For example, detailed billing information for services purchased through a Cloud Solution Provider must be obtained directly from your CSP. Review [understand cost management data<sup>16</sup>](#) for information on supported cost data.

## Optimizing Azure Costs

When the first calculation is close to on-premises in terms of the cost - customers prefer to migrate to the cloud. And after migration, continue to optimize the infrastructure by using the right types/sizes of VMs and arrange the scale-down of unused resources.

For example, looking at a VM running the SAP on Azure project can show you how initially the VM was sized based on the size of existing hardware server (with cost around €1 K per month), but the real utilization of VM was not more than 25% - but simple choosing the right VM size in the cloud we can achieve 75% saving (resize saving). And by applying the snoozing you can get additional 14% of economy:

---

<sup>14</sup> <https://docs.microsoft.com/azure/cost-management/quick-acm-cost-analysis>

<sup>15</sup> <https://docs.microsoft.com/azure/advisor/advisor-cost-recommendations>

<sup>16</sup> <https://docs.microsoft.com/azure/cost-management/understand-cost-mgt-data>

## Run cost optimization methods



It is easy to handle cost comparison when you are well equipped and for this Microsoft provides the set of specific services and tools that help you to understand and plan costs. These include the TCO Calculator, Azure Pricing Calculator, Azure Cost Management (Cloudyn), Azure Migrate, Cosmos DB Sizing Calculator, and the Azure Site Recovery Deployment Planner.

As we are talking about financial things - the way how you purchase cloud services, in which selling channel, may also bring the difference into the final cost. Consider the following methods of purchasing Azure and ways of modifying your pricing:

- Enterprise Agreement
- Enterprise Dev Test Subscription
- Cloud Service Provider (Partner Program)
- Azure Hybrid Use Benefit
- Azure Reserved Instances

**Azure Advisor** enables you to act on cost management recommendations from within the Azure portal, such as resizing virtual machines. **Act on recommendations**<sup>17</sup>. Make sure that all stakeholders agree regarding the implementation and timing of this change. Resizing a virtual machine does require the VM to be shut down and restarted, causing a period when it will be unavailable, so time this carefully for minimal business impact.

<sup>17</sup> <https://docs.microsoft.com/azure/cost-management/tutorial-acm-opt-recommendations>

## Module 15 Review Questions

### Module 15 Review Questions



#### Review Question 1

You are analyzing the company virtual network and think it would be helpful to get a visual representation of the networking elements. Which feature can you use? Select one.

- Network Watcher Auditing
- Network Watcher Connection Troubleshoot
- Network Watcher Flows
- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology

#### Review Question 2

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 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

# Answers

## Review Question 1

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 2

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 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.*