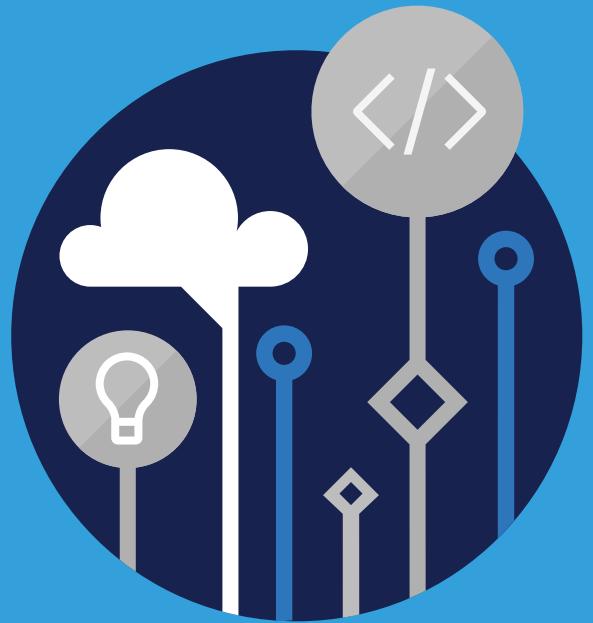


Microsoft  
Official  
Course



AZ-304T00

Microsoft Azure Architect  
Design

AZ-304T00

**Microsoft Azure Architect Design**

---

## 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 Design a Compute Solution</b>	11
	Choose an Azure Compute Service	11
	Determine Appropriate Compute Technologies	16
	Recommend a Solution for Containers	18
	Provisioning Solutions for Azure Compute Infrastructure	22
	Module 1 Review Questions	30
■	<b>Module 2 Design a Network Solution</b>	33
	Planning Virtual Networks	33
	Recommend a Solution for Network Addressing and Name Resolution	38
	Recommend Solutions for Network Security	42
	Recommendation for Hybrid Networks	46
	Implement a Secure Hybrid Network	50
	Module 2 Review Questions	53
■	<b>Module 3 Design for Migration</b>	57
	Planning Azure Migration	57
	Assessment using Azure Migrate	63
	Migrate Servers with Azure Migrate	66
	Migrate Databases with Azure Database Migration Service	69
	Migrate On-Premises Data to Cloud Storage with AzCopy	73
	Lab	79
	Module 3 Review Questions	82
■	<b>Module 4 Design Authentication and Authorization</b>	85
	Tips for Identity and Access Management	85
	Recommend a Solution for Multi-Factor Authentication	89
	Five Steps for Securing Identity Infrastructure	95
	Recommend a Solution for Single-Sign On (SSO)	103
	Recommend a Solution for a Hybrid Identity	107
	Recommend a Solution for B2B Integration	113
	Recommend a Hierarchical Structure for Management Groups, Subscriptions and Resource Groups	117
	Lab	123
	Module 4 Review Questions	126

■	<b>Module 5 Design Governance</b>	133
	Governance	133
	Recommend a Solution for using Azure Policy	135
	Recommend a Solution for using Azure Blueprint	146
	Module 5 Review Questions	149
■	<b>Module 6 Design a Solution for Databases</b>	153
	Select an Appropriate Data Platform Based on Requirements	153
	Overview of Azure Data Storage	158
	Recommend Database Service Tier Sizing	169
	Dynamically Scale Azure SQL Database and Azure SQL Managed Instances	174
	Recommend a Solution for Encrypting Data at Rest, Transmission, and In Use	177
	Lab	183
	Module 6 Review Questions	185
■	<b>Module 7 Select an Appropriate Storage Account</b>	189
	Choose Between Storage Tiers	189
	Recommend Storage Management Tools	193
	Module 7 Review Questions	198
■	<b>Module 8 Design Data Integration</b>	203
	Azure Data Platform End-to-End	203
	Recommend a Solution for Data Integration	208
	Recommend a Solution for Data Warehousing and Big Data Analytics Integration	213
	Module 8 Review Questions	218
■	<b>Module 9 Design a Solution for Logging and Monitoring</b>	223
	Monitoring	223
	Azure Monitor	226
	Module 9 Review Questions	255
■	<b>Module 10 Design a Solution for Backup and Recovery</b>	259
	Architectural Best Practices for Reliability	259
	Recommend an Azure Site Recovery Solution	265
	Design a Solution for Data Archiving and Retention	273
	Module 10 Review Questions	276
■	<b>Module 11 Design for High Availability</b>	279
	High Availability	279
	Applications in Multiple Azure Regions for High Availability	285
	Design HA Applications to Handle Disaster Recovery	288
	Module 11 Review Questions	293
■	<b>Module 12 Design for Cost Optimization</b>	297
	Recommend Solutions for Cost Management	297
	Recommendations for Minimizing Costs	309
	Cost Optimization Checklists	320
	Module 12 Review Questions	325
■	<b>Module 13 Design an Application Architecture</b>	329
	Recommend Event-Based Cloud Automation on Azure	329
	Microservices Architecture on Azure Service Fabric	336
	Designing APIs for Microservices	341
	Lab	343
	Module 13 Review Questions	346

■ <b>Module 14 Design Security for Applications</b> .....	<b>349</b>
Security for Applications and Services .....	<b>349</b>
Recommend a Solution using Key Vault .....	<b>357</b>
Recommend Solutions using Azure AD Managed Identities .....	<b>364</b>
Module 14 Review Questions .....	<b>367</b>



## Module 0 Welcome

### Start Here

### About this Course

#### **AZ-304: Microsoft Azure Architect Design**

### Course Description

This course teaches Solutions Architects how to translate business requirements into secure and reliable recommendations for infrastructure, governance, high availability, cost optimization, and data integration. Lessons include solutions for logging, multi-factor authentication, SSO, hybrid identity, backup and recovery, containers, microservices, monitoring, automation, networking, and application infrastructure. This course outlines how decisions in each area affects the 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 Solution Architects start this role with experience on operating systems, virtualization, cloud infrastructure, storage structures, governance, and networking.

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

## Expected learning

- Implementing Azure data storage solutions such as Azure SQL Database, Azure Cosmos DB, and Azure Files.
- Implementing Azure SQL Database Managed Instances and service tiers.
- Recommendations for Governance such as Azure Policy and Azure Blueprint.
- Recommendations for subscriptions, accounts, and Role-Based Access Control.
- Designs for Authentication and Authorization such as MFA and hybrid identities.
- Solutions for logging and monitoring such as Azure Monitor and Azure Monitoring solutions (Azure Security Center, Azure Application Insights, and Azure Sentinel).
- Recommendations for intra and intersite integration (name resolution, network security, internet protection, hybrid networks, and perimeter networks).
- Manage network traffic using network routing and service endpoints, Azure load balancer, and Azure Application Gateway.
- Solutions for Application Architecture such as event-based Cloud automation, microservices architecture on Azure Service Fabric, and designs for microservices APIs.
- Recommendations for 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: Design a Compute Solution

- Lesson 1: Choose an Azure Compute Service
- Lesson 2: Determine Appropriate Compute Technologies
- Lesson 3: Recommend a Solution for Containers
- Lesson 4: Provisioning Solutions for Azure Compute Infrastructure
- Lesson 6: Module 1 Review Questions

### Module 2: Design a Network Solution

- Lesson 1: Plan Virtual Networks

- Lesson 2: Recommend a Solution for Network Addressing and Name Resolution
- Lesson 3: Recommend Solutions for Network Security
- Lesson 4: Recommendation for Hybrid Networks
- Lesson 5: Implement a Secure Hybrid Network
- Lesson 6: Module 2 Review Questions

### **Module 3: Design for Migration**

- Lesson 1: Planning Azure Migration
- Lesson 2: Assessment using Azure Migrate
- Lesson 3: Migrate Servers with Azure Migrate
- Lesson 4: Migrate Databases with Azure Database Migration Service
- Lesson 5: Migrate On: Premises Data to Cloud Storage with AzCopy
- Lesson 6: Lab
- Lesson 7: Module 3 Review Questions

### **Module 4: Design Authentication and Authorization**

- Lesson 1: Tips for Identity and Access Management
- Lesson 2: Recommend a Solution for Multi Factor Authentication
- Lesson 3: Five Steps for Securing Identity Infrastructure
- Lesson 4: Recommend a Solution for Single Sign On (SSO)
- Lesson 5: Recommend a Solution for a Hybrid Identity
- Lesson 6: Recommend a Solution for B2B Integration
- Lesson 7: Recommend a Hierarchical Structure for Management Groups, Subscriptions and Resource Groups
- Lesson 10: Lab
- Lesson 11 Module 4 Review Questions

### **Module 5: Design Governance**

- Lesson 1: Governance
- Lesson 2: Recommend a Solution for using Azure Policy
- Lesson 3: Recommend a Solution for using Azure Blueprint
- Lesson 4: Module 5 Review Questions

### **Module 6: Design a Solution for Databases**

- Lesson 1: Select an Appropriate Data Platform Based on Requirements
- Lesson 2: Overview of Azure Data Storage
- Lesson 3: Recommend Database Service Tier Sizing
- Lesson 4: Dynamically Scale Azure SQL Database and Azure SQL Managed Instances
- Lesson 5: Recommend a Solution for Encrypting Data at Rest, Transmission, and In Use
- Lesson 6: Lab

- Lesson 7: Module 6 Review Questions

### **Module 7: Select an Appropriate Storage Account**

- Lesson 1: Choose Between Storage Tiers
- Lesson 2: Recommend Storage Management Tools
- Lesson 3: Module 7 Review Questions

### **Module 8: Design Data Integration**

- Lesson 1: Azure Data Platform End-to-End
- Lesson 2: Recommend a Solution for Data Integration
- Lesson 3: Recommend a Solution for Data Warehousing and Big Data Analytics Integration
- Lesson 4: Module 8 Review Questions

### **Module 9: Design a Solution for Logging and Monitoring**

- Lesson 1: Monitoring
- Lesson 2: Azure Monitor
- Lesson 3: Module 9 Review Questions

### **Module 10: Design a Solution for Backup and Recovery**

- Lesson 1: Architectural Best Practices for Reliability
- Lesson 2: Recommend an Azure Site Recovery Solution
- Lesson 3: Design a Solution for Data Archiving and Retention
- Lesson 4: Module 10 Review Questions

### **Module 11: Design for High Availability**

- Lesson 1: High Availability
- Lesson 2: Applications in Multiple Azure Regions for High Availability
- Lesson 3: Design HA Applications to Handle Disaster Recovery
- Lesson 4: Module 11 Review Questions

### **Module 12: Design for Cost Optimization**

- Lesson 1: Recommend Solutions for Cost Management
- Lesson 2: Recommendations for Minimizing Costs
- Lesson 3: Cost Optimization Checklists
- Lesson 4: Module 12 Review Questions

### **Module 13: Design an Application Architecture**

- Lesson 1: Recommend Event-Based Cloud Automation on Azure
- Lesson 2: Microservices Architecture on Azure Service Fabric
- Lesson 3: Designing APIs for Microservices
- Lesson 4: Lab
- Lesson 5: Module 13 Review Questions

**Module 14: Design Security for Applications**

- Lesson 1: Security for Applications and Services
- Lesson 2: Recommend a Solution using Key Vault
- Lesson 3: Recommend Solutions using Azure AD Managed Identities
- Lesson 4: Module 14 Review Questions

## Exam AZ-304: Microsoft Azure Architect Design

Candidates for this exam are Azure Solutions Architects 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.

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

AZ-304 Study Areas	Weights
Design monitoring	10-15%
Design identity and security	25-30%
Design data storage	15-20%
Design business continuity	10-15%
Design infrastructure	25-30%

**See:** Exam AZ-304: Microsoft Azure Architect Design: <https://docs.microsoft.com/en-us/learn/certifications/exams/az-304>

## 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.

### Identity

- [Create Azure users and groups in Azure Active Directory<sup>1</sup>](https://docs.microsoft.com/en-us/learn/modules/create-users-and-groups-in-azure-active-directory/)
- [Manage users and groups in Azure Active Directory<sup>2</sup>](https://docs.microsoft.com/en-us/learn/modules/manage-users-and-groups-in-aad/)
- [Secure your Azure resources with role-based access control<sup>3</sup>](https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/)
- [Secure Azure Active Directory users with Multi-Factor Authentication<sup>4</sup>](https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/)
- [Allow users to reset their password with Azure Active Directory self-service password reset<sup>5</sup>](https://docs.microsoft.com/en-us/learn/modules/allow-users-reset-their-password-with-azure-active-directory-self-service-password-reset/)
- [Secure your application by using OpenID Connect and Azure AD<sup>6</sup>](https://docs.microsoft.com/en-us/learn/modules/secure-your-application-by-using-openid-connect-and-azure-ad/)

<sup>1</sup> <https://docs.microsoft.com/en-us/learn/modules/create-users-and-groups-in-azure-active-directory/>

<sup>2</sup> <https://docs.microsoft.com/en-us/learn/modules/manage-users-and-groups-in-aad/>

<sup>3</sup> <https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/>

<sup>4</sup> <https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/>

<sup>5</sup> <https://docs.microsoft.com/en-us/learn/modules/allow-users-reset-their-password-with-azure-active-directory-self-service-password-reset/>

<sup>6</sup> <https://docs.microsoft.com/en-us/learn/modules/secure-your-application-by-using-openid-connect-and-azure-ad/>

## Governance and Compliance

- Analyze costs and create budgets with Azure Cost Management<sup>7</sup>
- Predict costs and optimize spending for Azure<sup>8</sup>
- Control and organize Azure resources with Azure Resource Manager<sup>9</sup>
- Apply and monitor infrastructure standards with Azure Policy<sup>10</sup>
- Create custom roles for Azure resources with role-based access control<sup>11</sup>
- Manage access to an Azure subscription by using Azure role-based access control<sup>12</sup>
- Secure your Azure resources with role-based access control<sup>13</sup>

## Azure Administration

- Core Cloud Services - Manage services with the Azure portal<sup>14</sup>
- Control and organize Azure resources with Azure Resource Manager<sup>15</sup>
- Build Azure Resource Manager templates<sup>16</sup>
- Automate Azure tasks using scripts with PowerShell<sup>17</sup>
- Manage virtual machines with the Azure CLI<sup>18</sup>

## Virtual Networking

- Networking Fundamentals - Principles<sup>19</sup>
- Design an IP addressing schema for your Azure deployment<sup>20</sup>
- Secure and isolate access to Azure resources by using network security groups and service endpoints<sup>21</sup>

## Intersite Connectivity

- Distribute your services across Azure virtual networks and integrate them by using virtual network peering<sup>22</sup>
- Connect your on-premises network to Azure with VPN Gateway<sup>23</sup>

---

<sup>7</sup> <https://docs.microsoft.com/en-us/learn/modules/analyze-costs-create-budgets-azure-cost-management/>

<sup>8</sup> <https://docs.microsoft.com/en-us/learn/modules/predict-costs-and-optimize-spending/>

<sup>9</sup> <https://docs.microsoft.com/en-us/learn/modules/control-and-organize-with-azure-resource-manager/>

<sup>10</sup> <https://docs.microsoft.com/en-us/learn/modules/intro-to-governance/>

<sup>11</sup> <https://docs.microsoft.com/en-us/learn/modules/create-custom-azure-roles-with-rbac/>

<sup>12</sup> <https://docs.microsoft.com/en-us/learn/modules/manage-subscription-access-azure-rbac/>

<sup>13</sup> <https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/>

<sup>14</sup> <https://docs.microsoft.com/en-us/learn/modules/tour-azure-portal/>

<sup>15</sup> <https://docs.microsoft.com/en-us/learn/modules/control-and-organize-with-azure-resource-manager/>

<sup>16</sup> <https://docs.microsoft.com/en-us/learn/modules/build-azure-vm-templates/>

<sup>17</sup> <https://docs.microsoft.com/en-us/learn/modules/automate-azure-tasks-with-powershell/>

<sup>18</sup> <https://docs.microsoft.com/en-us/learn/modules/manage-virtual-machines-with-azure-cli/>

<sup>19</sup> <https://docs.microsoft.com/en-us/learn/modules/network-fundamentals/>

<sup>20</sup> <https://docs.microsoft.com/en-us/learn/modules/design-ip-addressing-for-azure/>

<sup>21</sup> <https://docs.microsoft.com/en-us/learn/modules/secure-and-isolate-with-nsg-and-service-endpoints/>

<sup>22</sup> <https://docs.microsoft.com/en-us/learn/modules/integrate-vnets-with-vnet-peering/>

<sup>23</sup> <https://docs.microsoft.com/en-us/learn/modules/connect-on-premises-network-with-vpn-gateway/>

- Connect your on-premises network to the Microsoft global network by using ExpressRoute<sup>24</sup>

## Network Traffic Management

- Manage and control traffic flow in your Azure deployment with routes<sup>25</sup>
- Improve application scalability and resiliency by using Azure Load Balancer<sup>26</sup>
- Load balance your web service traffic with Application Gateway<sup>27</sup>
- Enhance your service availability and data locality by using Azure Traffic Manager<sup>28</sup>

## Azure Storage

- Create an Azure Storage account<sup>29</sup>
- Secure your Azure Storage<sup>30</sup>
- Optimize storage performance and costs using Blob storage tiers<sup>31</sup>
- Make your application storage highly available with read-access geo-redundant storage<sup>32</sup>
- Copy and move blobs from one container or storage account to another from the command line and in code<sup>33</sup>
- Move large amounts of data to the cloud by using Azure Data Box family<sup>34</sup>
- Monitor, diagnose, and troubleshoot your Azure storage<sup>35</sup>

## Azure Virtual Machines

- Build a scalable application with virtual machine scale sets<sup>36</sup>
- Deploy Azure virtual machines from VHD templates<sup>37</sup>
- Choose the right disk storage for your virtual machine workload<sup>38</sup>
- Add and size disks in Azure virtual machines<sup>39</sup>
- Protect your virtual machine settings with Azure Automation State Configuration<sup>40</sup>

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

<sup>25</sup> <https://docs.microsoft.com/en-us/learn/modules/control-network-traffic-flow-with-routes/>

<sup>26</sup> <https://docs.microsoft.com/en-us/learn/modules/improve-app-scalability-resiliency-with-load-balancer/>

<sup>27</sup> <https://docs.microsoft.com/en-us/learn/modules/load-balance-web-traffic-with-application-gateway/>

<sup>28</sup> <https://docs.microsoft.com/en-us/learn/modules/distribute-load-with-traffic-manager/>

<sup>29</sup> <https://docs.microsoft.com/en-us/learn/modules/create-azure-storage-account/>

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

<sup>31</sup> <https://docs.microsoft.com/en-us/learn/modules/optimize-archive-costs-blob-storage/>

<sup>32</sup> <https://docs.microsoft.com/en-us/learn/modules/ha-application-storage-with-grs/>

<sup>33</sup> <https://docs.microsoft.com/en-us/learn/modules/copy-blobs-from-command-line-and-code/>

<sup>34</sup> <https://docs.microsoft.com/en-us/learn/modules/move-data-with-azure-data-box/>

<sup>35</sup> <https://docs.microsoft.com/en-us/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

<sup>36</sup> <https://docs.microsoft.com/en-us/learn/modules/build-app-with-scale-sets/>

<sup>37</sup> <https://docs.microsoft.com/en-us/learn/modules/deploy-vms-from-vhd-templates/>

<sup>38</sup> <https://docs.microsoft.com/en-us/learn/modules/choose-the-right-disk-storage-for-vm-workload/>

<sup>39</sup> <https://docs.microsoft.com/en-us/learn/modules/add-and-size-disks-in-azure-virtual-machines/>

<sup>40</sup> <https://docs.microsoft.com/en-us/learn/modules/protect-vm-settings-with-dsc/>

## Serverless Computing

- Host a web application with Azure App service<sup>41</sup>
- Stage a web app deployment for testing and rollback by using App Service deployment slots<sup>42</sup>
- Scale an App Service web app to efficiently meet demand with App Service scale up and scale out<sup>43</sup>
- Dynamically meet changing web app performance requirements with autoscale rules<sup>44</sup>
- Capture and view page load times in your Azure web app with Application Insights<sup>45</sup>
- Run Docker containers with Azure Container Instances<sup>46</sup>
- Introduction to the Azure Kubernetes Service<sup>47</sup>

## Data Protection

- Protect your virtual machines by using Azure Backup<sup>48</sup>
- Back up and restore your Azure SQL database<sup>49</sup>
- Protect your Azure infrastructure with Azure Site Recovery<sup>50</sup>
- Protect your on-premises infrastructure from disasters with Azure Site Recovery<sup>51</sup>

## Monitoring

- Analyze your Azure infrastructure by using Azure Monitor logs<sup>52</sup>
- Improve incident response with alerting on Azure<sup>53</sup>
- Monitor the health of your Azure virtual machine by collecting and analyzing diagnostic data<sup>54</sup>
- Monitor, diagnose, and troubleshoot your Azure storage<sup>55</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>56</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.

---

<sup>41</sup> <https://docs.microsoft.com/en-us/learn/modules/host-a-web-app-with-azure-app-service/>

<sup>42</sup> <https://docs.microsoft.com/en-us/learn/modules/stage-deploy-app-service-deployment-slots/>

<sup>43</sup> <https://docs.microsoft.com/en-us/learn/modules/app-service-scale-up-scale-out/>

<sup>44</sup> <https://docs.microsoft.com/en-us/learn/modules/app-service-autoscale-rules/>

<sup>45</sup> <https://docs.microsoft.com/en-us/learn/modules/capture-page-load-times-application-insights/>

<sup>46</sup> <https://docs.microsoft.com/en-us/learn/modules/run-docker-with-azure-container-instances/>

<sup>47</sup> <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-kubernetes-service/>

<sup>48</sup> <https://docs.microsoft.com/en-us/learn/modules/protect-virtual-machines-with-azure-backup/>

<sup>49</sup> <https://docs.microsoft.com/en-us/learn/modules/backup-restore-azure-sql/>

<sup>50</sup> <https://docs.microsoft.com/en-us/learn/modules/protect-infrastructure-with-site-recovery/>

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

<sup>52</sup> <https://docs.microsoft.com/en-us/learn/modules/analyze-infrastructure-with-azure-monitor-logs/>

<sup>53</sup> <https://docs.microsoft.com/en-us/learn/modules/incident-response-with-alerting-on-azure/>

<sup>54</sup> <https://docs.microsoft.com/en-us/learn/modules/monitor-azure-vm-using-diagnostic-data/>

<sup>55</sup> <https://docs.microsoft.com/en-us/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

<sup>56</sup> <https://social.msdn.microsoft.com/Forums/en-US/home?category=windowsazureplatform>

- **Microsoft Learning Community Blog**<sup>57</sup>. Get the latest information about the certification tests and exam study groups.
- **Channel 9**<sup>58</sup>. Channel 9 provides a wealth of informational videos, shows, and events.
- **Azure Tuesdays with Corey**<sup>59</sup>. Corey Sanders answers your questions about Microsoft Azure - Virtual Machines, Web Sites, Mobile Services, Dev/Test etc.
- **Azure Fridays**<sup>60</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>61</sup>. Keep current on what's happening in Azure, including what's now in preview, generally available, news & updates, and more.
- **Azure Documentation**<sup>62</sup>. Stay informed on the latest products, tools, and features. Get information on pricing, partners, support, and solutions.
- **Azure Architecture Center**<sup>63</sup>. The Azure Architecture Center provides best practices for running your workloads on Azure.
- **Azure Reference Architectures**<sup>64</sup>. Architecture diagrams, reference architectures, example scenarios, and solutions for common workloads on Azure.
- **Cloud Design Patterns**<sup>65</sup>. Cloud design patterns for building reliable, scalable, secure applications in the cloud.
- **Tailwind Traders**<sup>66</sup>. A three-tier legacy app re-written for modern cloud app ARM Solution]
- **IoT Scenario Reference Architecture**<sup>67</sup>. Recommendations for architecture for IoT applications on Azure using PaaS (platform-as-a-service) components.
- **Bot Framework Reference Architecture**<sup>68</sup>. An architecture that describes how to build an enterprise-grade conversational bot (chatbot) using the Azure Bot Framework.

<sup>57</sup> <https://www.microsoft.com/en-us/learning/community-blog.aspx>

<sup>58</sup> <https://channel9.msdn.com/>

<sup>59</sup> <https://channel9.msdn.com/Shows/Tuesdays-With-Corey/>

<sup>60</sup> <https://channel9.msdn.com/Shows/Azure-Friday>

<sup>61</sup> <https://azure.microsoft.com/en-us/blog/>

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

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

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

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

<sup>66</sup> <https://github.com/microsoft/ignite-learning-paths-training-ops>

<sup>67</sup> <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/iot>

<sup>68</sup> <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/ai/conversational-bot>



## Module 1 Design a Compute Solution

### Choose an Azure Compute Service

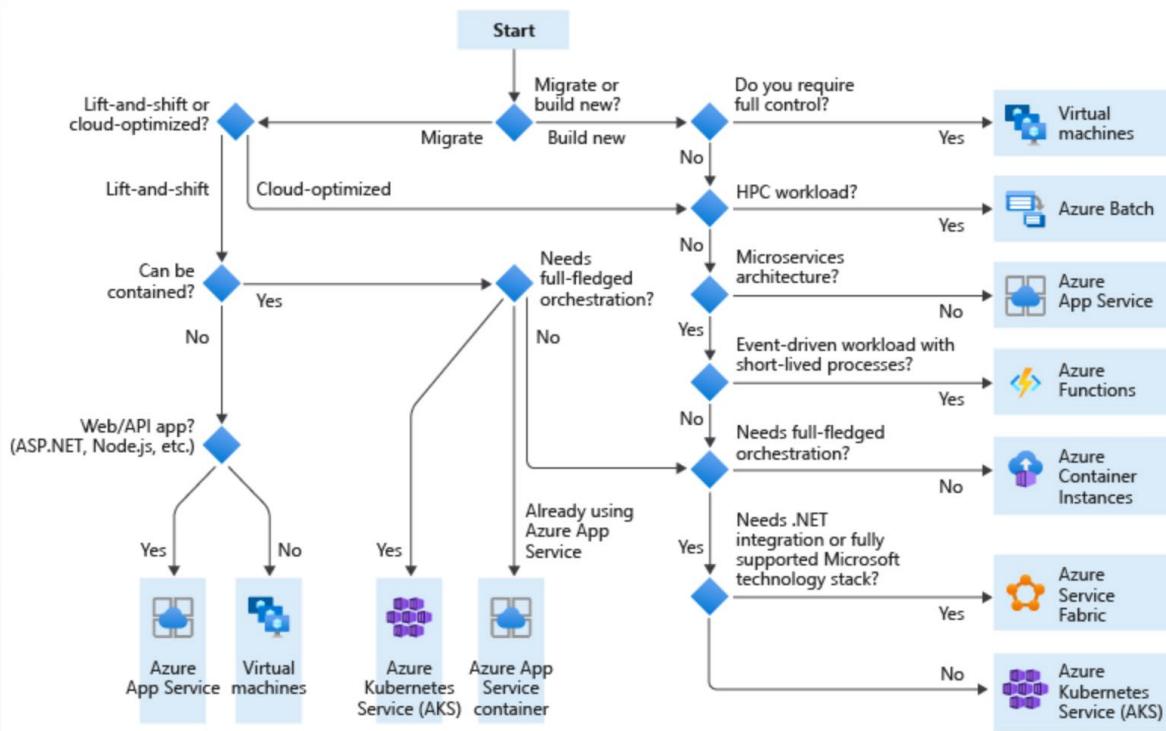
#### Choosing an Azure Compute Service

✓ **NOTE:** This lesson is a review of Azure compute services.

The term *compute* refers to the hosting model for the computing resources that your application runs on. The following flowchart will help you to choose a compute service for your application.

#### Choose a candidate service

Use the following flowchart to select a candidate compute service.



Definitions:

- **Lift and shift** is a strategy for migrating a workload to the cloud without redesigning the application or making code changes. Also called rehosting.
- **Cloud optimized** is a strategy for migrating to the cloud by refactoring an application to take advantage of cloud-native features and capabilities.

The output from this flowchart is a **starting point** for consideration. Next, perform a more detailed evaluation of the service to see if it meets your needs.

## The Features

If you need to review the Azure service features selected in the previous step, see the overview documentation to understand the basics of the service.

- **App Service**<sup>1</sup>. A managed service for hosting web apps, mobile app back ends, RESTful APIs, or automated business processes.
- **Azure Kubernetes Service**<sup>2</sup> (AKS). A managed Kubernetes service for running containerized applications.
- **Batch**<sup>3</sup>. A managed service for running large-scale parallel and high-performance computing (HPC) applications
- **Container Instances**<sup>4</sup>. The fastest and simplest way to run a container in Azure, without having to provision any virtual machines and without having to adopt a higher-level service.

<sup>1</sup> <https://docs.microsoft.com/en-us/azure/app-service/>

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes>

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview>

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview>

- **Virtual machines<sup>5</sup>**. Deploy and manage VMs inside an Azure virtual network.
- **Azure Service Fabric<sup>6</sup>**. Package, deploy, and manage scalable and reliable microservices and containers.

## Hosting Models

Cloud services, including Azure services, generally fall into three categories: IaaS or PaaS. (There is also SaaS, software-as-a-service, which is out of scope for this lesson).

**Infrastructure-as-a-Service** (IaaS) lets you provision individual VMs along with the associated networking and storage components.

**Platform-as-a-Service** (PaaS) provides a managed hosting environment, where you can deploy your application without needing to manage VMs or networking resources. Azure App Service is a PaaS service.

There is a spectrum from IaaS to pure PaaS. For example, Azure VMs can autoscale by using virtual machine scale sets. This automatic scaling capability isn't strictly PaaS, but it's the type of management feature found in PaaS services.

In general, there is a tradeoff between control and ease of management. IaaS gives the most control, flexibility, and portability, but you must provision, configure and manage the VMs and network components you create.

## Service Limits and Cost

Next, perform a more detailed evaluation, looking at the following aspects of the service:

- **Service limits**
- **Cost**
- **SLA**
- **Regional availability**

Based on this analysis, you may find that the initial candidate isn't suitable for your application or workload. In that case, expand your analysis to include other compute services.

The following tables contain additional comparison points, which may be useful when choosing.

Criteria	Virtual Machines	App Service	Service Fabric	Azure Functions	Azure Kubernetes Service	Container Instances	Azure Batch
<b>Application composition</b>	Agnostic	Applications, containers	Services, guest executables, containers	Functions	Containers	Containers	Scheduled jobs

<sup>5</sup> <https://docs.microsoft.com/en-us/azure/virtual-machines/>

<sup>6</sup> <https://docs.microsoft.com/en-us/azure/service-fabric/>

Criteria	Virtual Machines	App Service	Service Fabric	Azure Functions	Azure Kubernetes Service	Container Instances	Azure Batch
<b>Density</b>	Agnostic	Multiple apps per instance via app service plans	Multiple services per VM	Serverless	Multiple containers per node	No dedicated instances	Multiple apps per VM
<b>Minimum number of nodes</b>	1	1	5	Serverless	3 (recommendation for production environments)	No dedicated nodes	1
<b>State management</b>	Stateless or Stateful	Stateless	Stateless or stateful	Stateless	Stateless or Stateful	Stateless	Stateless
<b>Web hosting</b>	Agnostic	Built in	Agnostic	Not applicable	Agnostic	Agnostic	No
<b>Can be deployed to dedicated VNet?</b>	Supported	Supported	Supported	Supported	Supported	Supported	Supported
<b>Hybrid connectivity</b>	Supported	Supported	Supported	Supported	Supported	Not supported	Supported

## Scalability

Criteria	Virtual Machines	App Service	Service Fabric	Azure Functions	Azure Kubernetes Service	Container Instances	Azure Batch
Autoscaling	Virtual machine scale sets	Built-in service	Virtual machine scale sets	Built-in service	Pod auto-scaling, cluster auto-scaling	Not supported	N/A
Load balancer	Azure Load Balancer	Integrated	Azure Load Balancer	Integrated	Azure Load Balancer or Application Gateway	No built-in support	Azure Load Balancer

Criteria	Virtual Machines	App Service	Service Fabric	Azure Functions	Azure Kubernetes Service	Container Instances	Azure Batch
Scale limit	Platform image: 1000 nodes per scale set, Custom image: 600 nodes per scale set	30 instances, 100 with App Service Environment	100 nodes per scale set	200 instances per Function app	100 nodes per cluster (default limit)	20 container groups per subscription (default limit).	20 core limit (default limit).

## Availability

Criteria	Virtual Machines	App Service	Service Fabric	Azure Functions	Azure Kubernetes Service	Container Instances	Azure Batch
SLA	[SLA for Virtual Machines] [sla-vm]	[SLA for App Service] [sla-app-service]	[SLA for Service Fabric] [sla-sf]	[SLA for Functions] [sla-functions]	[SLA for AKS] [sla-acss]	<b>SLA for Container Instances</b> ( <a href="https://azure.microsoft.com/support/legal/sla/container-instances/">https://azure.microsoft.com/support/legal/sla/container-instances/</a> )	[SLA for Azure Batch] [sla-batch]
Multi region failover	Traffic manager	Traffic manager	Traffic manager, Multi-Region Cluster	Azure Front Door	Traffic manager	Not supported	Not Supported

### Summary:

The output from the flowchart at the beginning of this lesson is a starting point for consideration. Next, perform a more detailed evaluation of the service to see if it meets your needs.

# Determine Appropriate Compute Technologies

## Choosing an Azure Compute Option for Microservices

The term compute refers to the hosting model for the computing resources that your application runs on. For a microservices architecture, two approaches are especially popular:

- A **service orchestrator** that manages services running on dedicated nodes (VMs).
- A **serverless architecture** using functions as a service (PaaS).

While these aren't the only options, they are both proven approaches to building microservices. An application might include both approaches.

## Service Orchestrators

An orchestrator handles tasks related to deploying and managing a set of services. These tasks include placing services on nodes, monitoring the health of services, restarting unhealthy services, load balancing network traffic across service instances, service discovery, scaling the number of instances of a service, and applying configuration updates. Popular orchestrators include Kubernetes, Service Fabric, DC/OS, and Docker Swarm.

On the Azure platform, consider the following options:

- **Azure Kubernetes Service (AKS)** is a managed Kubernetes service. AKS provisions Kubernetes and exposes the Kubernetes API endpoints and hosts and manages the Kubernetes control plane, performing automated upgrades, automated patching, autoscaling, and other management tasks. You can think of AKS as being "Kubernetes APIs as a service."
- **Service Fabric** is a distributed systems platform for packaging, deploying, and managing microservices. Microservices can be deployed to Service Fabric as containers, as binary executables, or as Reliable Services. Using the Reliable Services programming model, services can directly use Service Fabric programming APIs to query the system, report health, receive notifications about configuration and code changes, and discover other services.
- Other options such as Docker Enterprise Edition and Mesosphere DC/OS can run in an IaaS environment on Azure. You can find deployment templates on Azure Marketplace

## Containers

Sometimes people talk about containers and microservices as if they were the same thing. While that's not true, you don't need containers to build microservices. Containers do have some benefits that are particularly relevant to microservices, such as:

- **Portability.** A container image is a standalone package that runs without needing to install libraries or other dependencies. That makes them easy to deploy. Containers can be started and stopped quickly, so you can spin up new instances to handle more load or to recover from node failures.
- **Density.** Containers are lightweight compared with running a virtual machine, because they share OS resources. That makes it possible to pack multiple containers onto a single node, which is especially useful when the application consists of many small services.
- **Resource isolation.** You can limit the amount of memory and CPU that is available to a container, which can help to ensure that a runaway process doesn't exhaust the host resources.

## Serverless (Functions as a Service)

With a serverless architecture, you don't manage the VMs or the virtual network infrastructure. Instead, you deploy code and the hosting service handles putting that code onto a VM and executing it. This approach tends to favor small granular functions that are coordinated using event-based triggers. For example, a message being placed onto a queue might trigger a function that reads from the queue and processes the message.

Azure Functions is a serverless compute service that supports various function triggers, including HTTP requests, Service Bus queues, and Event Hubs events. For a complete list,

## Orchestrator or serverless?

Below are some factors to consider when choosing between an orchestrator approach and a serverless approach.

**Manageability** A serverless application is easy to manage, because the platform manages all the compute resources for you. While an orchestrator abstracts some aspects of managing and configuring a cluster, it does not completely hide the underlying VMs. With an orchestrator, you will need to think about issues such as load balancing, CPU and memory usage, and networking.

**Flexibility and control.** An orchestrator gives you a great deal of control over configuring and managing your services and the cluster. The tradeoff is additional complexity. With a serverless architecture, you give up some degree of control because these details are abstracted.

**Portability.** All the orchestrators listed here (Kubernetes, DC/OS, Docker Swarm, and Service Fabric) can run on-premises or in multiple public clouds.

**Application integration.** It can be challenging to build a complex application using a serverless architecture, due to the need to coordinate, deploy, and manage many small independent functions. One option in Azure is to use Azure Logic Apps to coordinate a set of Azure Functions.

**Cost.** With an orchestrator, you pay for the VMs that are running in the cluster. With a serverless application, you pay only for the actual compute resources consumed. In both cases, you need to factor in the cost of any additional services, such as storage, databases, and messaging services.

**Scalability.** Azure Functions scales automatically to meet demand, based on the number of incoming events. With an orchestrator, you can scale out by increasing the number of service instances running in the cluster. You can also scale by adding additional VMs to the cluster.

# Recommend a Solution for Containers

## When to use Azure Kubernetes Service

This topic helps you to decide whether Azure Kubernetes Service (AKS) is the right choice for you.

You'll either approach your decision from a *green fields* or a *lift-and-shift* project point of view. A *green fields* project will allow you to evaluate AKS based on default features. A *lift-and-shift* project will force you to look at which features are best suited to support your migration.

We saw earlier that there are several features that enhance the AKS Kubernetes offering. Each of these features can be a compelling factor in your decision to use AKS.

Feature	Considerations and Decisions
<b>Identity and security management</b>	Do you already use existing Azure resources and make use of Azure AD? You can configure an AKS cluster to integrate with Azure AD and reuse existing identities and group membership.
<b>Integrated logging and monitoring</b>	AKS includes Azure Monitor for containers to provide performance visibility of the cluster. With a custom Kubernetes installation, you normally decided on a monitoring solution that requires installation and configuration.
<b>Auto Cluster node and pod scaling</b>	Deciding when to scale up or down in large containerization environment is tricky. AKS supports two auto cluster scaling options. You can use either the horizontal pod autoscaler or the cluster autoscaler to scale the cluster. The horizontal pod autoscaler watches the resource demand of pods and will increase pods to match demand. The cluster autoscaler component watches for pods that can't be scheduled because of node constraints. It will automatically scale cluster nodes to deploy scheduled pods.
<b>Cluster node upgrades</b>	Do you want to reduce the number of cluster management tasks? AKS manages Kubernetes software upgrades and the process of cordoning off nodes and draining them to minimize disruption to running applications. Once done, these nodes are upgraded one by one.
<b>GPU enabled nodes</b>	Do you have compute-intensive or graphic-intensive workloads? AKS supports GPU enabled node pools.
<b>Storage volume support</b>	Is your application stateful, and does it require persisted storage? AKS supports both static and dynamic storage volumes. Pods can attach and reattach to these storage volumes as they're created or rescheduled on different nodes.

Feature	Considerations and Decisions
<b>Virtual network support</b>	Do you need pod to pod network communication or access to on-premise networks from your AKS cluster? An AKS cluster can be deployed into an existing virtual network with ease.
<b>Ingress with HTTP application routing support</b>	Do you need to make your deployed applications publicly available? The HTTP application routing add-on makes it easy to access AKS cluster deployed applications.
<b>Docker image support</b>	Do you already use Docker images for your containers? AKS by default supports the Docker file image format.
<b>Private container registry</b>	Do you need a private container registry? AKS integrates with Azure Container Registry (ACR). You aren't limited to ACR though, you can use other container repositories, public, or private.

All the above features are configurable either when you create the cluster or following deployment.

## When to use Azure Container Instances

Azure Container Instances offers a fast and simple 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 solution for any scenario that can operate in isolated containers, including simple applications, task automation, and build jobs.

✓ **Important:** 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).

## 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.

## Persistent storage

To retrieve and persist state with Azure Container Instances, Microsoft offers direct mounting of Azure Files shares backed by Azure Storage.

## 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. For Windows container deployments, use images based on common Windows base images.

## Co-scheduled groups

Azure Container Instances supports scheduling of multi-container groups that share a host machine, local network, storage, and lifecycle. This enables you to combine your main application container with other supporting role containers, such as logging sidecars.

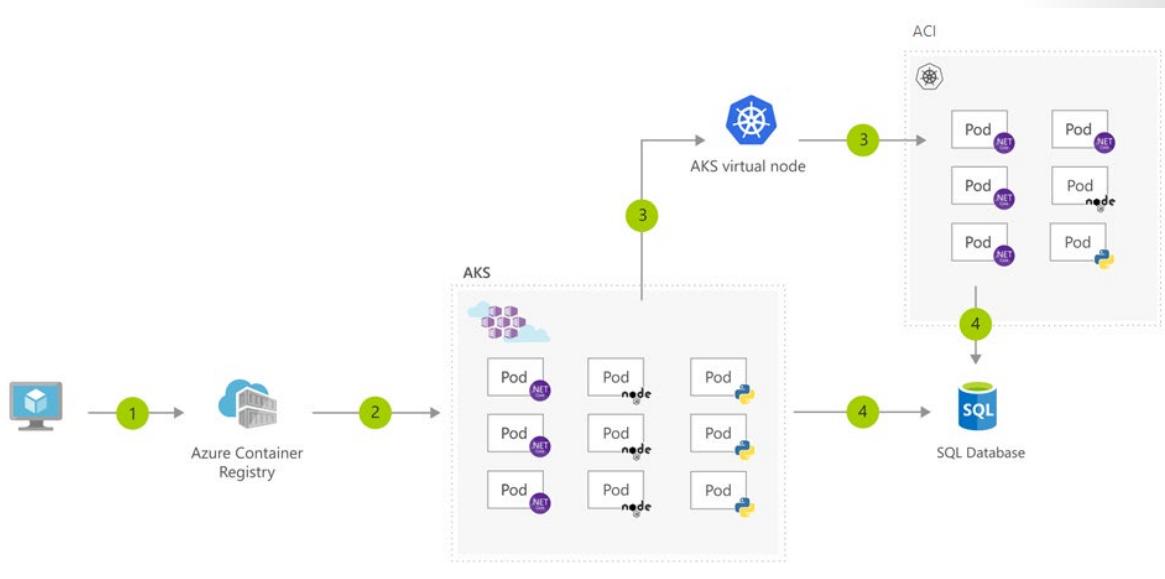
## Virtual network deployment

Currently available for production workloads in a subset of Azure regions, this feature of Azure Container Instances enables deployment of container instances into an Azure virtual network. By deploying container instances into a subnet within your virtual network, they can communicate securely with other resources in the virtual network, including those that are on premises (through VPN gateway or ExpressRoute).

## Bursting from AKS with ACI

Use the AKS virtual node to provision pods inside ACI that start in seconds. This enables AKS to run with just enough capacity for your average workload. As you run out of capacity in your AKS cluster, scale out additional pods in ACI without any additional servers to manage.

## Architecture



## Data Flow

1. User registers container in Azure Container Registry
2. Container images are pulled from the Azure Container Registry
3. AKS virtual node, a Virtual Kubelet implementation, provisions pods inside ACI from AKS when traffic comes in spikes.
4. AKS and ACI containers write to shared data store

# Provisioning Solutions for Azure Compute Infrastructure

## Provisioning Solutions for Azure Compute Infrastructure

Creating and managing compute resources manually requires much administration time and becomes a repetitive task. When administrators must do the same task regularly, mistakes can happen. You want to identify a way to automate the provisioning and management of compute resources. You need to research some of the tools that you can use to provision compute on Azure.

### Why automate compute provisioning?

It takes a long time to implement an architecture with many servers manually. You need to configure the operating system, install software, configure that software, and apply updates. You also need to do these tasks for each virtual machine. The tasks can become complex. When you have to carry out complex tasks many times, it's easy to make mistakes.

You might also need to redeploy your architecture, for example, to recover from an attack or disaster. Your architecture might need to support software testing, so you need to be able to redeploy it for every testing cycle. If your manual deployment takes several hours, it isn't ideal.

You need some way to automate the deployment of virtual machines to deal with these issues and difficulties. For each virtual machine, such a solution must be able to:

- Configure the virtual machine. For example, in Azure you need to specify an image from Azure Marketplace, a tier, a size, IP addresses, and other values.
- Configure the operating system for the virtual machine. For example, if the operating system includes a firewall, you must be able to set firewall rules that filter traffic.
- Install software. For example, you might need to install a web server or a database server.
- Apply updates. For example, you might need to apply service packs or hotfixes to the operating system and the installed software.

To reduce the complexity of a deployment configuration, create a complete architecture in the form of a script or a configuration file. Then deploy it in a single operation. This way, you can automate your configuration to reduce mistakes and accelerate deployment. You'll help your organization become more productive and cost effective.

### Custom Scripts

The custom script extension downloads and runs scripts on Azure virtual machines. This tool is useful for post-deployment configuration, software installation, or any other configuration or management task.

You can have a PowerShell script that's on your local file server, GitHub, Azure Storage, or other locations that are accessible to your virtual machine. The extension looks for the script that should be run on the virtual machine. The script is downloaded and then executed on the target virtual machine to apply the changes introduced by the script. You add a custom script extension to a virtual machine through Azure Resource Manager templates, PowerShell, or the Azure CLI.

The following custom script extension configuration can be added to an Azure Resource Manager template for a virtual machine. Use the `fileUris` property to point to your script file.

```
{  
    "apiVersion": "2019-06-01",  
    "type": "Microsoft.Compute/virtualMachines/extensions",  
    "name": "[concat(variables('virtual machineName'), '/', 'InstallWebServer')]",  
    "location": "[parameters('location')]",  
    "dependsOn": [  
        "[concat('Microsoft.Compute/virtualMachines/', variables('virtual  
machineName'))]"  
    ],  
    "properties": {  
        "publisher": "Microsoft.Compute",  
        "type": "CustomScriptExtension",  
        "typeHandlerVersion": "1.7",  
        "autoUpgradeMinorVersion": true,  
        "settings": {  
            "fileUris": [  
                "https://your-potential-file-location.com/your-script-file.  
ps1"  
            ],  
            "commandToExecute": "powershell.exe -ExecutionPolicy Unre-  
stricted -File your-script-file.ps1"  
        }  
    }  
}
```

## Desired State Configuration Extensions

Desired State Configuration (DSC) extensions make it possible for you to deal with the configurations on your infrastructure that might need more complex installation procedures, such as reboots. DSC helps you define a state for your machines instead of writing detailed manual instructions on how to achieve that state for each machine. State configurations are relatively easy to read and implement.

By using a DSC extension handler, which you can define for a virtual machine, you can enforce your states. The configurations for your states can be in various places, such as Azure Blob storage or your internal file storage. The DSC extension handler grabs the configuration and implements the state on the target virtual machine. If reboots are necessary for a configuration, DSC continues to execute the state configuration after the reboots are completed.

The following example defines a DSC extension handler for a virtual machine in an Azure Resource Manager template. The `script` property points to a configuration script in blob storage.

```
{  
    "type": "Microsoft.Compute/virtualMachines/extensions",  
    "name": "Microsoft.Powershell.DSC",  
    "apiVersion": "2018-06-30",  
    "location": "your-region",  
    "dependsOn": [  
        "[concat('Microsoft.Compute/virtualMachines/', parameters('virtu-  
al machineName'))]"  
    ],
```

```
"properties": {
    "publisher": "Microsoft.PowerShell",
    "type": "DSC",
    "typeHandlerVersion": "2.77",
    "autoUpgradeMinorVersion": true,
    "settings": {
        "configuration": {
            "url": "https://demo.blob.core.windows.net/iisin-
stall.zip",
            "script": "IisInstall.ps1",
            "function": "IISInstall"
        }
    },
    "protectedSettings": {
        "configurationUrlSasToken": "odLPL/U1p91vcnp..."
    }
}
```

## Azure Automation State Configuration

Azure automation state configuration is the service you use to make sure that your DSC configurations are managed properly and deployed across your nodes (virtual machines). Azure automation state configuration works with both Azure virtual machines and machines on-premises. It also works with machines on other cloud providers. Through an intuitive Azure portal process, you can apply configurations to all your nodes.

The screenshot shows the Azure portal interface for managing state configurations. At the top, there's a navigation bar with 'Home > Automation Accounts > automation - State configuration (DSC)'. Below this is a title bar for 'automation - State configuration (DSC) Automation Account'. The main area has tabs for 'Nodes' (selected), 'Configurations', 'Compiled configurations', and 'Gallery'. A summary section shows 'Configuration status' with 1 node: 0 Failed, 0 Pending, 0 Not Compliant, 0 In Progress, 0 Unresponsive, and 1 Compliant. Below this are filters for 'Nodes', 'Status', 'Node configuration', and 'VM DSC extension version'. A table at the bottom lists one node: ContosoVM1, Status: Compliant, Node Configuration: TestConfig.NotWebServer, Last Seen: 7/29/2018, 2:15 PM, Version: 2.76.0.0.

Azure automation state configuration makes it possible for you to ensure that all target machines are assigned the correct configurations automatically. It also ensures that each machine reports back on what its current state is and shows whether it has achieved the desired state. You can send this information for reporting and for further decision making. You can interact with Azure automation state configuration through the Azure portal or through Azure PowerShell.

## Chef

A Chef server can handle 10,000 nodes (machines) at a time. Chef makes it possible for you to automate the deployment of your infrastructure and fit it into your workflow, whether on-premises or in the cloud.

A Chef server is typically hosted for you and runs as a service. Chef works by using the Chef server to manage your recipes. Recipes are commands to run to achieve a configuration. Use Chef's knife tool to deploy virtual machines and simultaneously apply recipes to them. You install the knife tool on your admin workstation, which is the machine where you create policies and execute commands. Then run your knife commands from your admin workstation.

The following example shows how a knife command can be used to create a virtual machine on Azure. The command simultaneously applies a recipe that installs a web server on the machine.

```
knife azurerm server create `  
  --azure-resource-group-name rg-chefdeployment `  
  --azure-storage-account store `  
  --azure-vm-name chefvm `  
  --azure-vm-size 'Standard_DS2_v2' `  
  --azure-service-location 'eastus' `  
  --azure-image-reference-offer 'WindowsServer' `  
  --azure-image-reference-publisher 'MicrosoftWindowsServer' `  
  --azure-image-reference-sku '2016-Datacenter' `  
  --azure-image-reference-version 'latest' `  
  -x myuser `  
  -P yourPassword `  
  --tcp-endpoints '80,3389' `  
  --chef-daemon-interval 1 `  
  -r "recipe[webserver]"
```

You can also use the Chef extension to apply recipes to the target machines. The following example defines a Chef extension for a virtual machine in an Azure Resource Manager template. It points to a Chef server by using the `chef_server_url` property. It points to a recipe to run on the virtual machine to put it in the desired state.

```
{  
  "type": "Microsoft.Compute/virtualMachines/extensions",  
  "name": "[concat(variables('virtual machineName'), '/', variables('virtual  
  machineExtensionName'))]",  
  "apiVersion": "2015-05-01-preview",  
  "location": "[parameters('location')]",  
  "dependsOn": [  
    "[concat('Microsoft.Compute/virtualMachines/', variables('virtual  
  machineName'))]"  
  ],  
  "properties": {  
    "publisher": "Chef.Bootstrap.WindowsAzure",  
    "type": "LinuxChefClient",  
    "typeHandlerVersion": "1210.12",  
    "settings": {  
      "bootstrap_options": {  
        "chef_node_name": "chef_node_name",  
        "chef_server_url": "chef_server_url",  
        "validation_client_name": "validation_client_name"  
      },  
      "runlist": "recipe[your-recipe]",  
      "validation_key_format": "validation_key_format",  
    }
```

```
        "chef_service_interval": "chef_service_interval",
        "bootstrap_version": "bootstrap_version",
        "bootstrap_channel": "bootstrap_channel",
        "daemon": "service"
    },
    "protectedSettings": {
        "validation_key": "validation_key",
        "secret": "secret"
    }
}
```

A recipe might look like the one that follows. The recipe installs an IIS web server.

```
#install IIS on the node.
powershell_script 'Install IIS' do
  action :run
  code 'add-windowsfeature Web-Server'
end

service 'w3svc' do
  action [ :enable, :start ]
end
```

## Terraform

Terraform is an open-source infrastructure-as-code software tool. You can create infrastructures by using Hashicorp Configuration Language (HCL). This language is created by Hashicorp. You can also use JSON. Terraform lets you create relatively easy-to-read script templates that define what type of resources to create, regardless of the cloud service provider. You can build your environments by using different cloud service providers, such as Microsoft Azure and Amazon Web Services (AWS). This way you can ensure that your environments are identical across cloud providers. The process requires you to install Terraform, either locally or on Azure. You can then use Terraform to execute a Terraform script.

The following Terraform script example provisions a virtual machine on Azure:

```
# Configure the Microsoft Azure as a provider
provider "azurerm" {
  subscription_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
  client_id      = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
  client_secret   = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
  tenant_id       = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}

# Create a resource group
resource "azurerm_resource_group" "myterraformgroup" {
  name      = "myResourceGroup"
  location  = "eastus"

  tags = {
    environment = "Terraform Demo"
```

```
        }
    }

# Create the virtual machine
resource "azurerm_virtual_machine" "myterraformvirtual machine" {
    name                  = "myvirtual machine"
    location              = "eastus"
    resource_group_name   = "${azurerm_resource_group.myterraformgroup.name}"
    network_interface_ids = ["${azurerm_network_interface.myterraformnic.id}"]
    virtual_machine_size      = "Standard_DS1_v2"

    storage_os_disk {
        name          = "myOsDisk"
        caching       = "ReadWrite"
        create_option = "FromImage"
        managed_disk_type = "Premium_LRS"
    }

    storage_image_reference {
        publisher = "Canonical"
        offer     = "UbuntuServer"
        sku       = "16.04.0-LTS"
        version   = "latest"
    }

    os_profile {
        computer_name  = "myvirtual machine"
        admin_username = "azureuser"
    }

    os_profile_linux_config {
        disable_password_authentication = true
        ssh_keys {
            path      = "/home/azureuser/.ssh/authorized_keys"
            key_data = "ssh-rsa AAAAB3Nz{snip}hwhaa6h"
        }
    }

    boot_diagnostics {
        enabled      = "true"
        storage_uri = "${azurerm_storage_account.mystorageaccount.primary_blob_endpoint}"
    }

    tags = {
        environment = "Terraform Demo"
    }
}
```

To use this script, run the following command by using Terraform:

```
terraform apply
```

## Azure Resource Manager templates

Azure Resource Manager templates are JSON files that you can use to define the Azure resources you want to provision in Azure through object notation. You can define an entire infrastructure this way. They're relatively easy to read and work with, based on your exposure to JSON.

With Azure Resource Manager templates, you can make sure that your deployments are consistent. You can ensure, for example, that all virtual machines you create have the same properties. You can also embed extensions into virtual machines in a template to make sure that their configuration is the same. You deploy any Azure Resource Manager template through Azure PowerShell, the Azure CLI, or the Azure portal. Test Azure Resource Manager templates before they're deployed. When you test your deployment, you ensure that your template is something Azure can deploy before you attempt a real deployment.

The following example shows how a virtual machine is defined in an Azure Resource Manager template. You can see the virtual machine type, the operating system, and its storage details among other things.

```
{
  "type": "Microsoft.Compute/virtualMachines",
  "apiVersion": "2018-10-01",
  "name": "[variables('virtual machineName')]",
  "location": "[parameters('location')]",
  "dependsOn": [
    "[resourceId('Microsoft.Storage/storageAccounts/', variables('storage-
AccountName'))]",
    "[resourceId('Microsoft.Network/networkInterfaces/', variables('nic-
Name'))]"
  ],
  "properties": {
    "hardwareProfile": {
      "virtualMachineSize": "Standard_A2"
    },
    "osProfile": {
      "computerName": "[variables('virtual machineName')]",
      "adminUsername": "[parameters('adminUsername')]",
      "adminPassword": "[parameters('adminPassword')]"
    },
    "storageProfile": {
      "imageReference": {
        "publisher": "MicrosoftWindowsServer",
        "offer": "WindowsServer",
        "sku": "[parameters('windowsOSVersion')]",
        "version": "latest"
      },
      "osDisk": {
        "createOption": "FromImage"
      },
      "dataDisks": [
        {
          "diskSizeGB": 1023,
          "lun": 0,
        }
      ]
    }
  }
}
```

```
        "createOption": "Empty"
    }
]
},
"networkProfile": {
    "networkInterfaces": [
        {
            "id": "[resourceId('Microsoft.Network/networkInterfaces', variables('nicName'))]"
        }
    ]
},
"diagnosticsProfile": {
    "bootDiagnostics": {
        "enabled": true,
        "storageUri": "[reference(resourceId('Microsoft.Storage/storageAccounts/', variables('storageAccountName'))).primaryEndpoints.blob]"
    }
}
}
```

## Module 1 Review Questions

### Module 1 Review Questions



#### Review Question 1

You are designing a container solution in Azure that will include two containers. One container will host a web API that will be available to the public. The other container will perform health monitoring of the web API and will remain private. The two containers will be deployed together as a group.

You need to recommend a compute service for the containers. The solution must minimize costs and maintenance overhead.

What should you include in your recommendation?

- Azure Kubernetes Service (AKS)
- Azure Container Instances
- Azure Container registries
- Azure Service Fabric

#### Review Question 2

You are designing a solution for a company to deploy software for testing and production.

The solution must meet the following requirements:

- Applications must be deployed to several different environments and must run without installation dependencies.
- Existing published applications must be ported to the new solution.
- Application developers must be given flexibility when designing the architecture for their code.

What should you include in your solution for hosting applications?

- Azure Kubernetes Service (AKS)
- Azure Container Instances
- Azure Logic App
- Azure Batch

## Review Question 3

You are recommending solution for an organization that wants to run an image rendering application in Azure.

What is the best service to use to run the workload?

- Azure Kubernetes Service (AKS)
- Azure Container Instances
- Azure Function App
- Azure Batch Service

# Answers

## Review Question 1

You are designing a container solution in Azure that will include two containers. One container will host a web API that will be available to the public. The other container will perform health monitoring of the web API and will remain private. The two containers will be deployed together as a group.

You need to recommend a compute service for the containers. The solution must minimize costs and maintenance overhead.

What should you include in your recommendation?

- Azure Kubernetes Service (AKS)
- Azure Container Instances
- Azure Container registries
- Azure Service Fabric

*Explanation*

*Correct Answer: Azure Container Instances. Azure Container Instances (ACI) supports individual containers and multi-container groups as well as sidecars and health monitoring*

## Review Question 2

You are designing a solution for a company to deploy software for testing and production.

The solution must meet the following requirements:

What should you include in your solution for hosting applications?

- Azure Kubernetes Service (AKS)
- Azure Container Instances
- Azure Logic App
- Azure Batch

*Explanation*

*Correct Answer: Azure Kubernetes Service (AKS). Azure Kubernetes Service (AKS) provides a managed container service that gives architectural flexibility to the development team.*

## Review Question 3

You are recommending solution for an organization that wants to run an image rendering application in Azure.

What is the best service to use to run the workload?

- Azure Kubernetes Service (AKS)
- Azure Container Instances
- Azure Function App
- Azure Batch Service

*Explanation*

*Correct Answer: Azure Batch Service. Azure Batch Service uses a pool of compute resources (VMs) to carry out the batch process in parallel. Azure Batch Service is intended for running parallel processes.*

## Module 2 Design a Network Solution

### Planning Virtual Networks

#### Planning for Virtual Networks

The information in this lesson is most helpful if you're already familiar with virtual networks and have some experience working with them.

For a review of the fundamental elements of virtual networking, see below:

- **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.
- **Regions:** VNet is scoped to a single region/location; however, multiple virtual networks from different regions can be connected using Virtual Network Peering.
- **Subscription:** VNet is scoped to a subscription. You can implement multiple virtual networks within each Azure subscription and Azure region.

### Naming and Regions

All Azure resources have a name. The name must be unique within a scope, that may vary for each resource type. For example, the name of a virtual network must be unique within a resource group, but can be duplicated within a subscription or Azure region. Defining a naming convention that you can use consistently when naming resources is helpful when managing several network resources over time.

## Regions

All Azure resources are created in an Azure region and subscription. A resource can only be created in a virtual network that exists in the same region and subscription as the resource. You can, however, connect virtual networks that exist in different subscriptions and regions. When deciding which region(s) to deploy resources in, consider where consumers of the resources are physically located:

- Consumers of resources typically want the lowest network latency to their resources.
- Do you have data residency, sovereignty, compliance, or resiliency requirements? If so, choosing the region that aligns to the requirements is critical.
- Do you require resiliency across Azure Availability Zones within the same Azure region for the resources you deploy? You can deploy resources, such as virtual machines (VM) to different availability zones within the same virtual network. Not all Azure regions support availability zones however.

## Segmentation

You can create multiple virtual networks per subscription and per region. You can create multiple subnets within each virtual network. The considerations seen below will help you determine how many virtual networks and subnets you require:

## Virtual networks

A virtual network is a virtual, isolated portion of the Azure public network. Each virtual network is dedicated to your subscription. Things to consider when deciding whether to create one virtual network, or multiple virtual networks in a subscription:

- **Do any organizational security requirements exist for isolating traffic into separate virtual networks?** You can choose to connect virtual networks or not. If you connect virtual networks, you can implement a network virtual appliance, such as a firewall, to control the flow of traffic between the virtual networks.
- **Do any organizational requirements exist for isolating virtual networks into separate subscriptions or regions?**
- **How many network interfaces and private IP addresses do you require in a virtual network?** Each network interface has one or more private IP addresses assigned to it. There are **limits<sup>1</sup>** to the number of network interfaces and private IP addresses that you can have within a virtual network.
- **Do you want to connect the virtual network to another virtual network or on-premises network?** You may choose to connect some virtual networks to each other or on-premises networks, but not others. Each virtual network that you connect to another virtual network, or on-premises network, must have a unique address space. Each virtual network has one or more public or private address ranges assigned to its address space. An address range is specified in classless internet domain routing (CIDR) format, such as 10.0.0.0/16.
- **Do you have any organizational administration requirements for resources in different virtual networks?** If so, you might separate resources into separate virtual network to simplify permission assignment to individuals in your organization or to assign different policies to different virtual networks.

---

<sup>1</sup> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits?toc=/azure/virtual-network/toc.json>

## Subnets

A virtual network can be segmented into one or more subnets up to the limits. Things to consider when deciding whether to create one subnet, or multiple virtual networks in a subscription:

- Each subnet must have a unique address range, specified in CIDR format, within the address space of the virtual network. The address range cannot overlap with other subnets in the virtual network.
- If you plan to deploy some Azure service resources into a virtual network, they may require, or create, their own subnet, so there must be enough unallocated space for them to do so. For example, if you connect a virtual network to an on-premises network using an Azure VPN Gateway, the virtual network must have a dedicated subnet for the gateway.
- Azure routes network traffic between all subnets in a virtual network, by default. You can override Azure's default routing to prevent Azure routing between subnets, or to route traffic between subnets through a network virtual appliance, for example. If you require that traffic between resources in the same virtual network flow through a network virtual appliance (NVA), deploy the resources to different subnets.
- You can limit access to Azure resources such as an Azure storage account or Azure SQL database, to specific subnets with a virtual network service endpoint. Further, you can deny access to the resources from the internet. You may create multiple subnets, and enable a service endpoint for some subnets, but not others. Learn more about service endpoints, and the Azure resources you can enable them for.
- You can associate zero or one network security group to each subnet in a virtual network. You can associate the same, or a different, network security group to each subnet. Each network security group contains rules, which allow or deny traffic to and from sources and destinations.

## Network Security

You can filter network traffic to and from resources in a virtual network using network security groups and network virtual appliances. You can control how Azure routes traffic from subnets. You can also limit who in your organization can work with resources in virtual networks.

### Traffic filtering

- You can filter network traffic between resources in a virtual network using a network security group, an NVA that filters network traffic, or both. When using an NVA, you also create custom routes to route traffic from subnets to the NVA.
- A network security group contains several default security rules that allow or deny traffic to or from resources. A network security group can be associated to a network interface, the subnet the network interface is in, or both. To simplify management of security rules, it's recommended that you associate a network security group to individual subnets, rather than individual network interfaces within the subnet, whenever possible.
- If different VMs within a subnet need different security rules applied to them, you can associate the network interface in the VM to one or more application security groups. A security rule can specify an application security group in its source, destination, or both. That rule then only applies to the network interfaces that are members of the application security group.
- Azure creates several default security rules within each network security group. One default rule allows all traffic to flow between all resources in a virtual network. To override this behavior, use network security groups, custom routing to route traffic to an NVA, or both.

**✓ Note:**

You can view sample designs for implementing a perimeter network (also known as a DMZ) between Azure and the internet using an **NVA**<sup>2</sup>.

## Traffic routing

Azure creates several default routes for outbound traffic from a subnet. You can override Azure's default routing by creating a route table and associating it to a subnet. Common reasons for overriding Azure's default routing are:

- Because you want traffic between subnets to flow through an NVA.
- Because you want to force all internet-bound traffic through an NVA, or on-premises, through an Azure VPN gateway. Forcing internet traffic on-premises for inspection and logging is often referred to as forced tunneling.

## Connectivity

You can connect a virtual network to other virtual networks using virtual network peering, or to your on-premises network, using an Azure VPN gateway.

### Peering

When using virtual network peering, the virtual networks can be in the same, or different, supported Azure regions. The virtual networks can be in the same or different Azure subscriptions (even subscriptions belonging to different Azure Active Directory tenants). Bandwidth between resources in virtual networks peered in the same region is the same as if the resources were in the same virtual network.

### VPN gateway

You can use an Azure VPN Gateway to connect a virtual network to your on-premises network using a site-to-site VPN, or using a dedicated connection with Azure ExpressRoute.

You can combine peering and a VPN gateway to create hub and spoke networks, where spoke virtual networks connect to a hub virtual network, and the hub connects to an on-premises network, for example.

### Name resolution

Resources in one virtual network cannot resolve the names of resources in a peered virtual network using Azure's built-in DNS. To resolve names in a peered virtual network, deploy your own DNS server, or use Azure DNS private domains. Resolving names between resources in a virtual network and on-premises networks also requires you to deploy your own DNS server.

## Permissions and Policy

Azure utilizes role based access control (RBAC) to resources.

---

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz?toc=%2Fazure%2Fvirtual-network%2Ftoc.json>

## Permissions

Permissions are assigned to a scope in the following hierarchy: management group, subscription, resource group, and individual resource.

To work with Azure virtual networks and all of their related capabilities such as peering, network security groups, service endpoints, and route tables, you can assign members of your organization to the built-in Owner, Contributor, or Network contributor roles, and then assign the role to the appropriate scope

## Policy

Azure Policy enables you to create, assign, and manage policy definitions. Policy definitions enforce different rules over your resources, so the resources stay compliant with your organizational standards and service level agreements. Azure Policy runs an evaluation of your resources, scanning for resources that are not compliant with the policy definitions you have. For example, you can define and apply a policy that allows creation of virtual networks in only a specific resource group or region. Another policy can require that every subnet has a network security group associated to it. The policies are then evaluated when creating and updating resources.

Policies are applied to the following hierarchy: management group, subscription, and resource group.

# Recommend a Solution for Network Addressing and Name Resolution

## Name Resolution for Resources in Azure Virtual Networks

When resources deployed in virtual networks need to resolve domain names to internal IP addresses, they can use one of three methods:

- **Azure DNS private zones**
- **Azure-provided name resolution**
- **Name resolution that uses your own DNS server** (which might forward queries to the Azure-provided DNS servers)

The following table illustrates scenarios and corresponding name resolution solutions:

- ✓ **Note** Azure DNS private zones is the preferred solution and gives you flexibility in managing your DNS zones and records
- ✓ **Note** If you use Azure Provided DNS then appropriate DNS suffix will be automatically applied to your virtual machines. For all other options you must either use Fully Qualified Domain Names (FQDN) or manually apply appropriate DNS suffix to your virtual machines.

Scenario	Solution	DNS Suffix
<b>Name resolution between VMs located in the same virtual network, or Azure Cloud Services role instances in the same cloud service.</b>	Azure DNS private zones or Azure-provided name resolution	Hostname or FQDN
<b>Name resolution between VMs in different virtual networks or role instances in different cloud services.</b>	Azure DNS private zones or, Customer-managed DNS servers forwarding queries between virtual networks for resolution by Azure (DNS proxy). See Name resolution using your own DNS server.	FQDN only
<b>Name resolution from an Azure App Service (Web App, Function, or Bot) using virtual network integration to role instances or VMs in the same virtual network.</b>	Customer-managed DNS servers forwarding queries between virtual networks for resolution by Azure (DNS proxy). See Name resolution using your own DNS server.	FQDN only
<b>Name resolution from App Service Web Apps to VMs in the same virtual network.</b>	Customer-managed DNS servers forwarding queries between virtual networks for resolution by Azure (DNS proxy). See Name resolution using your own DNS server.	FQDN only

Scenario	Solution	DNS Suffix
<b>Name resolution from App Service Web Apps in one virtual network to VMs in a different virtual network.</b>	Customer-managed DNS servers forwarding queries between virtual networks for resolution by Azure (DNS proxy). See Name resolution using your own DNS server.	FQDN only
<b>Resolution of on-premises computer and service names from VMs or role instances in Azure.</b>	Customer-managed DNS servers (on-premises domain controller, local read-only domain controller, or a DNS secondary synced using zone transfers, for example). See Name resolution using your own DNS server.	FQDN only
<b>Resolution of Azure hostnames from on-premises computers.</b>	Forward queries to a customer-managed DNS proxy server in the corresponding virtual network, the proxy server forwards queries to Azure for resolution. See Name resolution using your own DNS server.	FQDN only
<b>Reverse DNS for internal IPs.</b>	Azure DNS private zones or Azure-provided name resolution or Name resolution using your own DNS server.	Not applicable
<b>Name resolution between VMs or role instances located in different cloud services, not in a virtual network.</b>	Not applicable. Connectivity between VMs and role instances in different cloud services is not supported outside a virtual network.	Not applicable

## Azure-Provided Name Resolution

Azure provided name resolution provides only basic authoritative DNS capabilities. If you use this option the DNS zone names and records will be automatically managed by Azure and you will not be able to control the DNS zone names or the life cycle of DNS records. If you need a fully featured DNS solution for your virtual networks you must use **Azure DNS private zones** or **Customer-managed DNS servers**.

Azure provides internal name resolution for VMs and role instances that reside within the same virtual network or cloud service. VMs and instances in a cloud service share the same DNS suffix, so the host name alone is sufficient. But in virtual networks deployed using the classic deployment model, different cloud services have different DNS suffixes. In this situation, you need the FQDN to resolve names between different cloud services.

In virtual networks deployed using the Azure Resource Manager deployment model, the DNS suffix is consistent across all virtual machines within a virtual network, so the FQDN is not needed. DNS names can be assigned to both VMs and network interfaces.

## Azure-provided name resolution features

Azure-provided name resolution includes the following features:

- No configuration is required.
- High availability. You don't need to create and manage clusters of your own DNS servers.
- You can use the service in conjunction with your own DNS servers, to resolve both on-premises and Azure host names.
- You can use name resolution between VMs and role instances within the same cloud service, without the need for an FQDN.
- You can use name resolution between VMs in virtual networks that use the Azure Resource Manager deployment model, without need for an FQDN. Virtual networks in the classic deployment model require an FQDN when you are resolving names in different cloud services.

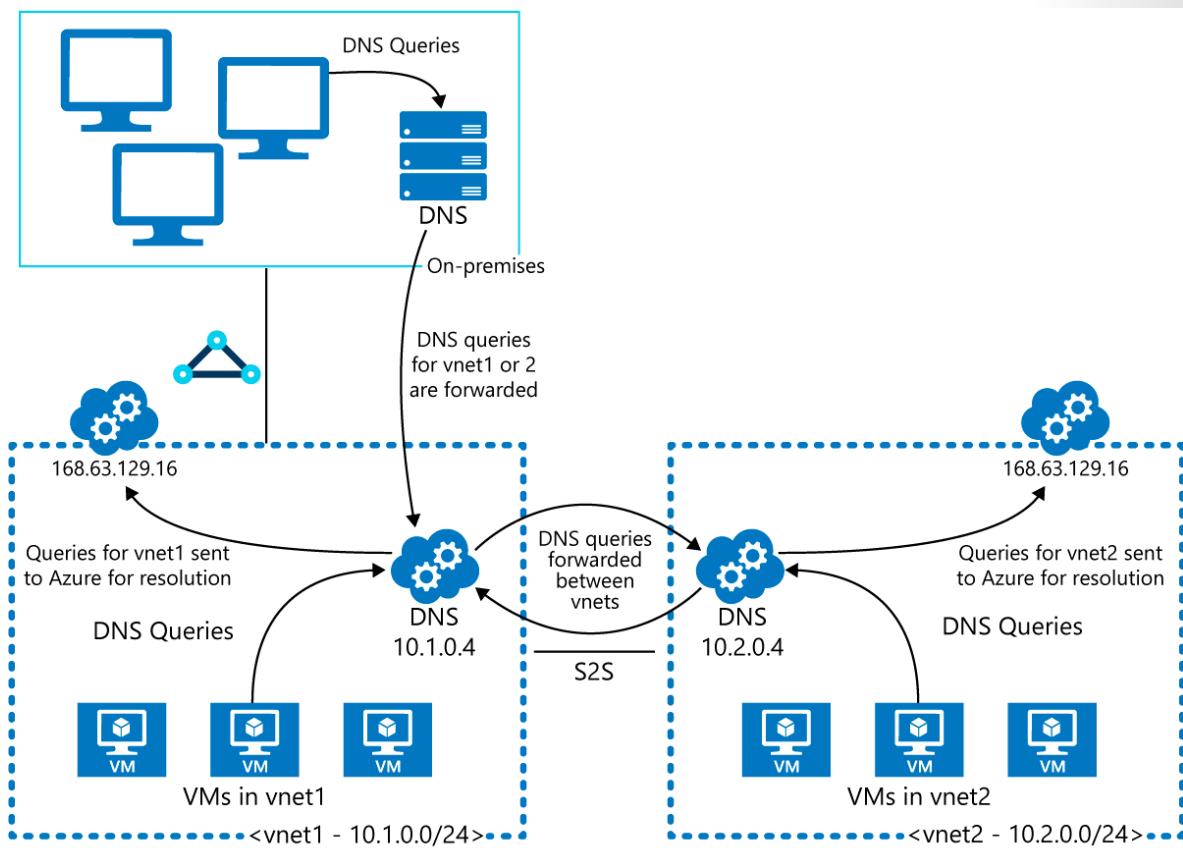
## Name Resolution using your own DNS Server

Azure provides the ability for you to use your own DNS servers. DNS servers within a virtual network can forward DNS queries to the recursive resolvers in Azure. This enables you to resolve host names within that virtual network.

Forwarding queries allows VMs to see both your on-premises resources (via the DC) and Azure-provided host names (via the forwarder). Access to the recursive resolvers in Azure is provided via the virtual IP 168.63.129.16.

DNS forwarding also enables DNS resolution between virtual networks and allows your on-premises machines to resolve Azure-provided host names. In order to resolve a VM's host name, the DNS server VM must reside in the same virtual network, and be configured to forward host name queries to Azure.

Because the DNS suffix is different in each virtual network, you can use conditional forwarding rules to send DNS queries to the correct virtual network for resolution. The following image shows two virtual networks and an on-premises network doing DNS resolution between virtual networks, by using this method.



✓ **Note:** A role instance can perform name resolution of VMs within the same virtual network. It does so by using the FQDN, which consists of the VM's host name and **internal.cloudapp.net** DNS suffix. However, in this case, name resolution is only successful if the role instance has the VM name defined in the Role Schema (.cscfg file). <Role name="**<role-name>**" vmName="**<vm-name>**">. Role instances that need to perform name resolution of VMs in another virtual network (FQDN by using the internal. **cloudapp.net** suffix) have to do so by using the method described in this section (custom DNS servers forwarding between the two virtual networks).

# Recommend Solutions for Network Security

## Network Security

Network security is protecting the communication of resources within and outside of your network. The goal is to limit exposure at the network layer across your services and systems. By limiting this exposure, you decrease the likelihood that your resources can be attacked. In the focus on network security, efforts can be focused on the following areas:

- Securing traffic flow between applications and the internet
- Securing traffic flow amongst applications
- Securing traffic flow between users and the application

Securing traffic flow between applications and the internet focuses on limiting exposure outside your network. Network attacks will most frequently start outside your network, so by limiting the internet exposure and securing the perimeter, the risk of being attacked can be reduced.

Securing traffic flow amongst applications focuses on data between applications and their tiers, between different environments, and in other services within your network. By limiting exposure between these resources, you reduce the effect a compromised resource can have.

Securing traffic flow between users and the application focuses on securing the network flow for your end users.

### Traffic filtering

- You can filter network traffic between resources in a virtual network using a network security group, an NVA that filters network traffic, or both. When using an NVA, you also create custom routes to route traffic from subnets to the NVA.
- A network security group contains several default security rules that allow or deny traffic to or from resources. A network security group can be associated to a network interface, the subnet the network interface is in, or both. To simplify management of security rules, it's recommended that you associate a network security group to individual subnets, rather than individual network interfaces within the subnet, whenever possible.
- If different VMs within a subnet need different security rules applied to them, you can associate the network interface in the VM to one or more application security groups. A security rule can specify an application security group in its source, destination, or both. That rule then only applies to the network interfaces that are members of the application security group.
- Azure creates several default security rules within each network security group. One default rule allows all traffic to flow between all resources in a virtual network. To override this behavior, use network security groups, custom routing to route traffic to an NVA, or both.

✓ **Note:**

You can view sample designs for implementing a perimeter network (also known as a DMZ) between Azure and the internet using an **NVA<sup>3</sup>**.

---

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz?toc=%2Fazure%2Fvirtual-network%2Ftoc.json>

## Traffic routing

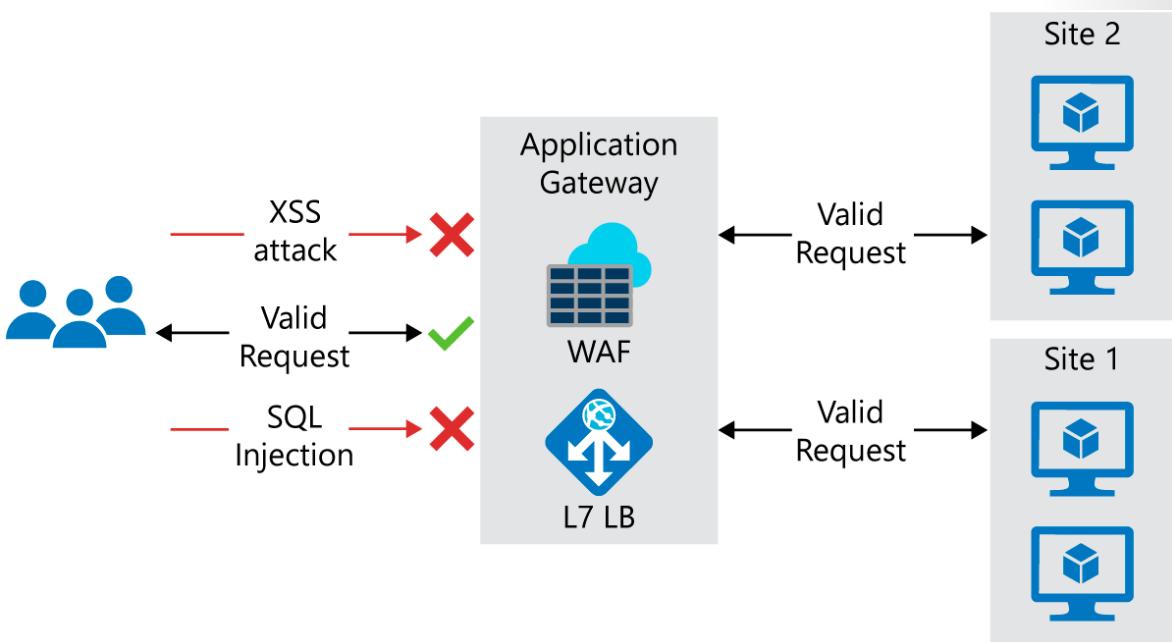
Azure creates several default routes for outbound traffic from a subnet. You can override Azure's default routing by creating a route table and associating it to a subnet. Common reasons for overriding Azure's default routing are:

- Because you want traffic between subnets to flow through an NVA.
- Because you want to force all internet-bound traffic through an NVA, or on-premises, through an Azure VPN gateway. Forcing internet traffic on-premises for inspection and logging is often referred to as forced tunneling.

## Internet Protection

Start by assessing the resources that are internet-facing, and only allow inbound and outbound communication where necessary. Identify all resources that are allowing inbound network traffic of any type, and ensure they are necessary and restricted to only the ports/protocols required. Azure Security Center will identify internet-facing resources that don't have network security groups associated with them, as well as resources that are not secured behind a firewall.

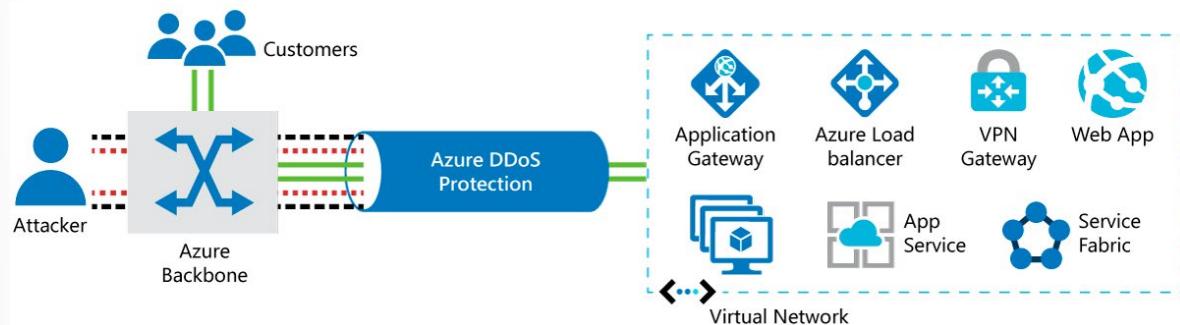
To provide inbound protection at the perimeter, there are a couple of ways to do this. Application Gateway is a Layer 7 load balancer that also includes a web application firewall (WAF) to provide advanced security for your HTTP-based services. The WAF is based on rules from the OWASP 3.0 or 2.2.9 core rule sets and provides protection from commonly known vulnerabilities such as cross-site scripting and SQL injection.



For protection of non-HTTP-based services or for increased customization, network virtual appliances (NVA) can be used to secure your network resources.

NVAs are similar to firewall appliances you might find in on-premises networks, and are available from many of the most popular network security vendors. NVAs can provide greater customization of security for those applications that require it, but can come with increased complexity, so careful consideration of requirements is advised.

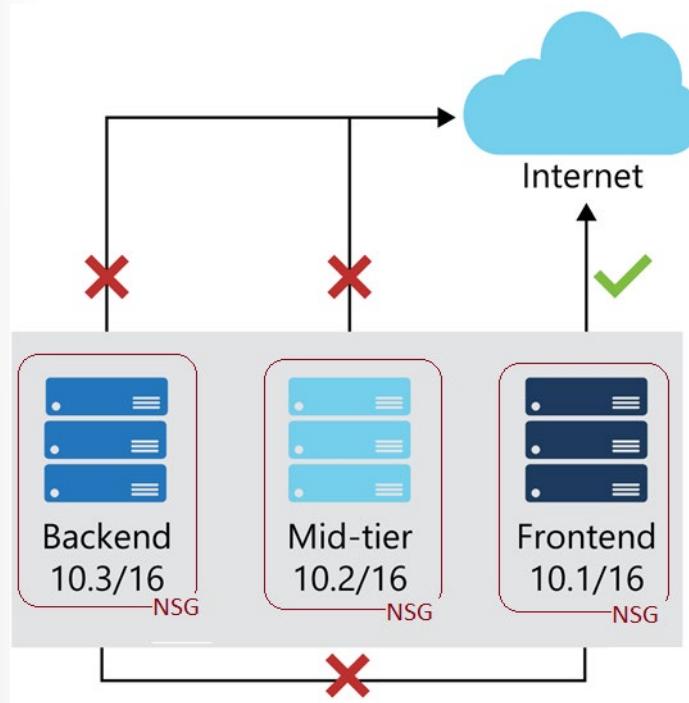
Any resource exposed to the internet is at risk of being attacked by a denial-of-service attack. These types of attacks attempt to overwhelm a network resource by sending so many requests that the resource becomes slow or unresponsive. To mitigate these attacks, Azure DDoS provides basic protection across all Azure services and enhanced protection for further customization for your resources. DDoS protection blocks attack traffic and forwards the remaining traffic to its intended destination. Within a few minutes of attack detection, you are notified using Azure Monitor metrics.



## Virtual Network Security

Once inside a virtual network, it's important to limit communication between resources to only what is required.

For communication between virtual machines, network security groups are a critical piece to restrict unnecessary communication. Network security groups operate at layers 3 & 4 and provide a list of allowed and denied communication to and from network interfaces and subnets. Network security groups are fully customizable and give you the ability to fully lock down network communication to and from your virtual machines. By using network security groups, you can isolate applications between environments, tiers, and services.



To isolate Azure services to only allow communication from virtual networks, use virtual network service endpoints. With service endpoints, Azure service resources can be secured to your virtual network.

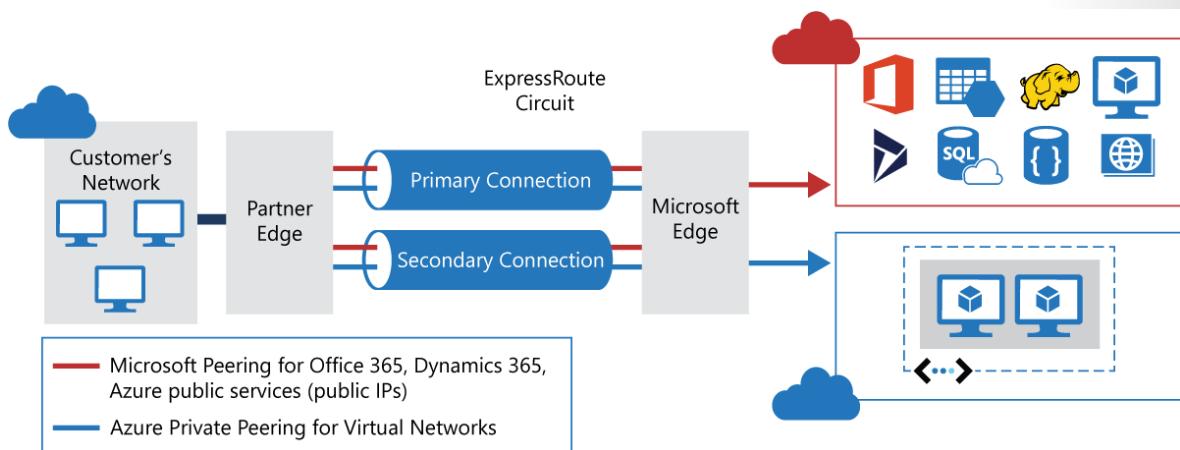
Securing service resources to a virtual network provides improved security by fully removing public internet access to resources, and allowing traffic only from your virtual network. This reduces the attack surface for your environment, reduces the administration required to limit communication between your virtual network and Azure services, and provides optimal routing for this communication.

## Network Integration

It's common to have existing network infrastructure that needs to be integrated to provide communication from on-premises networks, or to provide improved communication between services in Azure. There are a few key ways to handle this integration and improve the security of your network.

Virtual private network (VPN) connections are a common way of establishing secure communication channels between networks, and this is no different when working with virtual networking on Azure. Connection between Azure virtual networks and an on-premises VPN device is a great way to provide secure communication between your network and your virtual machines on Azure.

To provide a dedicated, private connection between your network and Azure, you can use ExpressRoute. ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365. This improves the security of your on-premises communication by sending this traffic over the private circuit instead of over the internet.



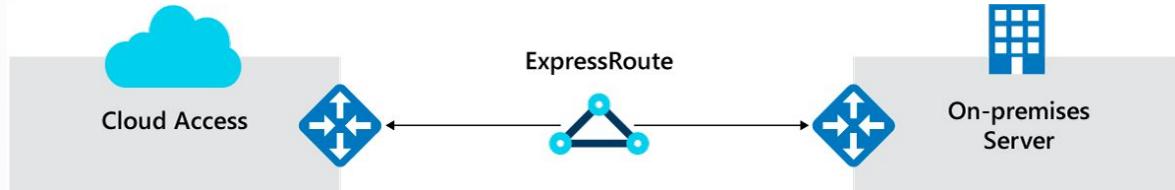
To integrate multiple virtual networks in Azure, virtual network peering establishes a direct connection between designated virtual networks. Once established, you can use network security groups to provide isolation between resources in the same way you secure resources within a virtual network.

This integration gives you the ability to provide the same fundamental layer of security across any peered virtual networks. Communication is only allowed between directly connected virtual networks.

## Recommendation for Hybrid Networks

### Azure ExpressRoute for Hybrid Networks

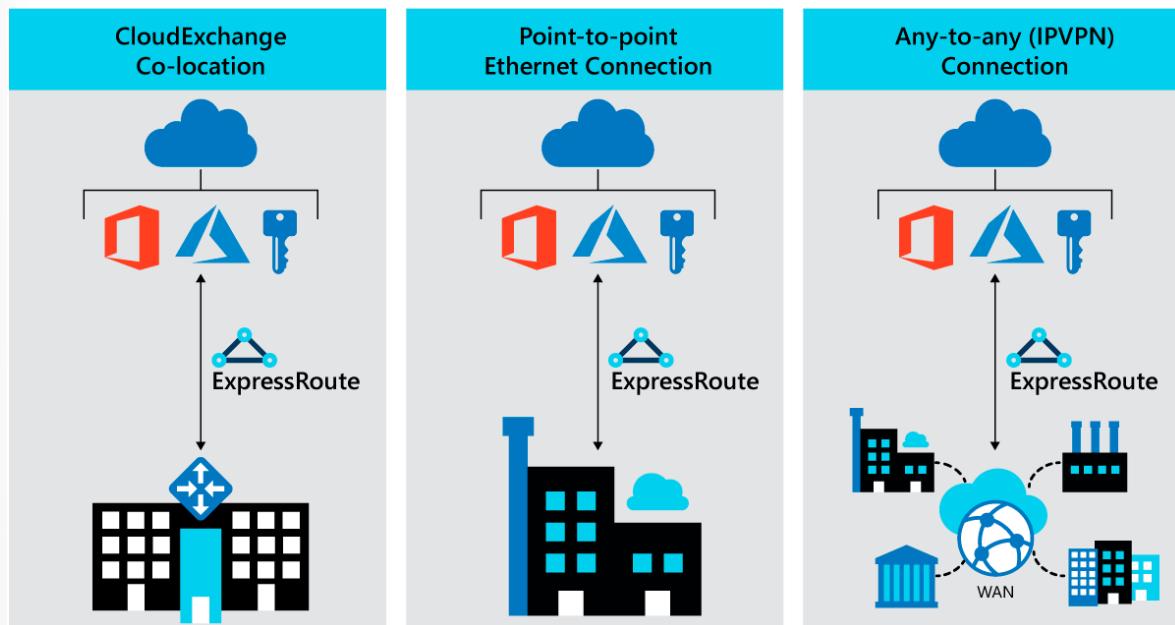
Azure ExpressRoute is an Azure service that allows you to extend on-premises networks over a private connection. A connectivity provider helps make this connection. ExpressRoute extends beyond Azure and lets you establish connections to other Microsoft cloud services, such as Office 365.



ExpressRoute connections don't use the public internet. By using a dedicated connection between your on-premises network and Azure, you achieve greater resilience, faster speeds, higher security, and lower latency.

### ExpressRoute Connectivity Types

There are three ExpressRoute connectivity types, each serving a different need, as shown in the following diagram:



- **CloudExchange:** With the CloudExchange method, you cross-connect to Azure by using the Ethernet exchange that's provided by your colocation facility.
- **Any-to-any:** With the any-to-any network method, you integrate your WAN with Azure by using an IP virtual private network (VPN) provider. This connection type offers links between branch offices and datacenters. When it's enabled, the connection to Azure is similar to any other branch office that's connected via the WAN.

- **Point-to-point:** With the point-to-point Ethernet network method, you connect on-premises data-centers and offices to Azure through a point-to-point Ethernet link.

## ExpressRoute Circuits

With ExpressRoute, the logical connection between your on-premises network and your Azure network is called a circuit. You configure traffic management and routing in ExpressRoute by using circuits. You can have multiple circuits, which exist across various regions. ExpressRoute circuits also support connections through many connectivity providers.

Each circuit has multiple routing domains and peerings associated with it. Examples include Azure public peering, Azure private peering, and Microsoft peering. Each type has identical properties. Each circuit uses a pair of routers in either an active-active or load-sharing configuration, which creates a high availability environment. An ExpressRoute circuit doesn't map to anything physical.

## Azure private peering

Private peering is a trusted extension of your core network in Azure with bidirectional connectivity. By using this peering model, you can connect to virtual machines and cloud services directly on their private IP addresses.

## Microsoft peering

Microsoft peering provides connectivity to all Microsoft online services: Office 365, Dynamics 365, and Azure platform as a service (PaaS). This model requires a public IP address, owned by you or your connectivity provider, which adheres to a set of predefined rules.

Each circuit is assigned a globally unique identifier (GUID), or service key. This key is the only information exchanged between the three parties and is a one-to-one mapping for each circuit.

## Circuit bandwidth

You can have as many circuits as you need, each matching the bandwidth you require. For example, you might want a higher bandwidth between your datacenter and the cloud, but a lower bandwidth for your satellite offices. Bandwidth speeds come in fixed tiers:

- 50 Mbps
- 100 Mbps
- 200 Mbps
- 500 Mbps
- 1 Gbps
- 10 Gbps
- 100 Gbps

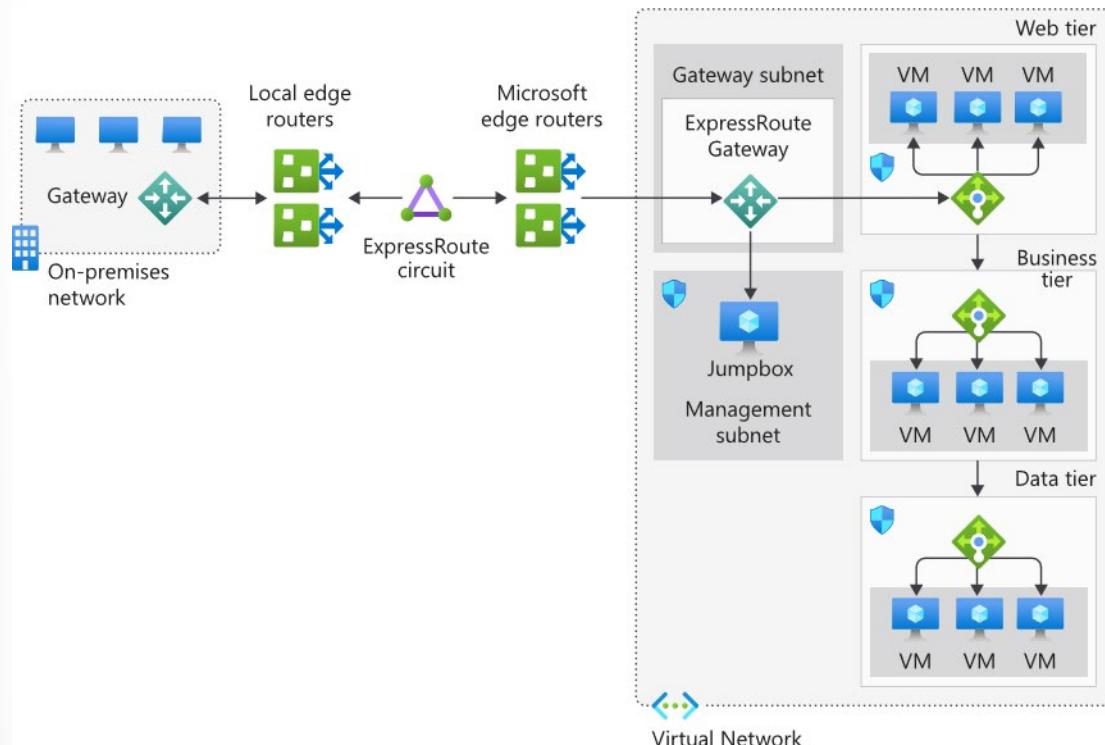
The bandwidth gets shared across any peering in the circuit and is mapped to the connectivity provider and peering location.

## Coexisting connections and ExpressRoute

To use ExpressRoute, you must have a private connection, which is provided by a connectivity partner. However, ExpressRoute can exist alongside any of your current site-to-site, point-to-site, or VPN-to-VPN connections.

## ExpressRoute Reference Architecture

The reference architecture that's illustrated in the following diagram shows how to connect your on-premises network to your Azure virtual networks.



The architecture model includes several components:

- The **on-premises network** is your local Active Directory-managed network.
- **Local edge routers** connect your on-premises network to the connectivity provider's circuit.
- An **ExpressRoute circuit**, supplied by your connectivity provider, operates as a layer 3 circuit. It provides the link between the Azure edge routers and your on-premises edge router.
- The **Microsoft edge routers** are the cloud-side connection between your on-premises network and the cloud. There are always two edge routers, which provides a highly available active-active connection.
- The **Azure virtual network** is where you'll segment your network and assets into tiers. Each application tier, or subnet, can manage specific business operations (for example, web, business, and data).

## ExpressRoute Considerations

When you're evaluating ExpressRoute, consider the following.

## Benefits

Implementing ExpressRoute in your organization helps produce the following benefits:

- ExpressRoute is better suited to high-speed and critical business operations.
- ExpressRoute circuits support a maximum bandwidth of 100 Gbps.
- ExpressRoute provides dynamic scalability to help meet your organizational needs.
- ExpressRoute uses layer 3 connectivity and security standards.

## Considerations

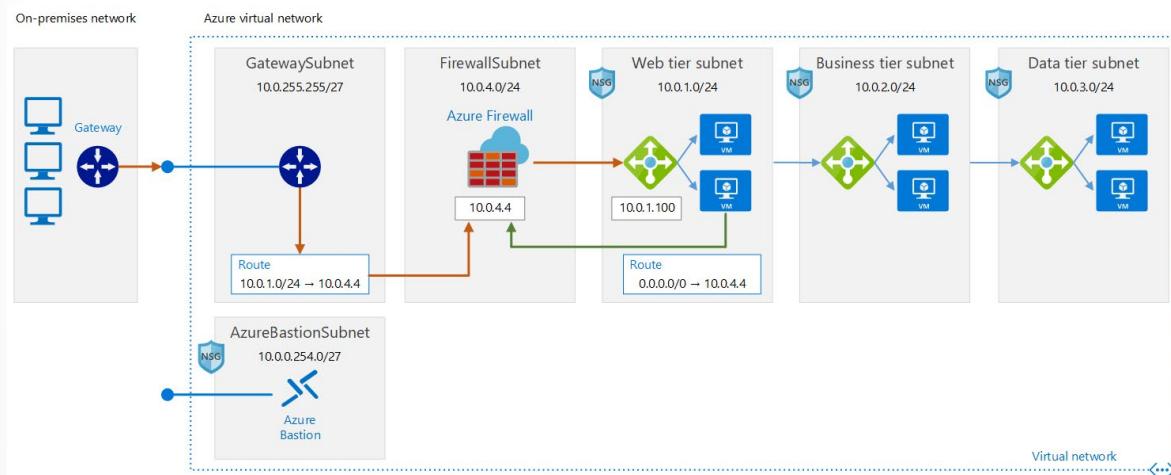
The following list identifies a few key considerations:

- The setup and configuration for ExpressRoute is more complex, and will require collaboration with the connectivity provider.
- ExpressRoute requires the on-premises installation of high-bandwidth routers.
- The ExpressRoute circuit is handled and managed by the connectivity provider.
- ExpressRoute doesn't support the Hot Standby Router Protocol (HSRP). You'll need to enable a Border Gateway Protocol (BGP) configuration.
- ExpressRoute operates on a layer 3 circuit and requires a network security appliance to manage threats.
- Monitoring the connectivity between your on-premises network and Azure must use the Azure Connectivity Toolkit.
- To improve network security, ExpressRoute requires network security appliances between the provider's edge routers and your on-premises network.

# Implement a Secure Hybrid Network

## Implement a Perimeter Network to On-Premises Datacenter

This reference architecture shows a secure hybrid network that extends an on-premises network to Azure. The architecture implements a *perimeter network*, between the on-premises network and an Azure virtual network. All inbound and outbound traffic passes through Azure Firewall.



This architecture requires a connection to your on-premises datacenter, using either a VPN gateway or an ExpressRoute connection. Typical uses for this architecture include:

- Hybrid applications where workloads run partly on-premises and partly in Azure.
- Infrastructure that requires granular control over traffic entering an Azure virtual network from an on-premises datacenter.
- Applications that must audit outgoing traffic. This is often a regulatory requirement of many commercial systems and can help to prevent public disclosure of private information.

✓ **Note:** Deploy the solution

A deployment for a reference architecture that implements these recommendations is available on [GitHub<sup>4</sup>](#).

## Architecture

The architecture consists of the following components.

- **On-premises network.** A private local-area network implemented in an organization.
- **Azure virtual network.** The virtual network hosts the application and other resources running in Azure.
- **Gateway.** The gateway provides connectivity between the routers in the on-premises network and the virtual network. The gateway is placed in its own subnet.
- **Azure Firewall.** Azure Firewall is a managed firewall as a service. The Firewall instance is placed in its own subnet.

<sup>4</sup> <https://github.com/mspnp/reference-architectures/tree/master/dmz/secure-vnet-hybrid>

- **Virtual network routes.** Virtual network routes define the flow of IP traffic within the Azure virtual network. In the diagram shown above, there are two user-defined route tables.
  - In the gateway subnet, traffic sent to the web-tier subnet (10.0.1.0/24) is routed through the Azure Firewall instance.
  - In the web tier subnet, Since there is no route for address space of the VNet itself to point to Azure firewall, web tier instances are able to communicate directly to each other, not via Azure Firewall.
- **Network security groups.** Use security groups to restrict network traffic within the virtual network. For example, in the deployment provided with this reference architecture, the web tier subnet allows TCP traffic from the on-premises network and from within the virtual network; the business tier allows traffic from the web tier; and the data tier allows traffic from the business tier.
- **Bastion.** Azure Bastion allows you to log into VMs in the virtual network through SSH or remote desktop protocol (RDP) without exposing the VMs directly to the internet. Use Bastion to manage the VMs in the virtual network.

## Recommendations

The following recommendations apply for most scenarios. Follow these recommendations unless you have a specific requirement that overrides them.

### Access control recommendations

Use role-based access control (RBAC) to manage the resources in your application. Consider creating the following custom roles:

- A DevOps role with permissions to administer the infrastructure for the application, deploy the application components, and monitor and restart VMs.
- A centralized IT administrator role to manage and monitor network resources.
- A security IT administrator role to manage secure network resources such as the firewall.

The DevOps and IT administrator roles should not have access to the firewall resources. This should be restricted to the security IT administrator role.

### Resource group recommendations

Azure resources such as VMs, virtual networks, and load balancers can be easily managed by grouping them together into resource groups. Assign RBAC roles to each resource group to restrict access.

Create the following resource groups:

- A resource group containing the virtual network (excluding the VMs), NSGs, and the gateway resources for connecting to the on-premises network. Assign the centralized IT administrator role to this resource group.
- A resource group containing the VMs for the Azure Firewall instance and the user-defined routes for the gateway subnet. Assign the security IT administrator role to this resource group.
- Separate resource groups for each application tier that contain the load balancer and VMs. Note that this resource group shouldn't include the subnets for each tier. Assign the DevOps role to this resource group.

## Networking recommendations

To accept inbound traffic from the internet, add a Destination Network Address Translation (DNAT) rule to Azure Firewall.

- Destination address = Public IP address of the firewall instance.
- Translated address = Private IP address within the virtual network.

The example deployment routes internet traffic for port 80 to the web tier load balancer.

Force-tunnel all outbound internet traffic through your on-premises network using the site-to-site VPN tunnel, and route to the internet using network address translation (NAT). This prevents accidental leakage of any confidential information stored in your data tier and allows inspection and auditing of all outgoing traffic.

**✓ Important:**

Don't completely block internet traffic from the application tiers, as this will prevent these tiers from using Azure PaaS services that rely on public IP addresses, such as VM diagnostics logging, downloading of VM extensions, and other functionality. Azure diagnostics also requires that components can read and write to an Azure Storage account.

Lastly, consider using Application Gateway or Azure Front Door for SSL termination.

## Security Considerations

This reference architecture implements multiple levels of security.

### Routing all on-premises user requests through Azure Firewall

The user-defined route in the gateway subnet blocks all user requests other than those received from on-premises. The route passes allowed requests to the firewall, and these requests are passed on to the application if they are allowed by the firewall rules.

You can add other routes, but make sure they don't inadvertently bypass the firewall or block administrative traffic intended for the management subnet.

### Using NSGs to block/pass traffic between application tiers

Traffic between tiers is restricted by using NSGs. The business tier blocks all traffic that doesn't originate in the web tier, and the data tier blocks all traffic that doesn't originate in the business tier. If you have a requirement to expand the NSG rules to allow broader access to these tiers, weigh these requirements against the security risks. Each new inbound pathway represents an opportunity for accidental or purposeful data leakage or application damage.

### DevOps access

Use RBAC to restrict the operations that DevOps can perform on each tier. When granting permissions, use the principle of least privilege. Log all administrative operations and perform regular audits to ensure any configuration changes were planned.

## Module 2 Review Questions

### Module 2 Review Questions



#### Review Question 1

*You are designing a solution for an on-premises network to deploy a virtual appliance.*

*The plan is to deploy several Azure virtual machines and connect the on-premises network to Azure by using a site-to-site connection.*

*All network traffic that will be directed from the Azure virtual machines to a specific subnet must flow through the virtual appliance.*

*You need to recommend a solution to manage network traffic.*

*What is the solution?*

- Implement an Azure virtual network
- Implement Azure ExpressRoute
- Implement Azure Batch Service
- Configure Azure Traffic Manager

#### Review Question 2

*You are designing a solution for on-premises networks and Azure virtual networks.*

*You need a secure private connection between on-premises networks and the Azure virtual networks. The connection must offer a redundant pair of cross connections to provide high availability.*

*What should you recommend?*

- Virtual network peering
- Azure Load Balancer
- VPN Gateway
- ExpressRoute

## Review Question 3

You use a virtual network to extend an on-premises IT environment into the cloud. The virtual network has two virtual machines that store sensitive data.

The data must only be available using internal communication channels. Internet access to those VMs is not permitted.

You need to ensure that the VMs cannot access the Internet.

What should you recommend?

- Azure ExpressRoute
- Azure Load Balancer
- Source Network Address Translation (SNAT)
- Network Security Groups (NSG)

# Answers

## Review Question 1

You are designing a solution for an on-premises network to deploy a virtual appliance.

The plan is to deploy several Azure virtual machines and connect the on-premises network to Azure by using a site-to-site connection.

All network traffic that will be directed from the Azure virtual machines to a specific subnet must flow through the virtual appliance.

You need to recommend a solution to manage network traffic.

What is the solution?

- Implement an Azure virtual network
- Implement Azure ExpressRoute
- Implement Azure Batch Service
- Configure Azure Traffic Manager

### Explanation

*Correct Answer: Implement an Azure virtual network. Implement an Azure virtual network is correct because Azure Virtual Network manages User defined routes (UDR's). Also, another possible solution is to configure an Azure Routing table to use Azure Forced Tunneling.*

## Review Question 2

You are designing a solution for on-premises networks and Azure virtual networks.

You need a secure private connection between on-premises networks and the Azure virtual networks. The connection must offer a redundant pair of cross connections to provide high availability.

What should you recommend?

- Virtual network peering
- Azure Load Balancer
- VPN Gateway
- ExpressRoute

### Explanation

*Correct Answer: ExpressRoute. ExpressRoute allows connections between on-premises networks and Azure virtual networks.*

**Review Question 3**

You use a virtual network to extend an on-premises IT environment into the cloud. The virtual network has two virtual machines that store sensitive data.

The data must only be available using internal communication channels. Internet access to those VMs is not permitted.

You need to ensure that the VMs cannot access the Internet.

What should you recommend?

- Azure ExpressRoute
- Azure Load Balancer
- Source Network Address Translation (SNAT)
- Network Security Groups (NSG)

*Explanation*

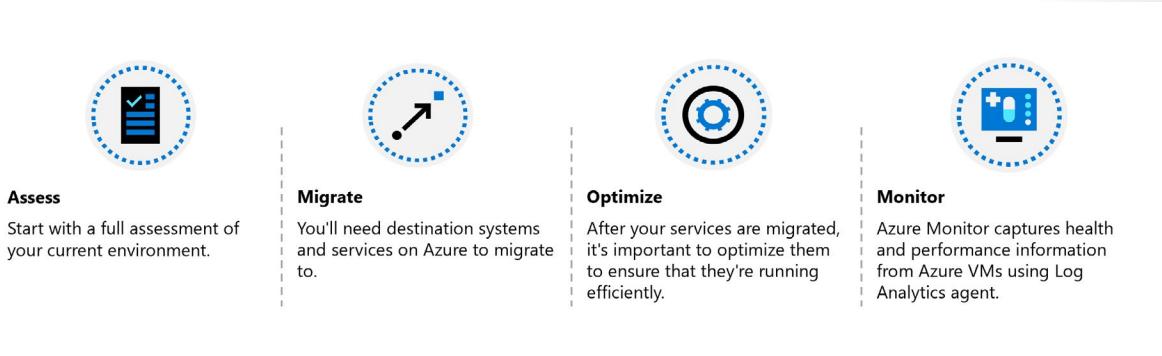
*Correct Answer: Network Security Groups (NSG). For communication between virtual machines, network security groups are a critical piece to restrict unnecessary communication. Network security groups operate at layers 3 & 4 and provide a list of allowed and denied communication to and from network interfaces and subnets. Network security groups are fully customizable and give you the ability to fully lock down network communication to and from your virtual machines. By using network security groups, you can isolate applications between environments, tiers, and services.*

## Module 3 Design for Migration

### Planning Azure Migration

#### Planning Azure Migration

You can use a framework of Assess, Migrate, Optimize, and Monitor as a path for migration. Each stage focuses on an aspect of ensuring the success of a migration.



### Assess



### Discovery and Evaluation

Start with a full assessment of your current environment. Identify the servers, applications, and services that are in scope for migration. You can then bring in the IT and business teams that work with those services.

Next, produce a full inventory and dependency map of servers and services that are in scope for migration. The inventory and map determine how those services communicate with each other. Each application must be fully investigated before any work takes place.

For each application, there are multiple migration options:

- **Rehost:** Recreate your existing infrastructure in Azure. Choosing this approach has the least impact because it requires minimal changes. It typically involves moving virtual machines from your data center to virtual machines on Azure.
- **Refactor:** Move services running on virtual machines to platform-as-a-service (PaaS) services. This approach can reduce operational requirements, improve release agility, and keep your costs low. Small enhancements to run more efficiently in the cloud can have large impacts on performance.
- **Rearchitect:** You might be forced to rearchitect some systems so that they can be migrated. Other apps could be changed to become cloud native, or to take advantage of new approaches to software, such as containers or microservices.
- **Rebuild:** You might need to rebuild software if the cost to rearchitect it is more than that of starting from scratch.
- **Replace:** While you're reviewing your estate, it's possible you'll find that third-party applications could completely replace your custom applications. Evaluate software-as-a-service (SaaS) options that can be used to replace existing applications.

Review each application to determine which option is the best fit.

## Involve key stakeholders

Applications are used by specific sections of the business. The owners and superusers of applications have a wealth of experience to call on. Involving these people in the planning stage increases the chance of a successful migration. These resources can offer guidance in areas where the person running the migration project might have knowledge gaps.

## Estimate cost savings

Part of the business's plan to migrate to Azure could be to reduce costs, because moving to the cloud offers cost savings over running your own on-premises estate. After you complete the initial scoping exercise, use the Azure Total Cost of Ownership (TCO) Calculator to estimate the real costs of supporting the project in light of the company's longer-term financial goals.

## Identify Tools

Several tools and services are available to help you plan and complete the four stages of migration. In some migrations, you may only need to use one or two of these tools.

Service or tool	Stage	Use
<b>Azure Migrate</b>	Assess and migrate	Perform assessment and migration of VMware VMs, Hyper-V VMs, cloud VMs, and physical servers, as well as databases, data, virtual desktop infrastructure, and web applications, to Azure.

Service or tool	Stage	Use
<b>Service Map</b>	Assess	Maps communication between application components on Windows or Linux. Helps you identify dependencies when scoping what to migrate.
<b>Azure TCO Calculator</b>	Assess	Estimates your monthly running costs in Azure versus on-premises.
<b>Azure Database Migration Service</b>	Migrate	Uses the Data Migration Assistant and the Azure portal to migrate database workloads to Azure.
<b>Data Migration Tool</b>	Migrate	Migrates existing databases to Azure Cosmos DB.
<b>Azure Cost Management</b>	Optimize	Helps you monitor, control, and optimize ongoing Azure costs.
<b>Azure Advisor</b>	Optimize	Helps optimize your Azure resources for high availability, performance, and cost.
<b>Azure Monitor</b>	Monitor	Enables you to monitor your entire estate's performance. Includes application-health monitoring via enhanced telemetry, and setting up notifications.
<b>Azure Sentinel</b>	Monitor	Provides intelligent security analytics for your applications.

## Migrate



Migrate

## Deploy Cloud Infrastructure Targets

You'll need destination systems and services on Azure to migrate to. The scope of your migration has been defined as your company's current VMware machines and existing relational databases. In this scenario, you don't need to create the resources in Azure beforehand. The two tools you'll use to do the migration, Azure Site Recovery and the Azure Database Migration Service, will create the required Azure resources for you.

## Migrate workloads

It's often best to start with a small migration instead of migrating a large, business-critical workload. This approach lets you become familiar with the tools, processes, and procedures for migration. It can reduce

the risk of issues when you migrate larger workloads. As you become more comfortable with the migration process, you can progress to larger and more business-critical workloads.

Each tool will guide you through the migration. The steps to complete them are covered in later units. At a high level, the steps are:

1. Prepare the source (vCenter Server) and target (Azure) environments.
2. Set up and start the replication between the two.
3. Test that the replication has worked.
4. Fail over from the source servers to Azure.

For the database migrations, the high-level steps are:

1. Assess your on-premises databases.
2. Migrate the schemas.
3. Create and run an Azure Database Migration Service project to move the data.
4. Monitor the migration.

## Decommission on-premises infrastructure

After all migrated workloads have been tested and verified as successfully migrated to Azure, you can decommission all your on-premises systems. Even after you decommission them, it can be useful to keep backups and archive data from the migrated systems. This practice gives you a historical archive of data in case it's needed. This data could be stored on-premises, or in a cloud-storage service such as Azure Blob storage.

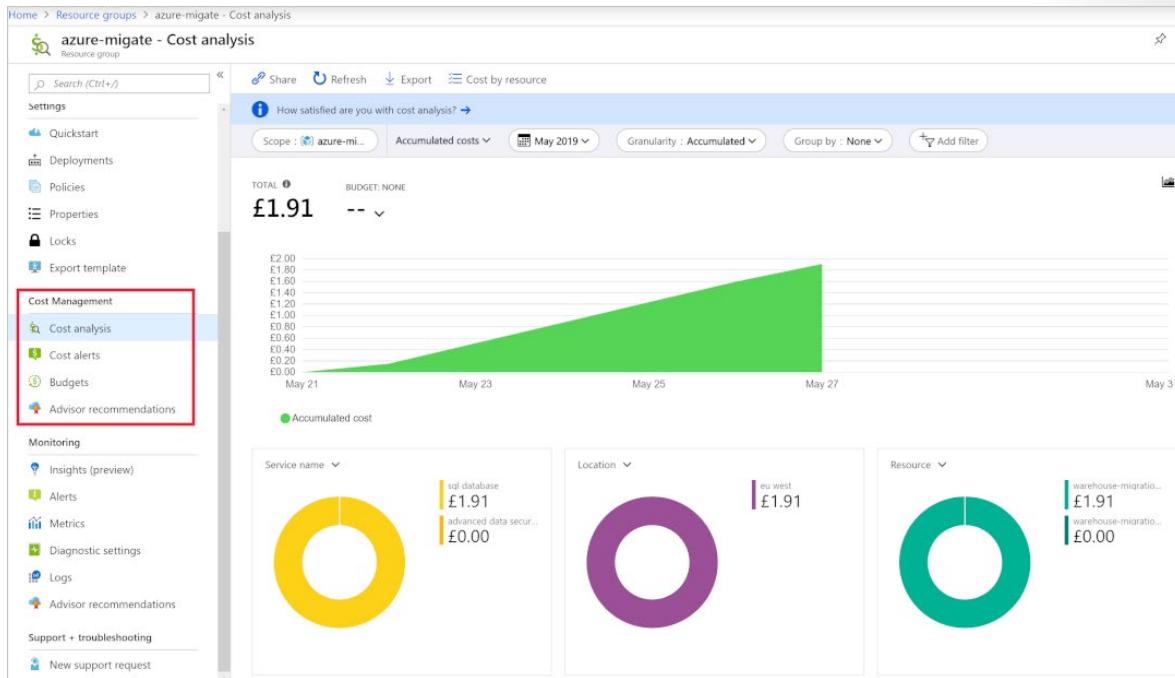
## Optimize



After your services are migrated, it's important to optimize them to ensure that they're running as efficiently as possible from a cost and performance standpoint.

## Analyze Running Costs

Use Azure Cost Management to start analyzing your Azure costs at different management scopes. For example, by choosing a subscription in the portal, you can see a breakdown of all the resources for that subscription. Or, you could view a resource group to see all the costs associated with all the resources in just the selected group:



## Review Opportunities to Improve

Azure Cost Management shows you cost-reduction advice from Azure Advisor. The advice includes suggestions like reducing the performance of underused VMs, making use of additional discounts, or reserving resources instead of paying as you go. Azure Advisor also shows you recommendations for network security, high availability, and performance. Review the recommendations that Advisor presents to further optimize your environment.

## Monitor



## Integrate health and performance monitoring

Azure Monitor can capture health and performance information from Azure VMs if you install a Log Analytics agent. You can install the agent on machines running either Windows or Linux, and you can then set up alerting and reporting.

You can set up alerts based on a range of data sources, such as:

- Specific metric values like CPU usage.
- Specific text in log files.
- Health metrics.
- An Autoscale metric.

It's also important to have event logging and visibility into security events across your enterprise. Azure Sentinel provides security information and event-management (SIEM) capabilities, along with artificial intelligence to help you protect against, detect, and respond to security events. This information helps security operations (SecOps) teams triage critical alerts and prioritize work effectively.

# Assessment using Azure Migrate

## Using Azure Migrate to Assess Environment

Using Azure Migrate, you can perform an agentless environment discovery or use agents to perform a dependency analysis. The Azure portal helps you assess your current on-premises workloads. After the assessment, Azure Migrate makes recommendations for the size of VM you'll need to provision.

Because the server workloads are based primarily on VMware, you want to begin with those machines. You want to assess readiness for the move to Azure. You also want to identify estimated costs for the resources that those machines will consume, so the management team can set the budgets.

In this lesson, you'll look at Azure Migrate, a service you use to assess readiness and assist with migration to Azure from an on-premises environment.

Azure Migrate helps with performance-based sizing calculations (virtual machine sizing, compute/storage) for the machines that you'll migrate and estimate the ongoing cost of running these machines in Azure.

Azure Migrate can assess both Hyper-V and VMware-based virtual machines, as well as physical servers. Azure Migrate also supports the visualization of dependencies for those machines. It helps you create groups of machines that can be assessed together and ultimately migrated to Azure at the same time.

## Work with Azure Migrate

When you use Azure Migrate, the assessments it produces are created within a project that is set up in the Azure portal. Before creating a project, you can group the VMs according to the various types of VM workloads that you have, assessing and potentially migrating them together..

After you create a project, Azure Migrate requires you to complete two steps to produce an assessment:

1. Discover your virtual machines.
2. Create assessments.

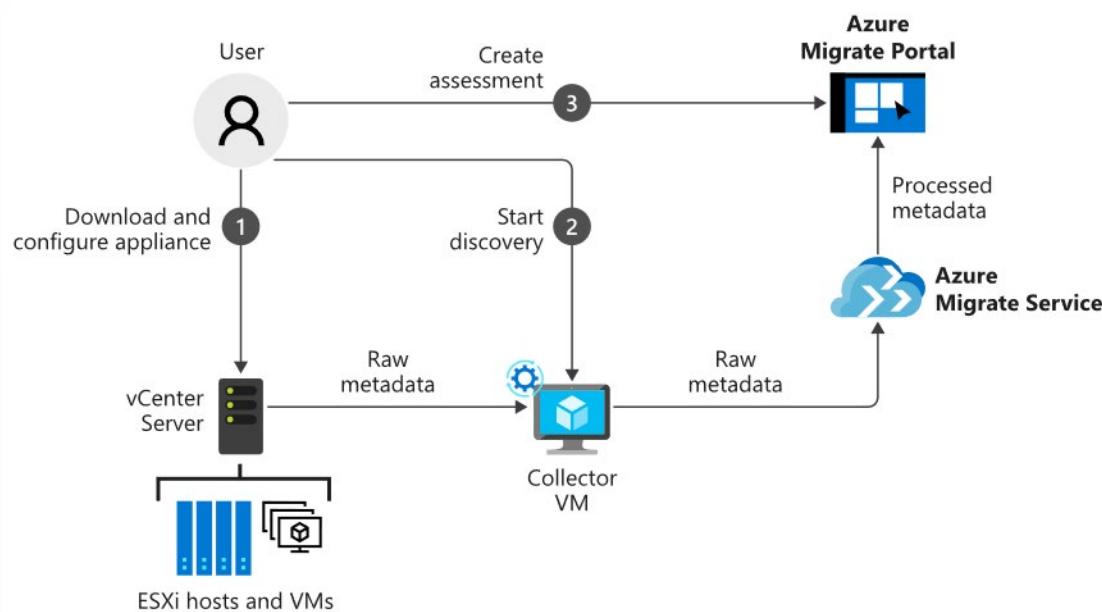
## Discover Machines

To perform an agentless discovery, the Azure Migrate: Server Assessment tool guides you through downloading a lightweight collector appliance, which carries out the discovery of systems in your environment. The collector appliance is available to download to VMware or Hyper-V environment. Import and spin up the collector appliance, and then complete its configuration to connect it to the Azure Migrate project.

The collector gathers data about VM cores, memory, disk sizes, and network adapters. Where applicable, the collector also gathers performance data like CPU and memory usage, disk IOPS, disk throughput, and network output.

When the data collection is complete, it's pushed to your Azure Migrate project. On the Azure portal, you can now view all the discovered systems or download a report to review.

For VMware environments, the process can be visualized as follows:



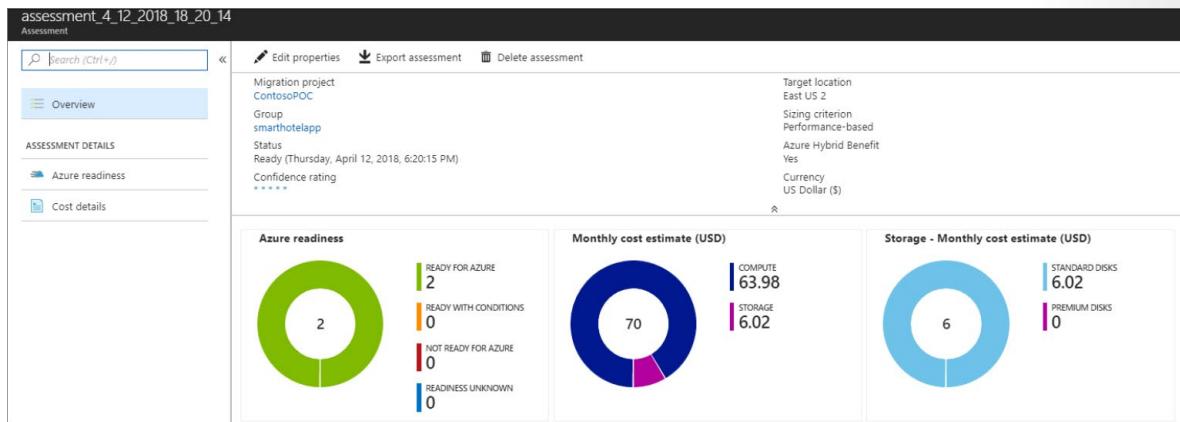
If your company wants details about how the VMs are related to each other (via a visualization of dependencies), you can install agents to collect that data. Azure Migrate will prompt you to install the Microsoft Monitoring Agent and Dependency Agent on each VM. The agents are available for both Windows and Linux.

NAME	DEPENDENCIES
OSTICKETMYSQL	ⓘ Requires agent installation
OSTICKETWEB	ⓘ Requires agent installation
CONTOSODC1	ⓘ Requires agent installation
vcenter	ⓘ Requires agent installation
CONTOSOGW	ⓘ Requires agent installation
CONTOSODC2	ⓘ Requires agent installation
WEBVM	ⓘ Requires agent installation
AZUREMIGRATE	ⓘ Requires agent installation
SQLVM	ⓘ Requires agent installation

After these agents are installed and configured, they collect data like fully qualified domain name (FQDN), OS, IP addresses, MAC addresses, running processes, and incoming and outgoing TCP connections.

## Create an Assessment

Azure Migrate can now assess your environment's readiness to be migrated to Azure. In the portal, select the Assessments section, and then select Create assessment. An assessment is created with default settings. You can change these settings later by editing the properties of the assessment.



## Migrate Servers with Azure Migrate

### Migrate Servers with Azure Migrate

After using Azure Migrate for your assessment, you can decide which of your servers are good candidates to be migrated to Azure.

Azure Migrate can also perform an agentless migration of virtual and physical servers into Azure. You've chosen to use Azure Migrate to complete the migration of virtual machines.

In this lesson, you'll review Azure Migrate and how to use it to migrate specific workloads to Azure.

### Virtual machine replication

Add **Azure Migrate: Server Migration** to your Azure Migrate dashboard, which carries over machines and insights from the assessment. You can get begin your replication by clicking Replicate in the tool window. Azure Migrate replicates up to 100 VMs simultaneously.

Times for replication will vary based on number and size of virtual machines along with connection speeds between your data center and Azure.

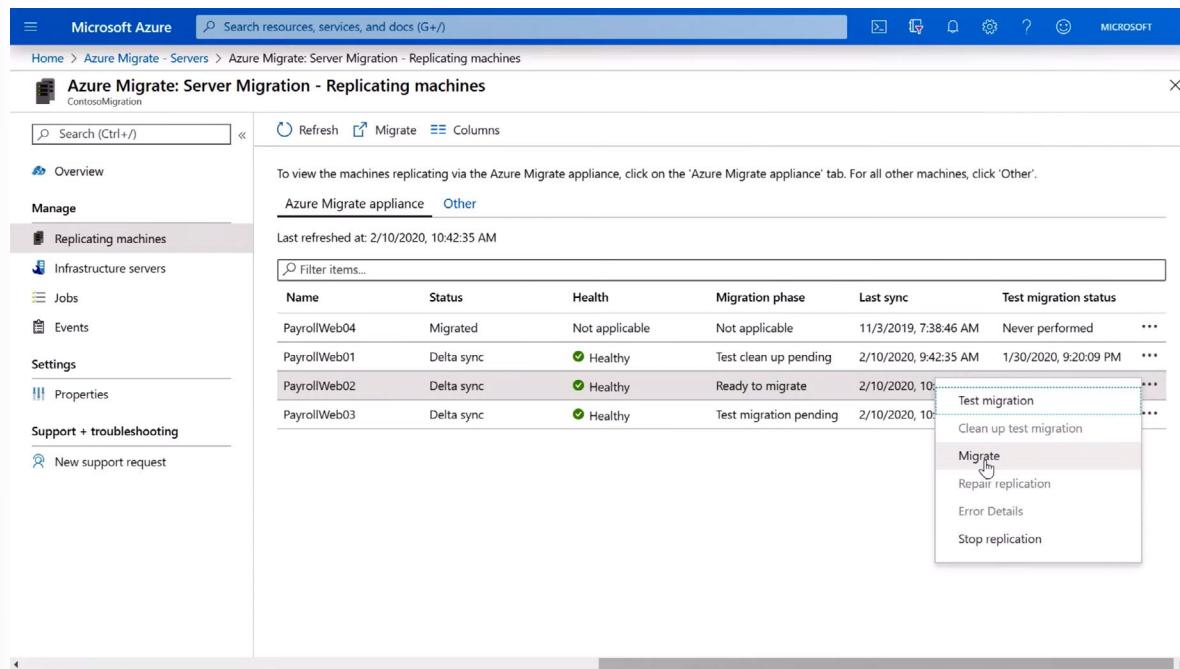
The screenshot shows the Microsoft Azure Azure Migrate service page. The left sidebar includes links for Home, Get started, Explore more, Migration goals (Windows, Linux and SQL Server, SQL Server (only), VDI, Web Apps, Data Box), Manage (Discovered items, Properties), Support + troubleshooting (New support request), and a search bar. The main content area is divided into two sections: 'Assessment tools' and 'Migration tools'. The 'Assessment tools' section features the 'Azure Migrate: Discovery and assessment' tool with tabs for Discover, Dependency analysis (Preview), Assess, and Overview. It includes a 'Quick start' guide with steps 1: Discover, 2: Analyse dependencies, and 3: Assess. The 'Migration tools' section features the 'Azure Migrate: Server Migration' tool with tabs for Discover, Replicate, Migrate, and Overview. It includes a 'Quick start' guide with steps 1: Discover, 2: Replicate, and 3: Migrate.

## Test migrated virtual machines

Once all your targeted virtual machines are replicated into Azure, before you migrate them into production, you can test your virtual machines to ensure everything works. The process runs a prerequisite check, prepares for the test, creates a new test virtual machine, and starts it.

## Migrating the Virtual Machines to Production

Once you're ready for the production migration, select **Migrate** from the replicating machines window. That process will prompt you to shut down the virtual machine to avoid any data loss and perform a final replication. It is recommended to do this during off peak business hours, because the virtual machine will be down for a few minutes.



Now it will run through the production migration process and you can check the status as it validates the pre-requisites, prepares for migration, creates the Azure VM and starts the Azure VM.

# Post-Migration Steps

After the migration has taken place, review the security settings of the virtual machine after the migration. Restrict network access for unused services by using network security groups. Deploy Azure Disk Encryption to secure the disks from data theft and unauthorized access.

Consider improving the resilience of the migrated machines by:

- Adding a backup schedule that uses Azure Backup.
  - Replicating the machines to a secondary region using Azure Site Recovery.

Complete clean-up tasks for the remaining on-premises servers. Such tasks may include removing the servers from local backups and removing their raw disk files from storage-area network (SAN) storage to free up space. Update documentation related to the migrated servers to reflect their new IP addresses and locations in Azure.

# Migrate Databases with Azure Database Migration Service

## Migrate Databases with Azure Database Migration Service

Azure Database Migration Service enables online and offline migrations from multiple database sources to Azure data platforms, all with minimal downtime. The service uses the Microsoft Data Migration Assistant to generate assessment reports. Identified tasks are then performed by the Database Migration Service.

In this lesson, you'll see how to use the Data Migration Assistant and Database Migration Service together. They provide a way to move on-premises SQL Server databases efficiently to Azure.

### Offline vs. online migration

The migration service provides two different ways to migrate SQL Server databases: offline migration or online migration. An offline migration requires shutting down the server at the start of the migration, which means downtime for the service. An online migration uses a continuous synchronization of live data, allowing a cutover to the Azure replica database at any time. The online option is the better of the two if you need to minimize downtime for your workload.

Azure Database Migration Service has two pricing tiers:

- **Standard:** Supports only offline migrations. There's no charge to use this tier.
- **Premium:** Supports both offline and online migrations. There's no charge for the first six months. After that period, you'll incur charges.

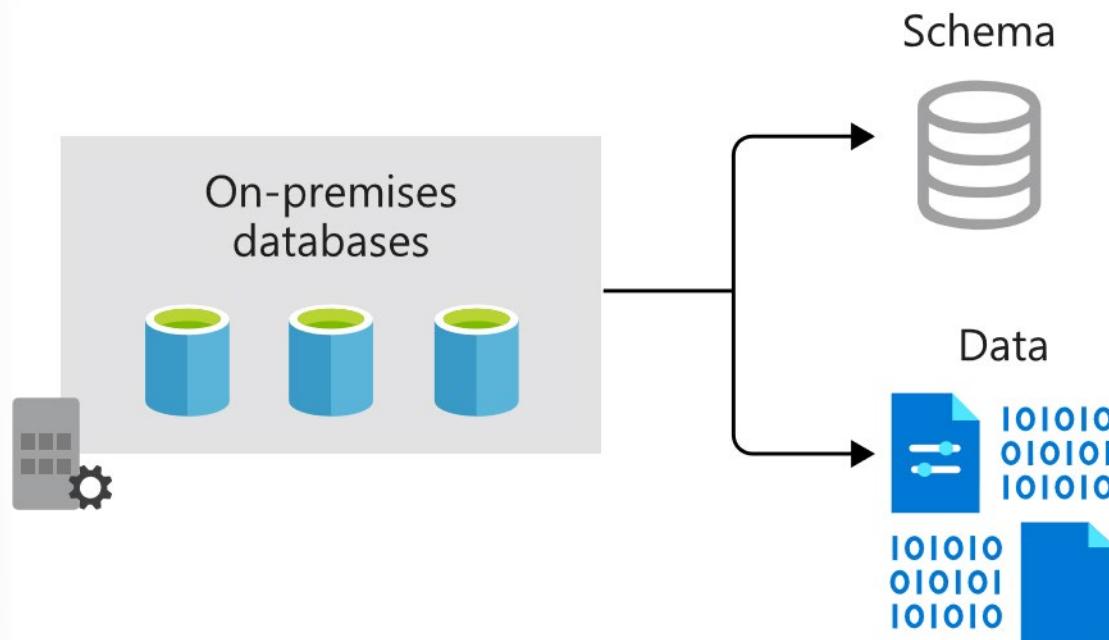
### Destinations

Your relational database can be migrated to a number of different destinations in Azure:

- **Single Azure SQL Database instance:** A fully managed, single SQL database.
- **Azure SQL Database managed instance:** 100% compatible with SQL Server Enterprise Edition Database Engine, but missing some minor SQL Server features.
- **SQL Server on Azure Virtual Machines:** An infrastructure-as-a-service (IaaS) offering that runs a full version of SQL Server and supports all the features of SQL Server.
- **Azure Database for MySQL:** An Azure database service based on the MySQL Community Edition, versions 5.6 and 5.7.
- **Azure Database for PostgreSQL:** An Azure database service based on the community version of the PostgreSQL database engine.
- **Azure Cosmos DB:** A globally distributed, multi-model, fully managed database service.

### Overview of Database Migration

The Data Migration Assistant guides you through the process of migrating databases. You take an existing relational database, split out the database schemas, and then recreate them in the destination Azure SQL Database instance.



With the new schema in place, the data for each database can then be copied to Azure.

Finally, you'll check that the new databases are performing as expected.

## Prerequisites

Both offline and online migrations have the same prerequisite tasks:

- **Download the Data Migration Assistant:** Download and install the assistant locally on your on-premises servers running SQL Server.
- **Create an Azure Virtual Network instance:** This virtual network is for Azure Database Migration Service when it uses the Azure Resource Manager deployment model. The virtual network provides connectivity to the on-premises environment.
- **Configure the network security group:** The security group associated with the new virtual network should allow inbound connectivity to the service via ports 443, 53, 9354, 445, and 12000.
- **Configure the Windows Firewall:** You must configure the firewall to allow the Database Migration Service to connect over port 1433. You can also open port 1434 if multiple named instances or dynamic ports exist on the same server. If you have a named instance(s) you will have to add the port(s) for the named instance(s).
- **Configure credentials**
  - Add CONTROL SERVER permissions to the credentials used to connect to the source SQL Server instance.
  - Add CONTROL DATABASE permissions to the credentials used to connect to the target Azure SQL Database instance.
- **Provision your target database in Azure:** Create the database that is to be the target of the migration. Size it appropriately for the migrated workload.

## Assess the On-Premises Databases

Ensure that all the communication ports are open, and check the connectivity between the source and destination servers before the migration tasks begin. Using the Data Migration Assistant, create an **Assessment** project, give the project a name, and select the source and target servers. Provide the connection details for the source server, including credentials with permission to access it. On the database selection screen, choose the database you want to migrate.

The assessment will generate a report on completion, including a set of recommendations and alternative approaches that could be taken for the migration. You'll see any compatibility issues between the source and destination databases that could cause the migration to fail. Address the issues in the report, running it as many times as you need to make sure that the issues have been fixed.

A Data Migration Assistant report looks like this:

The screenshot shows the Data Migration Assistant interface with the following details:

- Project Name:** warehouse-move
- Step:** 3 Review results
- Target Platform:** Azure SQL Database
- localhost / SQL Server 2017**
- Feature parity (5)**
  - Unsupported features (3):**
    - File groups not supported in A... (Impact: 1)
    - Filestream not supported in A... (Impact: 1)
    - Windows authentication not s... (Impact: N/A)
  - Partially-supported features (2):**
    - In-memory tables only support... (Impact: 1)
    - Table partitioning consideratio... (Impact: 1)
- File groups not supported in Azure SQL Database**

Details	Impacted objects
Some selected databases use file groups, which are not supported in Azure SQL Database.	Type: Database Name: WideWorldImporters
- Object details**

Type: Database  
Name: WideWorldImporters  
This database contains file groups.
- Export report** button

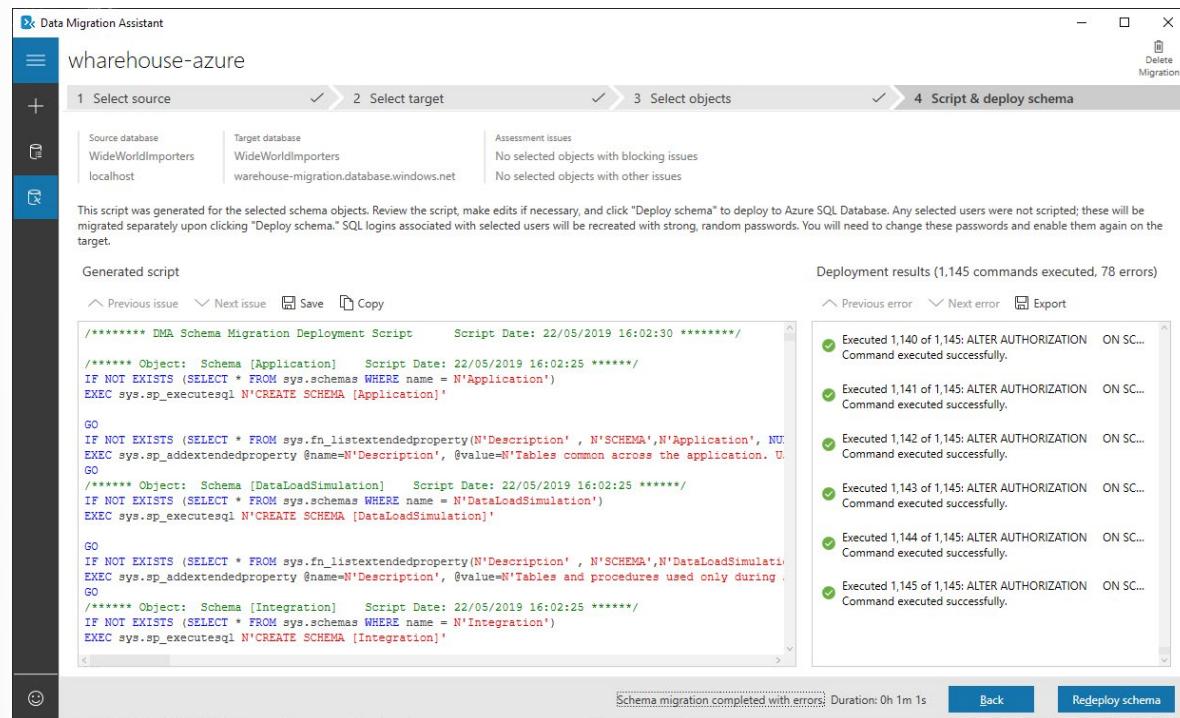
## Migrate the Schema using the Data Migration Assistant

Each database has a schema that represents its entire structure. The schema defines the rules for how the data in it is organized and the relationships between data elements. You migrate the schema before you migrate all the data in the database. Doing this creates an empty structure on the new Azure SQL database, and that structure matches that of the on-premises source database. Migrating the schema also validates the connectivity before you do the full data migration.

To use the Data Migration Assistant to migrate the schema, create a new **Migration** project.

Select your on-premises SQL Server instance as the source server, and your Azure SQL Database instance as the target server. Set the scope of the migration to **Schema Only**. After you connect to the source database, choose the schema objects to deploy to the new SQL database.

The Data Migration Assistant will create a script to take the required actions. Then, select **Deploy Schema** to run the script. When the script is complete, check the target server to make sure the database has been configured correctly.



## Migrate Data with Database Migration Service

In the Azure portal, follow these steps to create an instance of Azure Database Migration Service, and then to run it to migrate the data in your databases:

1. Create an instance of Azure Database Migration Service. Choose the pricing tier based on whether you need an online or offline migration.
2. Create a new migration project. Choose the type of migration you want to perform, either offline or online.
3. Specify source and target server details, including the authentication information.
4. Identify the databases. Map the relevant target database on the target server to the source server.
5. Run and monitor the migration.
  - Select the **Run migration** button to start the migration. The migration activity screen will appear.
  - Track the progress until the process shows as completed.
6. After all the required databases are migrated, check them to make sure they're working.

When these steps are complete, your schema and data have been migrated to the Azure SQL Database instance. You can then shut down and decommission your on-premises databases and servers.

# Migrate On-Premises Data to Cloud Storage with AzCopy

## Migrate On-Premises Data to Cloud Storage with AzCopy

AzCopy is a command-line tool for copying data to or from Azure Blob storage, Azure Files, and Azure Table storage, by using simple commands.

The commands are designed for optimal performance.

Additionally, using AzCopy to move files, such as log files from a web server a storage target, can significantly reduce costs.

Using AzCopy, you can either copy data between a file system and a storage account, or between storage accounts. AzCopy may be used to copy data from local (on-premises) data to a storage account.

In this lesson, you learn how to:

- Create a storage account.
- Use AzCopy to upload all your data.
- Modify the data for test purposes.
- Create a scheduled task or cron job to identify new files to upload.

### Prerequisites

For this lesson, Windows users should use Schtasks.exe to schedule a task.

Linux users should use crontab.

To create a general-purpose v2 storage account in the Azure portal, follow these steps:

1. On the Azure portal menu, 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, as shown in the following image.

The screenshot shows the Microsoft Azure 'Create storage account' wizard. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar. Below the header, the breadcrumb navigation shows 'Home > Storage accounts > Create storage account'. The main title 'Create storage account' is centered above the form fields.

The 'Basics' tab is selected in the top navigation bar, followed by 'Networking', 'Advanced', 'Tags', and 'Review + create'.

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

**Project details**

Select the 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 \***: A dropdown menu with the following options: AZ-303RG, AZ304Demo, AZ304firewallpolicy, NetworkWatcherRG. The 'Select existing...' option is highlighted.

**Instance details**

The default deployment model is Resource Manager. You can choose the classic deployment model instead. [Choose](#)

**Storage account name \***: (Input field)

**Location \***: (US) Central US

**Performance**: Standard (radio button selected) or Premium

**Account kind**: StorageV2 (general purpose v2)

**Replication**: Read-access geo-redundant storage (RA-GRS)

**Access tier (default)**: Cool (radio button) or Hot (radio button selected)

At the bottom, there are three buttons: 'Review + create' (blue), '< Previous' (disabled), and 'Next : Networking >'.

5. Next, 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:

Field	Value
Deployment model	Resource Manager
Performance	Standard
Account kind	StorageV2 (general-purpose v2)
Replication	Read-access geo-redundant storage (RA-GRS)
Access tier	Hot

8. If you plan to use **Azure Data Lake Storage**, choose the **Advanced** tab, and then set **Hierarchical namespace** to **Enabled**.

9. Select **Review + Create** to review your storage account settings and create the account.

10. Select **Create**.

## Create a Container

Blobs must always be uploaded into a container. Containers are used as a method of organizing groups of blobs like you would files on your computer, in folders.

Follow these steps to create a container:

1. Select the **Storage accounts** button from the main page, and select the storage account that you created.
2. Select **Containers** under **Blob Services**, and then select **Container**.

Container names must start with a letter or number. They can contain only letters, numbers, and the hyphen character (-).

The screenshot shows the Azure Storage Accounts blade. In the left sidebar, under 'Storage accounts' for 'rag304', the 'Containers' option is selected. A red box highlights this selection. In the main content area, there's a 'New container' card with a red border. It contains fields for 'Name\*' (with a red asterisk) and 'Public access level' (set to 'Private (no anonymous access)'). Below the card, a message says 'You don't have any containers yet. Click '+ Container' to get started.' At the top of the blade, there's a search bar and several navigation links: 'Container', 'Change access level', 'Refresh', and 'Delete'.

## Download AzCopy

Download the AzCopy V10 executable file.

- **Windows<sup>1</sup>** (zip)
- **Linux<sup>2</sup>** (tar)
- **MacOS<sup>3</sup>** (zip)

Place the AzCopy file anywhere on your computer. Add the location of the file to your system path variable so that you can refer to this executable file from any folder on your computer.

## Authenticate with Azure AD

Assign the **Storage Blob Data Contributor** role to your identity.

Then, open a command prompt, type the following command, and press the ENTER key.

```
azcopy login
```

This command returns an authentication code and the URL of a website. Open the website, provide the code, and then choose the **Next** button.

A sign-in window will appear. In that window, sign into your Azure account by using your Azure account credentials. After you've successfully signed in, you can close the browser window and begin using AzCopy.

## Upload Contents of a Folder to Blob Storage

You can use AzCopy to upload all files in a folder to Blob storage on Windows or Linux. To upload all blobs in a folder, enter the following AzCopy command:

```
azcopy copy "<local-folder-path>" "https://<storage-account-name>.<blob or  
dfs>.core.windows.net/<container-name>" --recursive=true
```

- Replace the <local-folder-path> placeholder with the path to a folder that contains files (For example: C:\myFolder or /mnt/myFolder).
- Replace the <storage-account-name> placeholder with the name of your storage account.
- Replace the <container-name> placeholder with the name of the container that you created.

To upload the contents of the specified directory to Blob storage recursively, specify the --recursive option. When you run AzCopy with this option, all subfolders and their files are uploaded as well.

## Upload Modified Files to Blob Storage

You can use AzCopy to upload files based on their last-modified time.

To try this, modify or create new files in your source directory for test purposes. Then, use the AzCopy sync command.

---

<sup>1</sup> <https://aka.ms/downloadazcopy-v10-windows>

<sup>2</sup> <https://aka.ms/downloadazcopy-v10-linux>

<sup>3</sup> <https://aka.ms/downloadazcopy-v10-mac>

```
azcopy sync "<local-folder-path>" "https://<storage-account-name>.blob.core.windows.net/<container-name>" --recursive=true
```

- Replace the <local-folder-path> placeholder with the path to a folder that contains files (For example: C:\myFolder or /mnt/myFolder).
- Replace the <storage-account-name> placeholder with the name of your storage account.
- Replace the <container-name> placeholder with the name of the container that you created.

## Create a Scheduled Task

You can create a scheduled task or cron job that runs an AzCopy command script. The script identifies and uploads new on-premises data to cloud storage at a specific time interval.

Copy the AzCopy command to a text editor. Update the parameter values of the AzCopy command to the appropriate values. Save the file as script.sh (Linux) or script.bat (Windows) for AzCopy.

These examples assume that your folder is named myFolder, your storage account name is mystorageaccount and your container name is mycontainer.

Linux:

```
azcopy sync "/mnt/myfiles" "https://mystorageaccount.blob.core.windows.net/mycontainer?sv=2018-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-05-30T06:57:40Z&st=2019-05-29T22:57:40Z&spr=https&sig=BXHippZxxx54h-Qn%2F4tBY%2BE2JHGCTRv52445rtoyqgFBUo%3D" --recursive=true
```

Windows:

```
azcopy sync "C:\myFolder" "https://mystorageaccount.blob.core.windows.net/mycontainer" --recursive=true
```

In this lesson, **Schtasks**<sup>4</sup> is used to create a scheduled task on Windows. The **Crontab**<sup>5</sup> command is used to create a cron job on Linux.

**Schtasks** enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote computer. **Cron** enables Linux and Unix users to run commands or scripts at a specified date and time by using **cron expressions**<sup>6</sup>.

To create a cron job on Linux, enter the following command on a terminal:

```
crontab -e  
*/5 * * * * sh /path/to/script.sh
```

Specifying the cron expression \*/5 \* \* \* \* in the command indicates that the shell script script.sh should run every five minutes. You can schedule the script to run at a specific time daily, monthly, or yearly.

For windows using PowerShell:

```
schtasks /CREATE /SC minute /MO 5 /TN "AzCopy Script" /TR C:\script.bat
```

<sup>4</sup> [https://msdn.microsoft.com/library/windows/desktop/bb736357\(v=vs.85\).aspx](https://msdn.microsoft.com/library/windows/desktop/bb736357(v=vs.85).aspx)

<sup>5</sup> <http://crontab.org/>

<sup>6</sup> <https://en.wikipedia.org/wiki/Cron>

To create a scheduled task on Windows, enter the following command at a command prompt or in PowerShell:

✓ **Note:** This example assumes that your script is in the root drive of your computer, but your script can be anywhere that you want.

```
schtasks /CREATE /SC minute /MO 5 /TN "AzCopy Script" /TR C:\script.bat
```

The command uses:

- The /SC parameter to specify a minute schedule.
- The /MO parameter to specify an interval of five minutes.
- The /TN parameter to specify the task name.
- The /TR parameter to specify the path to the `script.bat` file.

To validate that the scheduled task/cron job runs correctly, create new files in your `myFolder` directory. Wait five minutes to confirm that the new files have been uploaded to your storage account. Go to your log directory to view output logs of the scheduled task or cron job.

# Lab

## Lab: Migrating Hyper-V VMs to Azure by using Azure Migrate

✓ **Important:** To download the most recent version of this lab, please visit the AZ-304 [GitHub repository](#)<sup>7</sup>.

Direct link to [Lab: Migrating Hyper-V VMs to Azure by using Azure Migrate](#)<sup>8</sup>.

### Lab scenario



Despite its ambitions to modernize its workloads as part of migration to Azure, the Adatum Enterprise Architecture team realizes that, due to aggressive timelines, in many cases, it will be necessary to follow the lift-and-shift approach. To simplify this task, the Adatum Enterprise Architecture team started exploring the capabilities of Azure Migrate. Azure Migrate serves as a centralized hub to assess and migrate to Azure on-premises servers, infrastructure, applications, and data.

Azure Migrate provides the following features:

- Unified migration platform: A single portal to start, run, and track your migration to Azure.
- Range of tools: A range of tools for assessment and migration. Tools include Azure Migrate: Server Assessment and Azure Migrate: Server Migration. Azure Migrate integrates with other Azure services and with other tools and independent software vendor (ISV) offerings.
- Assessment and migration: In the Azure Migrate hub, you can assess and migrate:
- Servers: Assess on-premises servers and migrate them to Azure virtual machines.
- Databases: Assess on-premises databases and migrate them to Azure SQL Database or to SQL Managed Instance.
- Web applications: Assess on-premises web applications and migrate them to Azure App Service by using the Azure App Service Migration Assistant.
- Virtual desktops: Assess your on-premises virtual desktop infrastructure (VDI) and migrate it to Windows Virtual Desktop in Azure.
- Data: Migrate large amounts of data to Azure quickly and cost-effectively using Azure Data Box products.

While databases, web apps, and virtual desktops are in scope of the next stage of the migration initiative, Adatum Enterprise Architecture team wants to start by evaluating the use of Azure Migrate for migrating their on-premises Hyper-V virtual machines to Azure VM.

<sup>7</sup> <https://github.com/MicrosoftLearning/AZ-304-Microsoft-Azure-Architect-Design>

<sup>8</sup> [https://aka.ms/304\\_Module\\_3\\_Lab](https://aka.ms/304_Module_3_Lab)

## Objectives

After completing this lab, you will be able to:

- Prepare Hyper-V for assessment and migration by using Azure Migrate
- Assess Hyper-V for migration by using Azure Migrate
- Migrate Hyper-V VMs by using Azure Migrate

## 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\08\azuredeploy30308suba.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: Prepare for assessment and migration by using Azure Migrate

The main tasks for this exercise are as follows:

1. Configure Hyper-V environment
2. Create an Azure Migrate project
3. Implement the target Azure environment

### Exercise 2: Assess Hyper-V for migration by using Azure Migrate

The main tasks for this exercise are as follows:

1. Deploy and configure the Azure Migrate appliance
2. Configure, run, and view an assessment

### Exercise 3: Migrate Hyper-V VMs by using Azure Migrate

The main tasks for this exercise are as follows:

1. Prepare for migration of Hyper-V VMs

- 
- 2. Configure replication of Hyper-V VMs
  - 3. Perform migration of Hyper-V VMs
  - 4. Remove Azure resources deployed in the lab

## Module 3 Review Questions

### Module 3 Review Questions



#### Review Question 1

A company that you are consulting for has 400 virtual machines hosted in a VMWare environment. The virtual machines vary in size and have various utilization levels.

The plan to move all the virtual machines in Azure.

You need to recommend how many and what size Azure virtual machines will be required to move the current workloads to Azure. The solution must minimize administrative effort.

What should you recommend?

- Azure Pricing calculator
- Azure Cost Management
- Azure Advisor
- Azure Migrate

#### Review Question 2

You are advising an organization that has an on-premises Hyper-V cluster that hosts 30 virtual machines.

Some virtual machines run Window Server 2019 and some are running Linux.

The organization wants to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

You recommend implementing an Azure Storage account, and then using Azure Migrate.

Does the meet the goal?

- Yes
- No

# Answers

## Review Question 1

A company that you are consulting for has 400 virtual machines hosted in a VMWare environment. The virtual machines vary in size and have various utilization levels.

The plan to move all the virtual machines in Azure.

You need to recommend how many and what size Azure virtual machines will be required to move the current workloads to Azure. The solution must minimize administrative effort.

What should you recommend?

- Azure Pricing calculator
- Azure Cost Management
- Azure Advisor
- Azure Migrate

*Explanation*

*Correct Answer: Azure Migrate. Azure Migrate gathers performance monitor data to size a VM as well as pricing details.*

## Review Question 2

You are advising an organization that has an on-premises Hyper-V cluster that hosts 30 virtual machines. Some virtual machines run Window Server 2019 and some are running Linux.

The organization wants to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

You recommend implementing an Azure Storage account, and then using Azure Migrate.

Does the meet the goal?

- Yes
- No

*Explanation*

*Correct Answer: Azure Migrate. Azure Migrate is the recommended solution for migrating disks to Azure which can then be used in Azure as Virtual Machines.*



## Module 4 Design Authentication and Authorization

### Tips for Identity and Access Management

#### Identity and Access Management

In cloud-focused architecture, identity provides the basis of a large percentage of security assurances. While legacy IT infrastructure often heavily relied on firewalls and network security solutions at the internet egress points for protection against outside threats, these controls are less effective in cloud architectures with shared services being accessed across cloud provider networks or the internet.

It is challenging or impossible to write concise firewall rules when you don't control the networks where these services are hosted, different cloud resources spin up and down dynamically, cloud customers may share common infrastructure, and employees and users expect to be able to access data and services from anywhere.

To enable all these capabilities, you must manage access based on identity authentication and authorization controls in the cloud services to protect data and resources and to decide which requests should be permitted.

Additionally, using a cloud-based identity solution like Azure AD offers additional security features that legacy identity services cannot because they can apply threat intelligence from their visibility into a large volume of access requests and threats across many customers.

This lesson covers the following tips for identity and access management:

- Single Enterprise Directory
- Synchronize Identity Systems
- Use Cloud Provider Identity Source for Third Parties
- Passwordless, or Multi-Factor Authentication for Admins
- Block Legacy Authentication
- Don't Synchronize On-Premises Admin Accounts to Cloud Identity Providers
- Use Modern Password Protection Offerings

- Use Cross-Platform Credential Management

## Use a Single Enterprise Directory

Establish a single enterprise directory for managing identities of full-time employees and enterprise resources

A single authoritative source for identities increases clarity and consistency for all roles in IT and Security. This reduces security risk from human errors and automation failures resulting from complexity. By having a single authoritative source, teams that need to make changes to the directory can do so in one place and have confidence that their change will take effect everywhere.

For Azure, designate a single Azure Active Directory (Azure AD) instance directory as the authoritative source for corporate/organizational accounts.

## Synchronize Identity Systems

Synchronize your cloud identity with your existing identity systems.

Consistency of identities across cloud and on-premises will reduce human errors and resulting security risk. Teams managing resources in both environments need a consistent authoritative source to achieve security assurances.

For Azure, synchronize Azure AD with your existing authoritative on-premises Active Directory using Azure AD Connect. This is also required for an Office 365 migration, so it is often already done before Azure migration and development projects begin. Note that administrator accounts should be exempted from synchronization as described in **Critical impact account dependencies**<sup>1</sup>.

## Block Legacy Authentication

### Disable insecure legacy protocols for internet-facing services.

Legacy authentication methods are among the top attack vectors for cloud-hosted services. Created before multifactor authentication existed, legacy protocols don't support additional factors beyond passwords and are therefore prime targets for password spraying, dictionary, or brute force attacks.

As an example, nearly 100% of all password spray attacks against Office 365 customers use legacy protocols. Additionally, these older protocols frequently lack other attack countermeasures, such as account lockouts or back-off timers. Services running on Microsoft's cloud that block legacy protocols have observed a 66% reduction in successful account compromises.

### For Azure and other Azure AD-based accounts, configure Conditional Access to block legacy protocols.

Disabling legacy authentication can be difficult, as some users may not want to move to new client software that supports modern authentication methods. However, moving away from legacy authentication can be done gradually.

Start by using metrics and logging from your authentication provider to determine how many users still authenticate with old clients. Next, disable any down-level protocols that aren't in use, and set up conditional access for all users who aren't using legacy protocols. Finally, give plenty of notice and guidance to users on how to upgrade before blocking legacy authentication for all users on all services at a protocol level.

---

<sup>1</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/security/critical-impact-accounts>

## Don't Synchronize On-Premises Admin Accounts to Cloud Identity Providers

Don't synchronize accounts with the highest privilege access to on-premises resources as you synchronize your enterprise identity systems with cloud directories.

This mitigates the risk of an adversary pivoting to full control of on-premises assets following a successful compromise of a cloud account. This helps contain the scope of an incident from growing significantly.

For Azure, don't synchronize accounts to Azure AD that have high privileges in your existing Active Directory. This is blocked by default in the default Azure AD Connect configuration, so you only need to confirm you haven't customized this configuration.

This is related to the critical impact account dependencies guidance in the administration section that mitigates the inverse risk of pivoting from on-premises to cloud assets.

## Use Modern Password Protection Offerings

Provide modern and effective protections for accounts that cannot go *passwordless* (**Passwordless Or multi-factor authentication for admins<sup>2</sup>**).

Legacy identity providers mostly checked to make sure passwords had a good mix of character types and minimum length, but we have learned that these controls in practice led to passwords with less entropy that could be cracked easier:

- Microsoft - <https://www.microsoft.com/research/publication/password-guidance/>
- NIST - <https://pages.nist.gov/800-63-3/sp800-63b.html>

Identity solutions today need to be able to respond to types of attacks that didn't even exist one or two decades ago such as password sprays, breach replays (also called "credential stuffing") that test user-name/password pairs from other sites' breaches, and phishing man-in-the-middle attacks.

Cloud identity providers are uniquely positioned to offer protection against these attacks. Since they handle such large volumes of signons, they can apply better anomaly detection and use a variety of data sources to both proactively notify companies if their users' passwords have been found in other breaches, as well as validate that any given sign-in appears legitimate and is not coming from an unexpected or known-malicious host.

Additionally, synchronizing passwords to the cloud to support these checks also add resiliency during some attacks. Customers affected by (Not)Petya attacks were able to continue business operations when password hashes were synced to Azure AD (vs. near zero communications and IT services for customers affected organizations that had not synchronized passwords).

## Use Cross-Platform Credential Management

Use a single identity provider for authenticating all platforms (Windows, Linux, and others) and cloud services.

A single identity provider for all enterprise assets will simplify management and security, minimizing the risk of oversights or human mistakes. Deploying multiple identity solutions (or an incomplete solution) can result in unenforceable password policies, passwords not reset after a breach, proliferation of passwords (often stored insecurely), and former employees retaining passwords after termination.

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/security/critical-impact-accounts>

For example, Azure Active Directory can be used to authenticate Windows, Linux, Azure, Office 365, Amazon Web Services (AWS), Google Services, (remote access to) legacy on-premises applications, and third-party Software as a Service providers.

# Recommend a Solution for Multi-Factor Authentication

## Authentication vs Authorization

This topic defines authentication and authorization and briefly covers how you can use the Microsoft identity platform to authenticate and authorize users in your web apps, web APIs, or apps calling protected web APIs.

**Authentication** is the process of proving you are who you say you are. Authentication is sometimes shortened to AuthN. Microsoft identity platform implements the OpenID Connect protocol for handling authentication.

**Authorization** is the act of granting an authenticated party permission to do something. It specifies what data you're allowed to access and what you can do with that data. Authorization is sometimes shortened to AuthZ. Microsoft identity platform implements the OAuth 2.0 protocol for handling authorization.

## Authentication and authorization using Microsoft identity platform

Instead of creating apps that each maintain their own username and password information, which incurs a high administrative burden when you need to add or remove users across multiple apps, apps can delegate that responsibility to a centralized identity provider.

Delegating authentication and authorization to it enables scenarios such as Conditional Access policies that require a user to be in a specific location, the use of multi-factor authentication as well as enabling a user to sign in once and then be automatically signed in to all of the web apps that share the same centralized directory.

Microsoft identity platform simplifies authorization and authentication for application developers by providing identity as a service, with support for industry-standard protocols such as OAuth 2.0 and OpenID Connect, as well as open-source libraries for different platforms to help you start coding quickly. It allows developers to build applications that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or APIs that developers have built.

Following is a brief comparison of the various protocols used by Microsoft identity platform:

- **OAuth vs OpenID Connect:** OAuth is used for authorization and OpenID Connect (OIDC) is used for authentication. OpenID Connect is built on top of OAuth 2.0, so the terminology and flow are similar between the two. You can even both authenticate a user (using OpenID Connect) and get authorization to access a protected resource that the user owns (using OAuth 2.0) in one request.
- **OAuth vs SAML:** OAuth is used for authorization and SAML is used for authentication.
- **OpenID Connect vs SAML:** Both OpenID Connect and SAML are used to authenticate a user and are used to enable Single Sign On. SAML authentication is commonly used with identity providers such as Active Directory Federation Services (ADFS) federated to Azure AD and is therefore frequently used in enterprise applications. OpenID Connect is commonly used for apps that are purely in the cloud, such as mobile apps, web sites, and web APIs.

## Reasons for Multi-Factor Authentication

Protecting your cloud assets is one of the primary goals for security group. One of the primary ways unauthorized users get access to systems is by obtaining a valid username/password combination. Azure can help mitigate this with several features of Azure Active Directory including:

- **Password complexity rules.** This will force users to generate hard(er)-to-guess passwords.
- **Password expiration rules.** You can force users to change their passwords on a periodic basis (and avoid using previous-used passwords).
- **Self-service password reset (SSPR).** This allows users to self-serve and reset their password if they have forgotten it without involving an IT department.
- **Azure AD Identity Protection.** To help protect your organization's identities, you can configure risk-based policies that automatically respond to risky behaviors. These policies can either automatically block the behaviors or initiate remediation, including requiring password changes.
- **Azure AD password protection.** You can block commonly used and compromised passwords via a globally banned-password list.
- **Azure AD smart lockout.** Smart lockout helps lock out malicious hackers who are trying to guess your users' passwords or use brute-force methods to get in. It recognizes sign-ins coming from valid users and treats them differently than the ones of malicious hackers and other unknown sources.
- **Azure AD Application Proxy.** You can provision security-enhanced remote access to on-premises web applications.
- **Single sign-on (SSO)** access to your applications. This includes thousands of pre-integrated SaaS apps.
- **Azure AD Connect.** Create and manage a single identity for each user across your hybrid enterprise, keeping users, groups, and devices in sync.

These are all great options which deter someone *guessing* or *brute-forcing* a password. However, sometimes passwords are obtained through social engineering, or poor physical security. In these cases, the above features won't stop an intrusion. Instead, security administrators will want to turn to **Azure Multi-Factor Authentication (MFA)**.

## How Multi-Factor Authentication Works

Azure Multi-Factor Authentication (MFA) supplies added security for your identities by requiring two or more elements for full authentication.

These elements fall into three categories:

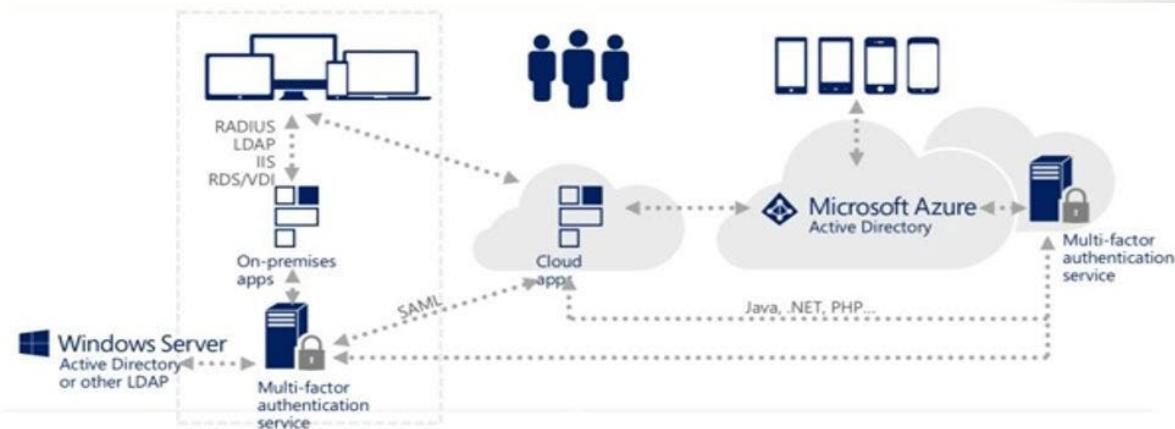
- **Something you know** - which might be a password or the answer to a security question.
- **Something you possess** - which might be a mobile app that receives a notification or a token-generating device.
- **Something you are** - which typically is a biometric property, such as a fingerprint or face scan used on many mobile devices.



Using Azure MFA increases identity security by limiting the impact of credential exposure. To fully authenticate, a malicious hacker who has a user's password would also need their phone or their fingerprint. Authentication with only a single factor is insufficient, and without authentication from Azure MFA, a malicious hacker is unable to use those credentials to authenticate. You should enable Azure MFA wherever possible, because it adds enormous benefits to security.

Azure MFA is the Microsoft two-step verification solution. Azure MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication via a range of verification methods, including phone call, text message, or mobile app verification. The security of Azure MFA lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for malicious hackers. Even if a malicious hacker manages to learn the user's password, it is useless without also possessing the trusted device. If the user loses the device, a person who finds it won't be able to use it without the user's password.

Here's what happens when someone tries to connect to a resource that's security enhanced by Azure MFA, and the service is on-premises:



1. The local Azure MFA service validates the initial sign-in request by passing the authentication request to on-premises Active Directory.
2. If the correct credentials were entered and validated, the service sends the request to **Azure Multi-Factor Authentication Server**.
3. The Azure Multi-Factor Authentication Server sends an additional verification challenge to the user. The methods you can easily configure are:
  - **Phone call.** Azure Multi-Factor Authentication Server places a call to the user's registered phone.

- **Text message.** Azure Multi-Factor Authentication Server sends a six-digit code to the user's mobile phone.
- **Mobile app notification.** Azure Multi-Factor Authentication Server sends a verification request to a user's smartphone, which asks them to complete the verification by selecting Verify in the mobile app.
- **Mobile app verification code.** Azure Multi-Factor Authentication Server sends a six-digit code to the user's mobile app. The user then enters this code on the sign-in page.
- **Initiative for Open Authentication (OATH) compliant tokens.** You can use these as a verification method.

If the service is running in Azure:

4. The service sends the sign-in request first to Azure AD for the initial validation and then to Azure Multi-Factor Authentication Server.
5. Azure Multi-Factor Authentication Server sends an additional verification challenge to the user, as just described.

Azure MFA allows the provider of the request service to validate that users are real people and not bots, that they have their devices with them, and that they can provide any additional information.

Azure MFA improves security for the requesting users, because someone can't easily impersonate them. You should require Azure MFA on all services, especially on mobile services.

## How to get Multi-Factor Authentication?

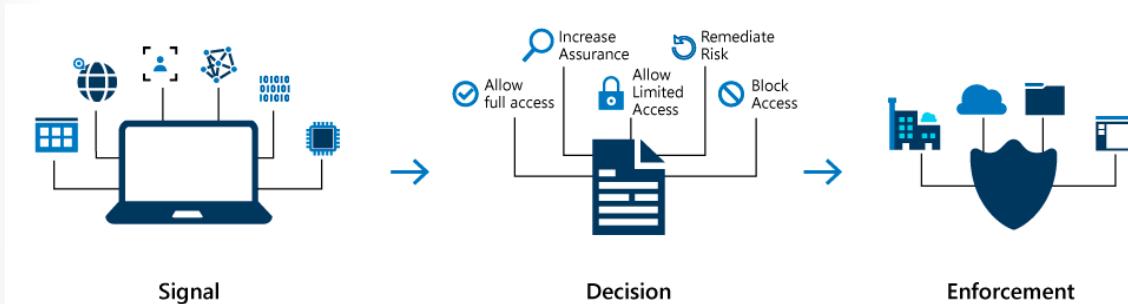
Multi-Factor Authentication comes as part of the following offerings:

- **Azure Active Directory Premium or Microsoft 365 Business** - Both of these offerings support Azure Multi-Factor Authentication using Conditional Access policies to require multi-factor authentication.
- **Azure AD Free** or standalone **Office 365** licenses - Use pre-created Conditional Access baseline protection policies to require multi-factor authentication for your users and administrators.
- **Azure Active Directory Global Administrators** - A subset of Azure Multi-Factor Authentication capabilities are available as a means to protect global administrator accounts.

## 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

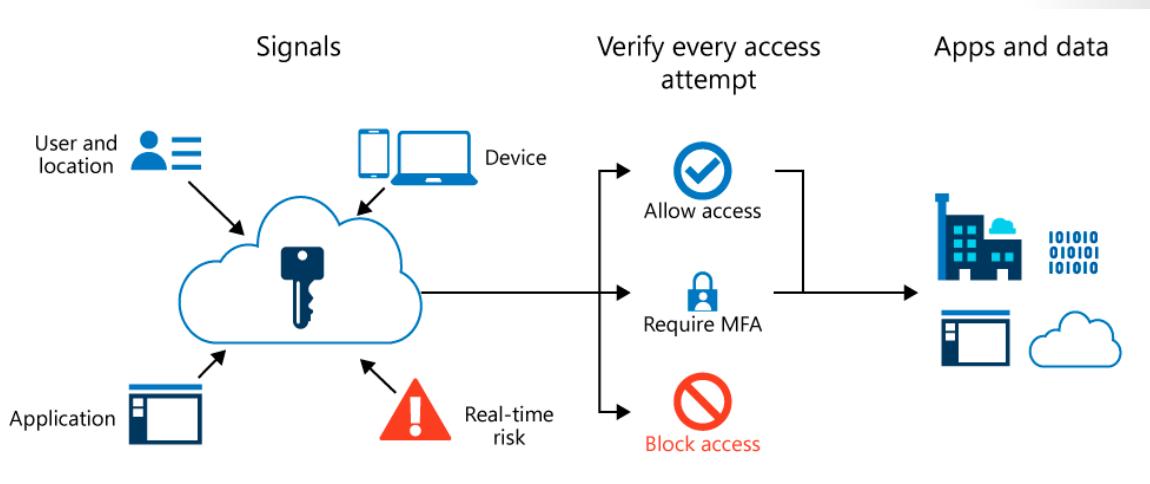
By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.

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.



## Plan for MFA Deployment

Consider rolling out MFA in waves. Start with a small group of pilot users to evaluate the complexity of your environment and identify any setup issues or unsupported apps or devices. Then broaden that group over time and evaluating the results with each pass until your entire company is enrolled.

Next, make sure to create a full communication plan. Azure MFA has several user interaction requirements including a registration process. Keep users informed every step of the way and let them know what they are required to do, important dates, and how to get answers to questions if they have trouble. Microsoft provides communication templates including posters, and email templates to help draft your communications.

## Azure MF policies

Azure Multi-factor Authentication is enforced with **Conditional Access** policies. Conditional Access policies are IF-THEN statements. **IF** a user wants to access a resource, **THEN** they must complete an action. For example, a payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it. Other common access requests that might require MFA include:

- **IF** a specific cloud application is accessed
- **IF** a user is accessing a specific network
- **IF** a user is accessing a specific client application
- **IF** a user is registering a new device

## Deciding supported authentication methods

When you turn on Azure MFA, you can choose the authentication methods you want to make available. You should always support more than one method so users have a backup option in case their primary method is unavailable. You can choose from the following methods:

Method	Description
Mobile App Verification code	A mobile authentication app such as the Microsoft Authenticator app can be used to retrieve an OATH verification code which is then entered into the sign-in interface. This code is changed every 30 seconds and the app works even if connectivity is limited. Note that this approach doesn't work in China on Android devices.
Call to a phone	Azure can call a supplied phone number. The user then approves the authentication using the keypad. This is a preferred backup method.
Text message to a phone	A text message with a verification code can be sent to a mobile phone. The user then enters the verification code into the sign-in interface to complete the authentication.

Administrators can enable one or more of the options above and then users can opt-in to each support authentication method they want to use.

## Selecting an authentication method

Finally, you must decide how users will register their selected methods. The easiest approach is to use Azure Active Directory Identity Protection. If your organization has licenses for Identity Protection, you can configure it to prompt users to register for MFA the next time they sign in.

Users can also be prompted to register for MFA when they try to use an application or service that requires multi-factor authentication. Finally, you can enforce registration using a Conditional Access policy applied to an Azure group containing all users in your organization. This approach requires some manual work to periodically review the group to remove registered users. There are some useful scripts in the documentation to automate some of this process.

# Five Steps for Securing Identity Infrastructure

## Five steps to Securing Identity Infrastructure

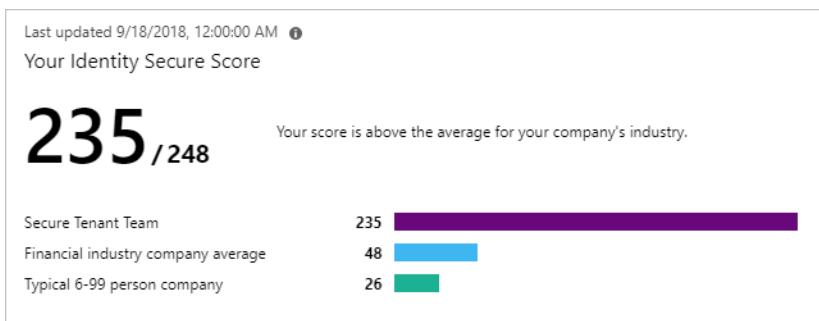
This lesson will help you get a more secure posture using the capabilities of Azure Active Directory by using a five-step checklist to inoculate your organization against cyber-attacks.

This checklist will help you quickly deploy critical recommended actions to protect your organization immediately by explaining how to:

- Step 1: Strengthen your credentials.
- Step 2: Reduce your attack surface area.
- Step 3: Automate threat response.
- Step 4: Utilize cloud intelligence.
- Step 5: Enable end-user self-service.

Many of the recommendations in this lesson apply only to applications that are configured to use Azure Active Directory as their identity provider. Configuring apps for Single Sign-On assures the benefits of credential policies, threat detection, auditing, logging, and other features add to those applications.

The recommendations in this lesson are aligned with the Identity Secure Score, an automated assessment of your Azure AD tenant's identity security configuration. Organizations can use the Identity Secure Score page in the Azure AD portal to find gaps in their current security configuration to ensure they follow current Microsoft best practices for security. Implementing each recommendation in the Secure Score page will increase your score and allow you to track your progress, plus help you compare your implementation against other similar size organizations or your industry.



## Step 1 - Strengthen Credentials

Most enterprise security breaches originate with an account compromised with one of a handful of methods such as password spray, breach replay, or phishing.

### Make sure your organization uses strong authentication

Given the frequency of passwords being guessed, phished, stolen with malware, or reused, it's critical to back the password with some form of strong credential.

To easily enable the basic level of identity security, you can use the one-click enablement with Azure AD Security Defaults. Security defaults enforce Azure MFA for all users in a tenant and blocks sign-ins from legacy protocols tenant-wide.

## Start banning commonly attacked passwords and turn off traditional complexity, and expiration rules.

Many organizations use the traditional complexity (requiring special characters, numbers, uppercase, and lowercase) and password expiration rules.

Azure AD's dynamic banned password feature uses current attacker behavior to prevent users from setting passwords that can easily be guessed. This capability is always on when users are created in the cloud, but is now also available for hybrid organizations when they deploy Azure AD password protection for Windows Server Active Directory. Azure AD password protection blocks users from choosing these common passwords and can be extended to block password containing custom keywords you specify. For example, you can prevent your users from choosing passwords containing your company's product names or a local sport team.

Microsoft recommends adopting the following modern password policy based on NIST guidance:

1. Require passwords have at least 8 characters. Longer isn't necessarily better, as they cause users to choose predictable passwords, save passwords in files, or write them down.
2. Disable expiration rules, which drive users to easily guessed passwords such as **Spring2019!**
3. Disable character-composition requirements and prevent users from choosing commonly attacked passwords, as they cause users to choose predictable character substitutions in passwords.

## Protect against leaked credentials and add resilience against outages

If your organization uses a hybrid identity solution with pass-through authentication or federation, then you should enable password hash sync for the following two reasons:

- The **Users with leaked credentials report** in the Azure AD management warns you of username and password pairs, which have been exposed on the "dark web." An incredible volume of passwords is leaked via phishing, malware, and password reuse on third-party sites that are later breached. Microsoft finds many of these leaked credentials and will tell you, in this report, if they match credentials in your organization – but only if you enable password hash sync!
- In the event of an on-premises outage (for example, in a ransomware attack) you can switch over to using cloud authentication using password hash sync. This backup authentication method will allow you to continue accessing apps configured for authentication with Azure Active Directory, including Office 365. In this case, IT staff won't need to resort to personal email accounts to share data until the on-premises outage is resolved.

## Implement AD FS extranet smart lockout

Organizations, which configure applications to authenticate directly to Azure AD benefit from Azure AD smart lockout. If you use AD FS in Windows Server 2012R2, implement AD FS extranet lockout protection. If you use AD FS on Windows Server 2016, implement extranet smart lockout. AD FS Smart Extranet lockout protects against brute force attacks, which target AD FS while preventing users from being locked out in Active Directory.

## Take advantage of intrinsically secure, easier to use credentials

Using Windows Hello, you can replace passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied securely to a device and uses a biometric or PIN.

## Step 2 - Reduce Attack Surface

Apps using their own legacy methods to authenticate with Azure AD and access company data, pose another risk for organizations. Examples of apps using legacy authentication are POP3, IMAP4, or SMTP clients. Legacy authentication apps authenticate on behalf of the user and prevent Azure AD from doing advanced security evaluations. The alternative, modern authentication, will reduce your security risk, because it supports multi-factor authentication and Conditional Access. We recommend the following three actions:

1. Block legacy authentication if you use AD FS.
2. Setup SharePoint Online and Exchange Online to use modern authentication.
3. If you have Azure AD Premium, use Conditional Access policies to block legacy authentication, otherwise use Azure AD Security Defaults.

## Block invalid authentication entry points

Using the assume breach mentality, you should reduce the impact of compromised user credentials when they happen. For each app in your environment consider the valid use cases: which groups, which networks, which devices and other elements are authorized – then block the rest. With Azure AD Conditional Access, you can control how authorized users access their apps and resources based on specific conditions you define.

## Restrict user consent operations

It's important to understand the various Azure AD application consent experiences, the types of permissions and consent, and their implications on your organization's security posture. By default, all users in Azure AD can grant applications that leverage the Microsoft identity platform to access your organization's data. While allowing users to consent by themselves does allow users to easily acquire useful applications that integrate with Microsoft 365, Azure and other services, it can represent a risk if not used and monitored carefully.

Microsoft recommends disabling future user consent operations to help reduce your surface area and mitigate this risk. If end-user consent is disabled, previous consent grants will still be honored but all future consent operations must be performed by an administrator. Admin consent can be requested by users through an integrated admin consent request workflow or through your own support processes. Before disabling end-user consent, use our recommendations to plan this change in your organization. For applications you wish to allow all users to access, consider granting consent on behalf of all users, making sure users who have not yet consented individually will be able to access the app. If you do not want these applications to be available to all users in all scenarios, use application assignment and Conditional Access to restrict user access to specific apps.

## Implement Azure AD Privileged Identity Management

Another impact of “assume breach” is the need to minimize the likelihood a compromised account can operate with a privileged role.

Azure AD Privileged Identity Management (PIM) helps you minimize account privileges by helping you:

- Identify and manage users assigned to administrative roles.
- Understand unused or excessive privilege roles you should remove.
- Establish rules to make sure privileged roles are protected by multi-factor authentication.
- Establish rules to make sure privileged roles are granted only long enough to accomplish the privileged task.

Enable Azure AD PIM, then view the users who are assigned administrative roles and remove unnecessary accounts in those roles. For remaining privileged users, move them from permanent to eligible. Finally, establish appropriate policies to make sure when they need to gain access to those privileged roles, they can do so securely, with the necessary change control.

## Step 3 - Automate Threat Response

Azure Active Directory has many capabilities that automatically intercept attacks, to remove the latency between detection and response. You can reduce the costs and risks, when you reduce the time criminals use to embed themselves into your environment. Here are the concrete steps you can take.

## Implement user risk security policy using Azure AD Identity Protection

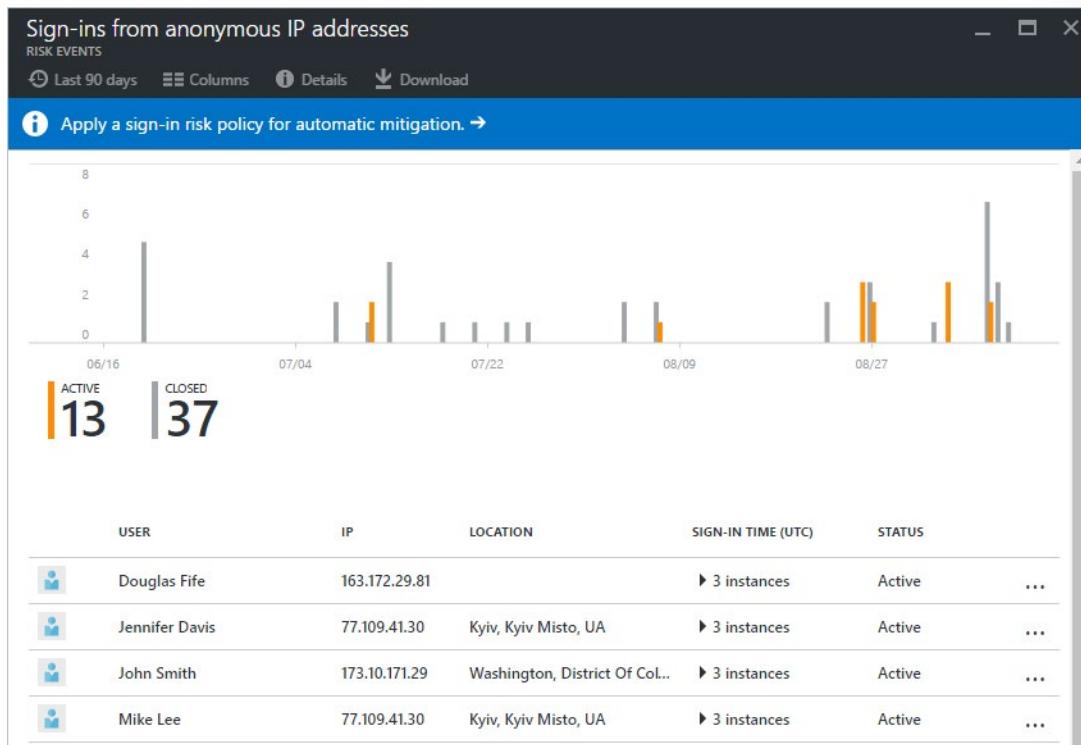
User risk indicates the likelihood a user's identity has been compromised and is calculated based on the user risk detections that are associated with a user's identity. A user risk policy is a Conditional Access policy that evaluates the risk level to a specific user or group. Based on Low, Medium, High risk-level, a policy can be configured to block access or require a secure password change using multi-factor authentication. Microsoft's recommendation is to require a secure password change for users on high risk.

The screenshot shows the Azure AD Identity Protection interface. The left sidebar includes sections for Overview, Getting started, Users flagged for risk (which is selected), Risk events, Vulnerabilities, Multi-factor authentication regi..., User risk policy, and Sign-in risk policy. The main content area has a search bar and a blue header bar with the text "Apply a user risk policy for automatic mitigation." Below this is a table with columns: USER, MFA, RISK LEVEL, RISK EVENTS, STATUS, and LAST UPDATED (UTC). The table lists several users with their respective details:

USER	MFA	RISK LEVEL	RISK EVENTS	STATUS	LAST UPDATED (UTC)
John Nash		High	215 risk events	At risk	12/7/2016 10:51 AM
Jon Doe	✓	Medium	1 risk event	At risk	11/15/2016 7:18 PM
Junpu Chen	✓	Medium	0 risk events	At risk	9/12/2016 10:57 AM
Security Admin	✓	Medium	0 risk events	At risk	8/23/2016 2:40 PM
Security Reader	✓	Medium	0 risk events	At risk	8/23/2016 2:40 PM
Ben Hecht		Secured	0 risk events	Remediated	1/31/2016 3:21 PM
On-Premises Directory Synchroniz...		Secured	0 risk events	Remediated	12/14/2015 7:21 PM
secReader2		Secured	0 risk events	Remediated	9/7/2016 5:18 AM

## Implement sign-in risk policy using Azure AD Identity Protection

Sign-in risk is the likelihood someone other than the account owner is attempting to sign on using the identity. A sign-in risk policy is a Conditional Access policy that evaluates the risk level to a specific user or group. Based on the risk level (high/medium/low), a policy can be configured to block access or force multi-factor authentication. Make sure you force multi-factor authentication on Medium or above risk sign-ins.



## Step 4 - Utilize Cloud Intelligence

Auditing and logging of security-related events and related alerts are essential components of an efficient protection strategy. Security logs and reports provide you with an electronic record of suspicious activities and help you detect patterns that may indicate attempted or successful external penetration of the network, and internal attacks. You can use auditing to monitor user activity, document regulatory compliance, do forensic analysis, and more. Alerts provide notifications of security events.

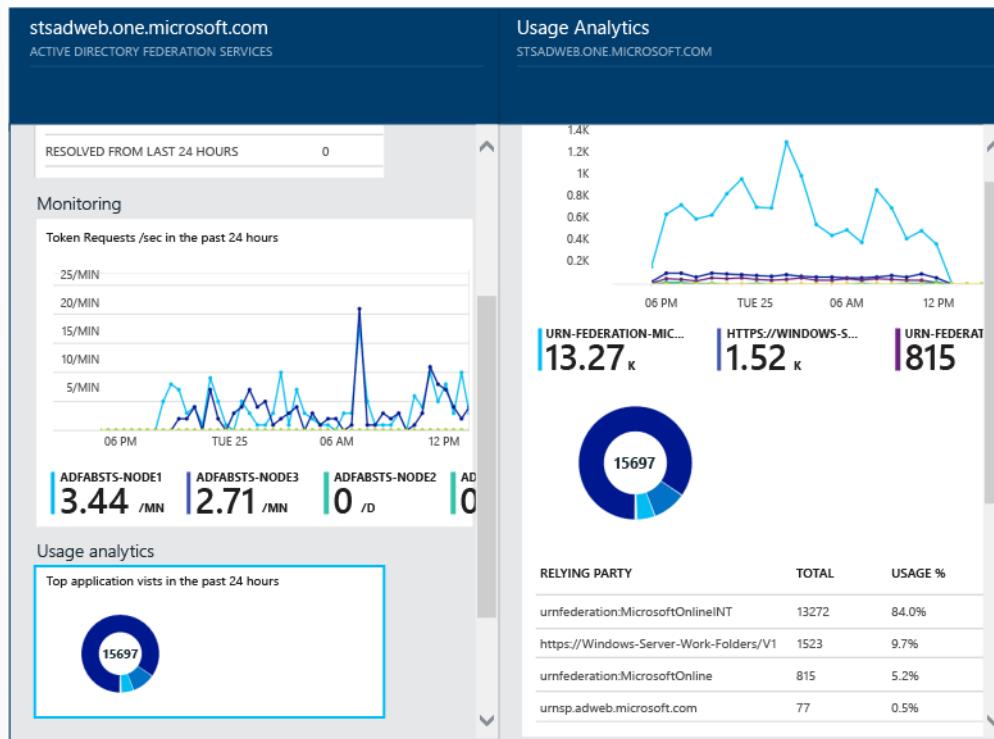
### Monitor Azure AD

Microsoft Azure services and features provide you with configurable security auditing and logging options to help you identify gaps in your security policies and mechanisms and address those gaps to help prevent breaches. You can use Azure Logging and Auditing and use Audit activity reports in the Azure Active Directory portal.

### Monitor Azure AD Connect Health in hybrid environments

Monitoring AD FS with Azure AD Connect Health provides you with greater insight into potential issues and visibility of attacks on your AD FS infrastructure. Azure AD Connect Health delivers alerts with details,

resolution steps, and links to related documentation; usage analytics for several metrics related to authentication traffic; performance monitoring and reports.

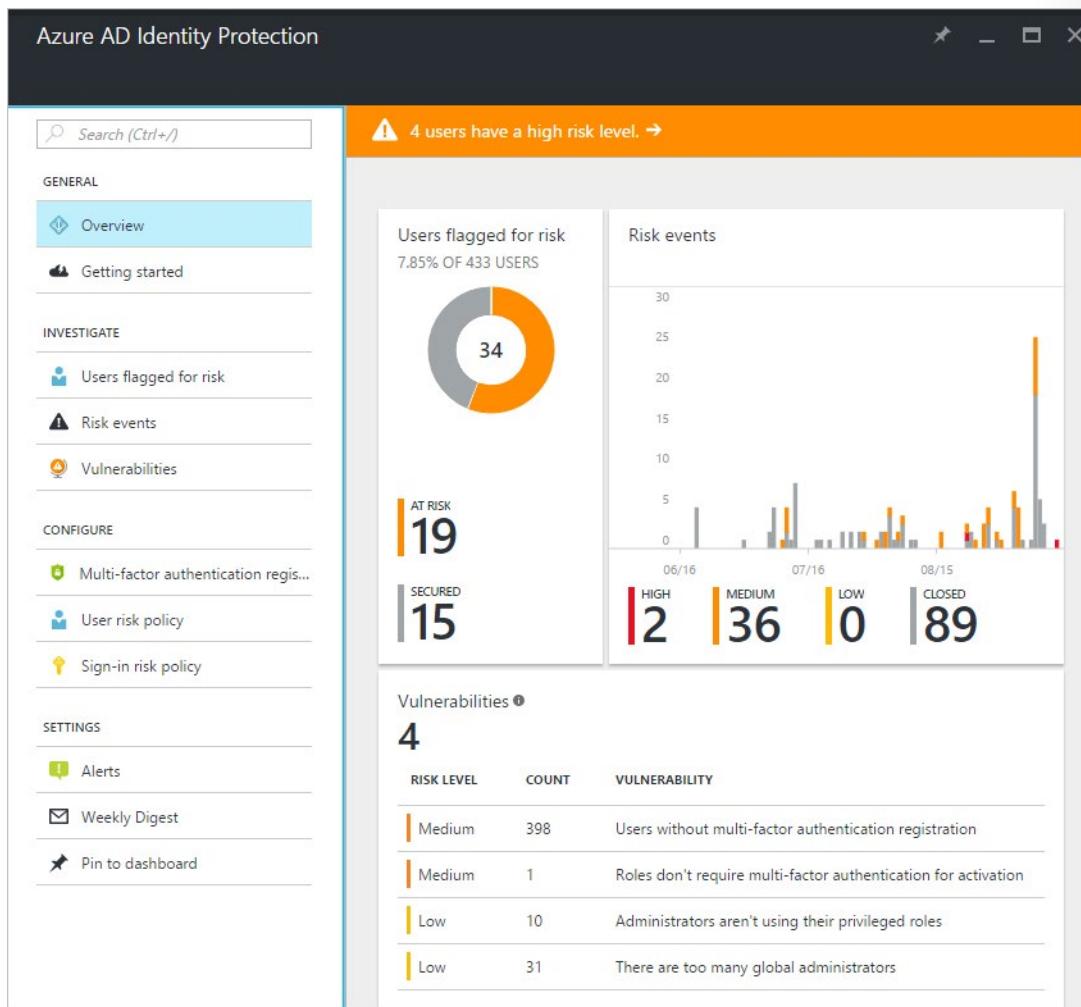


## Monitor Azure AD Identity Protection events

Azure AD Identity Protection is a notification, monitoring and reporting tool you can use to detect potential vulnerabilities affecting your organization's identities. It detects risk detections, such as leaked credentials, impossible travel, and sign-ins from infected devices, anonymous IP addresses, IP addresses associated with the suspicious activity, and unknown locations. Enable notification alerts to receive email of users at risk and/or a weekly digest email.

Azure AD Identity Protection provides two important reports you should monitor daily:

1. **Risky sign-in reports** will surface user sign-in activities you should investigate, the legitimate owner may not have performed the sign-in.
2. **Risky user reports** will surface user accounts that may have been compromised, such as leaked credential that was detected or the user signed in from different locations causing an impossible travel event.



## Audit apps and consented permissions

Users can be tricked into navigating to a compromised web site or apps that will gain access to their profile information and user data, such as their email. Administrators should review and audit the permissions given by users or disable the ability of users to give consent by default.

## Step 5 - Enable End-User Self-Service

As much as possible you'll want to balance security with productivity. Along the same lines of approaching your journey with the mindset that you're setting a foundation for security in the long run, you can remove friction from your organization by empowering your users while remaining vigilant.

## Implement self-service password reset

Azure AD's self-service password reset (SSPR) offers a simple means for IT administrators to allow users to reset or unlock their passwords or accounts without help desk or administrator intervention. The system includes detailed reporting that tracks when users have reset their passwords, along with notifications to alert you to misuse or abuse.

## Implement self-service group and application access

Azure AD provides the ability to non-administrators to manage access to resources, using security groups, Office 365 groups, application roles, and access package catalogs. Self-service group management enables group owners to manage their own groups, without needing to be assigned an administrative role. Users can also create and manage Office 365 groups without relying on administrators to handle their requests, and unused groups expire automatically.

Azure AD entitlement management further enables delegation and visibility, with comprehensive access request workflows and automatic expiration. You can delegate to non-administrators the ability to configure their own access packages for groups, Teams, applications, and SharePoint Online sites they own, with custom policies for who is required to approve access, including configuring employee's managers and business partner sponsors as approvers.

## Implement Azure AD access reviews

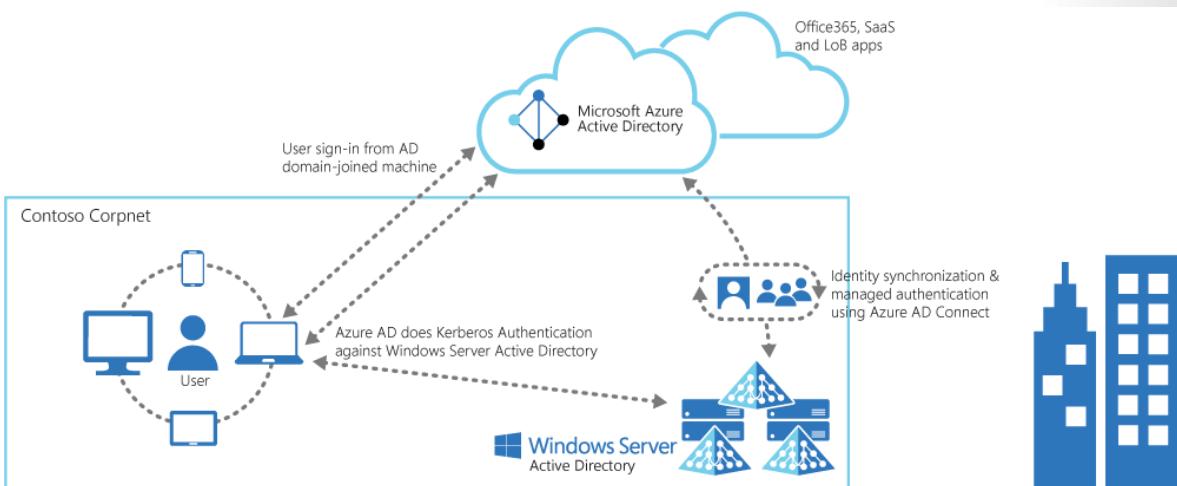
With Azure AD access reviews, you can manage access package and group memberships, access to enterprise applications, and privileged role assignments to make sure you maintain a security standard. Regular oversight by the users themselves, resource owners, and other reviewers ensure that users don't retain access for extended periods of time when they no longer need it.

## Recommend a Solution for Single-Sign On (SSO)

### Azure Active Directory Seamless Single Sign-On (SSO)

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods. Seamless SSO is not applicable to Active Directory Federation Services (ADFS).



✓ **Important**

Seamless SSO needs the user's device to be domain-joined only, but it is not used on Azure AD Joined or Hybrid Azure AD joined devices. SSO on Azure AD joined and Hybrid Azure AD joined works based on the primary refresh token.

### Key benefits

- User experience
  - Users are automatically signed into both on-premises and cloud-based applications.
  - Users don't have to enter their passwords repeatedly.
- Easy to deploy & administer
  - No additional components needed on-premises to make this work.
  - Works with any method of cloud authentication - Password Hash Synchronization or Pass-through Authentication.
  - Can be rolled out to some or all your users using Group Policy.
  - Register non-Windows 10 devices with Azure AD without the need for any AD FS infrastructure. This capability needs you to use version 2.1 or later of the workplace-join client.

## Features

- Sign-in username can be either the on-premises default username (`userPrincipalName`) or another attribute configured in Azure AD Connect (Alternate ID). Both use cases work because Seamless SSO uses the `securityIdentifier` claim in the Kerberos ticket to look up the corresponding user object in Azure AD.
- Seamless SSO is an opportunistic feature. If it fails for any reason, the user sign-in experience goes back to its regular behavior - i.e, the user needs to enter their password on the sign-in page.
- If an application (for example, `https://myapps.microsoft.com/contoso.com`) forwards a `domain_hint` (OpenID Connect) or `wrh` (SAML) parameter - identifying your tenant, or `login_hint` parameter - identifying the user, in its Azure AD sign-in request, users are automatically signed in without them entering usernames or passwords.
- Users also get a silent sign-on experience if an application (for example, `https://contoso.sharepoint.com`) sends sign-in requests to Azure AD's endpoints set up as tenants - that is, `https://login.microsoftonline.com/contoso.com/<...>` or `https://login.microsoftonline.com/<tenant_ID>/<...>` - instead of Azure AD's common endpoint - that is, `https://login.microsoftonline.com/common/<...>`.
- Sign out is supported. This allows users to choose another Azure AD account to sign in with, instead of being automatically signed in using Seamless SSO automatically.
- Office 365 Win32 clients (Outlook, Word, Excel, and others) with versions 16.0.8730.xxxx and above are supported using a non-interactive flow. For OneDrive, you will have to activate the OneDrive silent config feature for a silent sign-on experience.
- It can be enabled via Azure AD Connect.
- It is a free feature, and you don't need any paid editions of Azure AD to use it.
- It is supported on web browser-based clients and Office clients that support modern authentication on platforms and browsers capable of Kerberos authentication:

OS\Browser	Internet Explorer	Microsoft Edge	Google Chrome	Mozilla Firefox	Safari
Windows 10	Yes*	Yes	Yes	Yes***	N/A
Windows 8.1	Yes*	N/A	Yes	Yes***	N/A
Windows 8	Yes*	N/A	Yes	Yes***	N/A
Windows 7	Yes*	N/A	Yes	Yes***	N/A
Windows Server 2012 R2 or above	Yes**	N/A	Yes	Yes***	N/A
Mac OS X	N/A	N/A	Yes***	Yes***	Yes***

\*Requires Internet Explorer versions 10 or above

\*\*Requires Internet Explorer versions 10 or above. Disable Enhanced Protected Mode

\*\*\*Requires **additional configuration**<sup>3</sup>

✓ Note

For Windows 10, the recommendation is to use Azure AD Join for the optimal single sign-on experience with Azure AD.

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start>

# Considerations - Azure AD Seamless Single Sign-On

Below are key considerations for recommending Azure Active Directory Seamless Single Sign-On (Seamless SSO).

## What sign-in methods do Seamless SSO work with?

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods. This feature cannot be used with Active Directory Federation Services (ADFS).

## Is Seamless SSO a free feature?

Seamless SSO is a free feature and you don't need any paid editions of Azure AD to use it.

## Is Seamless SSO available in the Microsoft Azure Germany cloud and the Microsoft Azure Government cloud?

No. Seamless SSO is only available in the worldwide instance of Azure AD.

## What applications take advantage of domain\_hint or login\_hint parameter capability of Seamless SSO?

Listed below is a non-exhaustive list of applications that can send these parameters to Azure AD, and therefore provides users a silent sign-on experience using Seamless SSO (i.e., no need for your users to input their usernames or passwords):

Application name	Application URL to be used
Access panel	<a href="https://myapps.microsoft.com/contoso.com">https://myapps.microsoft.com/contoso.com</a>
Outlook on Web	<a href="https://outlook.office365.com/contoso.com">https://outlook.office365.com/contoso.com</a>
Office 365 portals	<a href="https://portal.office.com?domain_hint=contoso.com">https://portal.office.com?domain_hint=contoso.com</a> , <a href="https://www.office.com?domain_hint=contoso.com">https://www.office.com?domain_hint=contoso.com</a>

In addition, users get a silent sign-on experience if an application sends sign-in requests to Azure AD's endpoints set up as tenants - that is, `https://login.microsoftonline.com/contoso.com/<..>` or `https://login.microsoftonline.com/<tenant_ID>/<..>` – instead of Azure AD's common endpoint - that is, `https://login.microsoftonline.com/common/<...>`. Listed below is a non-exhaustive list of applications that make these types of sign-in requests.

Application name	Application URL to be used
SharePoint Online	<a href="https://contoso.sharepoint.com">https://contoso.sharepoint.com</a>
Azure portal	<a href="https://portal.azure.com/contoso.com">https://portal.azure.com/contoso.com</a>

In the above tables, replace "contoso.com" with your domain name to get to the right application URLs for your tenant.

If you want other applications using our silent sign-on experience, let us know in the feedback section.

## Does Seamless SSO support Alternate ID as the username, instead of userPrincipalName?

Yes. Seamless SSO supports Alternate ID as the username when configured in Azure AD Connect as shown [here<sup>4</sup>](#). Not all Office 365 applications support Alternate ID. Refer to the specific application's documentation for the support statement.

## What is the difference between the single sign-on experience provided by Azure AD Join and Seamless SSO?

Azure AD Join provides SSO to users if their devices are registered with Azure AD. These devices don't necessarily have to be domain-joined. SSO is provided using *primary refresh tokens* or PRTs, and not Kerberos. The user experience is most optimal on Windows 10 devices. SSO happens automatically on the Microsoft Edge browser. It also works on Chrome with the use of a browser extension.

You can use both Azure AD Join and Seamless SSO on your tenant. These two features are complementary. If both features are turned on, then SSO from Azure AD Join takes precedence over Seamless SSO.

## To register non-Windows 10 devices with Azure AD, without using AD FS, can Seamless SSO be used instead?

Yes, this scenario needs version 2.1 or later of the workplace-join client.

---

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

## Recommend a Solution for a Hybrid Identity

### Considerations - Multi-Factor Authentication for Hybrid Identity

An evaluation is important to define the technical requirements for setting up and enabling the organizations users for multi-factor authentication.

Answer the following:

- Is your company trying to secure Microsoft apps?
- How are apps published?
- Does your company provide remote access to allow employees to access on-premises apps?

If yes, what type of remote access? You also need to evaluate where the users who are accessing these applications will be located. This evaluation is another important step to define the proper multi-factor authentication strategy. Make sure to answer the following questions:

- Where are the users going to be located?
- Can they be located anywhere?
- Does your company want to establish restrictions according to the user's location?

It's important to also evaluate the user's requirements for multi-factor authentication. This evaluation is important because it will define the requirements for rolling out multi-factor authentication. Make sure to answer the following questions:

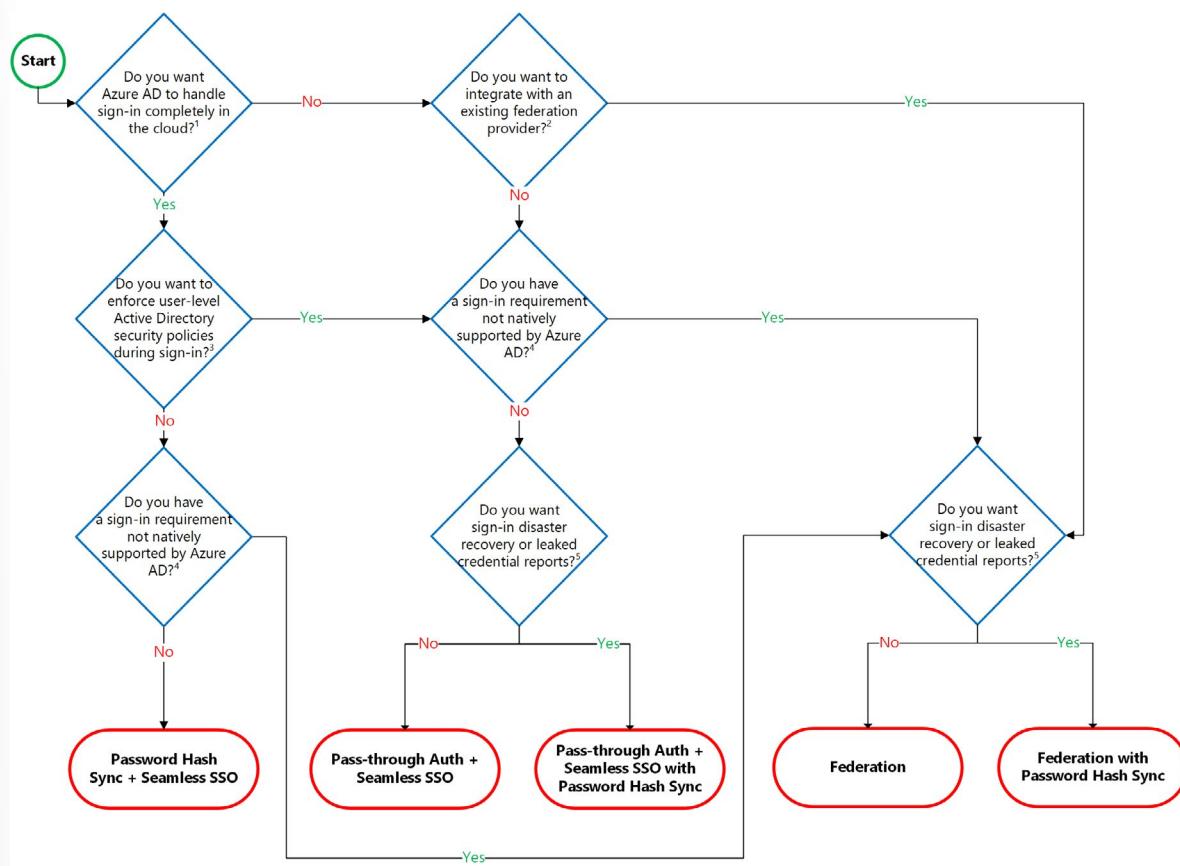
- Are the users familiar with multi-factor authentication?
- Will some uses be required to provide additional authentication?
- If yes, all the time, when coming from external networks, or accessing specific applications, or under other conditions?
  - Will the users require training on how to setup and implement multi-factor authentication?
  - What are the key scenarios that your company wants to enable multi-factor authentication for their users?

You should now understand if there are multi-factor authentication already implemented on-premises. This evaluation is important to define the technical requirements for setting up and enabling the organizations users for multi-factor authentication. Make sure to answer the following questions:

- Does your company need to protect privileged accounts with MFA?
- Does your company need to enable MFA for certain application for compliance reasons?
- Does your company need to enable MFA for all eligible users of these application or only administrators?
- Do you need have MFA always enabled or only when the users are logged outside of your corporate network?

### Hybrid Identity Decision Tree

The following topics helps you decide which authentication method is right for you by using a decision tree. It helps you determine whether to deploy cloud or federated authentication for your Azure AD hybrid identity solution.



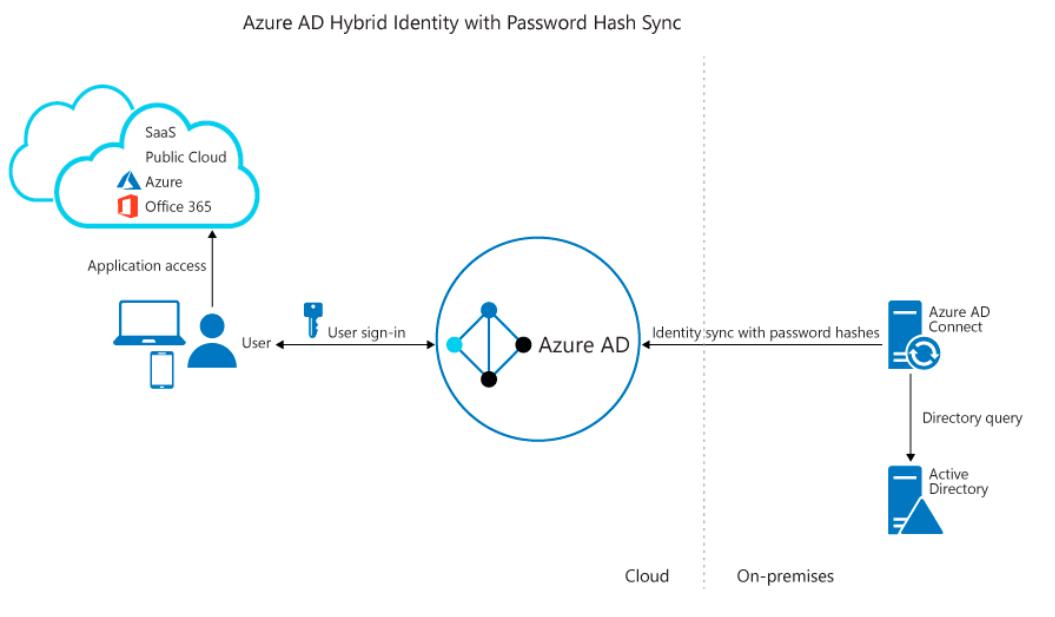
Details on decision questions:

1. Azure AD can handle sign-in for users without relying on on-premises components to verify passwords.
2. Azure AD can hand off user sign-in to a trusted authentication provider such as Microsoft's AD FS.
3. If you need to apply user-level Active Directory security policies such as account expired, disabled account, password expired, account locked out, and sign-in hours on each user sign-in, Azure AD requires some on-premises components.
4. Sign-in features not natively supported by Azure AD:
  - Sign-in using smartcards or certificates.
  - Sign-in using on-premises MFA Server.
  - Sign-in using third-party authentication solution.
  - Multi-site on-premises authentication solution.
5. Azure AD Identity Protection requires Password Hash Sync regardless of which sign-in method you choose, to provide the Users with leaked credentials report. Organizations can fail over to Password Hash Sync if their primary sign-in method fails and it was configured before the failure event.

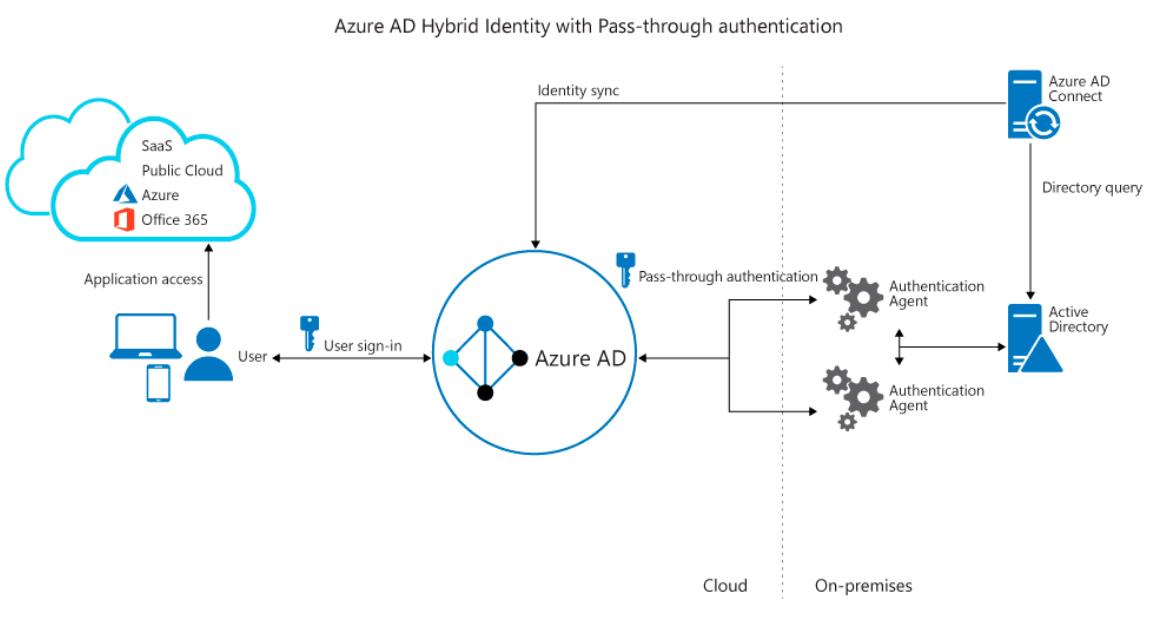
## Authentication Architecture

The following diagrams outline the high-level architecture components required for each authentication method you can use with your Azure AD hybrid identity solution. They provide an overview to help you compare the differences between the solutions.

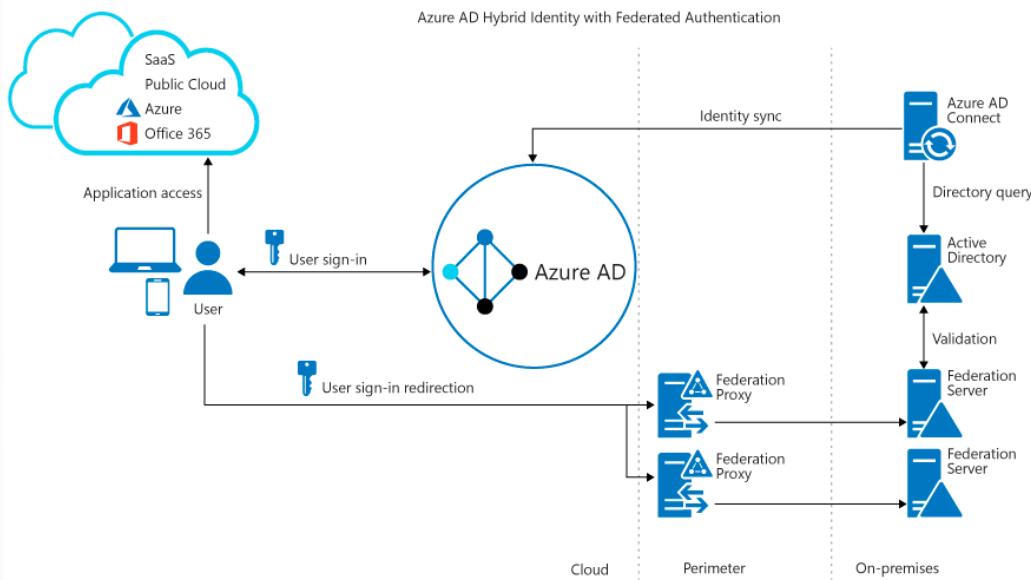
- Simplicity of a password hash synchronization solution:



- Agent requirements of pass-through authentication, using two agents for redundancy:



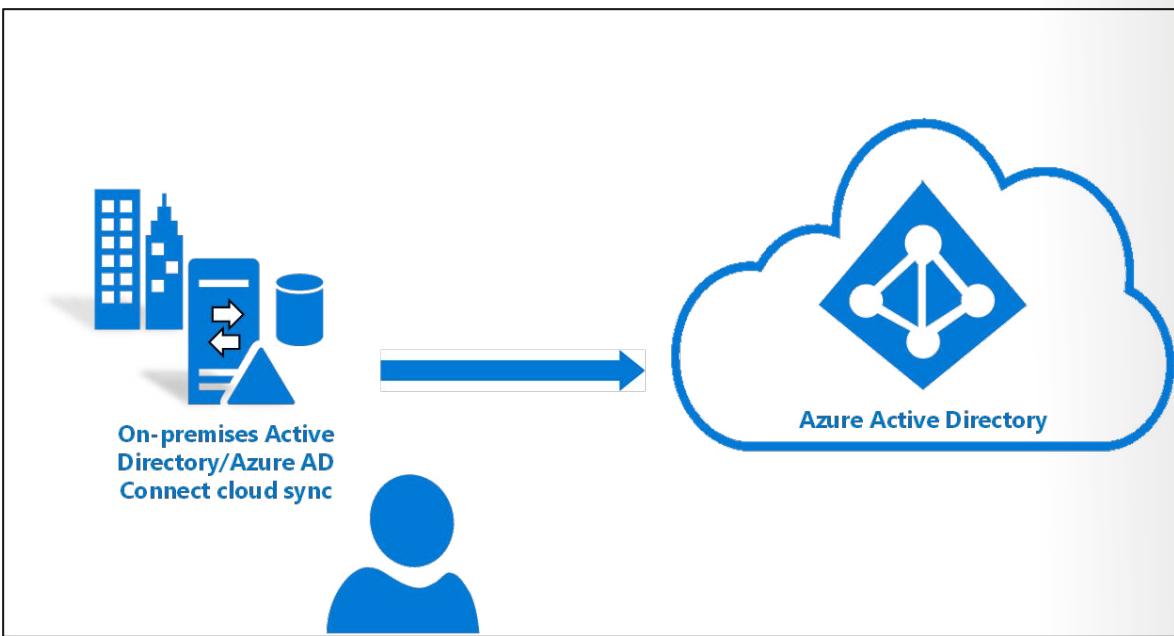
- Components required for federation in your perimeter and internal network of your organization:



## Azure AD Connect cloud sync

Azure AD Connect cloud sync is new offering from Microsoft designed to meet and accomplish your hybrid identity goals for synchronization of users, groups and contacts to Azure AD. It accomplishes this by using the Azure AD cloud provisioning agent instead of the Azure AD Connect application. However, it can be used alongside Azure AD Connect sync and it provides the following benefits:

- Support for synchronizing to an Azure AD tenant from a multi-forest disconnected Active Directory forest environment: The common scenarios include merger & acquisition (where the acquired company's AD forests are isolated from the parent company's AD forests), and companies that have historically had multiple AD forests.
- Simplified installation with light-weight provisioning agents: The agents act as a bridge from AD to Azure AD, with all the sync configuration managed in the cloud.
- Multiple provisioning agents can be used to simplify high availability deployments, particularly critical for organizations relying upon password hash synchronization from AD to Azure AD.
- Support for large groups with up to 50K members. It is recommended to use only the OU scoping filter when synchronizing large groups.



## Comparing Authentication Methods

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
<b>Where does authentication happen?</b>	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
<b>What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?</b>	None	One server for each additional authentication agent
<b>What are the requirements for on-premises Internet and networking beyond the provisioning system?</b>	None	Outbound Internet access from the servers running authentication agents
<b>Is there a TLS/SSL certificate requirement?</b>	No	No
<b>Is there a health monitoring solution?</b>	Not required	Agent status provided by Azure Active Directory admin center
<b>Do users get single sign-on to cloud resources from domain-joined devices within the company network?</b>	Yes with Seamless SSO	Yes with Seamless SSO
<b>What sign-in types are supported?</b>	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID

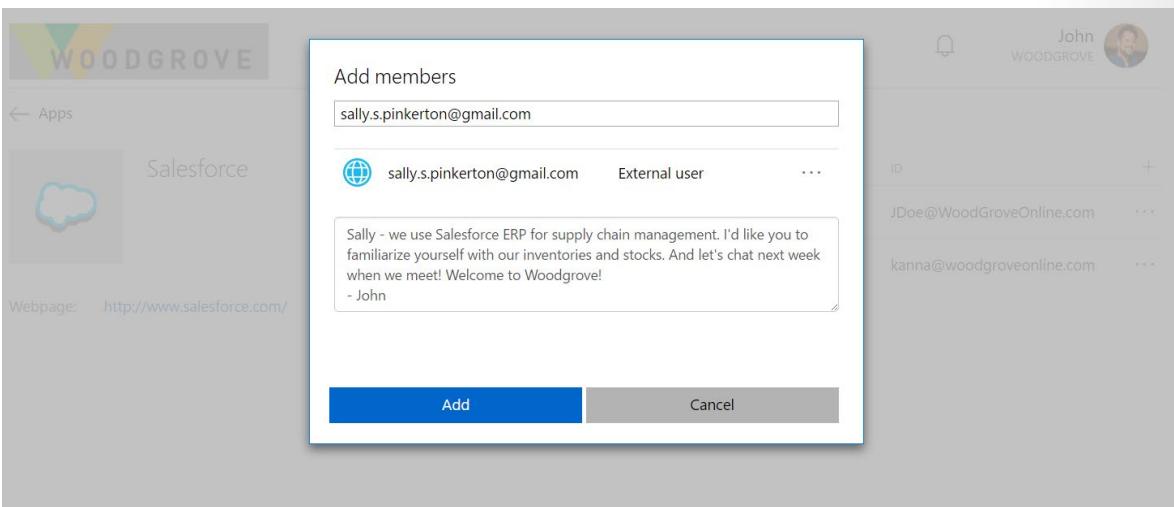
Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
<b>What are the multifactor authentication options?</b>	Azure MFA      Custom Controls with Conditional Access*	Azure MFA      Custom Controls with Conditional Access*
<b>What are the Conditional Access options?</b>	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

## Recommend a Solution for B2B Integration

### Azure Active Directory B2B

With Azure AD B2B, the partner uses their own identity management solution, so there is no external administrative overhead for your organization.

- The partner uses their own identities and credentials.
- You don't need to manage external accounts or passwords.
- You don't need to sync accounts or manage account lifecycles.



### Invite guest users with a simple invitation and redemption process

Guest users sign in to your apps and services with their own work, school, or social identities. If the guest user doesn't have a Microsoft account or an Azure AD account, one is created for them when they redeem their invitation.

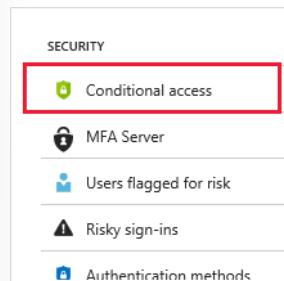
- Invite guest users using the email identity of their choice.
- Send a direct link to an app, or send an invitation to the guest user's own Access Panel.
- Guest users follow a few simple redemption steps to sign in.



### Use policies to securely share your apps and services

You can use authorization policies to protect your corporate content. Conditional Access policies, such as multi-factor authentication, can be enforced:

- At the tenant level.
- At the application level.
- For specific guest users to protect corporate apps and data.



## Add Guest Users in the Azure AD Portal

As an administrator, you can easily add guest users to your organization in the Azure portal.

- Create a new guest user in Azure AD, similar to how you'd add a new user.
- The guest user immediately receives a customizable invitation that lets them sign in to their Access Panel.
- Guest users in the directory can be assigned to apps or groups.

New user - Microsoft Azure

Microsoft Azure

Home > Users - All users > New user

**New user**

Identity

Email address \*

**Personal message**

Hello! We're excited to have you with us on the new project.

Accept this invitation and you'll get access to all the apps that you need. Let me know if you have any questions.

Thanks,  
Tami Weiss, Contoso administrator

**Invite**

## Let application and group owners manage their own guest users

You can delegate guest user management to application owners so that they can add guest users directly to any application they want to share, whether it's a Microsoft application or not.

- Administrators set up self-service app and group management.
- Non-administrators use their Access Panel to add guest users to applications or groups.

Access Panel Applications

Secure | https://account.activedirectory.windowsazure.com/#/applications

contoso

Sam  
CONTOSO

Apps

+ Add app

Search apps

Box	Concur	G Suite	Groups
GoToMeeting	Jive	Lucidchart	
Salesforce	Security & Compli...	Store	

**Open**

**Manage app**

## Integrate with Identity Providers

Azure AD supports external identity providers like Facebook, Microsoft accounts, Google, or enterprise identity providers. You can set up federation with identity providers so your external users can sign in with their existing social or enterprise accounts instead of creating a new account just for your application. Learn more about identity providers for External Identities.

The screenshot shows the 'External Identities | All identity providers' page in Microsoft Azure Active Directory. On the left, there's a sidebar with links like 'Get started', 'All identity providers' (which is selected and highlighted in grey), 'External collaboration settings', 'Diagnose and solve problems', 'Self-service sign up', 'Custom user attributes (Preview)', 'User flows (Preview)', 'Lifecycle management', and 'Terms of use'. The main area has a search bar at the top. Below it, there are two sections: 'Social identity providers' (with 'Facebook' listed) and 'SAML/WS-Fed identity providers' (with a search bar). At the bottom, there are filters for 'Domain', 'Protocol', and 'Issuer'.

## Create a self-service sign-up user flow

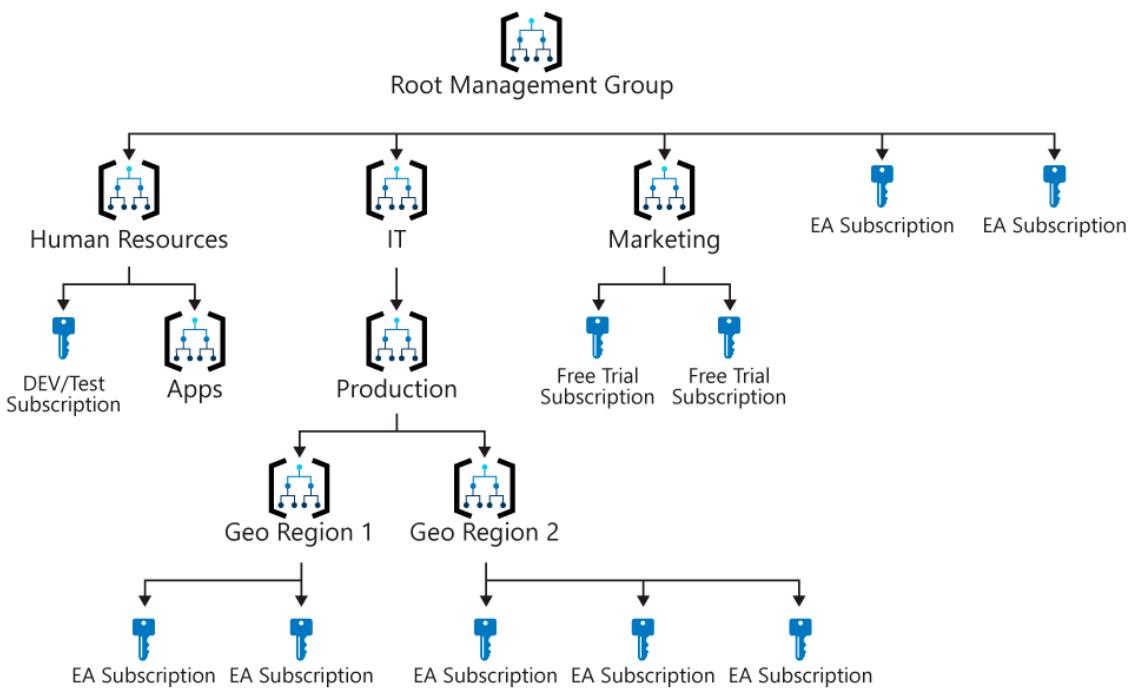
With a self-service sign-up user flow, you can create a sign-up experience for external users who want to access your apps. As part of the sign-up flow, you can provide options for different social or enterprise identity providers, and collect information about the user. Learn about self-service sign-up and how to set it up.

The screenshot shows the 'User Flows' management page in Microsoft Azure Active Directory. The left sidebar includes 'Overview' (selected), 'Settings', 'Identity providers', 'User attributes', 'Customize', 'Page layouts', 'Languages', 'Use', and 'Applications'. The main area has a 'Delete' button and a feedback message: 'Got a second? We would love your feedback on the user flows management experience →'. Below that, there are three sections: 'Settings' (with 'Identity providers' listed as 'Azure Active Directory Sign up' and 'Facebook'), 'User attributes' (with 'Email Address' and 'Postal Code' listed), and 'Customize' (with 'Page layouts' listed as 'Classic').

# Recommend a Hierarchical Structure for Management Groups, Subscriptions and Resource Groups

## Hierarchy of Management Groups and Subscriptions

You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management. The following diagram shows an example of creating a hierarchy for governance using management groups.



You can create a hierarchy that applies a policy, for example, which limits VM locations to the US West Region in the group called "Production". This policy will inherit onto all the Enterprise Agreement (EA) subscriptions that are descendants of that management group and will apply to all VMs under those subscriptions. This security policy cannot be altered by the resource or subscription owner allowing for improved governance.

Another scenario where you would use management groups is to provide user access to multiple subscriptions. By moving multiple subscriptions under that management group, you can create one role-based access control (RBAC) assignment on the management group, which will inherit that access to all the subscriptions. One assignment on the management group can enable users to have access to everything they need instead of scripting RBAC over different subscriptions.

### Important facts about management groups

- 10,000 management groups can be supported in a single directory.

- A management group tree can support up to six levels of depth.
  - This limit doesn't include the Root level or the subscription level.
- Each management group and subscription can only support one parent.
- Each management group can have many children.
- All subscriptions and management groups are within a single hierarchy in each directory.

## Root Management Group for Each Directory

Each directory is given a single top-level management group called the "Root" management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and RBAC assignments to be applied at the directory level. The Azure AD Global Administrator needs to elevate themselves to the User Access Administrator role of this root group initially. After elevating access, the administrator can assign any RBAC role to other directory users or groups to manage the hierarchy.

### Important facts about the Root management group

- By default, the root management group's display name is **Tenant Root Group** and can not be changed. The ID is the Azure Active Directory ID.
- To change the display name of any child Management Groups display name, your account must be assigned the Owner or Contributor role on the root management group.
- The root management group can't be moved or deleted, unlike other management groups.
- All subscriptions and management groups fold up to the one root management group within the directory.
  - All resources in the directory fold up to the root management group for global management.
  - New subscriptions are automatically defaulted to the root management group when created.
- All Azure customers can see the root management group, but not all customers have access to manage that root management group.
  - Everyone who has access to a subscription can see the context of where that subscription is in the hierarchy.
  - No one is given default access to the root management group. Azure AD Global Administrators are the only users that can elevate themselves to gain access. Once they have access to the root management group, the global administrators can assign any RBAC role to other users to manage

it.

## Initial Setup of Management Groups

When any user starts using management groups, there's an initial setup process that happens. The first step is the root management group is created in the directory. Once this group is created, all existing subscriptions that exist in the directory are made children of the root management group. The reason for this process is to make sure there's only one management group hierarchy within a directory.

The single hierarchy within the directory allows administrative customers to apply global access and policies that other customers within the directory can't bypass. Anything assigned on the root will apply

to the entire hierarchy, which includes all management groups, subscriptions, resource groups, and resources within that Azure AD Tenant.

## Management Group Access

Azure management groups support Azure Role-Based Access Control (RBAC) for all resource accesses and role definitions. These permissions are inherited to child resources that exist in the hierarchy. Any RBAC role can be assigned to a management group that will inherit down the hierarchy to the resources. For example, the RBAC role VM contributor can be assigned to a management group. This role has no action on the management group, but will inherit to all VMs under that management group.

The following chart shows the list of roles and the supported actions on management groups.

RBAC Role Name	Create	Rename	Move	Delete	Assign Access	Assign Policy	Read
<b>Owner</b>	X	X	X	X	X	X	X
<b>Contributor</b>	X	X	X	X			X
<b>MG Contributor*</b>	X	X	X	X			X
<b>Reader</b>							X
<b>MG Reader*</b>							X
<b>Resource Policy Contributor</b>						X	
<b>User Access Administrator</b>					X	X	

\* MG Contributor and MG Reader only allow users to do those actions on the management group scope.

## Custom RBAC Role Definition and Assignment

Custom RBAC role support for management groups is currently in preview with some limitations. You can define the management group scope in the Role Definition's assignable scope. That custom RBAC Role will then be available for assignment on that management group and any management group, subscription, resource group, or resource under it. This custom role will inherit down the hierarchy like any built-in role.

### Example definition

Defining and creating a custom role does not change with the inclusion of management groups. Use the full path to define the management group /providers/Microsoft.Management/managementgroups/{groupId}.

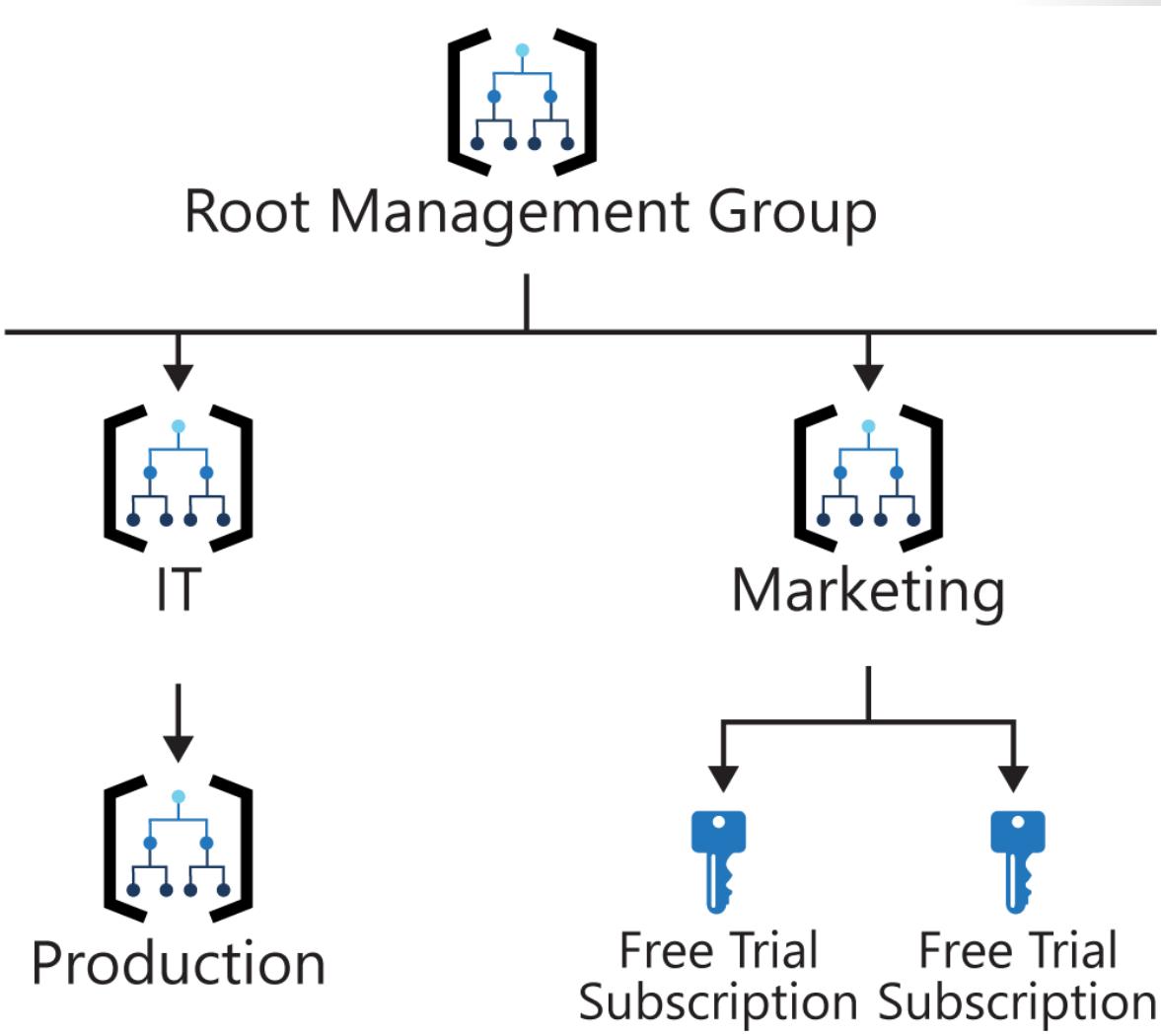
Use the management group's ID and not the management group's display name. This common error happens since both are custom-defined fields when creating a management group.

```
...
{
    "Name": "MG Test Custom Role",
    "Id": "id",
    "IsCustom": true,
    "Description": "This role provides members understand custom roles.",
    "Actions": [
        "Microsoft.Management/managementgroups/delete",
        "Microsoft.Management/managementgroups/read",
        "Microsoft.Management/managementgroup/write",
        "Microsoft.Management/managementgroup/subscriptions/delete",
        "Microsoft.Management/managementgroup/subscriptions/write",
        "Microsoft.resources/subscriptions/read",
        "Microsoft.Authorization/policyAssignments/*",
        "Microsoft.Authorization/policyDefinitions/*",
        "Microsoft.Authorization/policySetDefinitions/*",
        "Microsoft.PolicyInsights/*",
        "Microsoft.Authorization/roleAssignments/*",
        "Microsoft.Authorization/roledefinitions/*"
    ],
    "NotActions": [],
    "DataActions": [],
    "NotDataActions": [],
    "AssignableScopes": [
        "/providers/microsoft.management/managementGroups/ContosoCorporate"
    ]
}
...
...
```

## Issues with breaking the role definition and assignment hierarchy path

Role definitions are assignable scope anywhere within the management group hierarchy. A role definition can be defined on a parent management group while the actual role assignment exists on the child subscription. Since there's a relationship between the two items, you'll receive an error when trying to separate the assignment from its definition.

For example, let's look at a small section of a hierarchy for a visual.



Suppose there's a custom role defined on the Marketing management group. That custom role is then assigned on the two free trial subscriptions.

If we try to move one of those subscriptions to be a child of the Production management group, this move would break the path from subscription role assignment to the Marketing management group role definition. In this scenario, you'll receive an error saying the move isn't allowed since it will break this relationship.

There are a couple different options to fix this scenario:

- Remove the role assignment from the subscription before moving the subscription to a new parent MG.
- Add the subscription to the Role Definition's assignable scope.
- Change the assignable scope within the role definition. In the above example, you can update the assignable scopes from Marketing to Root Management Group so that the definition can be reached by both branches of the hierarchy.
- Create an additional Custom Role that will be defined in the other branch. This new role will require the role assignment to be changed on the subscription also.

## Limitations

There are limitations that exist when using custom roles on management groups.

- **You can only define one management group in the assignable scopes of a new role.** This limitation is in place to reduce the number of situations where role definitions and role assignments are disconnected. This situation happens when a subscription or management group with a role assignment is moved to a different parent that doesn't have the role definition.
- **RBAC Data Plane actions can't be defined in management group custom roles.** This restriction is in place as there's a latency issue with RBAC actions updating the data plane resource providers. This latency issue is being worked on and these actions will be disabled from the role definition to reduce any risks.
- **The Azure Resource Manager doesn't validate the management group's existence in the role definition's assignable scope.** If there's a typo or an incorrect management group ID listed, the role definition will still be created.

# Lab

## Lab - Managing Azure AD Authentication and Authorization

✓ **Important:** To download the most recent version of this lab, please visit the AZ-304 [GitHub repository<sup>5</sup>](#).

Direct link to the [Lab: Managing Azure AD Authentication and Authorization<sup>6</sup>](#).

### Lab scenario



As part of its migration to Azure, Adatum Corporation needs to define its identity strategy. Adatum has a single domain Active Directory forest named adatum.com and owns the corresponding, publicly registered DNS domain. As the Adatum Enterprise Architecture team is exploring the option of transitioning some of the on-premises workloads to Azure, it intends to evaluate integration between its Active Directory Domain Services (AD DS) environment and the Azure Active Directory (Azure AD) tenant associated with the target Azure subscription as the core component of its longer-term authentication and authorization model.

The new model should facilitate single sign-on, along with per-application step-up authentication that leverages multi-factor authentication capabilities of Azure AD. To implement single sign-on, the Architecture team plans to deploy Azure AD Connect and configure it for password hash synchronization, resulting in matching user objects in both identity stores. Choosing the optimal authentication method is the first concern for organizations wanting to move to the cloud. Azure AD password hash synchronization is the simplest way to implement single sign-on authentication for on-premises users when accessing Azure AD-integrated resources. This method is also required by some premium Azure AD features, such as Identity Protection.

To implement step-up authentication, the Adatum Enterprise Architecture team intends to take advantage of Azure AD Conditional Access policies. Conditional Access policies support enforcement of multi-factor authentication depending on the type of application or resource being accessed. Conditional Access policies are enforced after the first-factor authentication has been completed. Conditional Access can be based on a wide range of factors, including:

- 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/regions 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.

<sup>5</sup> <https://github.com/MicrosoftLearning/AZ-304-Microsoft-Azure-Architect-Design>

<sup>6</sup> [https://aka.ms/304\\_Module\\_4\\_Lab](https://aka.ms/304_Module_4_Lab)

- 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.

To accomplish these objectives the Adatum Enterprise Architecture team intends to test integration of its Active Directory Domain Services (AD DS) forest with its Azure Active Directory (Azure AD) tenant and evaluate the conditional access functionality for its pilot users.

## Objectives

After completing this lab, you will be able to:

- Deploy an Azure VM hosting an AD DS domain controller
- Create and configure an Azure AD tenant
- Integrate an AD DS forest with an Azure AD tenant

## 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\10\azuredeploy30310suba.json

## Instructions

### Exercise 0: Prepare the lab environment

The main tasks for this exercise are as follows:

1. Identify an available DNS name for an Azure VM deployment
2. Deploy an Azure VM running an AD DS domain controller by using an Azure Resource Manager QuickStart template

### Exercise 1: Create and configure an Azure AD tenant

The main tasks for this exercise are as follows:

1. Create an Azure AD tenant
2. Create and configure Azure AD users
3. Activate and assign Azure AD Premium P2 licensing

## Exercise 2: Integrate an AD DS forest with an Azure AD tenant

The main tasks for this exercise are as follows:

1. Assign a custom domain name to the Azur AD tenant
2. Configure AD DS in the Azure VM
3. Install Azure AD Connect
4. Configure properties of synchronized user accounts

## Exercise 3: Implement Azure AD conditional access

The main tasks for this exercise are as follows:

1. Disable Azure AD security defaults.
2. Create an Azure AD conditional access policy
3. Verify Azure AD conditional access
4. Remove Azure resources deployed in the lab

## Module 4 Review Questions

### Module 4 Review Questions



#### Review Question 1

A company you advise wants to deploy Azure AD Connect to synchronize identity information from their on-premises AD DS directory to an Azure AD tenant.

The synchronized identity information includes group memberships, user accounts, and credential hashes (password sync).

The company plans to deploy VMs (Linux and Windows).

The requirements for the VMs include:

- Must allow users to sign in to the domain with their credential from their organization and connect remotely to VMs using Remote Desktop.
- Must support Group Policy, Kerberos and NTLM authorization, LDAP read and bind, and domain join.

Which service should you recommend?

- Azure AD Domain Services
- Azure AD Privileged Identity Management (PIM)
- Azure Managed Identity
- Application Insights

#### Review Question 2

You advise an organization that has an existing hybrid deployment of Azure AD. They have asked you to recommend a solution that makes certain that the Azure AD tenant can only be managed from the computers that are within the on-premises network.

What should you recommend?

- A user assigned Managed Service Identity
- A custom RBAC role
- Azure Managed Identity
- A conditional access policy

## Review Question 3

You are advising an organization that is exploring the possibility of using an Azure AD hybrid identity as a solution. They have asked you to recommend a solution that ensures their users can authenticate, even if the internet connection is not available. They require the proposed solution should keep the authentication prompts to a minimum for users on the system.

What would you include in the solution?

- Pass-through Authentication and Azure AD Seamless SSO
- A custom RBAC role
- Password hash synchronization and Azure AD Seamless SSO
- Active Directory Federation Services

## Review Question 4

You are recommending a design for a SaaS app that will allow Azure AD users to create and publish reviews online.

There will be a front-end web app and a back-end web API.

The web app will be dependent on web API to handle updates to the customer reviews.

You need to recommend a design for authorization flow for the SaaS app that meets the following:

- Access to the back-end web API, the web app must authenticate using OAuth 2 bearer tokens.
- The web app must authenticate using identities of the individual users.

If tokens are generated by Azure AD, which part of the solution performs the authorization?

- Azure AD
- The web API
- The web app
- Azure Key Vault

## Review Question 5

An organization you are consulting with has an existing Azure AD tenant.

They plan to deploy multiple Azure Cosmos DB databases will use the SQL API.

You are asked to recommend a solution that provides Azure AD user accounts with read access to the Cosmos DB databases.

What do you recommend?

- Master keys and Azure Information Protection policies
- A resource token and an Azure control (IAM) role assignment
- SAS and conditional access policies
- Azure Key Vault and certificates

## Review Question 6

An organization has asked you to make a recommendation on whether to use Azure Active Directory Domain Services (Azure AD DS).

They have an existing Azure AD tenant.

They want to provide access to shared files with Azure Storage. The users will be provided different levels of access to the Azure file shares based on their user account or group membership.

They ask that you recommend which Azure services to use.

What do you recommend?

- Azure Information Protection
- An Azure AD DS instance
- Azure Information Protection
- Azure Key Vault and certificates

# Answers

## Review Question 1

A company you advise wants to deploy Azure AD Connect to synchronize identity information from their on-premises AD DS directory to an Azure AD tenant.

The synchronized identity information includes group memberships, user accounts, and credential hashes (password sync).

The company plans to deploy VMs (Linux and Windows).

The requirements for the VMs include:

Which service should you recommend?

- Azure AD Domain Services
- Azure AD Privileged Identity Management (PIM)
- Azure Managed Identity
- Application Insights

*Explanation*

*Azure AD Domain Services supports LDAP, NTLM and Group Policies that fulfills the requirements.*

## Review Question 2

You advise an organization that has an existing hybrid deployment of Azure AD. They have asked you to recommend a solution that makes certain that the Azure AD tenant can only be managed from the computers that are within the on-premises network.

What should you recommend?

- A user assigned Managed Service Identity
- A custom RBAC role
- Azure Managed Identity
- A conditional access policy

*Explanation*

*Correct Answer: Use a conditional access policy. Add the on-premises IPs to the Trusted IP section in a CA policy and set the Azure Management cloud app.*

**Review Question 3**

You are advising an organization that is exploring the possibility of using an Azure AD hybrid identity as a solution. They have asked you to recommend a solution that ensures their users can authenticate, even if the internet connection is not available. They require the proposed solution should keep the authentication prompts to a minimum for users on the system.

What would you include in the solution?

- Pass-through Authentication and Azure AD Seamless SSO
- A custom RBAC role
- Password hash synchronization and Azure AD Seamless SSO
- Active Directory Federation Services

*Explanation*

*Correct Answer: Password hash synchronization and Azure AD Seamless SSO. The password hash synchronization agent transmits the hashed password with Azure AD Connect to Azure AD over SSL every 2 minutes. It functions as if there is no internet connection. The hashed passwords are local in AD and in AAD. When users synchronize a password, it overwrites the existing cloud password. Users can sign-in locally and to cloud services with the same credentials.*

**Review Question 4**

You are recommending a design for a SaaS app that will allow Azure AD users to create and publish reviews online.

There will be a front-end web app and a back-end web API.

The web app will be dependent on web API to handle updates to the customer reviews.

You need to recommend a design for authorization flow for the SaaS app that meets the following:

If tokens are generated by Azure AD, which part of the solution performs the authorization?

- Azure AD
- The web API
- The web app
- Azure Key Vault

*Explanation*

*Correct Answer: The web API. Azure AD is used here as the identity provider that generates the access tokens and the authorization is managed by the web API.*

**Review Question 5**

An organization you are consulting with has an existing Azure AD tenant.

They plan to deploy multiple Azure Cosmos DB databases will use the SQL API.

You are asked to recommend a solution that provides Azure AD user accounts with read access to the Cosmos DB databases.

What do you recommend?

- Master keys and Azure Information Protection policies
- A resource token and an Azure control (IAM) role assignment
- SAS and conditional access policies
- Azure Key Vault and certificates

*Explanation*

*Correct Answer: A resource token and an Azure control (IAM) role assignment. You can use a resource token (by creating Cosmos DB users and permissions) when you want to provide access to resources in your Cosmos DB account to a client that cannot be trusted with the master key. To add Azure Cosmos DB account reader access to your user account, use Access control (IAM) option in Azure portal..*

**Review Question 6**

An organization has asked you to make a recommendation on whether to use Azure Active Directory Domain Services (Azure AD DS).

They have an existing Azure AD tenant.

They want to provide access to shared files with Azure Storage. The users will be provided different levels of access to the Azure file shares based on their user account or group membership.

They ask that you recommend which Azure services to use.

What do you recommend?

- Azure Information Protection
- An Azure AD DS instance
- Azure Information Protection
- Azure Key Vault and certificates

*Explanation*

*Correct Answer: A resource token and an Azure control (IAM) role assignment. Azure Files supports identity-based authentication over Server Message Block (SMB) through Azure Active Directory Domain Services (Azure AD DS). Without Azure AD DS it is not possible to provide different levels of access to Azure Files based on user identity or their group membership.*



## Module 5 Design Governance

### Governance

#### Governance

To achieve an effective return on investment (ROI) organizations must prioritize where they will invest. Implementation of security across the organization is also constrained by this, so to achieve an appropriate ROI on security the organization needs to first understand and define its security priorities.

**Governance:** How is the organization's security going to be monitored, audited, and reported? Design and implementation of security controls within an organization is only the beginning of the story. How does the organization know that things are actually working? Are they improving? Are there new requirements? Is there mandatory reporting? Similar to compliance there may be external industry, government or regulatory standards that need to be considered.

**Risk:** What types of risks does the organization face while trying to protect identifiable information, Intellectual Property (IP), financial information? Who may be interested or could use this information if stolen, including external and internal threats as well as unintentional or malicious? A commonly forgotten but extremely important consideration within risk is addressing Disaster Recovery and Business Continuity.

**Compliance:** Are there specific industry, government, or regulatory requirements that dictate or provide recommendation on criteria that your organization's security controls must meet? Examples of such standards, organizations, controls, and legislation are ISO27001, NIST, PCI-DSS.

The collective role of organization(s) is to manage the security standards of the organization through their lifecycle:

- **Define** - Set organizational standards and policies for practices, technologies, and configurations based on internal factors (organizational culture, risk appetite, asset valuation, business initiatives, etc.) and external factors (benchmarks, regulatory standards, threat environment, and more)
- **Improve** – Continually push these standards incrementally forward towards the ideal state to ensure continual risk reduction.
- **Sustain** – Ensure the security posture doesn't degrade naturally over time by instituting auditing and monitoring compliance with organizational standards.

## Clear Lines Of Responsibility

Designate the parties responsible for specific functions in Azure

Clearly documenting and sharing the contacts responsible for each of these functions will create consistency and facilitate communication. Based on our experience with many cloud adoption projects, this will avoid confusion that can lead to human and automation errors that create security risk.

Designate groups (or individual roles) that will be responsible for these key functions:

Group or individual role	Responsibility
<b>Network Security</b>	Typically existing network security team. Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.
<b>Network Management</b>	Typically existing network operations team. Enterprise-wide virtual network and subnet allocation.
<b>Server Endpoint Security</b>	Typically IT operations, security, or jointly. Monitor and remediate server security (patching, configuration, endpoint security, etc.).
<b>Incident Monitoring and Response</b>	Typically security operations team. Investigate and remediate security incidents in Security Information and Event Management (SIEM) or source console.
<b>Policy Management</b>	Typically GRC team + Architecture. Set Direction for use of Role Based Access Control (RBAC), Azure Security Center, Administrator protection strategy, and Azure Policy to govern Azure resources.
<b>Identity Security and Standards</b>	Typically Security Team + Identity Team jointly. Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards.

## Audit and Enforce Policy Compliance

Ensure that the security team is auditing the environment to report on compliance with the security policy of the organization. Security teams may also enforce compliance with these policies.

Organizations of all sizes will have security compliance requirements. Industry, government, and internal corporate security policies all need to be audited and enforced. Policy monitoring is critical to check that initial configurations are correct and that it continues to be compliant over time.

In Azure, you can take advantage of Azure Policy to create and manage policies that enforce compliance. Like Azure Blueprints, Azure Policies are built on the underlying Azure Resource Manager capabilities in the Azure platform (and Azure Policy can also be assigned via Azure Blueprints).

# Recommend a Solution for using Azure Policy

## Compliance with Azure Policy

Planning out a consistent cloud infrastructure starts with setting up policy. Your policies will enforce your rules for created resources, so your infrastructure stays compliant with your corporate standards, cost requirements, and any service-level agreements (SLAs) you have with your customers.



**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. Azure Policy meets this need by evaluating your resources for noncompliance with assigned policies. For example, you might have a policy that allows virtual machines of only a certain size in your environment. After this policy is implemented, new and existing resources are evaluated for compliance. With the right type of policy, existing resources can be brought into compliance.

Imagine we allow anyone in our organization to create virtual machines (VMs). We want to control costs, so the administrator of our Azure tenant defines a policy that prohibits the creation of any VM with more than 4 CPUs. Once the policy is implemented, Azure Policy will stop anyone from creating a new VM outside the list of allowed stock keeping units (SKUs). Also, if you try to update an existing VM, it will be checked against policy. Finally, Azure Policy will audit all the existing VMs in our organization to ensure our policy is enforced. It can audit non-compliant resources, alter the resource properties, or stop the resource from being created. You can even integrate Azure Policy with Azure DevOps, by applying any continuous integration and delivery pipeline policies that affect the pre-deployment and post-deployment of your applications.

### 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 like 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**.

### Which to use?

What's the difference between Azure policy and Azure initiatives? Why would you use one over the other? It depends on the Azure services and the use cases for each.

As mentioned earlier, **Azure Policy** is a service in Azure which allows you create policies which enforce and control the properties of a resource. When these policies are used they enforce different rules and effects over your resources, so those resources stay compliant with your IT governance standards.

So, Azure policy is really three components: policy definition , assignment and parameters.

- **Policy definition** is the conditions which you want controlled. There are built in definitions such as controlling what type of resources can be deployed to enforcing the use of tags on all resources.

- **Policy assignment** is the scope of what the policy definition can take effect around. Scope of assignment can be assigned to a individual resource, resource group, or management group. Policy assignments are inherited by all child resources.
- **Policy parameters** help simplify your policy management by reducing the number of policy definitions you must create. Parameters would be used to define which type of VM SKUs to deploy or defining a specific location.

Home > Policy | Assignments >

## Assign policy

The screenshot shows the 'Assign policy' page in the Azure portal. At the top, there are tabs: 'Basics' (which is selected), 'Parameters', 'Remediation', and 'Review + create'. Below the tabs, there are two main sections: 'Scope' and 'Exclusions'. The 'Scope' section contains a field with the value 'Azure Pass - Sponsorship' and a '... more' button. The 'Exclusions' section contains a placeholder 'Optional select resources to exclude from the policy assignment.' and a '... more' button. The 'Basics' section contains fields for 'Policy definition \*' (empty), 'Assignment name \*' (empty), and 'Description' (empty). It also includes a 'Policy enforcement' section with 'Enabled' selected. At the bottom, there are buttons for 'Review + create', 'Cancel', 'Previous', and 'Next'.

Basics    Parameters    Remediation    Review + create

Scope

Scope [Learn more about setting the scope \\*](#)

Azure Pass - Sponsorship [...](#)

Exclusions

Optionally select resources to exclude from the policy assignment. [...](#)

Basics

Policy definition \*

Assignment name \* ⓘ

Description

Policy enforcement ⓘ

Enabled  Disabled

Assigned by

Review + create    Cancel    Previous    Next

An **Azure Initiative** is a collection of Azure policy definitions that are grouped together towards a specific goal or purpose in mind. Azure initiatives simplify management of your policies by grouping a set of policies together as one single item. For example, you could use the PCI-DSS built-in initiative which has all the policy definitions that are centered around meeting PCI-DSS compliance.

Like Azure Policy, initiatives have definitions ( a bunch of policies ), assignments, and parameters. Once you determine the definitions that you want, you would assign the initiative to a scope so that it can be applied.

[Home](#) > [Policy | Assignments](#) >

## Assign initiative

Basics    Parameters    Remediation    Review + create

Scope  
Scope [Learn more about setting the scope \\*](#)

Azure Pass - Sponsorship

Exclusions  
Optional select resources to exclude from the policy assignment.

Basics

Initiative definition \*

Assignment name \* ⓘ

Description

Policy enforcement ⓘ

Enabled  Disabled

Assigned by

[Review + create](#) [Cancel](#) [Previous](#) [Next](#)

Depending on your organization's requirement it may be appropriate to use a single policy. However, in most cases it would be best, and probably easier to manage in the future, to begin by using Azure initiatives. Some recommend using initiatives even for a single policy because once an initiative is assigned then any additional policy definitions that are added to the initiative become part of the assignment.

For example, instead of managing 20 separate policies for PCI-DSS compliance, you would only be managing the initiative because all those individual policies are being evaluated, and at the same time.

# 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 particular storage type from being created, or force a specific version of SQL Server to be used.

Here are some of 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.
<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).

Here 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.

## Applying Azure Policy

To apply a policy, we can use the Azure portal, or one of the command-line tools such as Azure PowerShell by adding the `Microsoft.PolicyInsights` extension.

```
# Register the resource provider if it's not already registered
Register-AzResourceProvider -ProviderNamespace 'Microsoft.PolicyInsights'
```

Once we have registered the provider, we can create a policy assignment. For example, here's a policy definition that identifies virtual machines not using managed disks.

```
# Get a reference to the resource group that will be the scope of the
assignment
$rg = Get-AzResourceGroup -Name '<resourceGroupName>'

# Get a reference to the built-in policy definition that will be assigned
$definition = Get-AzPolicyDefinition | Where-Object { $_.Properties.DisplayName -eq 'Audit VMs that do not use managed disks' }

# Create the policy assignment with the built-in definition against your
resource group
New-AzPolicyAssignment -Name 'audit-vm-manageddisks' -DisplayName 'Audit
VMs without managed disks Assignment' -Scope $rg.ResourceId -PolicyDefinition $definition
```

## Identifying Non-Compliant Resources

We can use the applied policy definition to identify resources that aren't compliant with the policy assignment through the Azure portal.

The results match what you see in the Resource compliance tab of a policy assignment in the Azure portal:

The screenshot shows the Azure Policy - Compliance blade. On the left, there's a navigation menu with options like Overview, Getting started, Compliance (which is selected and highlighted with a red box), Remediation, Authoring, Assignments, Definitions, Blueprints, and Blueprints (preview). The main area displays the following metrics:

Overall resource compliance	Non-compliant initiatives	Non-compliant policies	Non-compliant resources
100%	0 out of 1	0 out of 39	0 out of 4

Below these metrics is a table listing policy assignments:

NAME	SCOPE	COMPLIANCE STATE	COMPLIANCE	NON-COMPLIANT RESOURCES	NON-COMPLIANT POLICIES
<a href="#">Audit VMs that do not use managed disks</a> ...	Contoso/PolicyTarget	Compliant	100%	0	0
<a href="#">[Preview]: Enable Monitoring ...</a> ...	Contoso/PolicyTarget	Compliant	100%	0	0

Or we can again use the command-line tools to identify the resources in your resource group that are non-compliant to the policy assignment

```
Get-AzPolicyState -ResourceGroupName $rg.ResourceGroupName -PolicyAssignmentName 'audit-vm-manageddisks' -Filter 'IsCompliant eq false'
```

Here's an example of the output we might get:

```
Timestamp : 3/9/19 9:21:29 PM
ResourceId : /subscriptions/{subscriptionId}/resourcegroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/{vmId}
PolicyAssignmentId : /subscriptions/{subscriptionId}/providers/microsoft.authorization/policyassignments/audit-vm-manageddisks
PolicyDefinitionId : /providers/Microsoft.Authorization/policyDefinitions/06a78e20-9358-41c9-923c-fb736d382a4d
IsCompliant : False
SubscriptionId : {subscriptionId}
ResourceType : /Microsoft.Compute/virtualMachines
ResourceTags : tbd
PolicyAssignmentName : audit-vm-manageddisks
PolicyAssignmentOwner : tbd
PolicyAssignmentScope : /subscriptions/{subscriptionId}
PolicyDefinitionName : 06a78e20-9358-41c9-923c-fb736d382a4d
PolicyDefinitionAction : audit
PolicyDefinitionCategory : Compute
ManagementGroupIds : {managementGroupId}
```

## Policy Effects

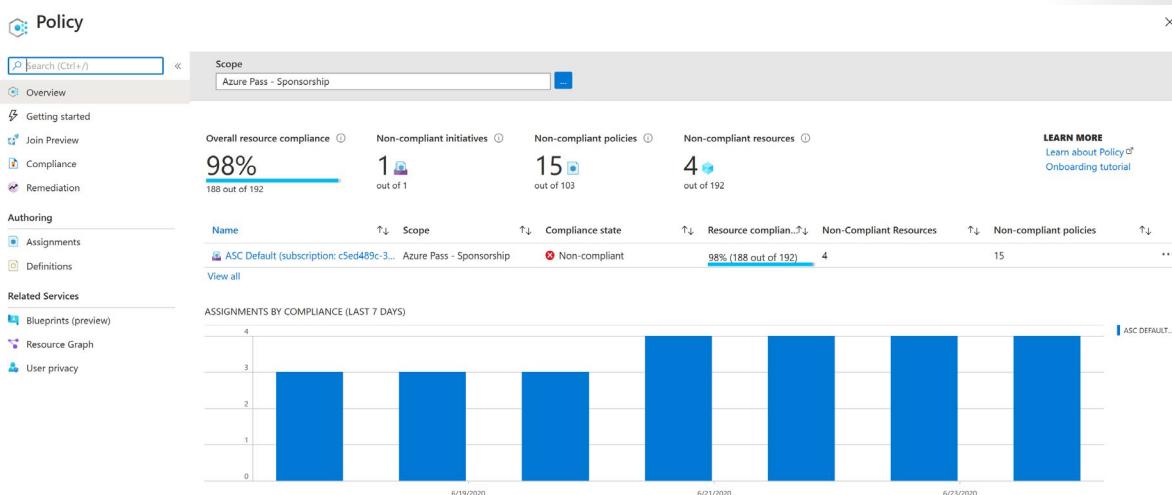
Requests to create or update a resource through Azure Resource Manager are evaluated by Azure Policy first. Policy creates a list of all assignments that apply to the resource and then evaluates the resource against each definition. Policy processes several of the effects before handing the request to the appropriate Resource Provider to avoid any unnecessary processing if the resource violates policy.

Each policy definition in Azure Policy has a single effect. That effect determines what happens when the associated policy rule is matched. When that happens, Azure Policy will take a specific action based on the assigned effect.

Policy Effect	What happens?
<b>Deny</b>	Used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
<b>Disabled</b>	Used for testing situations or for when the policy definition has parameterized the effect.
<b>Append</b>	Used to add additional fields to the requested resource during creation or update. A common example is adding tags on resources such as Cost Center or specifying allowed IPs for a storage resource.
<b>Audit, AuditIfNotExists</b>	Used to create a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request. AuditIfNotExists enables auditing of resources related to the resource that matches the if condition, but don't have the properties specified in the details of the then condition.
<b>DeployIfNotExists</b>	DeployIfNotExists policy definition executes a template deployment when the condition is met.
<b>Modify</b>	Used to add, update, or remove tags on a resource during creation or update.

## View Policy Evaluation Results

Azure Policy can allow a resource to be created even if it doesn't pass validation. In these cases, you can have it trigger an audit event that can be viewed in the Azure Policy portal, or through command-line tools. The easiest approach is in the portal as it provides a nice graphical overview that you can explore. You can find the Azure Policy section through the search field or *All Services*.



From this screen, you can spot resources that are not compliant and take action to correct them.

## Organize Policy with Initiatives

Initiatives work alongside policies in Azure Policy. An *initiative definition* is a set or group of policy definitions to help track your compliance state for a larger goal. Even if you have a single policy, we recommend using initiatives if you anticipate increasing the number of policies over time.

Like a policy assignment, an *initiative assignment* is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope. This scope could also range from a management group to a resource group.

Once defined, initiatives can be assigned just as policies can - and they apply all the associated policy definitions.

### Defining initiatives

Initiative definitions simplify the process of managing and assigning policy definitions by grouping a set of policies into a single item. For example, you could create an initiative named *Enable Monitoring in Azure Security Center*, with a goal to monitor all the available security recommendations in your Azure Security Center.

Under this initiative, you would have the following policy definitions:

Policy definition	Purpose
<b>Monitor unencrypted SQL Database in Security Center</b>	For monitoring unencrypted SQL databases and servers.
<b>Monitor OS vulnerabilities in Security Center</b>	For monitoring servers that do not satisfy the configured baseline.
<b>Monitor missing Endpoint Protection in Security Center</b>	For monitoring servers without an installed endpoint protection agent.

You can define initiatives using the Azure portal, or command-line tools. In the portal, you use the "Authoring" section.

Name	Definition location	Policies	Type
azuresecuritypack...	Non Production	3	Custom
azuresecuritypack...	Non Production	3	Custom
audit ssh auth_1.3	Non Production	4	Custom
audit ssh auth_1.1	Non Production	2	Custom
azuresecuritypack...	5e116433-8b65-49e...	3	Custom
azuresecuritypack...	5e116433-8b65-49e...	3	Custom
audit ssh auth_1.1	5e116433-8b65-49e...	2	Custom
audit ssh auth_1.1	Demonstration	2	Custom
Audit Windows V...		2	Built-in

## Demonstration - Manage Tag Governance with Azure Policy

Tags are a crucial part of organizing your Azure resources into a taxonomy.

Azure Policy's **Modify** effect is designed to aid in the governance of tags no matter what stage of resource governance you are in. **Modify** helps when:

- You're new to the cloud and have no tag governance
- Already have thousands of resources with no tag governance
- Already have an existing taxonomy that you need changed

In this demonstration, you'll complete the following tasks:

- Identify your business requirements
- Map each requirement to a policy definition
- Group the tag policies into an initiative

### Identify Requirements

Like any good implementation of governance controls, the requirements should come from your business needs and be well understood before creating technical controls. For this demonstration, the following items are our business requirements:

- Two required tags on all resources: *CostCenter* and *Env*
- *CostCenter* must exist on all containers and individual resources
  - Resources inherit from the container they're in, but may be individually overridden

- *Env* must exist on all containers and individual resources
  - Resources determine environment by container naming scheme and may not be overridden
  - All resources in a container are part of the same environment

## Configure the CostCenter tag

In terms specific to an Azure environment managed by Azure Policy, the *CostCenter* tag requirements call for the following:

- Deny resource groups missing the *CostCenter* tag
- Modify resources to add the *CostCenter* tag from the parent resource group when missing

### Deny resource groups missing the *CostCenter* tag

Since the *CostCenter* for a resource group can't be determined by the name of the resource group, it must have the tag defined on the request to create the resource group. The following policy rule with the Deny effect prevents the creation or updating of resource groups that don't have the *CostCenter* tag:

```
"policyRule": {
    "if": {
        "field": "tags['CostCenter']",
        "exists": "false"
    },
    "then": {
        "effect": "modify",
        "details": {
            "roleDefinitionIds": [
                "/providers/microsoft.authorization/roleDefinitions/
b24988ac-6180-42a0-ab88-20f7382dd24c"
            ],
            "operations": [
                {
                    "operation": "add",
                    "field": "tags['CostCenter']",
                    "value": "[resourcegroup().tags['CostCenter']]"
                }
            ]
        }
    }
}
```

#### ✓ Note

This policy only matches resource groups with the sample naming scheme used for production resources of prd-. More complex naming schemes can be achieved with several **match** conditions instead of the single **like** in this example.

### Modify resources to inherit the *Env* tag

The business requirement calls for all resources to have the *Env* tag that their parent resource group does. This tag can't be overridden, so we'll use the **addOrReplace** operation with the **Modify** effect. The sample Modify policy looks like the following rule:

```
"policyRule": {
    "if": {
        "anyOf": [

```

```
        "field": "tags['Env']",
        "notEquals": "[resourcegroup().tags['Env']]"
    },
    {
        "field": "tags['Env']",
        "exists": false
    }
]
},
"then": {
    "effect": "modify",
    "details": {
        "roleDefinitionIds": [
            "/providers/microsoft.authorization/roleDefinitions/
b24988ac-6180-42a0-ab88-20f7382dd24c"
        ],
        "operations": [
            {
                "operation": "addOrReplace",
                "field": "tags['Env']",
                "value": "[resourcegroup().tags['Env']]"
            }
        ]
    }
}
}
```

As this policy rule targets resources that support tags, the *mode* on the policy definition must be 'Indexed'. This configuration also ensures this policy skips resource groups.

This policy rule looks for any resource that doesn't have its parent resource groups value for the *Env* tag or is missing the *Env* tag. Matching resources have their *Env* tag set to the parent resource groups value, even if the tag already existed on the resource but with a different value.

## Assign the initiative and remediate resources

Once the tag policies above are created, join them into a single initiative for tag governance and assign them to a management group or subscription. The initiative and included policies then evaluate compliance of existing resources and alters requests for new or updated resources that match the *if* property in the policy rule. However, the policy doesn't automatically update existing non-compliant resources with the defined tag changes.

Like **deployIfNotExists** policies, the **Modify** policy uses remediation tasks to alter existing non-compliant resources.

# Recommend a Solution for using Azure Blueprint

## Azure Blueprints

To help you with auditing, traceability, and compliance of your deployments, use **Azure Blueprint** artifacts and tools.



Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, **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 portal interface for 'Blueprints - Getting started'. The left sidebar has a 'Getting started' section with 'Blueprint definitions' and 'Assigned blueprints' options. The main area features a 'Welcome to Azure Blueprints PREVIEW' message with a diagram of a person working on a blueprint. Below this are three cards: 'Create a blueprint' (Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints), 'Apply to a scope' (Apply your blueprint to one or more subscriptions), and 'Track assignments' (Track where blueprints have been applied and share them across your organization). A red box highlights the 'Create' button in the first card.

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

**Tip**

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 Blueprints Differ 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.

There's no need to choose between a Resource Manager template and a 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 Blueprints Differ 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.

## Module 5 Review Questions

### Module 5 Review Questions



#### Review Question 1

You have been asked to recommend a solution to developers which grants them the ability to provision virtual machines. The requirements are scoped to the following:

- Allow creation of VMs for in specific regions
- Allow specific sizes for the VMs

What do you recommend?

- ARM templates
- Azure Policy
- Conditional Access policies
- RBAC

#### Review Question 2

You are advising a company that has an Azure subscription with several resource groups including a group call Tailwind\_RG1.

An administrator named Tailwind\_admin1 has been assigned the Owner role for the subscription.

You are asked to prevent Tailwind\_admin1 from modifying resources in Tailwind\_RG1.

However, you need to provide a solution that allows Tailwind\_admin1 to manage the resources in other resource groups

What do you recommend?

- An Azure Blueprint
- An Azure Policy
- A Conditional Access policy
- A custom role

## Review Question 3

You advise a company that plans to deploy multiple Azure App Service instances that will use Azure SQL Databases.

The instances will be deployed contemporaneously with the Azure SQL Databases.

The company has requirements to deploy App Service instances to specific regions. Also, the resources for the App Service instances must be in the same region.

You need to recommend a solution that meets the requirements.

You recommend using an Azure policy initiative that enforces location.

Does your recommendation meet the requirements?

Yes

No

## Review Question 4

You are asked to provide a recommendation for a governance solution for an auto parts wholesaler.

They ask that all the Azure resources are identifiable based on the following:

- Loc: the location of the warehouse
- CostCenter: the Cost Center to be tracked by accounting
- Categ: the category of parts
- PartNum: the part number

You need to make sure that they can use the operational information when they generate the report

What do you recommend?

- Azure management groups and RBAC
- Azure policy that enforces tagging rules
- Custom role assignments
- Azure Advisor Alerts

# Answers

## Review Question 1

You have been asked to recommend a solution to developers which grants them the ability to provision virtual machines. The requirements are scoped to the following:

What do you recommend?

- ARM templates
- Azure Policy
- Conditional Access policies
- RBAC

*Explanation*

*Correct Answer: Azure Policy. Azure Policy has the ability to limit regions and VM size families.*

## Review Question 2

You are advising a company that has an Azure subscription with several resource groups including a group call Tailwind\_RG1.

An administrator named Tailwind\_admin1 has been assigned the Owner role for the subscription.

You are asked to prevent Tailwind\_admin1 from modifying resources in Tailwind\_RG1.

However, you need to provide a solution that allows Tailwind\_admin1 to manage the resources in other resource groups

What do you recommend?

- An Azure Blueprint
- An Azure Policy
- A Conditional Access policy
- A custom role

*Explanation*

*Correct Answer: An Azure Blueprint allows architects to create artifacts and definitions that can include deny permissions in the deployments. This is something that ARM templates also cannot solve alone. Azure policies can be part of a blueprint but will not on their own provide deny permissions as asked for in the stem.*

## Review Question 3

You advise a company that plans to deploy multiple Azure App Service instances that will use Azure SQL Databases.

The instances will be deployed contemporaneously with the Azure SQL Databases.

The company has requirements to deploy App Service instances to specific regions. Also, the resources

for the App Service instances must be in the same region.

You need to recommend a solution that meets the requirements.

You recommend using an Azure policy initiative that enforces location.

Does your recommendation meet the requirements?

Yes

No

*Explanation*

*Correct answer: Yes. An Azure Initiative is a collection of Azure policy definitions that are grouped together towards a specific goal or purpose in mind. Azure initiatives simplify management of your policies by grouping a set of policies together as one single item.*

**Review Question 4**

You are asked to provide a recommendation for a governance solution for an auto parts wholesaler.

They ask that all the Azure resources are identifiable based on the following:

You need to make sure that they can use the operational information when they generate the report

What do you recommend?

- Azure management groups and RBAC
- Azure policy that enforces tagging rules
- Custom role assignments
- Azure Advisor Alerts

*Explanation*

*Correct answer: Azure policy that enforces tagging rules. Tags are a crucial part of organizing Azure resources into a taxonomy. An Azure policy for tagging items helps to identify business requirements.*

## Module 6 Design a Solution for Databases

### Select an Appropriate Data Platform Based on Requirements

#### Recommending the Right Data Store

Recommending the right data store for your requirements is a key design decision. There are hundreds of implementations to choose from among SQL and NoSQL databases. Data stores are often categorized by how they structure data and the types of operations they support. This lesson describes several of the most common storage models.

Note that a data store technology may support multiple storage models. For example, a relational database management systems (RDBMS) may also support key/value or graph storage. In fact, there is a general trend for so-called multi-model support, where a single database system supports several models. But it's still useful to understand the different models at a high level.

This lesson provides an overview of the following database systems:

- Relational database management systems
- Key/Value stores
- Document databases
- Graph databases
- Data analytics

#### Relational Database Management Systems

Relational databases organize data as a series of two-dimensional tables with rows and columns. Each table has its own columns, and every row in a table has the same set of columns. This model is mathematically based, and most vendors provide a dialect of the Structured Query Language (SQL) for retrieving and managing data. An RDBMS typically implements a transactionally consistent mechanism that conforms to the ACID (Atomic, Consistent, Isolated, Durable) model for updating information.

An RDBMS typically supports a schema-on-write model, where the data structure is defined ahead of time, and all read or write operations must use the schema. This is in contrast to most NoSQL data stores, particularly key/value types, where the schema-on-read model assumes that the client will be imposing its own interpretive schema on data coming out of the database, and is agnostic to the data format being written.

An RDBMS is very useful when strong consistency guarantees are important where all changes are atomic, and transactions always leave the data in a consistent state.

**Relevant Azure services:**

- Azure SQL Database
- Azure Database for MySQL

## Key/Value Stores

A key/value store is a large hash table. You associate each data value with a unique key, and the key/value store uses this key to store the data by using an appropriate hashing function. The hashing function is selected to provide an even distribution of hashed keys across the data storage.

Most key/value stores only support simple query, insert, and delete operations. To modify a value (either partially or completely), an application must overwrite the existing data for the entire value. In most implementations, reading or writing a single value is an atomic operation. If the value is large, writing may take some time.

An application can store arbitrary data as a set of values, although some key/value stores impose limits on the maximum size of values. The stored values are opaque to the storage system software. Any schema information must be provided and interpreted by the application. Essentially, values are blobs and the key/value store simply retrieves or stores the value by key.

Key	Value
AAAAA	110100111010100110101111...
AABAB	1001100001011001101011110....
DFA766	000000000101010110101010...
FABCC4	11101101101010100101101...

Key/value stores are highly optimized for applications performing simple lookups, but are less suitable for systems that need to query data across different key/value stores. Key/value stores are also not optimized for scenarios where querying by value is important, rather than performing lookups based only on keys. For example, with a relational database, you can find a record by using a WHERE clause, but key/values stores usually do not have this type of lookup capability for values.

**Relevant Azure services:**

- **Cosmos DB<sup>1</sup>**
- **Azure Cache for Redis<sup>2</sup>**
- **Azure Tables<sup>3</sup>**

## Document Databases

A document database is conceptually similar to a key/value store, except that it stores a collection of named fields and data (known as documents), each of which could be simple scalar items or compound elements such as lists and child collections. The data in the fields of a document can be encoded in a variety of ways, including XML, YAML, JSON, BSON, or even stored as plain text. Unlike key/value stores, the fields in documents are exposed to the storage management system, enabling an application to query and filter data by using the values in these fields.

A document store does not require that all documents have the same structure. This free-form approach provides a great deal of flexibility. Applications can store different data in documents as business requirements change.

---

<sup>1</sup> <https://docs.microsoft.com/azure/cosmos-db/table-introduction>

<sup>2</sup> <https://azure.microsoft.com/services/cache>

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/storage/tables/table-storage-overview>

Key	Document
1001	{ "CustomerID": 99, "OrderItems": [ {"ProductID": 2010, "Quantity": 2, "Cost": 520 }, {"ProductID": 4365, "Quantity": 1, "Cost": 18 }], "OrderDate": "04/01/2017" }
1002	{ "CustomerID": 220, "OrderItems": [ {"ProductID": 1825, "Quantity": 1, "Cost": 120 }], "OrderDate": "05/08/2017" }

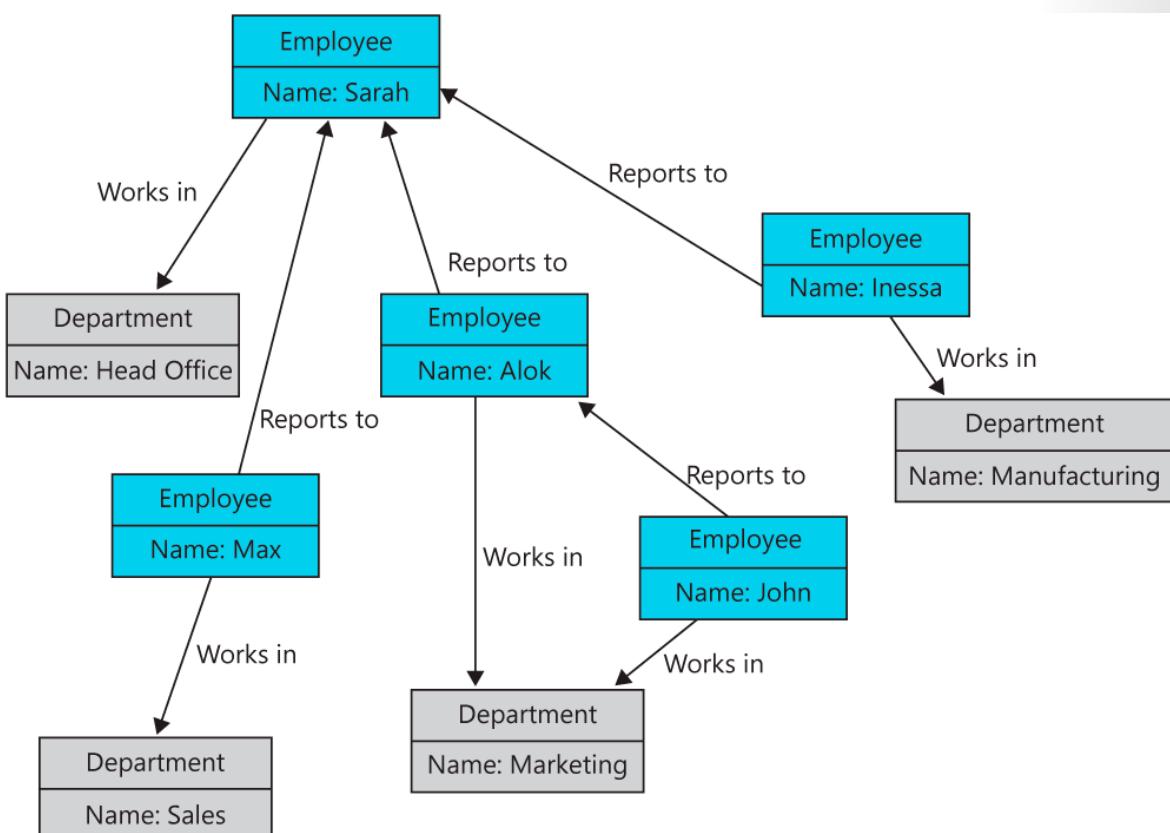
The application can retrieve documents by using the document key. This is a unique identifier for the document, which is often hashed, to help distribute data evenly. Some document databases create the document key automatically. Others enable you to specify an attribute of the document to use as the key.

**Relevant Azure service: Cosmos DB<sup>4</sup>**

## Graph Databases

A graph database stores two types of information, nodes and edges. You can think of nodes as entities. Edges which specify the relationships between nodes. Both nodes and edges can have properties that provide information about that node or edge, similar to columns in a table. Edges can also have a direction indicating the nature of the relationship.

The purpose of a graph database is to allow an application to efficiently perform queries that traverse the network of nodes and edges, and to analyze the relationships between entities. The following diagram shows an organization's personnel database structured as a graph. The entities are employees and departments, and the edges indicate reporting relationships and the department in which employees work. In this graph, the arrows on the edges show the direction of the relationships.



This structure makes it straightforward to perform queries such as "Find all employees who report directly or indirectly to Sarah" or "Who works in the same department as John?" For large graphs with lots of entities and relationships, you can perform very complex analyses very quickly. Many graph databases provide a query language that you can use to traverse a network of relationships efficiently.

**Relevant Azure service: Cosmos DB<sup>5</sup>**

<sup>4</sup> <https://docs.microsoft.com/azure/cosmos-db/table-introduction>

<sup>5</sup> <https://docs.microsoft.com/azure/cosmos-db/table-introduction>

# Overview of Azure Data Storage

## Azure SQL Database

Azure 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 the SQL Server database engine and patched OS with 99.99% availability. PaaS capabilities that are built into Azure SQL Database enable you to focus on the domain-specific database administration and optimization activities that are critical for your business.

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 enables you to process both relational data and non-relational structures, such as graphs, JSON, spatial, and XML.

Azure SQL Database is based on the latest stable version of the Microsoft SQL Server database engine. You can use advanced query processing features, such as high-performance in-memory technologies and intelligent query processing. In fact, the newest capabilities of SQL Server are released first to SQL Database, and then to SQL Server itself. You get the newest SQL Server capabilities with no overhead for patching or upgrading, tested across multiple databases.

SQL Database is available in two purchasing models: vCore-based purchasing model and a DTU-based purchasing model. SQL Database is a fully managed service that has built-in high availability, backups, and other common maintenance operations. Microsoft handles all patching and updating of the SQL and operating system code; you don't have to manage the underlying infrastructure.

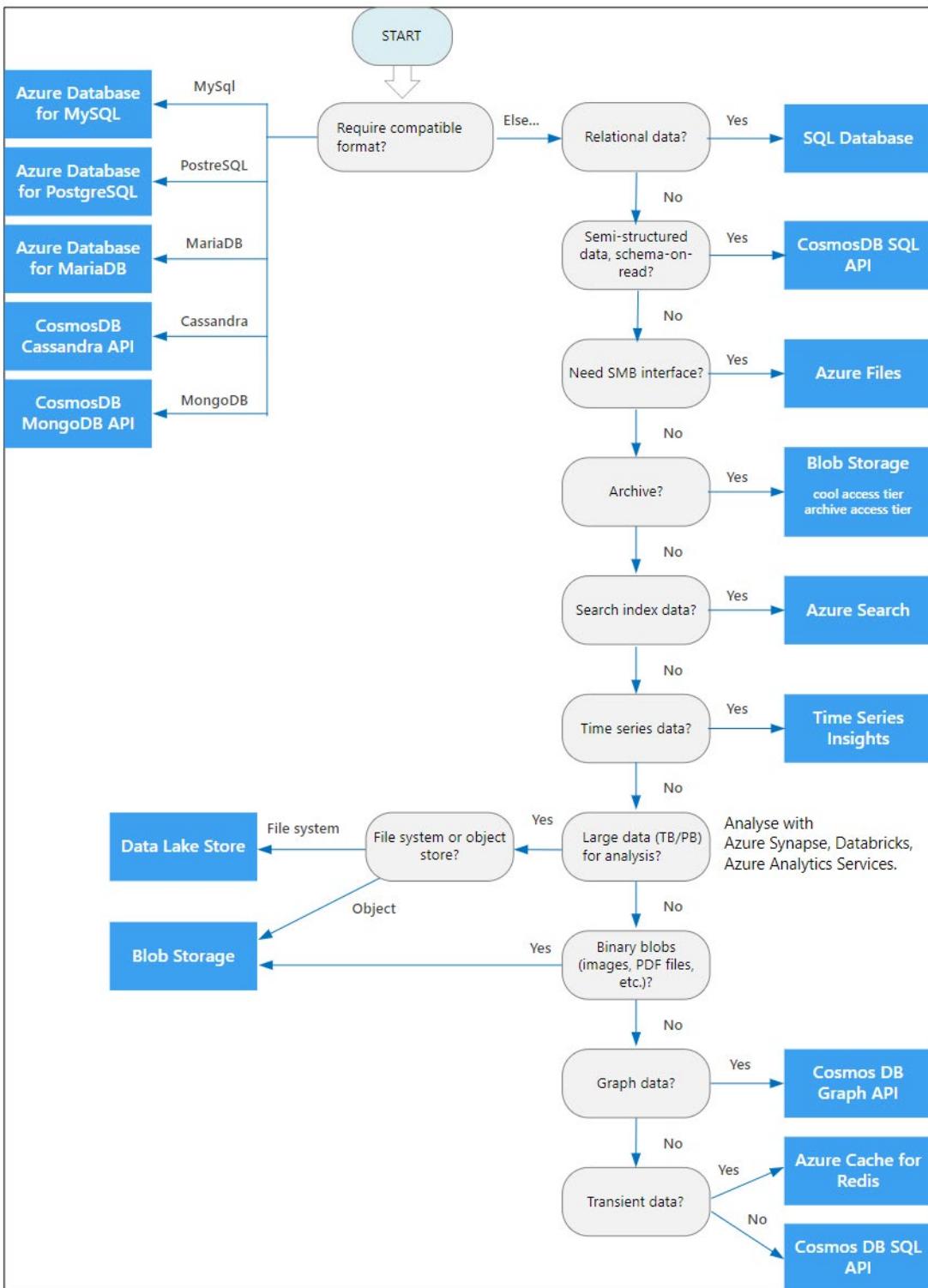
Azure SQL Database provides the following deployment options for a database:

- **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 the SQL Server database engine.
- **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.

## Choose a data store

If your application consists of multiple workloads, evaluate each workload separately. A complete solution may incorporate multiple data stores.

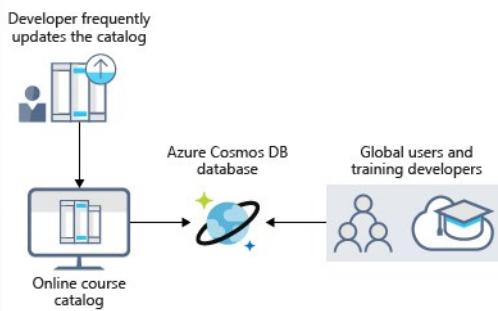
Use the following flowchart to select a candidate data store.



## Azure Cosmos DB

Azure Cosmos DB is a globally distributed database service. It supports schema-less data that lets you build highly responsive and **Always On** applications to support constantly changing data. You can use this feature to store data that is updated and maintained by users around the world.

The following illustration shows a sample Azure Cosmos DB database that's used to store data that's accessed by people located across the globe.



Azure Cosmos DB is schema-agnostic. It automatically indexes all the data without requiring you to deal with schema and index management. It's also multi-model, natively supporting document, key-value, graph, and column-family data models.

Azure Cosmos DB features:

- Geo-replication
- Elastic scaling of throughput and storage worldwide
- Five well-defined consistency levels

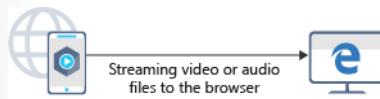
## Azure Blob Storage

Azure Blob Storage is *unstructured*, meaning that there are no restrictions on the kinds of data it can hold. Blobs are highly scalable and apps work with blobs in much the same way as they would work with files on a disk, such as reading and writing data. Blob Storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an Internet connection.

Blobs aren't limited to common file formats. A blob could contain gigabytes of binary data streamed from a scientific instrument, an encrypted message for another application, or data in a custom format for an app you're developing.

Azure Blob storage lets you stream large video or audio files directly to the user's browser from anywhere in the world. Blob storage is also used to store data for backup, disaster recovery, and archiving. It can store up to 8 TB of data for virtual machines.

The following illustration shows an example usage of Azure blob storage.



Blobs are basically files. They store pictures, documents, HTML files, virtual hard disks (VHDs), big data such as logs, database backups — pretty much anything. Blobs are stored in containers, which are similar to folders. A container provides a grouping of a set of blobs. A storage account can contain an unlimited number of containers, and a container can store an unlimited number of blobs.

Azure Blob storage can be accessed from Hadoop (available through HDInsight). HDInsight can use a blob container in Azure Storage as the default file system for the cluster. Through a Hadoop distributed file system (HDFS) interface provided by a WASB driver, the full set of components in HDInsight can

operate directly on structured or unstructured data stored as blobs. Azure Blob storage can also be accessed via Azure Synapse Analytics using its PolyBase feature.

Other features that make Azure Storage a good choice are:

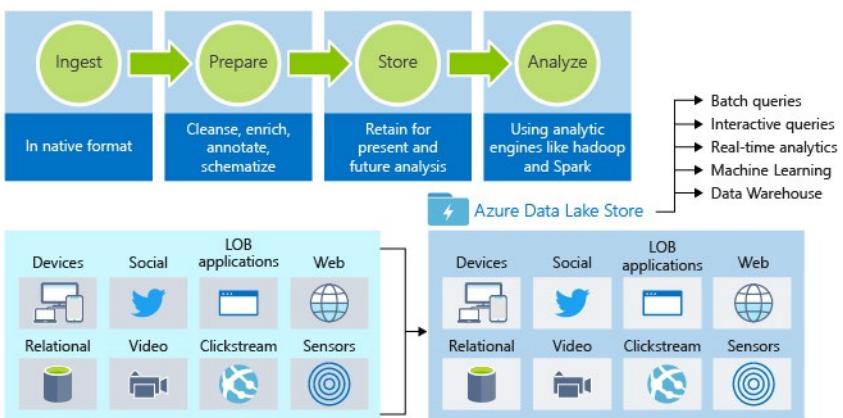
- Multiple concurrency strategies.
- Disaster recovery and high availability options.
- Encryption at rest.
- Role-based access control (RBAC) to control access using Azure Active Directory users and groups.

## Azure Data Lake Storage

The Data Lake feature allows you to perform analytics on your data usage and prepare reports. Data Lake is a large repository that stores both structured and unstructured data.

Azure Data Lake Storage combines the scalability and cost benefits of object storage with the reliability and performance of the Big Data file system capabilities.

The following illustration shows how Azure Data Lake stores all your business data and makes it available for analysis.



Azure Data Lake Store is an enterprise-wide hyperscale repository for big data analytic workloads. Data Lake enables you to capture data of any size, type, and ingestion speed in one single secure location for operational and exploratory analytics.

Data Lake Store does not impose any limits on account sizes, file sizes, or the amount of data that can be stored in a data lake. Data is stored durably by making multiple copies and there is no limit on the duration of time that the data can be stored in the Data Lake. In addition to making multiple copies of files to guard against any unexpected failures, Data lake spreads parts of a file over a number of individual storage servers. This improves the read throughput when reading the file in parallel for performing data analytics.

Data Lake Store can be accessed from Hadoop (available through HDInsight) using the WebHDFS-compatible REST APIs. You may consider using this as an alternative to Azure Storage when your individual or combined file sizes exceed that which is supported by Azure Storage.

# Comparison - Azure Data Lake Store and Azure Blob Storage Containers

The following tables summarize the key differences between Azure Data Lake Store and Azure Blob Storage containers capabilities.

Capability	Azure Data Lake Store	Azure Blob Storage containers
<b>Purpose</b>	Optimized storage for big data analytics workloads	General purpose object store for a wide variety of storage scenarios
<b>Use cases</b>	Batch, streaming analytics, and machine learning data such as log files, IoT data, click streams, large datasets	Any type of text or binary data, such as application back end, backup data, media storage for streaming, and general purpose data
<b>Structure</b>	Hierarchical file system	Object store with flat namespace
<b>Authentication</b>	Based on Azure Active Directory Identities	Based on shared secrets Account Access Keys and Shared Access Signature Keys, and role-based access control (RBAC)
<b>Authentication protocol</b>	OAuth 2.0. Calls must contain a valid JWT (JSON web token) issued by Azure Active Directory	Hash-based message authentication code (HMAC). Calls must contain a Base64-encoded SHA-256 hash over a part of the HTTP request.
<b>Authorization</b>	POSIX access control lists (ACLs). ACLs based on Azure Active Directory identities can be set file and folder level.	For account-level authorization use Account Access Keys. For account, container, or blob authorization use Shared Access Signature Keys.
<b>Auditing</b>	Available.	Available
<b>Encryption at rest</b>	Transparent, server side	Transparent, server side; Client-side encryption
<b>Developer SDKs</b>	.NET, Java, Python, Node.js	.Net, Java, Python, Node.js, C++, Ruby
<b>Analytics workload performance</b>	Optimized performance for parallel analytics workloads, High Throughput and IOPS	Not optimized for analytics workloads
<b>Size limits</b>	No limits on account sizes, file sizes or number of files	Specific limits documented here
<b>Geo-redundancy</b>	Locally-redundant (LRS), globally redundant (GRS), read-access globally redundant (RA-GRS), zone-redundant (ZRS).	Locally redundant (LRS), globally redundant (GRS), read-access globally redundant (RA-GRS), zone-redundant (ZRS). See here for more information

## Azure Files

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol.

Azure file shares can be mounted concurrently by cloud or on-premises deployments. Azure Files SMB file shares are accessible from Windows, Linux, and macOS clients. Azure Files NFS file shares are accessible from Linux or macOS clients. Additionally, Azure Files SMB file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

The following illustration shows Azure Files being used to share data between two geographical locations. Azure Files uses the Server Message Block (SMB) protocol that ensures the data is encrypted at rest and in transit.

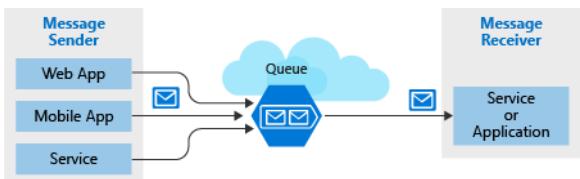
## Azure Queue

Azure Queue storage is a service for storing large numbers of messages that can be accessed from anywhere in the world.

Azure Queue Storage can be used to help build flexible applications and separate functions for better durability across large workloads. When application components are decoupled, they can scale independently. Queue storage provides asynchronous message queueing for communication between application components, whether they are running in the cloud, on the desktop, on-premises, or on mobile devices.

Typically, there are one or more sender components and one or more receiver components. Sender components add messages to the queue, while receiver components retrieve messages from the front of the queue for processing.

The following illustration shows multiple sender applications adding messages to the Azure Queue and one receiver application retrieving the messages.



You can use queue storage to:

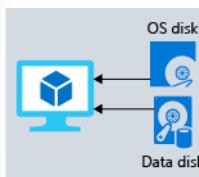
- Create a backlog of work and to pass messages between different Azure web servers.
- Distribute load among different web servers/infrastructure and to manage bursts of traffic.
- Build resilience against component failure when multiple users access your data at the same time.

## Disk Storage

Disk storage provides disks for virtual machines, applications, and other services to access and use as they need, similar to how they would in on-premises scenarios. Disk storage allows data to be persistently stored and accessed from an attached virtual hard disk. The disks can be managed or unmanaged by Azure, and therefore managed and configured by the user. Typical scenarios for using disk storage are if you want to lift and shift applications that read and write data to persistent disks, or if you are storing data that is not required to be accessed from outside the virtual machine to which the disk is attached.

Disk come in many different sizes and performance levels, from solid-state drives (SSDs) to traditional spinning hard disk drives (HDDs), with varying performance abilities.

When working with VMs, you can use standard SSD and HDD disks for less critical workloads, and premium SSD disks for mission-critical production applications. Azure Disks have consistently delivered enterprise-grade durability, with an industry-leading ZERO% annualized failure rate. The following illustration shows an Azure virtual machine using separate disks to store different data.



## Walk-Through - Working with Azure Storage Queues in .NET Core

Azure Queue storage implements cloud-based queues to enable communication between components of a distributed application. Each queue maintains a list of messages that can be added by a sender component and processed by a receiver component. With a queue, your application can scale immediately to meet demand.

This demonstration shows the basic steps for working with an Azure storage queue.

In this demonstration, you will see how to:

- Create an Azure storage account
- Create the app
- Add the Azure client libraries
- Add support for asynchronous code
- Create a queue
- Insert messages into a queue
- Dequeue messages

The C#, Visual Basic, and F# languages can be used to write applications and libraries for .NET Core. These languages can be used in your preferred text editor or Integrated Development Environment (IDE), including:

- Visual Studio
- Visual Studio Code

For an overview of .NET Core, see: <https://docs.microsoft.com/en-us/dotnet/core/about>

✓ **Note:** The commands done below are using .NET v12.

### Create an Azure storage account

First, create an Azure storage account. For a step-by-step guide to creating a storage account, see the Create a storage account quickstart. This is a separate step you perform after creating a free Azure account in the prerequisites.

## Create the app

Create a .NET Core application named **QueueApp**. For simplicity, this app will both send and receive messages through the queue.

1. In a console window (such as CMD, PowerShell, or Azure CLI), use the dotnet new command to create a new console app with the name **QueueApp**. This command creates a simple "Hello World" C# project with a single source file: **Program.cs**.

```
dotnet new console -n QueueApp
```

2. Switch to the newly created **QueueApp** folder and build the app to verify that all is well.

```
cd QueueApp  
dotnet build
```

## Add the Azure client libraries

1. Add the Azure Storage client libraries to the project by using the dotnet add package command. Execute the following command from the project folder in the console window.

```
dotnet add package Azure.Storage.Queues
```

## Add using statements

1. From the command line in the project directory, type code. to open Visual Studio Code in the current directory. Keep the command-line window open. There will be more commands to execute later. If you're prompted to add C# assets required to build and debug, click the **Yes** button.
2. Open the **Program.cs** source file and add the following namespaces right after the `using System;` statement. This app uses types from these namespaces to connect to Azure Storage and work with queues.

```
using System.Threading.Tasks;  
using Azure.Storage.Queues;  
using Azure.Storage.Queues.Models;
```

3. Save the **Program.cs** file.

## Add support for asynchronous code

Since the app uses cloud resources, the code runs asynchronously.

1. Update the **Main** method to run asynchronously. Replace **void** with an **async Task** return value.

```
static async Task Main(string[] args)
```

2. Save the **Program.cs** file.

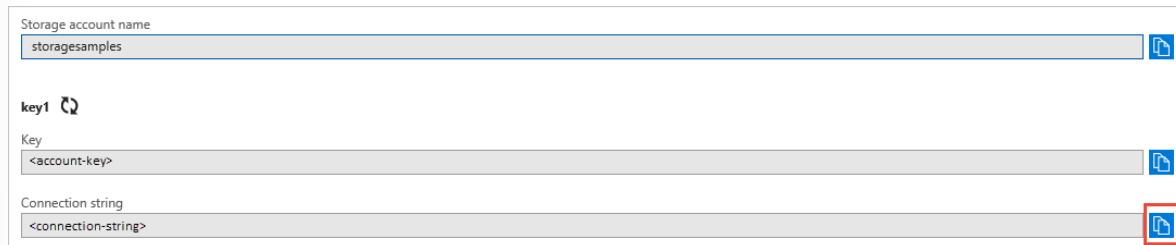
## Create a queue

Before making any calls into Azure APIs, you must get your credentials from the Azure portal.

## Copy your credentials from the Azure portal

When the sample application makes a request to Azure Storage, it must be authorized. To authorize a request, add your storage account credentials to the application as a connection string. View your storage account credentials by following these steps:

1. Sign in to the [Azure portal<sup>6</sup>](https://portal.azure.com/).
2. Locate your storage account.
3. In the **Settings** section of the storage account overview, select **Access keys**. Here, you can view your account access keys and the complete connection string for each key.
4. Find the **Connection string** value under **key1**, and select the **Copy** button to copy the connection string. You will add the connection string value to an environment variable in the next step.



## Configure your storage connection string

After you have copied your connection string, write it to a new environment variable on the local machine running the application. To set the environment variable, open a console window, and follow the instructions for your operating system. Replace <yourconnectionstring> with your actual connection string.

### Windows

```
setx AZURE_STORAGE_CONNECTION_STRING "<yourconnectionstring>"
```

After you add the environment variable in Windows, you must start a new instance of the command window.

### Linux

```
export AZURE_STORAGE_CONNECTION_STRING=<yourconnectionstring>"
```

### Restart programs

After you add the environment variable, restart any running programs that will need to read the environment variable. For example, restart your development environment or editor before continuing.

## Add the connection string to the app

Add the connection string into the app so it can access the storage account.

1. Switch back to Visual Studio Code.

---

<sup>6</sup> <https://portal.azure.com/>

2. In the **Main** method, replace the `Console.WriteLine("Hello World!");` code with the following line that gets the connection string from the environment variable.

```
string connectionString = Environment.GetEnvironmentVariable("AZURE_STORAGE_CONNECTION_STRING");
```

Add the following code to **Main** to create a queue object, which is later passed into the send and receive methods.

```
QueueClient queue = new QueueClient(connectionString, "mystoragequeue");
```

3. Save the file.

## Insert messages into the queue

Create a new method to send a message into the queue.

1. Add the following **InsertMessageAsync** method to your **Program** class.

This method is passed a queue reference. A new queue is created, if it doesn't already exist, by calling `CreateIfNotExistsAsync`. Then, it adds the `newMessage` to the queue by calling `SendMessageAsync`.

```
static async Task InsertMessageAsync(QueueClient theQueue, string newMessage)
{
    if (null != await theQueue.CreateIfNotExistsAsync())
    {
        Console.WriteLine("The queue was created.");
    }
    await theQueue.SendMessageAsync(newMessage);
}
```

## Dequeue messages

Create a new method to retrieve a message from the queue. Once the message is successfully received, it's important to delete it from the queue so it isn't processed more than once.

1. Add a new method called `** RetrieveNextMessageAsync**` to your **Program** class.

This method receives a message from the queue by calling `ReceiveMessagesAsync`, passing 1 in the first parameter to retrieve only the next message in the queue. After the message is received, delete it from the queue by calling `DeleteMessageAsync`.

```
static async Task<string> RetrieveNextMessageAsync(QueueClient theQueue)
{
    if (await theQueue.ExistsAsync())
    {
        QueueProperties properties = await theQueue.GetPropertiesAsync();
        if (properties.ApproximateMessagesCount > 0)
        {
            QueueMessage[] retrievedMessage = await theQueue.ReceiveMessagesAsync(1);
            string theMessage = retrievedMessage[0].MessageText;
        }
    }
}
```

```
    await theQueue.DeleteMessageAsync(retrievedMessage[0].MessageId, re-
trievedMessage[0].PopReceipt);
    return theMessage;
}
return null;
}
return null;
}
```

2. Save the file.

## Recommend Database Service Tier Sizing

### Azure SQL Database and Azure SQL Managed Instance Service Tiers

Azure SQL Database and Azure SQL Managed Instance are based on SQL Server database engine architecture that's adjusted for the cloud environment to ensure 99.99 percent availability, even if there is an infrastructure failure. Two service tiers are used by Azure SQL Database and Azure SQL Managed Instance, each with a different architectural model.

These service tiers are:

- **General purpose**, which is designed for budget-oriented workloads.
- **Business critical**, which is designed for low-latency workloads with high resiliency to failures and fast failovers.

Azure SQL Database has an additional service tier:

- **Hyperscale**, which is designed for most business workloads, providing highly scalable storage, read scale-out, and fast database restore capabilities.

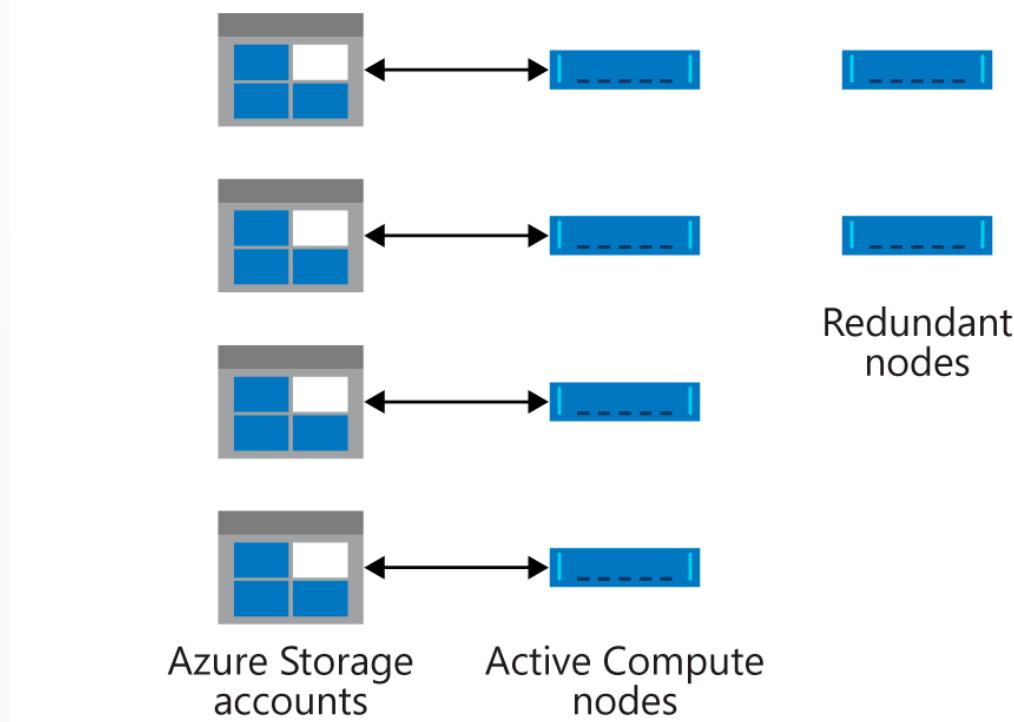
This lesson discusses differences between the service tiers for the general purpose and business critical service tiers in the vCore-based purchasing model.

### General Purpose Service Tier for Azure SQL Database & SQL Managed Instance

Azure SQL Database and Azure SQL Managed Instance are based on SQL Server database engine architecture adapted for the cloud environment in order to ensure 99.99% availability even in the cases of infrastructure failures.

The architectural model for the general-purpose service tier is based on a separation of compute and storage. This architectural model relies on high availability and reliability of Azure Blob storage that transparently replicates database files and guarantees no data loss if underlying infrastructure failure happens.

The following figure shows four nodes in standard architectural model with the separated compute and storage layers.



In the architectural model for the general-purpose service tier, there are two layers:

- **A stateless compute layer** that is running the `sqlservr.exe` process and contains only transient and cached data (for example – plan cache, buffer pool, column store pool). This stateless node is operated by Azure Service Fabric that initializes process, controls health of the node, and performs failover to another place if necessary.
- **A stateful data layer** with database files (.mdf/.ldf) that are stored in Azure Blob storage. Azure Blob storage guarantees that there will be no data loss of any record that is placed in any database file. Azure Storage has built-in data availability/redundancy that ensures that every record in log file or page in data file will be preserved even if the process crashes.

## When to choose this service tier

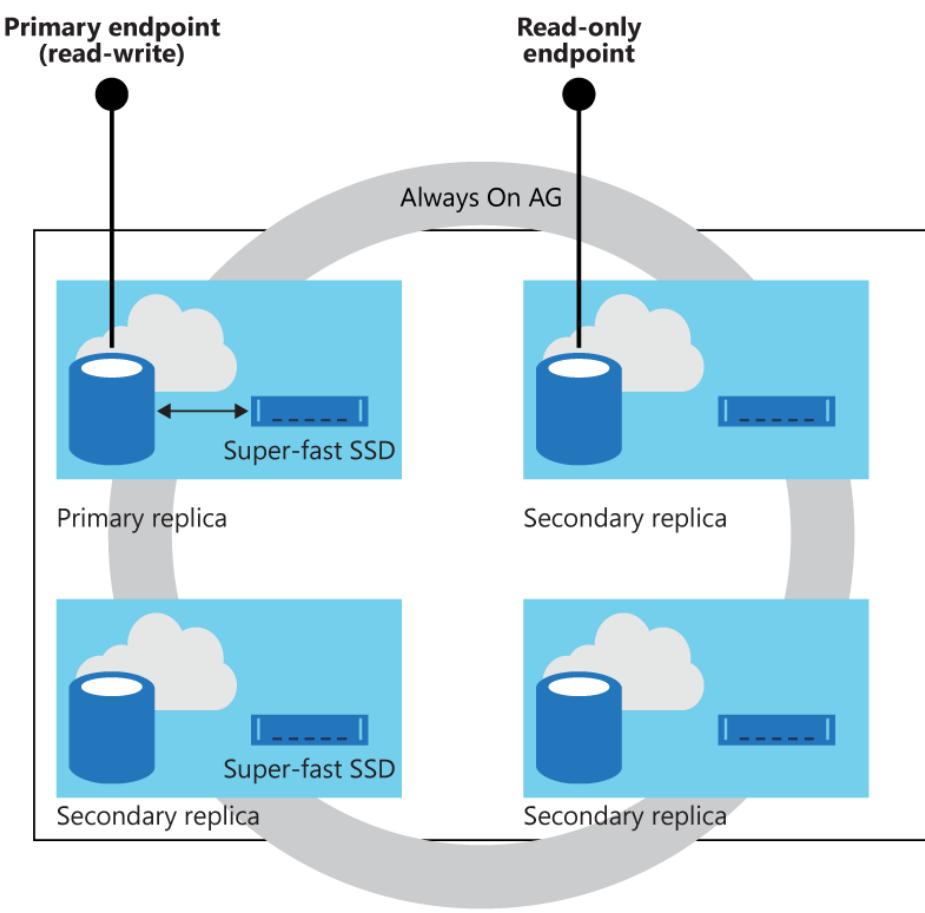
General Purpose service tier is a default service tier in Azure SQL Database and Azure SQL Managed Instance that is designed for most of generic workloads. If you need a fully managed database engine with 99.99% SLA with storage latency between 5 and 10 ms that match SQL Server on an Azure VM in most of the cases, General Purpose tier is the option for you.

## Business Critical Tier for Azure SQL Database & SQL Managed Instance

Premium/Business Critical service tier model is based on a cluster of database engine processes. This architectural model relies on a fact that there is always a quorum of available database engine nodes and has minimal performance impact on your workload even during maintenance activities.

Premium availability is enabled in Premium and Business Critical service tiers and it is designed for intensive workloads that cannot tolerate any performance impact due to the ongoing maintenance operations.

Compute and storage is integrated on the single node in the premium model. High availability in this architectural model is achieved by replication of compute (SQL Server database engine process) and storage (locally attached SSD) deployed to a four node cluster, using technology similar to SQL Server Always On availability groups.



## When to choose this service tier?

Business Critical service tier is designed for applications that require low-latency responses from the underlying SSD storage (1-2 ms in average), fast recovery if the underlying infrastructure fails, or need to off-load reports, analytics, and read-only queries to the free of charge readable secondary replica of the primary database.

The key reasons why you should choose Business Critical service tier instead of General Purpose tier are:

- Low IO latency requirements
- Frequent communication between application and database

- Long running transactions that modify data.
- Workload with reporting and analytic queries
- Higher resiliency and faster recovery from failures.
- Higher availability
- Fast geo-recovery

## Service Tier Comparison

The following table describes the key differences between service tiers for the latest generation (Gen5). Note that service tier characteristics might be different in SQL Database and SQL Managed Instance.

	<b>Resource type</b>	<b>General Purpose</b>	<b>Hyperscale</b>	<b>Business Critical</b>
<b>Best for</b>		Offers budget oriented balanced compute and storage options.	Most business workloads. Auto-scaling storage size up to 100 TB, fluid vertical and horizontal compute scaling, fast database restore.	OLTP applications with high transaction rate and low IO latency. Offers highest resilience to failures and fast failovers using multiple synchronously updated replicas.
<b>Available in resource type:</b>		SQL Database / SQL Managed Instance	Single Azure SQL Database	SQL Database / SQL Managed Instance
<b>Compute size</b>	SQL Database	1 to 80 vCores	1 to 80 vCores	1 to 80 vCores
	SQL Managed Instance	4, 8, 16, 24, 32, 40, 64, 80 vCores	N/A	4, 8, 16, 24, 32, 40, 64, 80 vCores
	SQL Managed Instance pools	2, 4, 8, 16, 24, 32, 40, 64, 80 vCores	N/A	N/A
<b>Storage type</b>	All	Premium remote storage (per instance)	De-coupled storage with local SSD cache (per instance)	Super-fast local SSD storage (per instance)
<b>Database size</b>	SQL Database	5 GB – 4 TB	Up to 100 TB	5 GB – 4 TB
	SQL Managed Instance	32 GB – 8 TB	N/A	32 GB – 4 TB
<b>Storage size</b>	SQL Database	5 GB – 4 TB	Up to 100 TB	5 GB – 4 TB
	SQL Managed Instance	32 GB – 8 TB	N/A	32 GB – 4 TB
<b>Availability</b>	All	99.99%	99.95% with one secondary replica, 99.99% with more replicas	99.99% 99.995% with zone redundant single database

	<b>Resource type</b>	<b>General Purpose</b>	<b>Hyperscale</b>	<b>Business Critical</b>
<b>Backups</b>	All	RA-GRS, 7-35 days (7 days by default)	RA-GRS, 7 days, constant time point-in-time recovery (PITR)	RA-GRS, 7-35 days (7 days by default)
<b>Pricing/billing</b>	SQL Database	vCore, reserved storage, and backup storage are charged. IOPS is not charged.	vCore for each replica and used storage are charged. IOPS not yet charged.	vCore, reserved storage, and backup storage are charged. IOPS is not charged.
	SQL Managed Instance	vCore, reserved storage, and backup storage is charged. IOPS is not charged	N/A	vCore, reserved storage, and backup storage is charged. IOPS is not charged.
<b>Discount models</b>		Reserved instances Azure Hybrid Benefit (not available on dev/ test subscriptions) Enterprise and Pay-As-You-Go Dev/Test subscrip- tions	Azure Hybrid Benefit (not available on dev/ test subscriptions) Enterprise and Pay-As-You-Go Dev/Test subscrip- tions	Reserved instances Azure Hybrid Benefit (not available on dev/ test subscriptions) Enterprise and Pay-As-You-Go Dev/Test subscrip- tion

## Dynamically Scale Azure SQL Database and Azure SQL Managed Instances

### Dynamically Scale Azure SQL Database and Azure SQL Managed Instance

Azure SQL Database enables you to change resources (CPU power, memory, IO throughput, and storage) allocated to your databases.

You can mitigate performance issues due to increased usage of your application that cannot be fixed using indexing or query rewrite methods. Adding more resources enables you to react when your database hits the current resource limits and needs more power to handle the incoming workload. Azure SQL Database also enables scale-down of resources when they are not needed to lower the cost.

Scaling the database can be done using Azure portal using a slider.



Azure SQL Database offers the DTU-based purchasing model and the vCore-based purchasing model, while Azure SQL Managed Instance offers just the vCore-based purchasing model.

- The **DTU-based purchasing model** offers a blend of compute, memory, and IO resources in three service tiers to support lightweight to heavyweight database workloads: Basic, Standard, and Premium. Performance levels within each tier provide a different mix of these resources, to which you can add additional storage resources.
- The **vCore-based purchasing model** lets you choose the number of vCores, the amount of memory, and the amount and speed of storage. This purchasing model offers three service tiers: General Purpose, Business Critical, and Hyperscale.

You can build apps on a small, single database at a low cost per month in the Basic, Standard, or General Purpose service tier and then change its service tier manually or programmatically at any time to the Premium or Business Critical service tier to meet the needs of your solution.

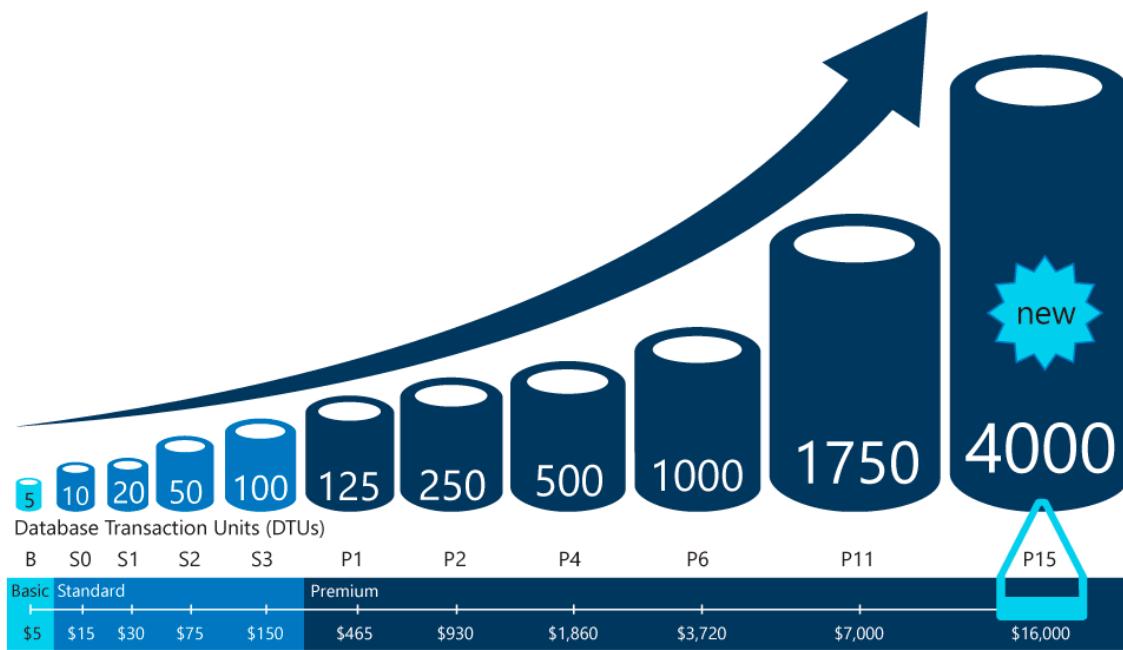
You can adjust performance without downtime to your app or to your customers. Dynamic scalability enables your database to transparently respond to rapidly changing resource requirements and enables you to only pay for the resources that you need when you need them.

✓ **Note** Dynamic scalability is different from autoscale. Autoscale is when a service scales automatically based on criteria, whereas dynamic scalability allows for manual scaling with a minimal downtime.

## Scale Single Databases in Azure SQL Database

Single databases in Azure SQL Database support manual dynamic scalability, but not autoscale. For a more *automatic* experience, consider using elastic pools, which allow databases to share resources in a pool based on individual database needs.

You can change DTU service tiers or vCore characteristics at any time with minimal downtime to your application (generally averaging under four seconds). For many businesses and apps, being able to create databases and dial performance up or down on demand is enough, especially if usage patterns are relatively predictable. But if you have unpredictable usage patterns, it can make it hard to manage costs and your business model. For this scenario, you use an elastic pool with a certain number of eDTUs that are shared among multiple databases in the pool.



Azure SQL Database offers the ability to dynamically scale your databases:

- With a single database, you can use either DTU or vCore models to define maximum amount of resources that will be assigned to each database.
- Elastic pools enable you to define maximum resource limit per group of databases in the pool.

# Recommend a Solution for Encrypting Data at Rest, Transmission, and In Use

## Data Encryption

Encryption is the process of making data unreadable and unusable. To use or read the encrypted data, it must be *decrypted*, which requires the use of a secret key. There are two top-level types of encryption: *symmetric* and *asymmetric*.

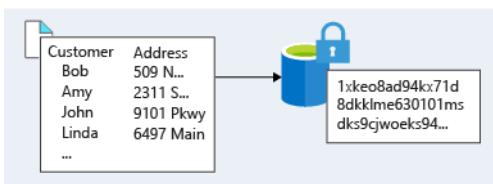
**Symmetric encryption** uses the same key to encrypt and decrypt the data. Consider a desktop password manager application. You enter your passwords and they are encrypted with your own personal key (your key is often derived from your master password). When the data needs to be retrieved, the same key is used and the data is decrypted.

**Asymmetric encryption** uses a public key and private key pair. Either key can encrypt but cannot decrypt its own encrypted data. To decrypt, you need the paired key. Asymmetric encryption is used for things like TLS (used in https), and data signing.

## Encryption at Rest

Data at rest is the data that has been stored on a physical medium. This could be data stored on the disk of a server, data stored in a database, or data stored in a storage account. Regardless of the storage mechanism, encryption of data at rest ensures that the stored data is unreadable without the keys and secrets needed to decrypt it. If an attacker obtained a hard drive with encrypted data and did not have access to the encryption keys, the attacker would not compromise the data without great difficulty. In such a scenario, an attacker would have to attempt attacks against encrypted data, which are much more complex and resource consuming than accessing unencrypted data on a hard drive.

The actual data that is encrypted could vary in its content, usage, and importance to the organization. This could be financial information critical to the business, intellectual property that has been developed by the business, personal data that the business stores about customers or employees, and even the keys and secrets used for the encryption of the data itself.



**Best practice:** Apply disk encryption to help safeguard your data.

- **Detail:** Use Azure Disk Encryption. It enables IT administrators to encrypt Windows and Linux IaaS VM disks. Disk Encryption combines the industry-standard Windows BitLocker feature and the Linux dm-crypt feature to provide volume encryption for the OS and the data disks.

Azure Storage and Azure SQL Database encrypt data at rest by default, and many services offer encryption as an option. You can use Azure Key Vault to maintain control of keys that access and encrypt your data. See Azure resource providers encryption model support to learn more.

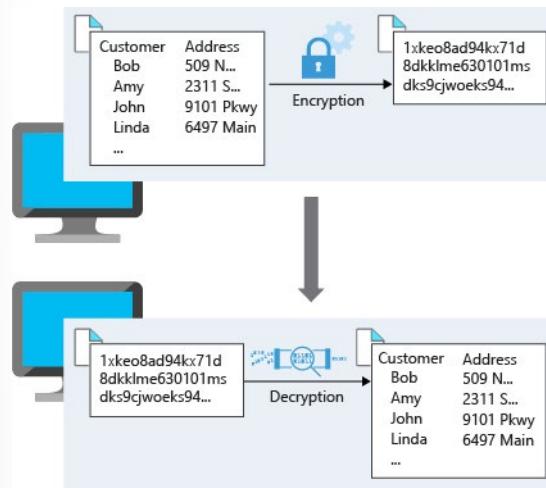
**Best practice:** Use encryption to help mitigate risks related to unauthorized data access.

- **Detail:** Encrypt your drives before you write sensitive data to them.

Organizations that don't enforce data encryption are more exposed to data-confidentiality issues. For example, unauthorized or rogue users might steal data in compromised accounts or gain unauthorized access to data coded in Clear Format. Companies also must prove that they are diligent and using correct security controls to enhance their data security in order to comply with industry regulations.

## Encryption in Transit

Data in transit is the data actively moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by encrypting the data prior to sending it over a network or setting up a secure channel to transmit unencrypted data between two systems. Encrypting data in transit protects the data from outside observers and provides a mechanism to transmit data while limiting risk of exposure.



## TLS/SSL encryption in Azure

Microsoft uses the Transport Layer Security (TLS) protocol to protect data when it's traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

## Identify and Classify Data

Suppose you have a scenario where previous incidents that exposed sensitive data, so there's a gap between what they are encrypting and what they should be encrypting. You should begin by identifying and classifying the types of data they are storing and align this with the business and regulatory requirements surrounding the storage of data. It's beneficial to classify this data as it relates to the impact of exposure to the organization, its customers, or partners.

An example classification could be as follows:

Data classification	Explanation	Examples
<b>Restricted</b>	Data classified as restricted poses significant risk if exposed, altered, or deleted. Strong levels of protection are required for this data.	Data containing Social Security numbers, credit card numbers, personal health records
<b>Private</b>	Data classified as private poses moderate risk if exposed, altered, or deleted. Reasonable levels of protection are required for this data. Data that is not classified as restricted or public will be classified as private.	Personal records containing information such as address, phone number, academic records, customer purchase records
<b>Public</b>	Data classified as public poses no risk if exposed, altered, or deleted. No protection is required for this data.	Public financial reports, public policies, product documentation for customers

By taking an inventory of the types of data being stored, they can get a better picture of where sensitive data may be stored and where existing encryption may or may not be happening.

A thorough understanding of the regulatory and business requirements that apply to data the organization stores is also important. The regulatory requirements an organization must adhere to will often drive a large part of the data encryption requirements.

## Encrypting Raw Storage

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 with 256-bit Advanced Encryption Standard (AES) encryption before persisting it to disk and decrypts the data during retrieval. This handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is transparent to applications using the services - you don't need to add any code or turn on any features.

You can use Microsoft-managed encryption keys with SSE, or you can use your own encryption keys by selecting the option in the Azure portal as shown below.

The screenshot shows the 'storagesample - Encryption' blade in the Azure Storage Explorer. On the left, a navigation pane lists several options: 'Diagnose and solve problems', 'SETTINGS', 'Storage Explorer (preview)', 'Access keys', 'Configuration', 'Encryption' (which is highlighted with a red box), 'Shared access signature', 'Firewalls and virtual networks', and 'Metrics (preview)'. The main content area contains information about Storage Service Encryption, stating that it protects data at rest by encrypting it as it's written in datacenters and decrypted upon access. It notes that by default, data is encrypted using Microsoft Managed Keys for Blobs, Tables, Files, and Queues. A note specifies that after enabling SSE, new data will be encrypted, while existing files will be retroactively encrypted. There is also a link to 'Learn more' and a section indicating that the storage account is currently encrypted with a Microsoft managed key, with an option to use a customer-managed key.

SSE automatically encrypts data in:

- All Azure Storage services including Azure Managed Disks, Azure Blob storage, Azure Files, Azure Queue storage, and Azure Table storage
- Both performance tiers (Standard and Premium)
- Both deployment models (Resource Manager and classic)

For your organization, SSE means that whenever they are using services that support storage service encryption, their data is encrypted on the physical medium of storage. In the highly unlikely event that access to the physical disk is obtained, data will be unreadable since it has been encrypted as written to the physical disk.

## Encrypting Virtual Machines

Storage Service encryption provides low-level encryption protection for data written to physical disk, but how do you protect the virtual hard disks (VHD) of virtual machines? If a malicious attacker gained access to your Azure subscription and exfiltrated the VHDs of your virtual machines, how would you ensure they would be unable to access data stored on the VHD?

Azure Disk Encryption (ADE) is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks. ADE leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets (and you can use managed identity for Azure services for accessing the key vault).

Disk Encryption for Windows IaaS and Linux VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage. When you apply the Disk Encryption management solution, you can satisfy the following business needs:

1. IaaS VMs are secured at rest by using industry-standard encryption technology to address organizational security and compliance requirements.
2. IaaS VMs boot under customer-controlled keys and policies. You can audit their usage in your key vault.

In addition, if you use Azure Security Center, you're alerted if you have VMs that aren't encrypted. The alerts display as High Severity, and the recommendation is to encrypt these VMs as shown below.

VIRTUAL MACHINES RECOMMENDATIONS		TOTAL					
Missing disk encryption		2 of 2 VMs					
Virtual machines							
NAME	ONBOARDING	SYSTEM UPDATES	ANTIMALWARE	BASELINE	DISK ENCRYPTION		
ASC-VM1	✓	✓	✓	✓	✓	!	!
ASC-VM2	✓	✓	✓	✓	✓	!	!

Your organization can apply ADE to their virtual machines to be sure any data stored on VHDs is secured to their organizational and compliance requirements. Because boot disks are also encrypted, they can control and audit usage.

## Encrypting Databases

Your organization has several databases deployed that store data that needs additional protection. They've moved many databases to Azure SQL Database and want to ensure that their data is encrypted within their database. If the data files, log files, or backup files were stolen, they want to ensure they are unreadable without access to the encryption keys.

Transparent data encryption (TDE) helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. By default, TDE is enabled for all newly deployed Azure SQL Databases.

TDE encrypts the storage of an entire database by using a symmetric key called the database encryption key. By default, Azure provides a unique encryption key per logical SQL Server and handles all the details. Bring-your-own-key is also supported with keys stored in Azure Key Vault.

Since TDE is enabled by default, your organization can be confident they have the proper protections in place for data stored in their databases.

For their on-premises Microsoft SQL Server databases, your organization has turned on the SQL Server Always Encrypted feature. Always Encrypted is designed to protect sensitive data, such as client personal information or financial data. This feature protects column data at rest and in transit by having the client application handle the encryption and decryption outside the SQL Server database through an installed driver. This allows your organization to minimize exposure of data as the database never works with unencrypted data. The Always Encrypted client driver performs the actual encryption and decryption processes, rewriting the T-SQL queries as necessary to encrypt data passed to the DB and decrypt the results, while keeping these operations transparent to the application.

## Encrypting Secrets

As mentioned earlier in this course, Azure Key Vault is a cloud service that works as a secure secrets store. Key Vault allows you to create multiple secure containers, called vaults. These vaults are backed by hardware security modules (HSMs). Vaults help reduce the chances of accidental loss of security information by centralizing the storage of application secrets. Key Vaults also control and log the access to

anything stored in them. Azure Key Vault can handle requesting and renewing Transport Layer Security (TLS) certificates, providing the features required for a robust certificate lifecycle management solution. Key Vault is designed to support any type of secret. These secrets could be passwords, database credentials, API keys and, certificates.

Because Azure AD identities can be granted access to use Azure Key Vault secrets, applications using managed identities for Azure services can automatically and seamlessly acquire the secrets they need.

Your organization can use Key Vault for the storage of all their sensitive application information, including the TLS certificates they use to secure communication between systems.

# Lab

## Lab: Implementing Azure SQL Database-Based Applications

✓ **Important:** To download the most recent version of this lab, please visit the AZ-304 GitHub repository<sup>7</sup>.

Direct link to the [Lab: Implementing Azure SQL Database-Based Applications<sup>8</sup>](#).

### Lab scenario



Adatum Corporation has a number two tier applications with .NET Core-based front end and SQL Server-based backend. The Adatum Enterprise Architecture team is exploring the possibility of implementing these applications by leveraging Azure SQL Database as the data tier. Given intermittent, unpredictable usage of the existing SQL Server backend and relatively high tolerance for latency built into the front-end apps, Adatum is considering the serverless tier of Azure SQL Database.

Serverless is a compute tier for individual Azure SQL Databases instances that automatically scales compute based on workload demand and bills for compute used per second. The serverless compute tier is also capable of automatically pausing databases during inactive periods when only storage is billed and automatically resumes databases when activity returns.

The Adatum Enterprise Architecture team is also interested in evaluating network-level security provided by the Azure SQL Databases, in order to ensure that it is possible to restrict inbound connections to specific ranges of IP addresses, in scenarios where the apps must be able to connect from its on-premises locations without relying on hybrid connectivity via Site-to-Site VPN or ExpressRoute.

To accomplish these objectives, the Adatum Architecture team will test Azure SQL Database-based applications, including:

- Implementing serverless tier of Azure SQL Database
- Implementing .NET Core console apps that use Azure SQL Database as their data store

### Objectives

After completing this lab, you will be able to:

- Implement serverless tier of Azure SQL Database
- Configure .NET Core-based console apps that use Azure SQL Database as their data store

### Lab Environment

Windows Server admin credentials

- User Name: **Student**

<sup>7</sup> <https://github.com/MicrosoftLearning/AZ-304-Microsoft-Azure-Architect-Design>

<sup>8</sup> [https://aka.ms/304\\_Module\\_6\\_Lab](https://aka.ms/304_Module_6_Lab)

- Password: **Pa55w.rd1234**

Estimated Time: 60 minutes

## Lab Files

- None

## Exercise 1: Implement Azure SQL Database

The main tasks for this exercise are as follows:

1. Create Azure SQL Database
2. Connect to and query Azure SQL Database

## Exercise 2: Implement a .NET Core console app that uses Azure SQL Database as their data store

The main tasks for this exercise are as follows:

1. Identify ADO.NET connection information of Azure SQL Database
2. Create and configure a .NET Core console app
3. Test the .NET Core console app
4. Configure Azure SQL database firewall
5. Verify the functionality of the .NET Core console app
6. Remove Azure resources deployed in the lab

## Module 6 Review Questions

### Module 6 Review Questions



#### Review Question 1

You are asked to recommend a data storage solution to fit the following requirements.

- Applications must be able to have access to data using a REST connection.
- The storage solution must hold costs to a minimum.
- The solution will host 30 independent tables of changing sizes and varied usage patterns.
- Automatic replication of the data to a second Azure region.

What do you recommend?

- Use of tables within an Azure Storage account using geo-redundant storage (GRS)
- An Azure SQL Database elastic database pool using active geo-replication
- Use of tables within an Azure Storage account using read-access geo-redundant storage (RA-GRS)
- An Azure SQL Database using active geo-replication.

#### Review Question 2

You are asked to recommend a solution for migrating an application data to Azure.

The scenario is as follows:

- An existing application instance that consume data from multiple databases.
- The application code references database tables using a combination of server, database, and table name.
- You need to migrate the application data to Azure.

Which service do you recommend?

- SQL Managed Instance
- An Azure SQL Database
- An Azure Storage account

#### Review Question 3

You are designing a solution for an organization with the following requirements.

- They are using Application Insights.

- They intend on using continuous export.
- Application Insights data needs to be stored for four years.

*Which service do you recommend?*

- Azure Storage
- Azure Backup
- Azure SQL Database
- Azure Storage Service Encryption (SSE)

## Review Question 4

*You are asked to design a message application can be run on a Linux VM.*

*The app runs on Azure Storage queues.*

*You are asked to recommend a solution for the app to interact with the storage queues.*

*The requirements are as below:*

- Upload messages every 15 minutes
  - To be scheduled using a CRON job
  - Can create and delete messages every 3 minutes
- What do you recommend to developers to work with the queue?

- A. AzCopy
- B. Azure Data Lake
- C. .NET Core

# Answers

## Review Question 1

You are asked to recommend a data storage solution to fit the following requirements.

What do you recommend?

- Use of tables within an Azure Storage account using geo-redundant storage (GRS)
- An Azure SQL Database elastic database pool using active geo-replication
- Use of tables within an Azure Storage account using read-access geo-redundant storage (RA-GRS)
- An Azure SQL Database using active geo-replication.

*Explanation*

*Correct Answer: Tables in an Azure storage account that use GRS. Tables in GRS are automatically replicated with the paired region. REST access works well with tables and is the most economical method to store the data for this scenario.*

## Review Question 2

You are asked to recommend a solution for migrating an application data to Azure.

The scenario is as follows:

Which service do you recommend?

- SQL Managed Instance
- An Azure SQL Database
- An Azure Storage account

*Explanation*

*Correct Answer: SQL Managed Instance. SQL Managed Instance is correct because it is a fully managed solution and similar to the on-premises SQL Server product. Your customer can continue running as an instance with the features that aren't compatible with the Azure SQL Database single database model.*

## Review Question 3

You are designing a solution for an organization with the following requirements.

Which service do you recommend?

- Azure Storage
- Azure Backup
- Azure SQL Database
- Azure Storage Service Encryption (SSE)

*Explanation*

*Correct Answer: Azure Storage. The raw Azure Application Insights data points are kept for up to 730 days. If you need to keep data longer than 730 days, you can use Continuous Export to copy it to a storage account during data ingestion.*

**Review Question 4**

You are asked to design a message application can be run on a Linux VM.

The app runs on Azure Storage queues.

You are asked to recommend a solution for the app to interact with the storage queues.

The requirements are as below:

- A. AzCopy
- B. Azure Data Lake
- C. .NET Core

*Explanation*

Correct answer: C. .NET Core. .NET Core is an open-source, general-purpose development platform. You can create .NET Core apps for Windows, macOS, and Linux for x64, x86, ARM32, and ARM64 processors using multiple programming languages.

## Module 7 Select an Appropriate Storage Account

### Choose Between Storage Tiers

#### Design for Azure Blob Storage Access Tiers

As mentioned earlier in this course, Azure storage offers different access tiers, which allow you to store blob object data in the most cost-effective manner. The available access tiers include:

- **Hot** - Optimized for storing data that is accessed frequently.
- **Cool** - Optimized for storing data that is infrequently accessed and stored for at least 30 days.
- **Archive** - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

The following considerations apply to the access tiers:

- Only the hot and cool access tiers can be set at the account level. The archive access tier isn't available at the account level.
- Hot, cool, and archive tiers can be set at the blob level during upload or after upload.
- Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.
- Archive storage stores data offline and offers the lowest storage costs but also the highest data rehydrate and access costs.

To manage costs for your expanding storage needs, it's helpful to organize your data based on attributes like frequency-of-access and planned retention period to optimize costs.

- Some data is actively accessed and modified throughout its lifetime.
- Some data is accessed frequently early in its lifetime, with access dropping drastically as the data ages.

- Some data remains idle in the cloud and is rarely, if ever, accessed after it's stored.

Each of these data access scenarios benefits from a different access tier that is optimized for an access pattern.

## Support Tiering for Storage Accounts

Object storage data tiering between hot, cool, and archive is only supported in Blob storage and General Purpose v2 (GPv2) accounts. General Purpose v1 (GPv1) accounts don't support tiering. You can convert their existing GPv1 or Blob storage accounts to GPv2 accounts using the Azure portal. GPv2 provides new pricing and features for blobs, files, and queues. Some features and prices cuts are only offered in GPv2 accounts.

Blob storage and GPv2 accounts expose the **Access Tier** attribute at the account level. This attribute allows you to specify the default access tier for any blob that doesn't have it explicit set at the object level. For objects with the tier set at the object level, the account tier won't apply. The archive tier can be applied only at the object level. You can switch between these access tiers at any time.

### Hot access tier

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs.

Example usage scenarios for the hot access tier include:

- Data that's in active use or expected to be accessed (read from and written to) frequently.
- Data that's staged for processing and eventual migration to the cool access tier.

### Cool access tier

The cool access tier has lower storage costs and higher access costs compared to hot storage. This tier is intended for data that will remain in the cool tier for at least 30 days. Example usage scenarios for the cool access tier include:

- Short-term backup and disaster recovery datasets.
- Older media content not viewed frequently anymore but is expected to be available immediately when accessed.
- Large data sets that need to be stored cost effectively while more data is being gathered for future processing. (For example, long-term storage of scientific data, raw telemetry data from a manufacturing facility)

### Archive access tier

The archive access tier has the lowest storage cost. But it has higher data retrieval costs compared to the hot and cool tiers. Data in the archive tier can take several hours to retrieve. Data must remain in the archive tier for at least 180 days or be subject to an early deletion charge.

While a blob is in archive storage, the blob data is offline and can't be read, overwritten, or modified. To read or download a blob in archive, you must first rehydrate it to an online tier. You can't take snapshots of a blob in archive storage. However, the blob metadata remains online and available, allowing you to list the blob and its properties.

Example usage scenarios for the archive access tier include:

- Long-term backup, secondary backup, and archival datasets

- Original (raw) data that must be preserved, even after it has been processed into final usable form.
- Compliance and archival data that needs to be stored for a long time and is hardly ever accessed.

## Account-level tiering

Blobs in all three access tiers can coexist within the same account. Any blob that doesn't have an explicitly assigned tier infers the tier from the account access tier setting. If the access tier comes from the account, you see the Access Tier Inferred blob property set to "true", and the Access Tier blob property matches the account tier. In the Azure portal, the access tier inferred property is displayed with the blob access tier as Hot (inferred) or Cool (inferred).

Changing the account access tier applies to all access tier inferred objects stored in the account that don't have an explicit tier set. If you toggle the account tier from hot to cool, you'll be charged for write operations (per 10,000) for all blobs without a set tier in GPv2 accounts only. There's no charge for this change in Blob storage accounts. You'll be charged for both read operations (per 10,000) and data retrieval (per GB) if you toggle from cool to hot in Blob storage or GPv2 accounts.

## Blob-level tiering

Blob-level tiering allows you to upload data to the access tier of your choice using the *Put Blob* or *Put Block List* operations and change the tier of your data at the object level using the *Set Blob Tier* operation or **Lifecycle management** feature. You can upload data to your required access tier then easily change the blob access tier among the hot, cool, or archive tiers as usage patterns change, without having to move data between accounts. All tier change requests happen immediately and tier changes between hot and cool are instantaneous. However, rehydrating a blob from archive can take several hours.

## Common Questions - Storage Tiers

### Should I use Blob storage or GPv2 accounts if I want to tier my data?

We recommend you use GPv2 instead of Blob storage accounts for tiering. GPv2 support all the features that Blob storage accounts support plus a lot more. Pricing between Blob storage and GPv2 is almost identical, but some new features and price cuts will only be available on GPv2 accounts. GPv1 accounts don't support tiering.

Pricing structure between GPv1 and GPv2 accounts is different and customers should carefully evaluate both before deciding to use GPv2 accounts. You can easily convert an existing Blob storage or GPv1 account to GPv2 through a simple one-click process.

### Can I store objects in all three (hot, cool, and archive) access tiers in the same account?

Yes. The Access Tier attribute set at the account level is the default account tier that applies to all objects in that account without an explicit set tier. Blob-level tiering allows you to set the access tier on at the object level regardless of what the access tier setting on the account is. Blobs in any of the three access tiers (hot, cool, or archive) may exist within the same account.

### Can I change the default access tier of my Blob or GPv2 storage account?

Yes, you can change the default account tier by setting the Access tier attribute on the storage account. Changing the account tier applies to all objects stored in the account that don't have an explicit tier set (for example, Hot (inferred) or Cool (inferred)). Toggling the account tier from hot to cool incurs write operations (per 10,000) for all blobs without a set tier in GPv2 accounts only and toggling from cool to hot incurs both read operations (per 10,000) and data retrieval (per GB) charges for all blobs in Blob storage and GPv2 accounts.

**Can I set my default account access tier to archive?**

No. Only hot and cool access tiers may be set as the default account access tier. Archive can only be set at the object level. On blob upload, You specify the access tier of your choice to be hot, cool, or archive regardless of the default account tier. This functionality allows you to write data directly into the archive tier to realize cost-savings from the moment you create data in blob storage.

**Do the blobs in the cool access tier behave differently than the ones in the hot access tier?**

Blobs in the hot access tier have the same latency as blobs in GPv1, GPv2, and Blob storage accounts. Blobs in the cool access tier have a similar latency (in milliseconds) as blobs in GPv1, GPv2, and Blob storage accounts. Blobs in the archive access tier have several hours of latency in GPv1, GPv2, and Blob storage accounts.

**Are the operations among the hot, cool, and archive tiers the same?**

All operations between hot and cool are 100% consistent. All valid archive operations including GetBlobProperties, GetBlobMetadata, ListBlobs, SetBlobTier, and DeleteBlob are 100% consistent with hot and cool. Blob data can't be read or modified while in the archive tier until rehydrated; only blob metadata read operations are supported while in archive.

# Recommend Storage Management Tools

## Tools for Working with Azure Storage

Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
<b>Azure portal</b>	Web	Yes	Yes	Yes	Yes	Yes	Yes
<b>Azure Storage Explorer</b>	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
<b>Microsoft Visual Studio Cloud Explorer</b>	Windows	Yes	Yes	Yes	Yes	Yes	No

## Linux

Storage Explorer is available in the [Snap Store](#)<sup>1</sup> for most common distributions of Linux. We recommend Snap Store for this installation. The Storage Explorer snap installs all of its dependencies and updates when new versions are published to the Snap Store.

For supported distributions, see the [snapd installation page](#)<sup>2</sup>.

## Demonstration - Manage Tiered Storage using Azure Tools

In this demonstration, you'll compare the methods for configuring and managing storage tiers using Azure tools.

## Azure Tools

There are several tools available that you can use to manage Azure Storage:

- Azure portal
- Azure Storage Explorer
- Azure CLI
- Azure Powershell

<sup>1</sup> <https://snapcraft.io/storage-explorer>

<sup>2</sup> <https://snapcraft.io/docs/installing-snapd>

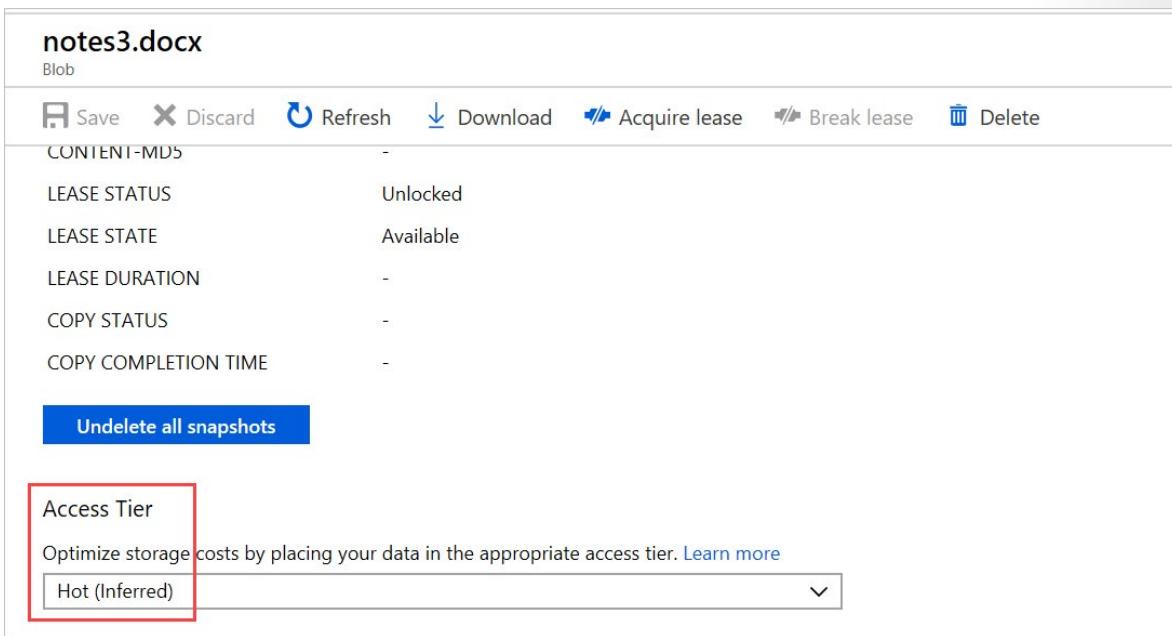
## Azure portal

Using the Azure portal, you can amend the Access Tier for the Storage Account, from Hot to Cool, or change the Replication options.

1. To manage storage tiers in the Azure portal, click **Storage Accounts**.
2. Click one of your storage accounts in the displayed list.
3. Click **Configuration**.

The screenshot shows the Azure portal configuration page for a storage account named 'rag304'. On the left, there's a sidebar with various navigation links like Overview, Activity log, and Configuration (which is currently selected). The main area displays settings for the storage account, including 'Account kind' set to 'StorageV2 (general purpose v2)', 'Performance' set to 'Standard', and 'Secure transfer required' set to 'Enabled'. The 'Access tier (default)' section is highlighted with a red box; it shows 'Hot' selected over 'Cool'. Other settings include 'Replication' set to 'Read-access geo-redundant storage (RA-GRS)', 'Large file shares' set to 'Disabled', and a note about the current combination of subscription, storage account kind, performance, and replication.

4. In the Storage Account, click **Blobs** and select a container.
5. Click your blob and scroll down to **Access Tier**.



**notes3.docx**  
Blob

Save Discard Refresh Download Acquire lease Break lease Delete

CONTENT-MD5 -

LEASE STATUS Unlocked

LEASE STATE Available

LEASE DURATION -

COPY STATUS -

COPY COMPLETION TIME -

**Undelete all snapshots**

**Access Tier**  
Optimize storage costs by placing your data in the appropriate access tier. [Learn more](#)

Hot (Inferred) ▾

6. Click the drop-down list and select the Access Tier you want to use.

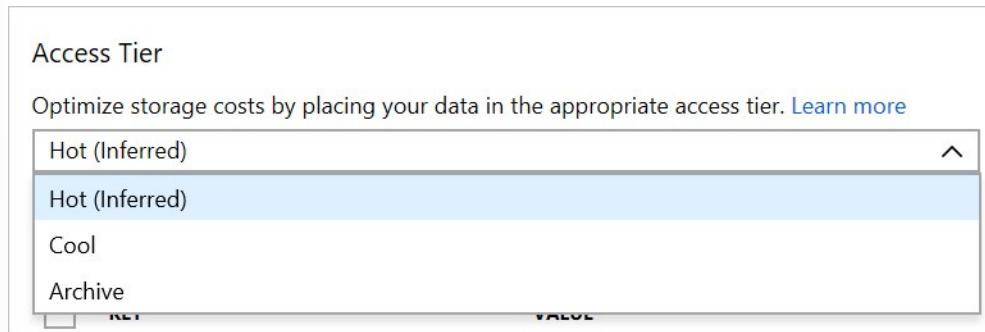
## Storage Explorer (preview)

- ◀ SUBSCRIPTIONS
  - ◀  Azure Pass - Sponsorship
  - ◀  rag304
    -  Blob containers
    - ▶  File shares
    - ▶  Queues
    - ▶  Tables

## Azure Storage Explorer

Azure Storage Explorer can be used to upload and download Blobs from Azure Storage. There are two versions of Storage Explorer, Portal Storage Explorer and standalone Storage Explorer.

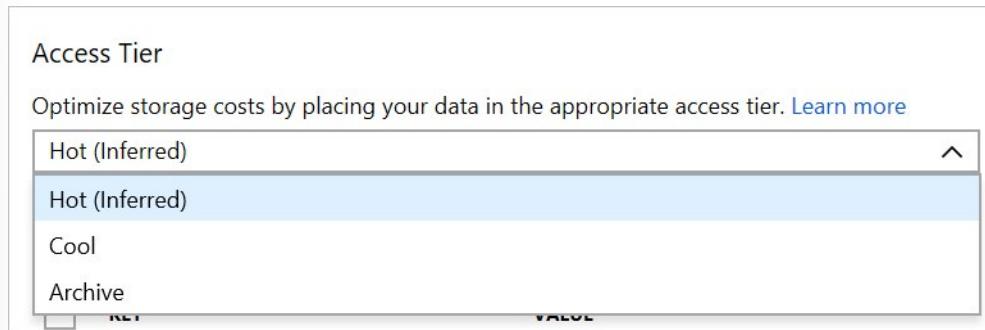
1. To use the Azure portal tool, under Storage account, click **Storage Explorer**:



2. Click **BLOB CONTAINERS** to view a list of your containers.
3. Select a container, and then select the Blob where you want to change the Access Tier.

The screenshot shows a list of blobs in a container named "test". The columns are NAME, ACCESS TIER, ACCESS TIER LAST MODIFIED, LAST MODIFIED, and BLO. A red box highlights the "ACCESS TIER" column header. A specific blob named "notes3.docx" has its "ACCESS TIER" value "Hot (inferred)" highlighted with a red box.

4. Right-click the Blob and click **Change Access Tier**.



- From the \*\*Access Tier
5. drop-down list, select the tier you want to assign to the Blob.

## Azure Powershell

You can use Powershell to manage the Access Tiers on a Storage Account and Blobs. Some of the cmdlets you can use to manage storage include:

Cmdlet	Description
Add-AzureRMAccount	Adds an authenticated account to use for Azure Resource Manager cmdlet requests.
Get-AzureStorageAccount	Gets the storage accounts for the current Azure subscription.
Set-AzureRmStorageAccount -AccessTier	Sets the Access Tier for a Storage account.

```
Set-AzureRmStorageAccount -ResourceGroupName "TestGroup" -AccountName  
"StorageAccountName" -AccessTier Cool
```

Here's another example, this time for changing Access Tier for multiple blobs in a container:

```
$Storage = "StorageAccountName"  
$Key = "StorageAccountKey"  
$Container = "BlobContainer"  
$blobs = Get-AzureStorageBlob -Container $Container  
$blob.icloudblob.setstandardblobtier("Cool")
```

## Azure CLI

You can also use Azure CLI to manage Access Tiers on Storage Accounts. Below are some of the cmdlets you can use:

```
az storage blob upload  
az storage blob list  
az storage blob download  
az storage blob set-tier
```

Example code to change Access Tier to Cool for a Blob:

```
az storage blob set-tier --name BlobName --container-name BlobContainer  
--account-name StorageAccountName --tier Cool
```

## Module 7 Review Questions

### Module 7 Review Questions



#### Review Question 1

You are recommending a solution for an auto parts wholesaler who is in the process of migrating to a new warehouse management system.

The warehouse managers must keep file-based database backups for five years to meet OEM agreement standards.

Given past experiences, using backups is not often necessary.

Where would you advise the wholesaler to store their backups?

- Azure Blob storage using the Cool tier
- Azure Blob storage using the Archive tier
- Azure Data Factory
- Azure Blob storage using the Hot access tier

#### Review Question 2

The same auto parts wholesaler has setup an Azure Storage account that contains two 4-GB data files named Partslist1 and Partslist2.

The data files have been set to use the Archive access tier.

You are asked to make sure that the Partslist2 data file is immediately accessible when a retrieval request has begun.

You recommend that the Partslist2 data file be set to Access tier Hot so that access is without delay.

Does this recommendation fulfill the requirements?

- Yes
- No

#### Review Question 3

The same auto parts wholesaler has setup an Azure Storage account that contains two 2-GB data files named OEMlist1 and OEMlist2.

The data files have been set to use the Archive access tier.

You are asked to make sure that the OEMlist1 data file is immediately accessible when a retrieval request has begun.

You recommend adding a new file share to the Azure Storage account.

Does this recommendation fulfill the requirements?

- Yes
- No

## Review Question 4

You are asked to make a recommendation for storing data in Blob storage for an auto parts distributor. The data will be stored in a cool access tier or an archive access tier depending on the access pattern of the data.

You are given the following data categories and their frequency of access.

- Part distribution barcodes: Deleted after 3 years
- Return location: Deleted after 220 days
- Refund transaction number: Deleted after 14 days

You recommend using the archive access tier to store the files listed above.

Which of the following below supports the recommendation?

- A. Access to data is guaranteed within 15 minutes
- B. Storage costs will be based on a minimum of 200 days
- C. Storage costs will be based on a minimum of 30 days

# Answers

## Review Question 1

You are recommending a solution for an auto parts wholesaler who is in the process of migrating to a new warehouse management system.

The warehouse managers must keep file-based database backups for five years to meet OEM agreement standards.

Given past experiences, using backups is not often necessary.

Where would you advise the wholesaler to store their backups?

- Azure Blob storage using the Cool tier
- Azure Blob storage using the Archive tier
- Azure Data Factory
- Azure Blob storage using the Hot access tier

*Explanation*

*Correct Answer: Azure Blob storage using the Archive tier. The Archive access tier makes it easy to copy a file into a blob container and reduces costs due to it being in the Archive tier.*

## Review Question 2

The same auto parts wholesaler has setup an Azure Storage account that contains two 4-GB data files named Partslist1 and Partslist2.

The data files have been set to use the Archive access tier.

You are asked to make sure that the Partslist2 data file is immediately accessible when a retrieval request has begun.

You recommend that the Partslist2 data file be set to Access tier Hot so that access is without delay.

Does this recommendation fulfill the requirements?

- Yes
- No

*Explanation*

*Correct Answer: Yes, the data file is set to Access tier Hot. Changing the access tier of a blob from Archive to Hot allows for immediate access for retrieval.*

## Review Question 3

The same auto parts wholesaler has setup an Azure Storage account that contains two 2-GB data files named OEMlist1 and OEMlist2.

The data files have been set to use the Archive access tier.

You are asked to make sure that the OEMlist1 data file is immediately accessible when a retrieval request has begun.

You recommend adding a new file share to the Azure Storage account.

Does this recommendation fulfill the requirements?

- Yes
- No

*Explanation*

*Correct Answer: No, a new file share to the Azure Storage account has no effect on whether the OEMlist1 data file will be immediately accessible once a retrieval request has begun.*

**Review Question 4**

You are asked to make a recommendation for storing data in Blob storage for an auto parts distributor. The data will be stored in a cool access tier or an archive access tier depending on the access pattern of the data.

You are given the following data categories and their frequency of access.

You recommend using the archive access tier to store the files listed above.

Which of the following below supports the recommendation?

- A. Access to data is guaranteed within 15 minutes
- B. Storage costs will be based on a minimum of 200 days
- C. Storage costs will be based on a minimum of 30 days

*Explanation*

*Correct answer: C. Data in the archive tier can take several hours to retrieve. Data must remain in the archive tier for at least 180 days or be subject to an early deletion charge.*



## Module 8 Design Data Integration

### Azure Data Platform End-to-End

### Azure Data Platform End-To-End



The scenario below demonstrates how to use the extensive family of Azure Data Services to build a modern data platform capable of handling the most common data challenges in an organization.

The solution described in this lesson combines a range of Azure services that will ingest, process, store, serve, and visualize data from different sources, both structured and unstructured.

This solution architecture demonstrates how a single, unified data platform can be used to meet the most common requirements for:

- Traditional relational data pipelines
- Big data transformations
- Unstructured data ingestion and enrichment with AI-based functions
- Stream ingestion and processing following the Lambda architecture
- Serving insights for data-driven applications and rich data visualization

Topics covered in this lesson include the following:

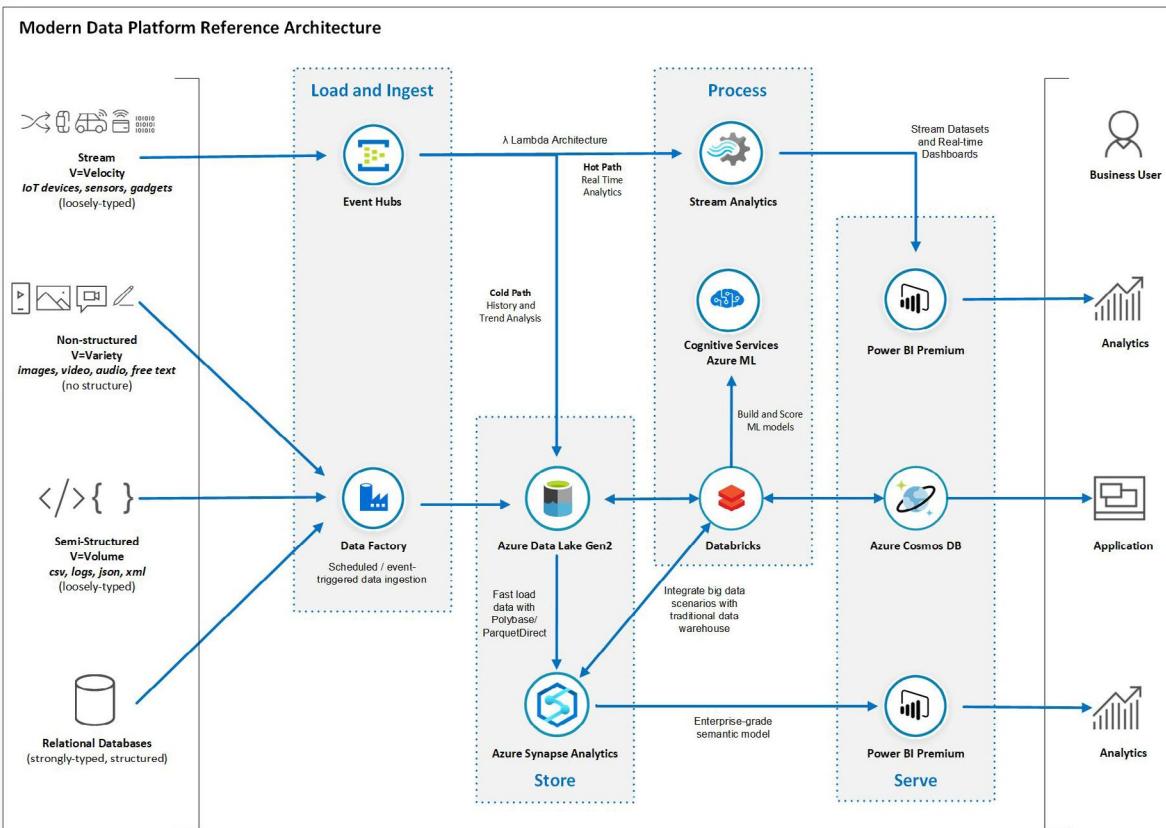
- Use Cases
- Architecture
- Architecture Components

# Architecture

## Use Cases (Reference Architecture)

This approach can also be used to:

- Establish an enterprise-wide data hub consisting of a data warehouse for structured data and a data lake for semi-structured and unstructured data. This data hub becomes the single source of truth for your data.
- Integrate relational data sources with other unstructured datasets with the use of big data processing technologies;
- Use semantic modeling and powerful visualization tools for simpler data analysis.



### ✓ Note

The services covered by this architecture are only a subset of a much larger family of Azure services. Similar outcomes can be achieved by using other services or features not covered by this design.

The data flows through the solution as follows (from bottom-up):

## Relational databases

- Use Azure Data Factory pipelines to pull data from a wide variety of databases, both on-premises and in the cloud. Pipelines can be triggered based on a pre-defined schedule, in response to an event or be explicitly called via REST APIs.

2. Still part of the Azure Data Factory pipeline, use Azure Data Lake Store Gen 2 to stage the data copied from the relational databases. You can save the data in delimited text format or compressed as Parquet files.
3. Use Azure Synapse PolyBase capabilities for fast ingestion into your data warehouse tables.
4. Load relevant data from the Azure Synapse data warehouse into Power BI datasets for data visualization. Power BI models implement a semantic model to simplify the analysis of business data and relationships.
5. Business analysts use Power BI reports and dashboards to analyze data and derive business insights.

## Semi-structured data sources

1. Use Azure Data Factory pipelines to pull data from a wide variety of semi-structured data sources, both on-premises and in the cloud. For example, you can ingest data from file-based locations containing CSV or JSON files. You can connect to No-SQL databases such as Cosmos DB or MongoDB.
2. Still part of the Azure Data Factory pipeline, use Azure Data Lake Store Gen 2 to save the original data copied from the semi-structured data source.
3. Azure Data Factory Mapping Data Flows or Azure Databricks notebooks can now be used to process the semi-structured data and apply the necessary transformations before data can be used for reporting. You can save the resulting dataset as Parquet files in the data lake.
4. Use Azure Synapse PolyBase capabilities for fast ingestion into your data warehouse tables.
5. Load relevant data from the Azure Synapse data warehouse into Power BI datasets for data visualization. Power BI models implement a semantic model to simplify the analysis of business data and relationships.
6. Business analysts use Power BI reports and dashboards to analyze data and derive business insights.

## Non-structured data sources

1. Use Azure Data Factory pipelines to pull data from a wide variety of unstructured data sources, both on-premises and in the cloud. For example, you can ingest video, image or free text log data from file-based locations. You can also call REST APIs provided by SaaS applications that will function as your data source for the pipeline.
2. Still part of the Azure Data Factory pipeline, use Azure Data Lake Store Gen 2 to save the original data copied from the unstructured data source.
3. You can invoke Azure Databricks notebooks from your pipeline to process the unstructured data. The notebook can make use of Cognitive Services APIs or invoke custom Azure Machine Learning Service models to generate insights from the unstructured data. You can save the resulting dataset as Parquet files in the data lake.
4. Use Azure Synapse PolyBase capabilities for fast ingestion into your data warehouse tables.
5. Load relevant data from the Azure Synapse data warehouse into Power BI datasets for data visualization. Power BI models implement a semantic model to simplify the analysis of business data and relationships.
6. Business analysts use Power BI reports and dashboards to analyze data and derive business insights.

## Streaming

1. Use Azure Event Hubs to ingest data streams generated by a client application. The Event Hub will then ingest and store streaming data preserving the sequence of events received. Consumers can then connect to Event Hub and retrieve the messages for processing.
2. Configure the Event Hub Capture to save a copy of the events in your data lake. This feature implements the “Cold Path” of the Lambda architecture pattern and allows you to perform historical and trend analysis on the stream data saved in your data lake using tools such as Azure Databricks notebooks.
3. Use a Stream Analytics job to implement the “Hot Path” of the Lambda architecture pattern and derive insights from the stream data in transit. Define at least one input for the data stream coming from your Event Hub, one query to process the input data stream and one Power BI output to where the query results will be sent to.
4. Business analysts then use Power BI real-time datasets and dashboard capabilities for to visualize the fast changing insights generated by your Stream Analytics query.

## Architecture Components

The following Azure services have been used in the architecture:

- Azure Data Factory
- Azure Data Lake Gen2
- Azure Synapse Analytics
- Azure Databricks
- Azure Cosmos DB
- Azure Cognitive Services
- Azure Event Hubs
- Azure Stream Analytics
- Microsoft Power BI

If you need further training resources or access to technical documentation, the table below links to Microsoft Learn and to each service's Technical Documentation.

Azure Service	Microsoft Learn	Technical Documentation
Azure Data Factory	<b>Data ingestion with Azure Data Factory</b> ( <a href="https://docs.microsoft.com/en-us/learn/modules/data-ingestion-with-azure-data-factory">https://docs.microsoft.com/en-us/learn/modules/data-ingestion-with-azure-data-factory</a> )	<b>Azure Data Factory Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/data-factory">https://docs.microsoft.com/en-us/azure/data-factory</a> )
Azure Synapse Analytics	<b>Implement a Data Warehouse with Azure Synapse Analytics</b> ( <a href="https://docs.microsoft.com/en-us/learn/paths/implement-sql-data-warehouse">https://docs.microsoft.com/en-us/learn/paths/implement-sql-data-warehouse</a> )	<b>Azure Synapse Analytics Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/sql-data-warehouse">https://docs.microsoft.com/en-us/azure/sql-data-warehouse</a> )

Azure Service	Microsoft Learn	Technical Documentation
Azure Data Lake Storage Gen2	<b>Large Scale Data Processing with Azure Data Lake Storage Gen2</b> ( <a href="https://docs.microsoft.com/en-us/learn/paths/data-processing-with-azure-adls">https://docs.microsoft.com/en-us/learn/paths/data-processing-with-azure-adls</a> )	<b>Azure Data Lake Storage Gen2 Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction">https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction</a> )
Azure Cognitive Services	<b>Cognitive Services Learning Paths and Modules</b> ( <a href="https://docs.microsoft.com/en-us/learn/browse/?term=cognitive">https://docs.microsoft.com/en-us/learn/browse/?term=cognitive</a> )	<b>Azure Cognitive Services Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/cognitive-services">https://docs.microsoft.com/en-us/azure/cognitive-services</a> )
Azure Cosmos DB	<b>Work with NoSQL data in Azure Cosmos DB</b> ( <a href="https://docs.microsoft.com/en-us/learn/paths/work-with-nosql-data-in-azure-cosmos-db">https://docs.microsoft.com/en-us/learn/paths/work-with-nosql-data-in-azure-cosmos-db</a> )	<b>Azure Cosmos DB Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/cosmos-db">https://docs.microsoft.com/en-us/azure/cosmos-db</a> )
Azure Databricks	<b>Perform data engineering with Azure Databricks</b> ( <a href="https://docs.microsoft.com/en-us/learn/paths/data-engineering-with-databricks">https://docs.microsoft.com/en-us/learn/paths/data-engineering-with-databricks</a> )	<b>Azure Databricks Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/azure-databricks">https://docs.microsoft.com/en-us/azure/azure-databricks</a> )
Azure Event Hubs	<b>Enable reliable messaging for Big Data applications using Azure Event Hubs</b> ( <a href="https://docs.microsoft.com/en-us/learn/modules/enable-reliable-messaging-for-big-data-apps-using-event-hubs">https://docs.microsoft.com/en-us/learn/modules/enable-reliable-messaging-for-big-data-apps-using-event-hubs</a> )	<b>Azure Event Hubs Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/event-hubs">https://docs.microsoft.com/en-us/azure/event-hubs</a> )
Azure Stream Analytics	<b>Implement a Data Streaming Solution with Azure Streaming Analytics</b> ( <a href="https://docs.microsoft.com/en-us/learn/paths/implement-data-streaming-with-asa">https://docs.microsoft.com/en-us/learn/paths/implement-data-streaming-with-asa</a> )	<b>Azure Stream Analytics Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/azure/stream-analytics">https://docs.microsoft.com/en-us/azure/stream-analytics</a> )
Power BI	<b>Create and use analytics reports with Power BI</b> ( <a href="https://docs.microsoft.com/en-us/learn/paths/create-use-analytics-reports-power-bi">https://docs.microsoft.com/en-us/learn/paths/create-use-analytics-reports-power-bi</a> )	<b>Power BI Technical Documentation</b> ( <a href="https://docs.microsoft.com/en-us/power-bi">https://docs.microsoft.com/en-us/power-bi</a> )

# Recommend a Solution for Data Integration

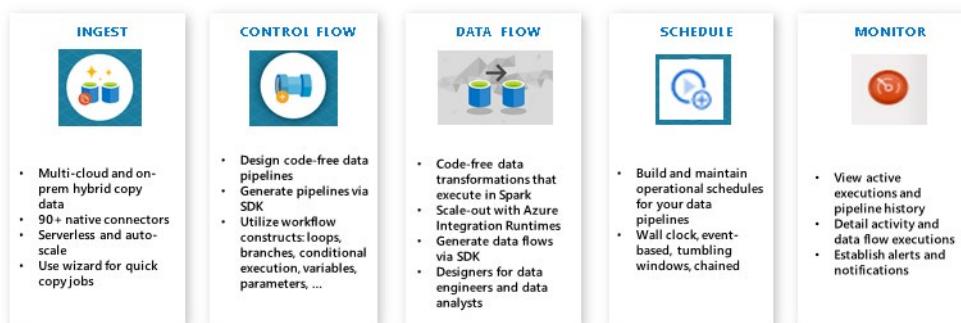
## Data Flows using Azure Data Factory

Azure Data Factory is a managed cloud service that's built for these complex hybrid extract-transform-load (ETL), extract-load-transform (ELT), and data integration projects.

Azure Data Factory is a cloud-based ETL and data integration service that allows you to create data-driven workflows for orchestrating data movement and transforming data at scale. Using Azure Data Factory, you can create and schedule data-driven workflows (called pipelines) that can ingest data from disparate data stores. You can build complex ETL processes that transform data visually with data flows or by using compute services such as Azure HDInsight Hadoop, Azure Databricks, and Azure SQL Database.

Also, you can publish your transformed data to data stores such as Azure SQL Data Warehouse for business intelligence (BI) applications to consume. Ultimately, through Azure Data Factory, raw data can be organized into meaningful data stores and data lakes for better business decisions.

### Code-Free ETL As a Service



## How Data Factory Works



Data Factory contains a series of interconnected systems that provide a complete end-to-end platform for data engineers.

## Connect and collect

The first step in building an information production system is to connect to all the required sources of data and processing, such as software-as-a-service (SaaS) services, databases, file shares, and FTP web services. The next step is to move the data as needed to a centralized location for subsequent processing.

With Data Factory, you can use the **Copy Activity** in a data pipeline to move data from both on-premises and cloud source data stores to a centralization data store in the cloud for further analysis. For example, you can collect data in Azure Data Lake Storage and transform the data later by using an Azure Data Lake Analytics compute service. You can also collect data in Azure Blob storage and transform it later by using an Azure HDInsight Hadoop cluster.

## Transform and enrich

After data is present in a centralized data store in the cloud, process or transform the collected data by using ADF mapping data flows. Data flows enable data engineers to build and maintain data transformation graphs that execute on Spark without needing to understand Spark clusters or Spark programming.

If you prefer to code transformations by hand, ADF supports external activities for executing your transformations on compute services such as HDInsight Hadoop, Spark, Data Lake Analytics, and Machine Learning.

## CI/CD and publish

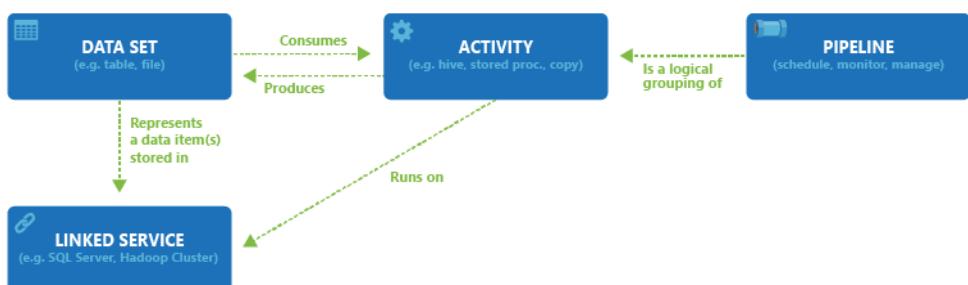
Data Factory offers full support for CI/CD of your data pipelines using Azure DevOps and GitHub. This allows you to incrementally develop and deliver your ETL processes before publishing the finished product. After the raw data has been refined into a business-ready consumable form, load the data into Azure Data Warehouse, Azure SQL Database, Azure CosmosDB, or whichever analytics engine your business users can point to from their business intelligence tools.

## Monitor

After you have successfully built and deployed your data integration pipeline, providing business value from refined data, monitor the scheduled activities and pipelines for success and failure rates. Azure Data Factory has built-in support for pipeline monitoring via Azure Monitor, API, PowerShell, Azure Monitor logs, and health panels on the Azure portal.

# Data Factory Key Concepts

An Azure subscription might have one or more Azure Data Factory instances (or data factories). Azure Data Factory is composed of four key components. These components work together to provide the platform on which you can compose data-driven workflows with steps to move and transform data.



## Pipeline

A data factory might have one or more pipelines. A pipeline is a logical grouping of activities that performs a unit of work. Together, the activities in a pipeline perform a task. For example, a pipeline can

contain a group of activities that ingests data from an Azure blob, and then runs a Hive query on an HDInsight cluster to partition the data.

The benefit of this is that the pipeline allows you to manage the activities as a set instead of managing each one individually. The activities in a pipeline can be chained together to operate sequentially, or they can operate independently in parallel.

## Mapping data flows

Create and manage graphs of data transformation logic that you can use to transform any-sized data. You can build-up a reusable library of data transformation routines and execute those processes in a scaled-out manner from your ADF pipelines. Data Factory will execute your logic on a Spark cluster that spins-up and spins-down when you need it. You won't ever have to manage or maintain clusters.

## Activity

Activities represent a processing step in a pipeline. For example, you might use a copy activity to copy data from one data store to another data store. Similarly, you might use a Hive activity, which runs a Hive query on an Azure HDInsight cluster, to transform or analyze your data. Data Factory supports three types of activities: data movement activities, data transformation activities, and control activities.

## Datasets

Datasets represent data structures within the data stores, which simply point to or reference the data you want to use in your activities as inputs or outputs.

## Linked services

Linked services are much like connection strings, which define the connection information that's needed for Data Factory to connect to external resources. Think of it this way: a linked service defines the connection to the data source, and a dataset represents the structure of the data. For example, an Azure Storage-linked service specifies a connection string to connect to the Azure Storage account. Additionally, an Azure blob dataset specifies the blob container and the folder that contains the data.

Linked services are used for two purposes in Data Factory:

- To represent a **data store** that includes, but isn't limited to, an on-premises SQL Server database, Oracle database, file share, or Azure blob storage account.
- To represent a **compute resource** that can host the execution of an activity. For example, the HDInsightHive activity runs on an HDInsight Hadoop cluster.

## Triggers

Triggers represent the unit of processing that determines when a pipeline execution needs to be kicked off. There are different types of triggers for different types of events.

## Pipeline runs

A pipeline run is an instance of the pipeline execution. Pipeline runs are typically instantiated by passing the arguments to the parameters that are defined in pipelines. The arguments can be passed manually or within the trigger definition.

## Parameters

Parameters are key-value pairs of read-only configuration. Parameters are defined in the pipeline. The arguments for the defined parameters are passed during execution from the run context that was created by a trigger or a pipeline that was executed manually. Activities within the pipeline consume the parameter values.

A dataset is a strongly typed parameter and a reusable/referenceable entity. An activity can reference datasets and can consume the properties that are defined in the dataset definition.

A linked service is also a strongly typed parameter that contains the connection information to either a data store or a compute environment. It is also a reusable/referenceable entity.

## Control flow

Control flow is an orchestration of pipeline activities that includes chaining activities in a sequence, branching, defining parameters at the pipeline level, and passing arguments while invoking the pipeline on-demand or from a trigger. It also includes custom-state passing and looping containers, that is, For-each iterators.

## Variables

Variables can be used inside of pipelines to store temporary values and can also be used in conjunction with parameters to enable passing values between pipelines, data flows, and other activities.

# Integrate Data Factory and Databricks

You can use Azure Data Factory to ingest raw data collected from different sources and work with Azure Databricks to restructure the data to meet your requirements.

As mentioned in a previous topic, Data Factory supports data workflow pipelines. These pipelines are a logical group of tasks and activities that allows end-to-end data-processing scenarios.

When you integrate Databricks with Data Factory, you can take advantage of the analytical and data-transformation capabilities of Databricks. Use a Databricks notebook within your data workflow pipeline to structure and transform raw data that's loaded into Data Factory from different sources. After the data is transformed by using Databricks, load it to any data warehouse.

Data ingestion and transformation by using the collective capabilities of Data Factory and Databricks involves the following steps:

1. **Create an Azure storage account.** You'll use this storage account to store your ingested and transformed data.
2. **Create a Data Factory instance.** After you set up your storage account, create your Data Factory instance by using the Azure portal.
3. **Create a data workflow pipeline.** To create the pipeline, copy data from your source by using a copy activity in Data Factory. A copy activity allows you to copy data from different on-premises and cloud sources.
4. **Add a Databricks notebook to the pipeline.** This notebook contains the code to transform and clean the raw data as required.
5. **Analyze the data.** Now that your data is cleaned up, use Databricks notebooks to further train the data or analyze it to output the required results.

You've learned how integrating Data Factory with Databricks helps you to load and transform your data. Now let's create an end-to-end sample data workflow.

# Recommend a Solution for Data Warehousing and Big Data Analytics Integration

## Azure Synapse Analytics

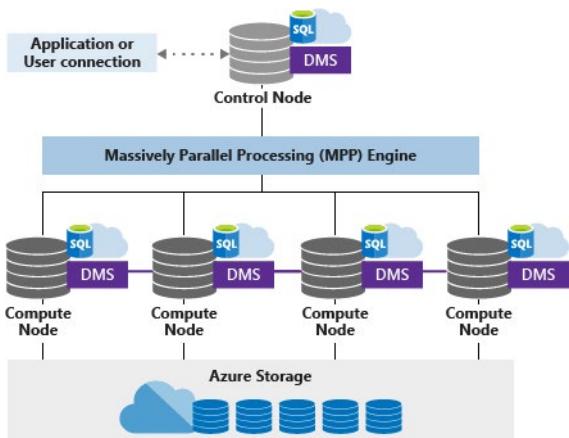
Azure Synapse is an analytics service that brings together enterprise data warehousing and Big Data analytics. It gives you the freedom to query data on your terms, using either serverless on-demand or provisioned resources. Azure Synapse brings these two worlds together with a unified experience to ingest, prepare, manage, and serve data for immediate BI and machine learning needs.

Azure Synapse has four components:

- Synapse SQL
- Spark
- Synapse Pipelines
- Studio

### Key component of a big data solution

Data warehousing is a key component of a cloud-based, end-to-end big data solution.



In a cloud data solution, data is ingested into big data stores from a variety of sources. Once in a big data store, Hadoop, Spark, and machine learning algorithms prepare and train the data. When the data is ready for complex analysis, Synapse SQL pool uses PolyBase to query the big data stores. PolyBase uses standard T-SQL queries to bring the data into Synapse SQL pool tables.

Synapse SQL pool stores data in relational tables with columnar storage. This format significantly reduces the data storage costs, and improves query performance. Once data is stored, you can run analytics at massive scale. Compared to traditional database systems, analysis queries finish in seconds instead of minutes, or hours instead of days.

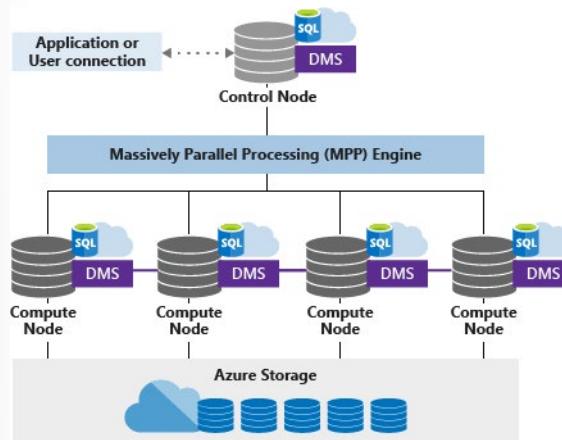
The analysis results can go to worldwide reporting databases or applications. Business analysts can then gain insights to make well-informed business decisions.

# Azure Synapse Analytics Architecture

Azure Synapse is a analytics service that brings together enterprise data warehousing and Big Data analytics. You can query data using either serverless on-demand or provisioned resources—at scale.

## Synapse SQL MPP architecture components

Synapse SQL leverages a scale-out architecture to distribute computational processing of data across multiple nodes. The unit of scale is an abstraction of compute power that is known as a data warehouse unit. Compute is separate from storage, which enables you to scale compute independently of the data in your system.



Synapse SQL uses a node-based architecture. Applications connect and issue T-SQL commands to a Control node, which is the single point of entry for Synapse SQL. The Control node runs the MPP engine, which optimizes queries for parallel processing, and then passes operations to Compute nodes to do their work in parallel.

The Compute nodes store all user data in Azure Storage and run the parallel queries. The Data Movement Service (DMS) is a system-level internal service that moves data across the nodes as necessary to run queries in parallel and return accurate results.

With decoupled storage and compute, when using Synapse SQL pool you can:

- Independently size compute power irrespective of your storage needs.
- Grow or shrink compute power, within a SQL pool (data warehouse), without moving data.
- Pause compute capacity while leaving data intact, so you only pay for storage.
- Resume compute capacity during operational hours.

## Azure Storage

Synapse SQL leverages Azure Storage to keep your user data safe. Since your data is stored and managed by Azure Storage, there is a separate charge for your storage consumption. The data is sharded into distributions to optimize the performance of the system. You can choose which sharding pattern to use to distribute the data when you define the table. These sharding patterns are supported:

- Hash
- Round Robin

- Replicate

## Control node

The Control node is the brain of the architecture. It is the front end that interacts with all applications and connections. The MPP engine runs on the Control node to optimize and coordinate parallel queries. When you submit a T-SQL query, the Control node transforms it into queries that run against each distribution in parallel.

## Compute nodes

The Compute nodes provide the computational power. Distributions map to Compute nodes for processing. As you pay for more compute resources, distributions are remapped to available Compute nodes. The number of compute nodes ranges from 1 to 60, and is determined by the service level for Synapse SQL.

Each Compute node has a node ID that is visible in system views. You can see the Compute node ID by looking for the node\_id column in system views whose names begin with sys.pdw\_nodes.

## Data Movement Service

Data Movement Service (DMS) is the data transport technology that coordinates data movement between the Compute nodes. Some queries require data movement to ensure the parallel queries return accurate results. When data movement is required, DMS ensures the right data gets to the right location.

## Distributions

A distribution is the basic unit of storage and processing for parallel queries that run on distributed data. When Synapse SQL runs a query, the work is divided into 60 smaller queries that run in parallel.

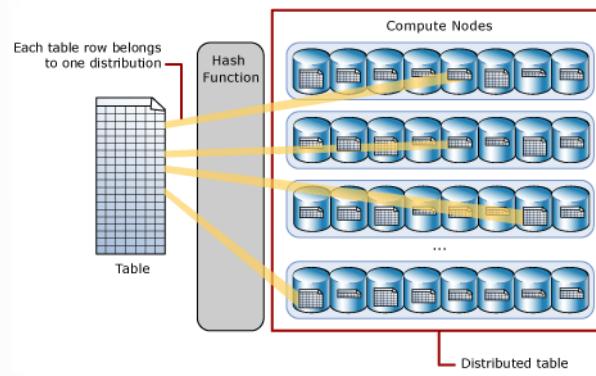
Each of the 60 smaller queries runs on one of the data distributions. Each Compute node manages one or more of the 60 distributions. A SQL pool with maximum compute resources has one distribution per Compute node. A SQL pool with minimum compute resources has all the distributions on one compute node.

## Hash-Distributed Tables

A hash distributed table can deliver the highest query performance for joins and aggregations on large tables.

To shard data into a hash-distributed table, a hash function is used to deterministically assign each row to one distribution. In the table definition, one of the columns is designated as the distribution column. The hash function uses the values in the distribution column to assign each row to a distribution.

The following diagram illustrates how a full (non-distributed table) gets stored as a hash-distributed table.



- Each row belongs to one distribution.
- A deterministic hash algorithm assigns each row to one distribution.
- The number of table rows per distribution varies as shown by the different sizes of tables.

There are performance considerations for the selection of a distribution column, such as distinctness, data skew, and the types of queries that run on the system.

## Round-Robin Distributed Tables

A round-robin table is the simplest table to create and delivers fast performance when used as a staging table for loads.

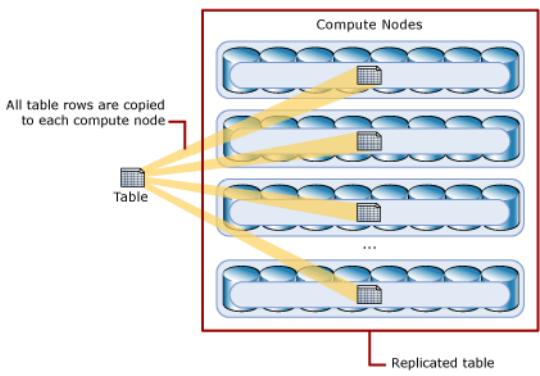
A round-robin distributed table distributes data evenly across the table but without any further optimization. A distribution is first chosen at random and then buffers of rows are assigned to distributions sequentially. It is quick to load data into a round-robin table, but query performance can often be better with hash distributed tables. Joins on round-robin tables require reshuffling data, which takes additional time.

## Replicated Tables

A replicated table provides the fastest query performance for small tables.

A table that is replicated caches a full copy of the table on each compute node. Consequently, replicating a table removes the need to transfer data among compute nodes before a join or aggregation. Replicated tables are best utilized with small tables. Extra storage is required and there is additional overhead that is incurred when writing data, which make large tables impractical.

The diagram below shows a replicated table that is cached on the first distribution on each compute node.



## Module 8 Review Questions

### Module 8 Review Questions



#### Review Question 1

You are designing a database migration solution for an organization with 80 SQL Server Integration Services (SSIS) packages that are configured to use eight on-premises SQL Server databases as targets.

Below are the specifics:

- They want to migrate 8 on-premises SQL Server databases to Azure SQL Database.
- The solution must be able to host the SSIS packages in Azure.
- The solution needs to ensure that the packages can target the SQL Database instances as destinations.

Which service do you recommend?

- Azure Migration Assistant
- Azure Backup
- Azure Data Factory
- Azure Data Catalog

#### Review Question 2

You are designing an automated process to facilitate the upload of data to an Azure SQL Database once a week.

Below are the specifics:

- Ensure that weekly reports are generated from web access logs.
- The web access logs data is stored in Azure Blob storage.

You need to recommend an automated process for uploading the data to an Azure SQL Database once a week.

Which of the options below do you recommend?

- Azure Migration Assistant
- Azure Backup
- Azure SQL Server Migration Assistant
- Azure Data Factory

## Review Question 3

You are recommending a service for an organization that has the following requirements. Ensure that

- The store data files in Azure Blob storage.
- They want to transform the files and move them to Azure Data Lake Storage.
- The solution must ensure that the data is transformed by mapping data flow.

Which of the service below do you recommend?

- Azure Databricks
- Azure Data Factory
- Azure Stack Hub
- Azure SQL Server Migration Assistant

## Review Question 4

You are advising a company that is wants to increase efficiency while reducing costs. The flow below shows the log files generated by the users to a web server.

- Log Files -> Azure Data Factory -> Azure Data Lake Storage -> Azure DataBricks -> Power BI
- The log files are consistent in format and there 500-900 MB of logs created in a day. Power BI is used to see the data.
- You are asked to recommend a solution that minimizes costs without affecting functionality.

What do you recommend?

- Replace Azure Data Lake Storage with Azure Storage
- Replace Azure DataBricks with Azure AI
- Replace Azure Data Factory with CRON jobs using AzCopy

## Review Question 5

Your organization has an Azure VM named OEM\_VM3 that runs on Windows Server 2019 and contains 1 TB of data files.

You are asked to design a solution using Azure Data Factory to transform the data files and then load them into Azure Data Lake Storage.

What should you deploy on OEM\_VM3 to support your design?

- A self-hosted integration runtime
- An Azure key vault in the same region as the storage account
- An on-premises data gateway
- An Azure runbook

# Answers

## Review Question 1

You are designing a database migration solution for an organization with 80 SQL Server Integration Services (SSIS) packages that are configured to use eight on-premises SQL Server databases as targets. Below are the specifics:

Which service do you recommend?

- Azure Migration Assistant
- Azure Backup
- Azure Data Factory
- Azure Data Catalog

*Explanation*

*Correct Answer: Azure Data Factory. Azure Data Factory allows for reusing SSIS packages through the SSIS runtime.*

## Review Question 2

You are designing an automated process to facilitate the upload of data to an Azure SQL Database once a week.

Below are the specifics:

You need to recommend an automated process for uploading the data to an Azure SQL Database once a week.

Which of the options below do you recommend?

- Azure Migration Assistant
- Azure Backup
- Azure SQL Server Migration Assistant
- Azure Data Factory

*Explanation*

*Correct Answer: Azure Data Factory. Azure Data Factory supports scheduled uploads from Azure Blob storage to Azure SQL Database.*

## Review Question 3

You are recommending a service for an organization that has the following requirements. Ensure that

Which of the service below do you recommend?

- Azure Databricks
- Azure Data Factory
- Azure Stack Hub
- Azure SQL Server Migration Assistant

*Explanation*

*Correct Answer: Azure Data Factory. Data flows are created in Azure Data Factory. You must first deploy Azure Data Factory before you can create a data flow.*

**Review Question 4**

You are advising a company that is wants to increase efficiency while reducing costs. The flow below shows the log files generated by the users to a web server.

What do you recommend?

- Replace Azure Data Lake Storage with Azure Storage
- Replace Azure DataBricks with Azure AI
- Replace Azure Data Factory with CRON jobs using AzCopy

*Explanation*

*Correct Answer: Replace Azure Data Factory with CRON jobs using AzCopy. Using AzCopy to move files, such as log files with consistent formats, from a web server a storage target, can significantly reduce costs.*

**Review Question 5**

Your organization has an Azure VM named OEM\_VM3 that runs on Windows Server 2019 and contains 1 TB of data files.

You are asked to design a solution using Azure Data Factory to transform the data files and then load them into Azure Data Lake Storage.

What should you deploy on OEM\_VM3 to support your design?

- A self-hosted integration runtime
- An Azure key vault in the same region as the storage account
- An on-premises data gateway
- An Azure runbook

*Explanation*

*Correct answer: A self-hosted integration runtime. A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network.*



# Module 9 Design a Solution for Logging and Monitoring

## Monitoring

### Monitoring Azure

Traditional application and infrastructure monitoring is based on whether the application is running or not, or what response time it is giving. However, cloud-based monitoring offer many more opportunities that you should be leveraging in order to give your users the best experience.

This lesson summarizes the following recommendations for:

- Application Monitoring
- Platform Monitoring
- Monitoring Best Practices

### Application Monitoring

**Application Insights** provides the following:

- Default dashboard with an *educated guess* of the most important metrics.
- By instrumenting applications, Application Insights will give performance statistics both from a client and server perspective.
- The Application Map shows application dependencies in other services such as backend APIs or databases, allowing visual determination where performance problems lie.
- Smart Detection will warn when anomalies in performance or utilization patterns happen.
- Usage Analysis can give telemetry on which features of applications are most frequently used, or whether all application functionality is being used.
- Release annotations are visual indicators in Application Insights charts of new builds and other events, so that it's possible to visually correlate changes in application performance to code releases and pinpoint performance problems.

- Cross-component transaction diagnostics allow following failed transactions to find the point in the architecture where the fault was originated.
- Snapshot Debugger, to automatically collect a snapshot of a live application in case of an exception, to analyze it at a later stage.

In order to use Application Insights you have two options: you can use **codeless monitoring**, where onboarding your app to Application Insights does not require any code change, or **code-based monitoring**, where you instrument your code to send telemetry to Application Insights using the Software Development Kit for your programming language of choice.

## Platform Monitoring

Databases, storage accounts, and data lakes should be closely monitored, since a low performance of the data tier of an application could have serious consequences.

## Container Insights

Azure Monitor monitors the state of clusters, nodes, and pods and provides visual and actionable information: CPU and memory pressure of nodes and logs for individual Kubernetes pods.

## Network monitoring

**Network Watcher** is a component of Azure Monitor that manages the network components using a collection of network monitoring and troubleshooting tools:

- **Traffic Analytics** provides an overview of the traffic in your Virtual Networks, as well as the percentage coming from malicious IP addresses, leveraging Microsoft Threat Intelligence databases.
- **Network Performance Manager** can generate synthetic traffic to measure the performance of network connections over multiple links, giving you a perspective on the evolution of WAN and Internet connections over time, as well as monitoring information about Microsoft ExpressRoute circuits.
- **VPN diagnostics troubleshoots** site-to-site VPN connections connecting applications to users on-premises.
- **Connection Monitor** measures the network availability between sets of endpoints.

## Monitoring Best Practices

### Event correlation

Create shared dashboards in order to expose relevant information to the different groups involved in operating applications, including Developers and Operators. If more complex visualizations are required, Azure Monitor data can be exported to Power BI for advanced data analysis.

### Notifications

Alerts should be used to send proactive notifications to the relevant individuals. Action groups in Azure Monitor can be used to notify multiple recipients, to trigger automated actions, or automatically open tickets in IT Service Management Tools such as **ServiceNow**.

Email shouldn't be the single notification method for critical issues. Instead, define actions to be executed upon receiving certain alerts (such as scaling up or down) for the system to be self-healing.

## Other monitoring tasks

Monitor the following events to make sure applications are running smoothly:

- Review Azure subscription limits for your resources, and make sure you are not coming too close.
- Understand Azure support plans. Refer to Azure support FAQs. Familiarize your team with Azure support.
- Make sure that you monitor expiration dates of digital certificates, or even better, configure automatic digital certificate renewal with Azure Key Vault.

## Azure Monitor

# Monitoring Azure Resources with Azure Monitor

When you have critical applications and business processes relying on Azure resources, you want to monitor those resources for their availability, performance, and operation. This lesson describes the monitoring data generated by Azure resources and how you can use the features of Azure Monitor to analyze and alert on this data.



### Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

[Explore Metr...](#)

### Query & Analyze Logs

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

[Search Logs](#)

### Setup Alert & Actions

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

[Create Alert](#)

## What is Azure Monitor?

Azure Monitor is a full stack monitoring service in Azure that provides a complete set of features to monitor your Azure resources in addition to resources in other clouds and on-premises. The Azure Monitor data platform collects data into logs and metrics where they can be analyzed together using a complete set of monitoring tools.

As soon as you create an Azure resource, Azure Monitor is enabled and starts collecting metrics and activity logs which you can view and analyze in the Azure portal. With some configuration, you can gather additional monitoring data and enable additional features.

## Costs Associated with Monitoring

There is no cost for analyzing monitoring data that is collected by default. This includes the following:

- Collecting platform metrics and analyzing them with metrics explorer.
- Collecting Activity log and analyzing it in the Azure portal.
- Creating an Activity log alert rule.

**Monitor | Usage and estimated costs**

Search (Ctrl+ /) << Help

Subscription \* ⓘ

Azure Pass - Sponsorship

The table below shows estimated monthly costs\* for monitoring features based on your current usage.

Filter subscription names, categories or types

Subscription Name	Meter Category
Azure Pass - Sponsorship	No usage data available**

**Your estimated monthly total**

\* Estimates do not include any free units which may be applicable because these are applied at the subscription level.  
\*\* No usage and cost data was found for this subscription, either because there is no monitoring usage or it is a free trial.

**Insights**

- Applications
- Virtual Machines
- Storage accounts
- Containers
- Networks (preview)
- Azure Cosmos DB
- Key Vaults (preview)
- Azure Cache for Redis (preview)
- ... More

**Settings**

- Diagnostics settings
- Autoscale
- Private Link Scopes

**Support + Troubleshooting**

- Usage and estimated costs
- Advisor recommendations

There are no Azure Monitor costs for collecting and exporting logs and metrics, but there may be related costs associated with the destination:

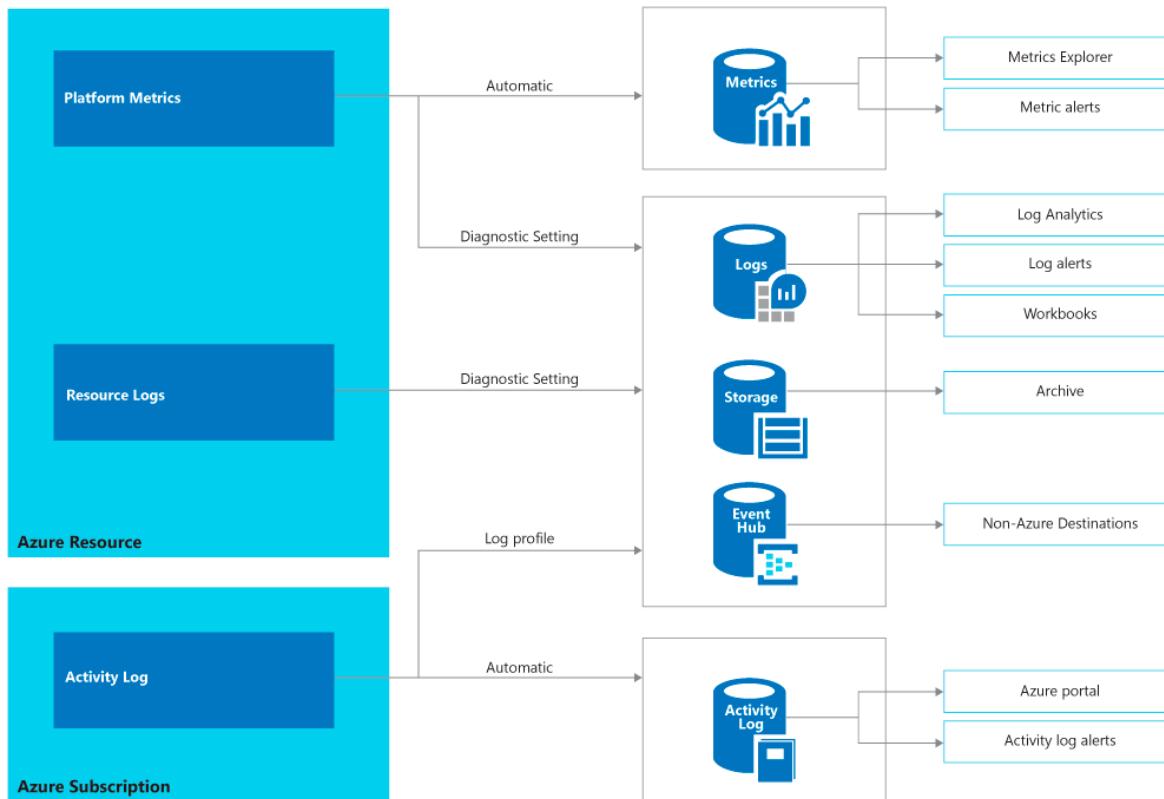
- **Costs associated with data ingestion and retention when collecting logs and metrics in Log Analytics workspace.** See [Azure Monitor pricing for Log Analytics<sup>1</sup>](https://azure.microsoft.com/pricing/details/monitor/).

<sup>1</sup> <https://azure.microsoft.com/pricing/details/monitor/>

- **Costs associated with data storage when collecting logs and metrics to an Azure storage account.** See [Azure Storage pricing for blob storage<sup>2</sup>](https://azure.microsoft.com/pricing/details/storage/blobs/).
- **Costs associated with event hub streaming when forwarding logs and metrics to Azure Event Hubs.** See [Azure Event Hubs pricing<sup>3</sup>](https://azure.microsoft.com/pricing/details/event-hubs/).

## Monitoring Data

Resources in Azure generate logs and metrics shown the following diagram. Refer to the documentation for each Azure services for the specific data they generate and any additional solutions or insights they provide.



- **Platform metrics** - Numerical values that are automatically collected at regular intervals and describe some aspect of a resource at a particular time.
- **Resource logs** - Provide insight into operations that were performed within an Azure resource (the data plane), for example getting a secret from a Key Vault or making a request to a database. The content and structure of resource logs varies by the Azure service and resource type.
- **Activity log** - Provides insight into the operations on each Azure resource in the subscription from the outside (the management plane), for example creating a new resource or starting a virtual machine. This is information about the what, who, and when for any write operations (PUT, POST, DELETE) taken on the resources in your subscription.

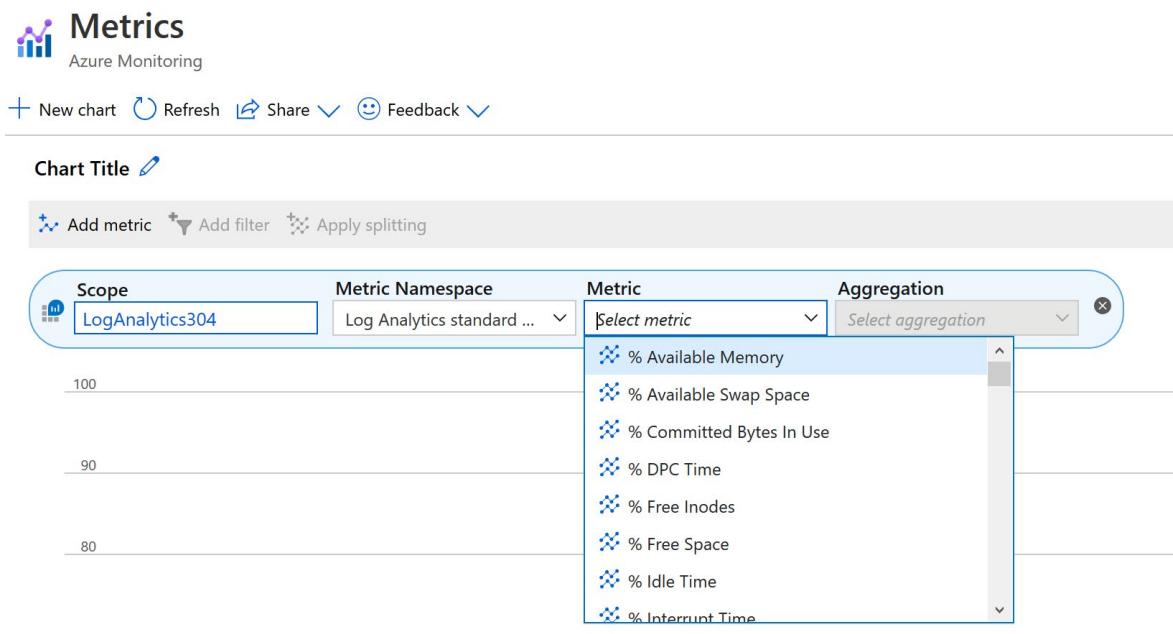
<sup>2</sup> <https://azure.microsoft.com/pricing/details/storage/blobs/>

<sup>3</sup> <https://azure.microsoft.com/pricing/details/event-hubs/>

# Configure Monitoring

Some monitoring data is collected automatically, but you may need to perform some configuration depending on your requirements. See the information below for specific information for each type of monitoring data.

- **Platform metrics** - Platform metrics are collected automatically into Azure Monitor Metrics with no configuration required. Create a diagnostic setting to send entries to Azure Monitor Logs or to forward them outside of Azure.
- **Resource logs** - Resource logs are automatically generated by Azure resources but not collected without a diagnostic setting. Create a diagnostic setting to send entries to Azure Monitor Logs or to forward them outside of Azure.
- **Activity log** - The Activity log is collected automatically with no configuration required and can be viewed in the Azure portal. Create a diagnostic setting to copy them to Azure Monitor Logs or to forward them outside of Azure.



The screenshot shows the Azure Metrics blade. At the top, there's a header with a 'Metrics' icon, the text 'Metrics', and 'Azure Monitoring'. Below the header are buttons for 'New chart', 'Refresh', 'Share', and 'Feedback'. A 'Chart Title' input field is present. Underneath, there are buttons for 'Add metric', 'Add filter', and 'Apply splitting'. The main area has three tabs: 'Scope' (set to 'LogAnalytics304'), 'Metric Namespace' (set to 'Log Analytics standard ...'), and 'Metric' (a dropdown menu). The 'Metric' dropdown is open, showing a list of metrics with checkboxes next to them. The visible metrics are: % Available Memory, % Available Swap Space, % Committed Bytes In Use, % DPC Time, % Free Inodes, % Free Space, % Idle Time, and % Interrupt Time. The 'Aggregation' dropdown is also visible next to the metric dropdown.

## Log Analytics Workspace

Collecting data into Azure Monitor Logs requires a Log Analytics workspace. You can start monitoring your service quickly by creating a new workspace, but there may be value in using a workspace that's collecting data from other services.

The screenshot shows the Azure Log Analytics workspace settings page for a workspace named 'LogAnalytics304'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (selected), Locks, Export template, Agents management, and Advanced settings. Under General, there are links for Quick Start, Workspace summary, View Designer, Workbooks, Logs, Solutions, Saved searches, Pricing tier, and Usage and estimated costs. The main content area displays basic workspace details: Resource group (change) 'az304demo', Status 'Active', Location 'Central US', Subscription (change) 'Azure Pass - Sponsorship', and Subscription ID. It also shows a section for Tags (change) with a link to 'Click here to add tags'. Below this is a 'Get started with Log Analytics' section. It includes two numbered steps: '1 Connect a data source' (Select one or more data sources to connect to the workspace, with options for Azure virtual machines (VMs), Windows, Linux and other sources, and Azure Activity logs) and '2 Configure monitoring solutions' (Add monitoring solutions that provide insights for applications and services in your environment, with a 'View solutions' link). A search bar at the top left and a delete button at the top right are also visible.

## Diagnostic Settings

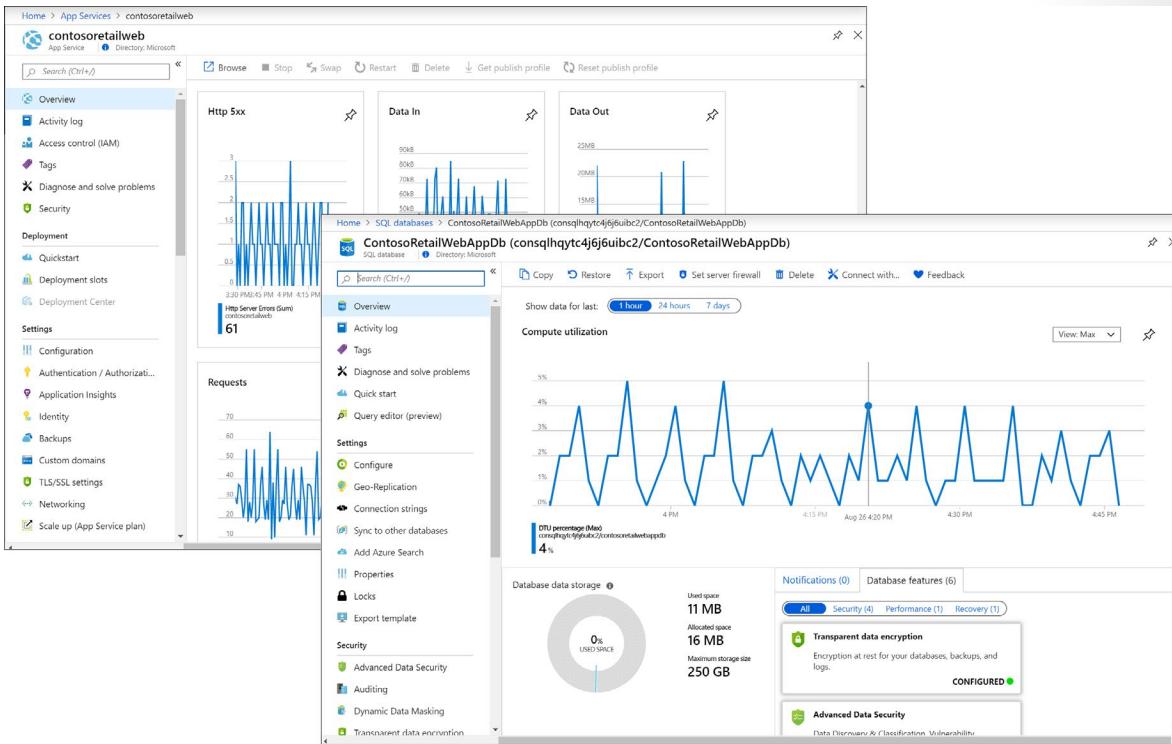
Diagnostic settings define where resource logs and metrics for a particular resource should be sent. Possible destinations are:

- **Log Analytics workspace** which allows you to analyze data with other monitoring data collected by Azure Monitor using powerful log queries and also to leverage other Azure Monitor features such as log alerts and visualizations.
- **Event hubs** to stream data to external systems such as third-party SIEMs and other log analytics solutions.
- **Azure storage account** which is useful for audit, static analysis, or backup.

## Monitoring in the Azure Portal

You can access monitoring data for most Azure resources from the resource's menu in the Azure portal. This will give you access to a single resource's data using standard Azure Monitor tools. Some Azure services will provide different options, so you should reference the documentation for that service for additional information. Use the Azure Monitor menu to analyze data from all monitored resources.

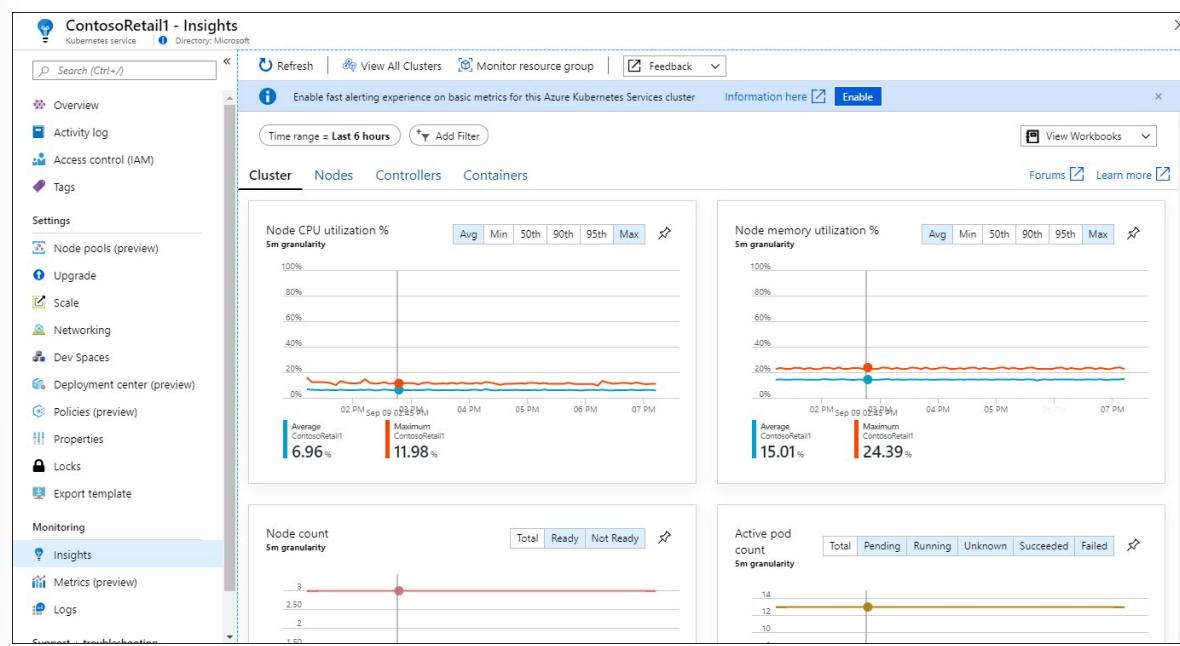
Many services will include monitoring data on their Overview page as a quick glance to their operation. This will typically be based on a subset of platform metrics stored in Azure Monitor Metrics. Other monitoring options will typically be available in a Monitoring section of the services.



## Insights and Solutions

Some services will provide tools beyond the standard features of Azure Monitor. Insights provide a customized monitoring experience built on the Azure Monitor data platform and standard features. Solutions provide predefined monitoring logic built on Azure Monitor Logs.

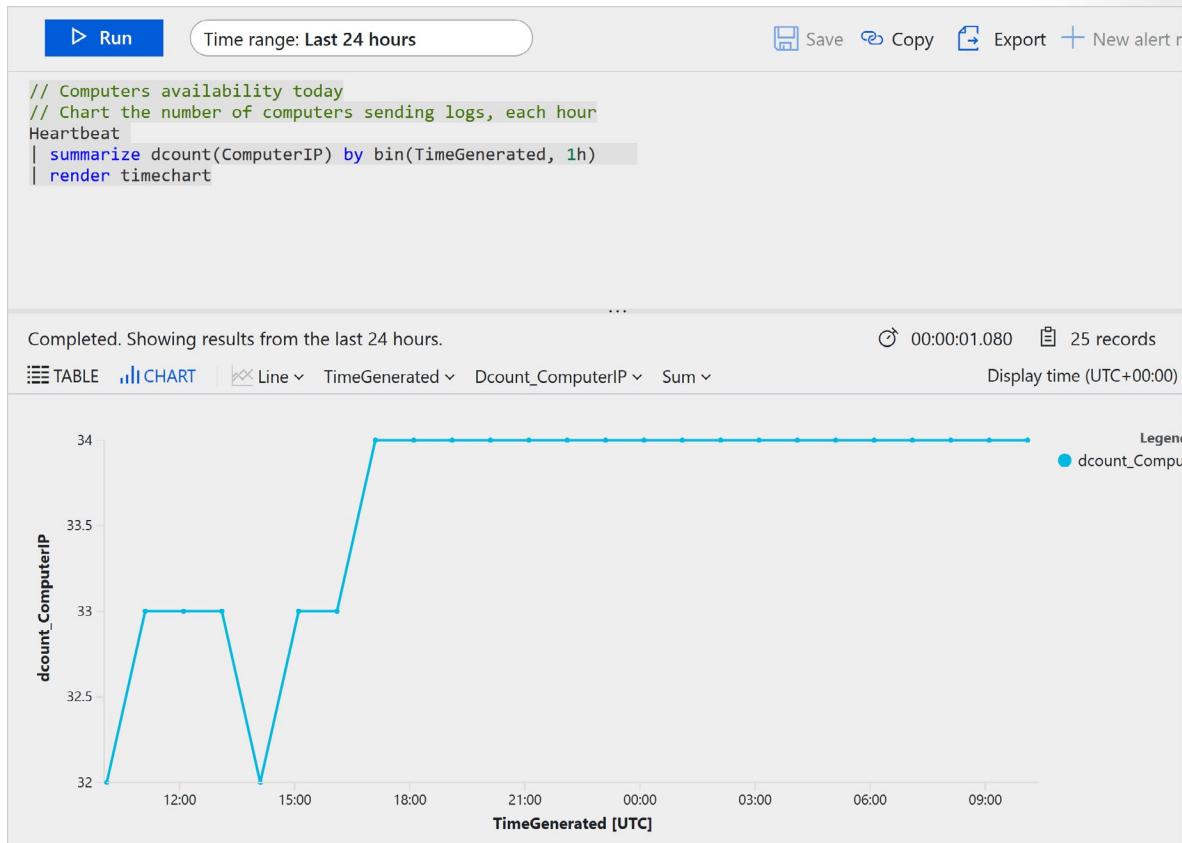
If a service has an Azure Monitor insight, you can access it from Monitoring in each resource's menu. Access all insights and solutions from the Azure Monitor menu.



## Azure Monitor Metrics

Metrics are numerical values that describe some aspect of a system at a point in time. Azure Monitor can capture metrics in near real time. The metrics are collected at regular intervals and are useful for alerting because of their frequent sampling. You can use a variety of algorithms to compare a metric to other metrics and observe trends over time.

Metrics are stored in a time-series database. This data store is most effective for analyzing time-stamped data. Metrics are suited for alerting and fast detection of issues. They can tell you about system performance. If needed, you can combine them with logs to identify the root cause of issues.



## Activity Log

View entries in the activity log in the Azure portal with the initial filter set to the current resource. Copy the activity log to a Log Analytics workspace to access it to use it in log queries and workbooks.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
► i DeployIfNotExists	Succeeded	3 h ago	Mon Sep 09 ...	Contoso IT - demo	Microsoft Azure Policy Insights
► i DeployIfNotExists	Succeeded	1 d ago	Sun Sep 08 ...	Contoso IT - demo	Microsoft Azure Policy Insights
► i DeployIfNotExists	Succeeded	2 d ago	Sat Sep 07 ...	Contoso IT - demo	Microsoft Azure Policy Insights
► i DeployIfNotExists	Succeeded	3 d ago	Fri Sep 06 2...	Contoso IT - demo	Microsoft Azure Policy Insights
► i Get Database Top Queries query	Succeeded	3 d ago	Fri Sep 06 2...	Contoso IT - demo	rosmithj@microsoft.com
► ▲ Audit	Succeeded	4 d ago	Thu Sep 05 ...	Contoso IT - demo	Microsoft Azure Policy Insights
► ▲ Audit	Succeeded	5 d ago	Wed Sep 04 ...	Contoso IT - demo	Microsoft Azure Policy Insights
► i Get Database Top Queries query	Succeeded	6 d ago	Tue Sep 03 ...	Contoso IT - demo	phnakorn@microsoft.com
► i Get Database Top Queries query	Succeeded	6 d ago	Tue Sep 03 ...	Contoso IT - demo	phnakorn@microsoft.com
► i Get Database Top Queries query	Succeeded	6 d ago	Tue Sep 03 ...	Contoso IT - demo	phnakorn@microsoft.com
► ▲ Audit	Succeeded	6 d ago	Tue Sep 03 ...	Contoso IT - demo	Microsoft Azure Policy Insights
► i Get Database Top Queries query	Succeeded	7 d ago	Tue Sep 03 ...	Contoso IT - demo	andersbe@microsoft.com

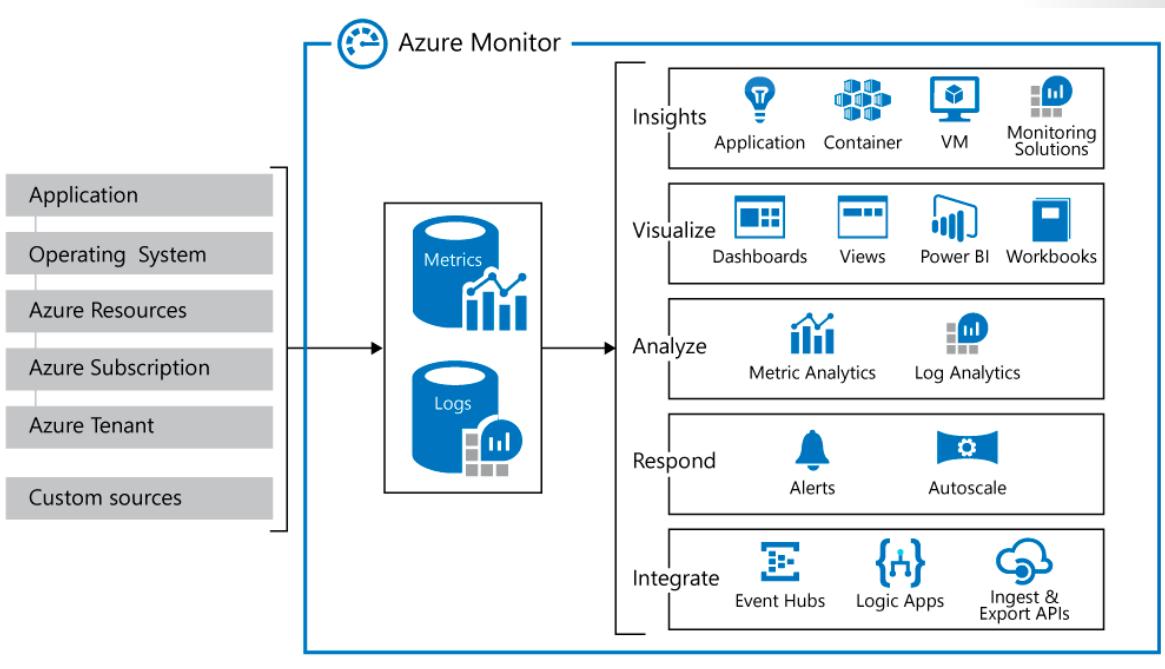
## Azure Monitor Logs

Azure Monitor is a service for collecting and analyzing telemetry. It helps you get maximum performance and availability for your cloud applications, and for your on-premises resources and applications. It shows how your applications are performing and identifies any issues with them.

## Data collection in Azure Monitor

Azure Monitor collects two fundamental types of data: metrics and logs. Metrics tell you how the resource is performing, and the other resources that it's consuming. Logs contain records that show when resources are created or modified.

The following diagram gives a high-level view of Azure Monitor. On the left are the sources of monitoring data: Azure, operating systems, and custom sources. At the center of the diagram are the data stores for metrics and logs. On the right are the functions that Azure Monitor performs with this collected data, such as analysis, alerting, and streaming to external systems.



Azure Monitor collects data automatically from a range of components. For example:

- **Application data**: Data that relates to your custom application code.
- **Operating system data**: Data from the Windows or Linux virtual machines that host your application.
- **Azure resource data**: Data that relates to the operations of an Azure resource, such as a web app or a load balancer.
- **Azure subscription data**: Data that relates to your subscription. It includes data about Azure health and availability.
- **Azure tenant data**: Data about your Azure organization-level services, such as Azure Active Directory.

Because Azure Monitor is an automatic system, it begins to collect data from these sources as soon as you create Azure resources such as virtual machines and web apps. You can extend the data that Azure Monitor collects by:

- **Enabling diagnostics**: For some resources, such as Azure SQL Database, you receive full information about a resource only after you have enabled diagnostic logging for it. You can use the Azure portal, the Azure CLI, or PowerShell to enable diagnostics.
- **Adding an agent**: For virtual machines, you can install the Log Analytics agent and configure it to send data to a Log Analytics workspace. This agent increases the amount of information that's sent to Azure Monitor.

Developers might also want to send data to Azure Monitor from custom code, such as a web app, an Azure function, or a mobile app. They send data by calling the Data Collector API. You communicate with this REST interface through HTTP. This interface is compatible with a variety of development frameworks, such as .NET Framework, Node.js, and Python. Developers can choose their favorite language and framework to log data in Azure Monitor.

## Compare Azure Monitor Metrics and Logs

The following table compares Metrics and Logs in Azure Monitor.

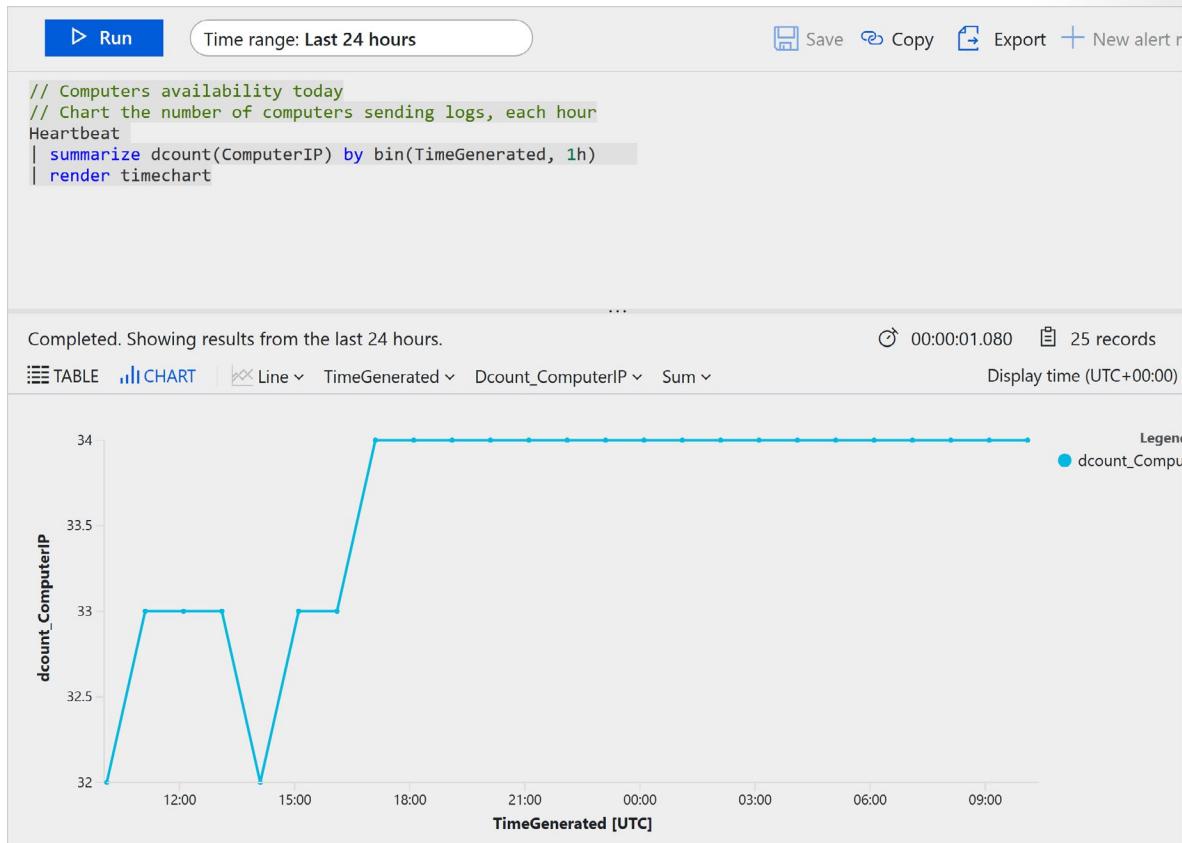
Attribute	Metrics	Logs
<b>Benefits</b>	Lightweight and capable of near-real time scenarios such as alerting. Ideal for fast detection of issues.	Analyzed with rich query language. Ideal for deep analysis and identifying root cause.
<b>Data</b>	Numerical values only	Text or numeric data
<b>Structure</b>	Standard set of properties including sample time, resource being monitored, a numeric value. Some metrics include multiple dimensions for further definition.	Unique set of properties depending on the log type.
<b>Collection</b>	Collected at regular intervals.	May be collected sporadically as events trigger a record to be created.
<b>View in Azure portal</b>	Metrics Explorer	Log Analytics
<b>Data sources include</b>	Platform metrics collected from Azure resources. Applications monitored by Application Insights. Custom defined by application or API.	Application and resource logs. Monitoring solutions. Agents and VM extensions. Application requests and exceptions. Azure Security Center. Data Collector API.

## Azure Monitor in a Log Analytics Workspace

Logs contain time-stamped information about changes made to resources. The type of information recorded varies by log source. The log data is organized into records, with different sets of properties for each type of record. The logs can include numeric values such as Azure Monitor metrics, but most include text data rather than numeric values.

The most common type of log entry records an event. Events can occur sporadically rather than at fixed intervals or according to a schedule. Events are created by applications and services, which provide the context for the events. You can store metric data in logs to combine them with other monitoring data for analysis.

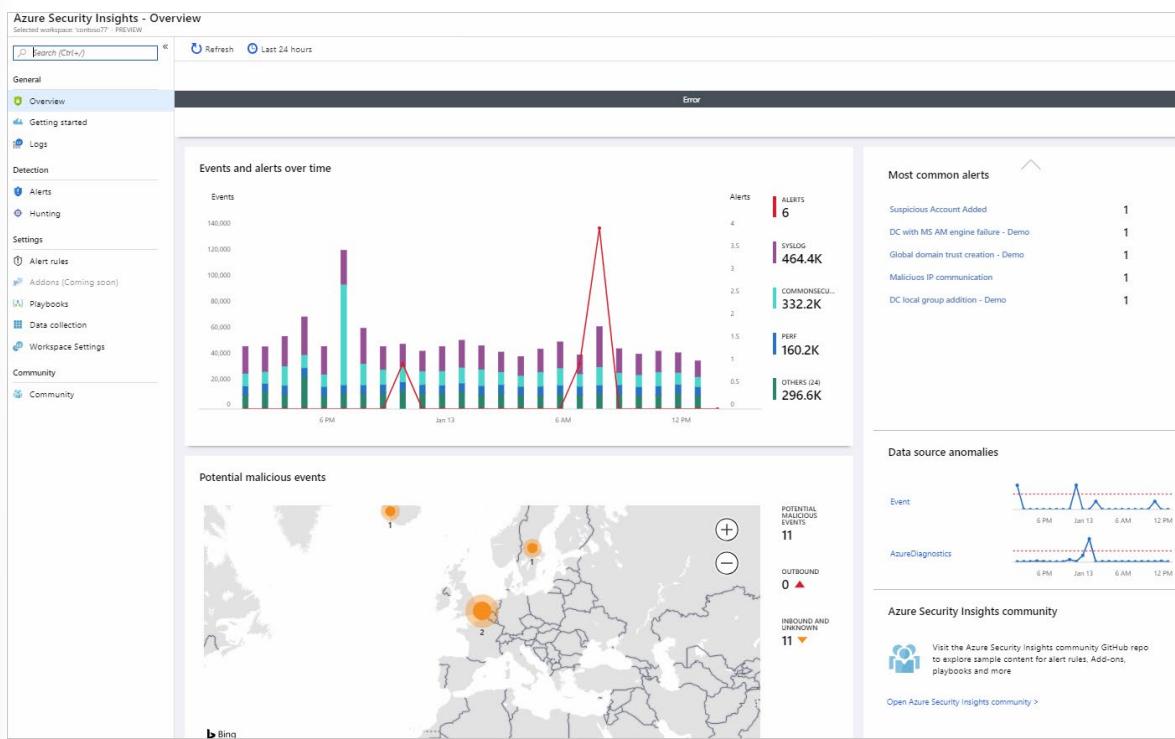
You log data from Azure Monitor in a Log Analytics workspace. Azure provides an analysis engine and a rich query language. The logs show the context of any problems and are useful for identifying root causes.



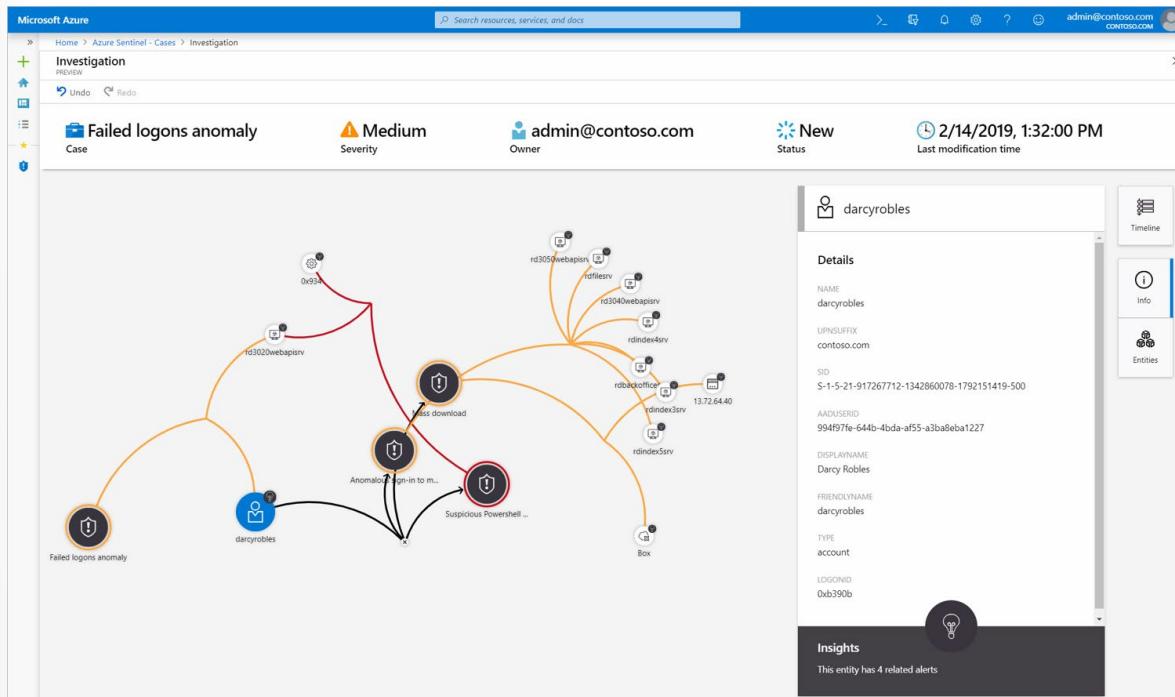
## Azure Sentinel

You use Azure Sentinel to collect data on the devices, users, infrastructure, and applications across your enterprise. Built-in threat intelligence for detection and investigation can help reduce false positives. Use Sentinel to proactively hunt for threats and anomalies and respond by using orchestration and automation.

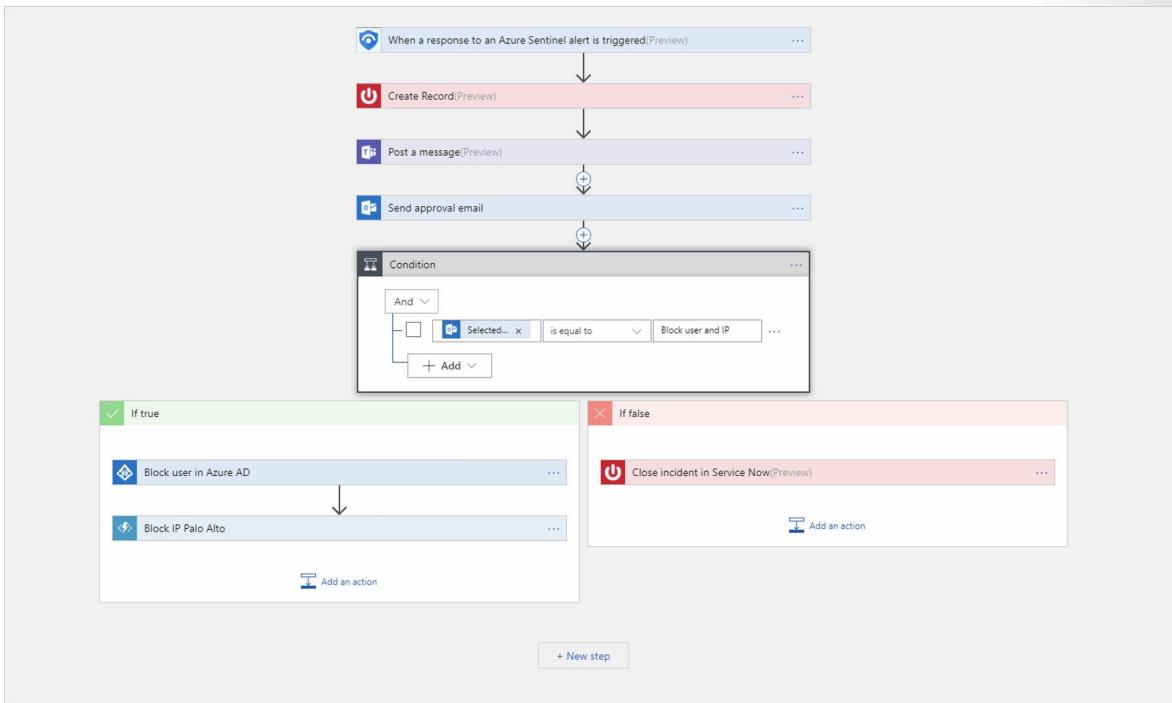
You connect your data sources to Sentinel. These sources include Microsoft services such as Office 365 and Azure Advanced Threat Protection. These sources can also include external solutions, such as AWS CloudTrail or on-premises sources. The dashboard shows detailed information collected from your sources.



Incidents help you group and combine alerts that are related. You use incidents to reduce the noise generated because of the scale of the data. Incidents also help you to further investigate any anomalous activities or threats that have raised alerts.



Use playbooks to automate your response to alerts in Sentinel. You configure playbooks by using Azure Logic Apps. Your playbook details the steps to take when an alert is triggered in Sentinel.



Use hunting queries to look for threats across your enterprise before alerts are raised. Microsoft security researchers maintain built-in hunting queries that act as a base for you to build your own queries.

The screenshot shows the Azure Sentinel Hunting interface. The left sidebar includes options like General, Threat management, Configuration, and Hunting (which is selected). The main area displays '19 Total Queries' and '106 Total Results'. A table lists various hunting queries, such as 'New processes observed in last 24 hours', 'Azure AD signins from new locations', and 'Processes executed from binaries hidden in Base64'. Each query row includes columns for QUERY, DESCRIPTION, PROVIDER, DATA SOURCES, RELEVANT TACTICS, and more. On the right, sections show 'New processes observed in last 24 hours' (with 103 results), 'Description' (explaining new processes observed), 'Query Information' (with a snippet of PowerShell code), and 'Entities' (listing tactics like Execution).

Use notebooks to automate your investigations. Notebooks are playbooks that can consist of investigation or hunting steps that you reuse or share with others. Use Azure Notebooks for Azure Sentinel to develop and run your notebooks. For example, you might use the **Guided hunting - Office365-Exploring** notebook to hunt for anomalous activities in Office 365 across your enterprise.

Azure-Sentinel-v4

Azure Sentinel  
Cloned from <https://github.com/Azure/Azure-Sentinel>  
Status: Stopped

Clone 0 Star 0 Project Settings Download Project Share

Run on Free Compute ▾

Search files, notebooks. Show hidden items + ▾ ↑

Name	Type	Modified On	Created On
config.json	JSON	Mar 19, 2019	
Get Started.ipynb	Notebook	Mar 19, 2019	
Guided Hunting - Office365-Exploring.ipynb	Notebook	Mar 19, 2019	
Guided Hunting - Windows-Host-Explorer.ipynb	Notebook	Mar 19, 2019	
Guided Investigation - Process-Alerts.ipynb	Notebook	Mar 19, 2019	
HowTos	Folder		
README.md	Markdown	Mar 19, 2019	
requirements.txt	Text	Mar 19, 2019	
Sample-Notebooks	Folder		
utils	Folder		

Showing 1 to 10 files

## Azure Security Center

Azure Security Center is a service that manages the security of your infrastructure from a centralized location. Use Security Center to monitor the security of your workloads, whether they're on-premises or in the cloud.

Improve your protection against security threats. Use Security Center to monitor the health of your resources and implement recommendations.

Secure score: 656 of 1444 (54 Active recommendations)

Resource health monitoring:

- 182 Compute & apps
- 126 Data & storage
- 83 Networking
- 3 Identity & access

Review and improve your secure score: Review and resolve security vulnerabilities to improve your secure score and secure your workload.

Search recommendations:

RECOMMENDATION	SECURE SCORE IMPACT	RESOURCE
Enable MFA for accounts with owner permissions on your subscription (Preview)	+50	3 of 3 subscriptions
Install system updates on virtual machine scale sets (Preview)	+40	4 of 5 virtual machine scale sets
Remediate vulnerabilities in container security configurations	+35	9 of 9 Container hosts
Enable Adaptive Application Controls	+25	5 of 100 virtual machines
Require secure transfer to storage account (Preview)	+20	100 of 102 storage accounts
Provision an Azure AD administrator for SQL server (Preview)	+20	7 of 7 SQL servers
Install monitoring agent on your machines	+17	5 of 15 computers

Ease the configuration of your security. Security Center is natively integrated with other Azure services, such as PaaS services like Azure SQL Database. For IaaS services, enable automatic provisioning in Security Center.

The screenshot shows a configuration section for 'Auto Provisioning'. At the top is a red-bordered 'Save' button. Below it is a descriptive text: 'Security Center collects security data and events from your resources and services to help you prevent, detect, and respond to threats.' followed by a 'Learn more >' link. Underneath is a heading 'Auto Provisioning' with the subtext: '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 agent will be provisioned.' followed by another 'Learn more >' link. At the bottom are two buttons: 'On' (highlighted in red) and 'Off'.

Security Center creates an agent on each supported virtual machine as it's created. It then automatically starts collecting data from the machine. You use Security Center to reduce the complexity of configuring security in this way.

## Demonstration - Monitor Azure Resources with Azure Monitor

Azure Monitor starts collecting data from Azure resources the moment that they're created. This demonstration provides a brief walkthrough of the data that's automatically collected for a resource and how to view it in the Azure portal for a resource. Later, you can add configuration to collect additional data and can go to the Azure Monitor menu to use the same tools to access data collected for all the resources in your subscription.

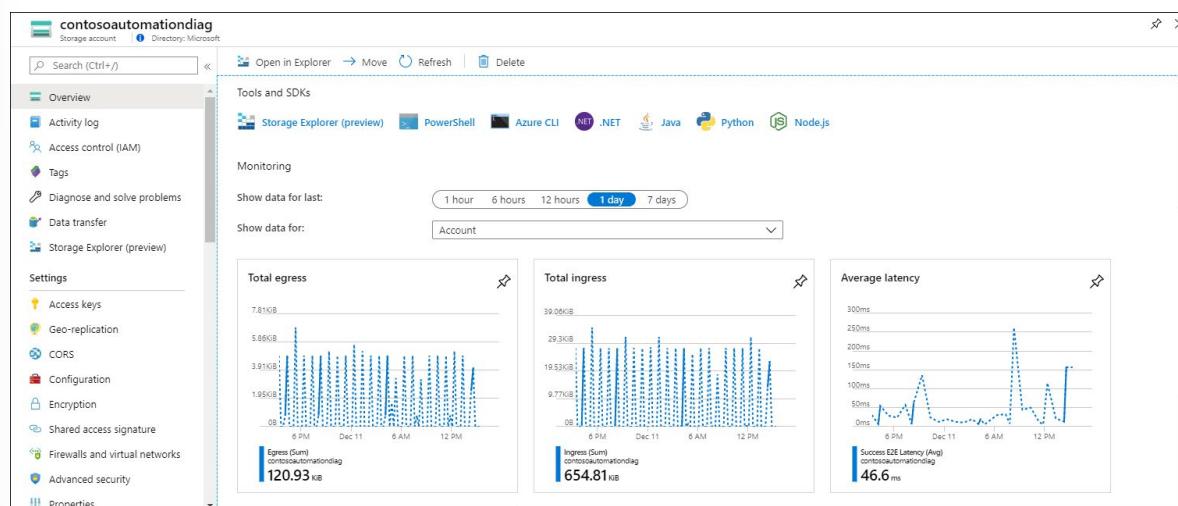
Sign in to the Azure portal at <https://portal.azure.com><sup>4</sup>.

### Overview page

Many services will include monitoring data on their Overview page as a quick glance to their operation. This will typically be based on a subset of platform metrics stored in Azure Monitor Metrics.

1. Locate an Azure resource in your subscription.
2. Go to the **Overview** page and note if there's any performance data displayed. This data will be provided by Azure Monitor. The example below is the **Overview** page for an Azure storage account, and you can see that there are multiple metrics displayed.

<sup>4</sup> <https://portal.azure.com/>

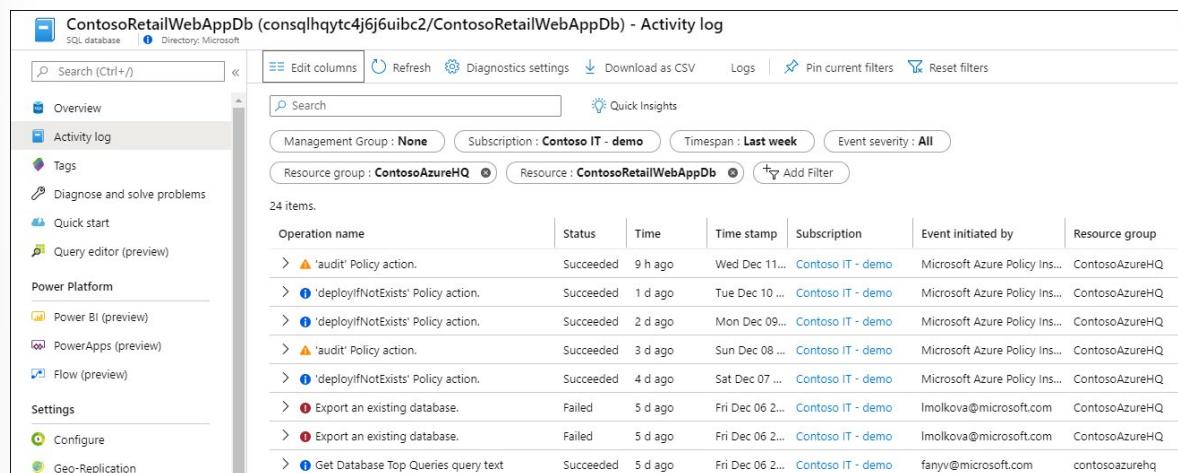


3. You can click on any of the graphs to open the data in metrics explorer which is described below.

## View the Activity log

The Activity log provides insight into the operations on each Azure resource in the subscription. This will include such information as when a resource is created or modified, when a job is started, or when a operation occurs.

1. At the top of the menu for your resource, select **Activity log**.
2. The current filter is set to events related to your resource. If you don't see any events, try changing the **Timespan** to increase the time scope.



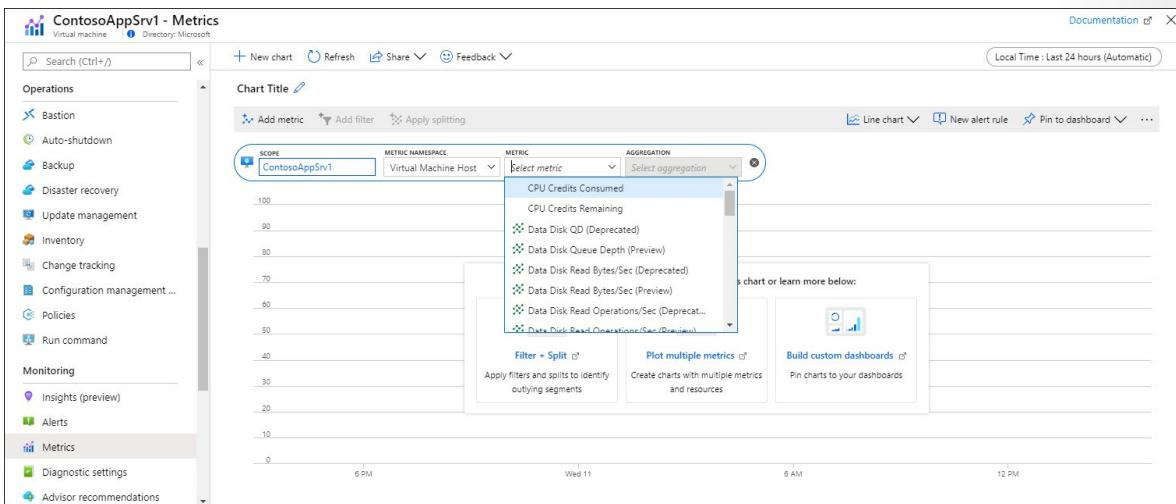
3. If you want to see events from other resources in your subscription, either change criteria in the filter or even remove filter properties.

ContosoRetailWebAppDb (contosqlhqytc4j6uibc2/ContosoRetailWebAppDb) - Activity log								
Search (Ctrl+ /)		Edit columns Refresh Diagnostics settings Download as CSV Logs Pin current filters Reset filters						
Overview		Search Quick Insights						
Activity log		Management Group: None Subscription: Contoso IT - demo Timespan: Last week Event severity: All Add Filter						
Tags		First 81 items.						
Diagnose and solve problems		Operation name	Status	Time	Time stamp	Subscription	Event initiated by	Resource group
> i 'deployIfNotExists' Policy action.		Succeeded	30 min ago	Wed Dec 11...	Contoso IT - demo	Microsoft Azure Policy Ins...	contosozurehq	Microsoft.Resources/... virtualMachines/Con...
> i Validate Deployment		Succeeded	31 min ago	Wed Dec 11...	Contoso IT - demo	d800f536368b4d93a5ba...	contosozurehq	Microsoft.Resources/... deployments/Policy...
> audit Policy action.		Succeeded	38 min ago	Wed Dec 11...	Contoso IT - demo	Microsoft Azure Policy Ins...	contosozurehq	Microsoft.Resources/... virtualMachines/Con...
> i Create or update Container Group		Failed	47 min ago	Wed Dec 11...	Contoso IT - demo	Contososh360KubCluster...	MC_Contososh360K...	Microsoft.Container... containerGroups/def...
> i Create or update Container Group		Failed	47 min ago	Wed Dec 11...	Contoso IT - demo	Contososh360KubCluster...	MC_Contososh360K...	Microsoft.Container... containerGroups/def...
> i Create or update Container Group		Failed	48 min ago	Wed Dec 11...	Contoso IT - demo	Contososh360KubCluster...	MC_Contososh360K...	Microsoft.Container... containerGroups/def...
> i Create or update Container Group		Failed	49 min ago	Wed Dec 11...	Contoso IT - demo	Contososh360KubCluster...	MC_Contososh360K...	Microsoft.Container... containerGroups/def...
> i List Storage Account Keys		Succeeded	49 min ago	Wed Dec 11...	Contoso IT - demo	Hyper-V Recovery Manager	contosorecoveryvalu...	Microsoft.Storage/st... storageAccounts/yql...

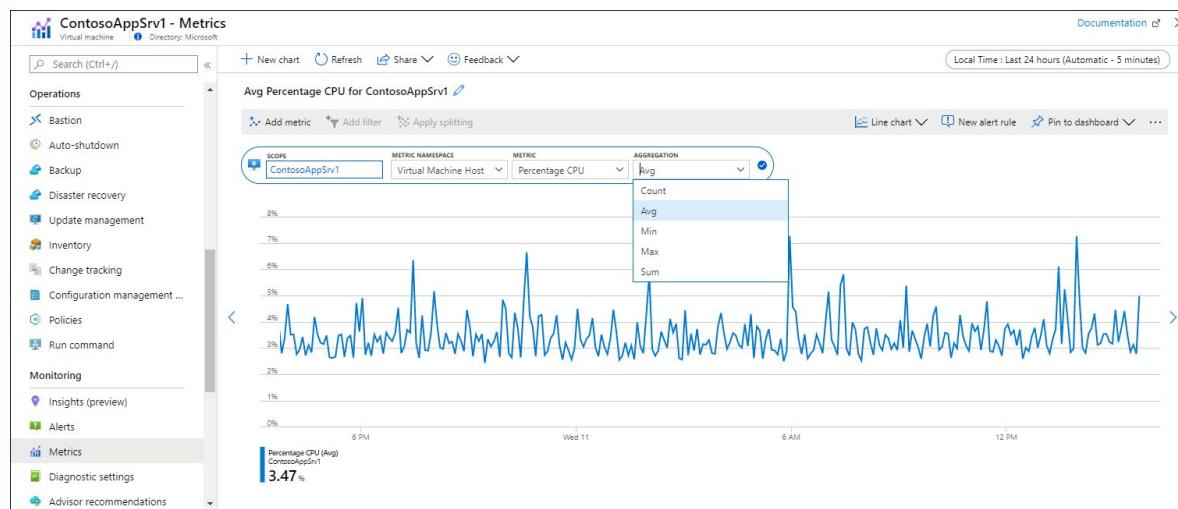
## View metrics

Metrics are numerical values that describe some aspect of your resource at a particular time. Azure Monitor automatically collects platform metrics at one minute intervals from all Azure resources. You can view these metrics using metrics explorer.

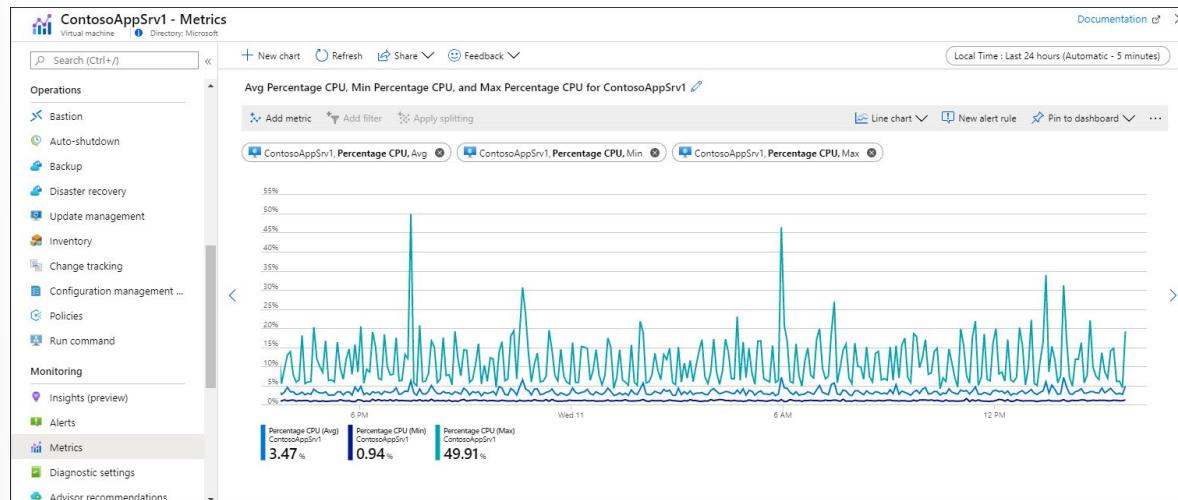
- Under the **Monitoring** section of your resource's menu, select **Metrics**. This opens metrics explorer with the scope set to your resource.
- Click **Add metric** to add a metric to the chart.



- Select a **Metric** from the dropdown list and then an **Aggregation**. This defines how the collected values will be sampled over each time interval.



4. Click **Add metric** to add additional metric and aggregation combinations to the chart.



## Demonstration - Collect and Analyze Resource Logs for Azure Resources

Resource logs provide insight into the detailed operation of an Azure resource and are useful for monitoring their health and availability. Azure resources generate resource logs automatically, but you must configure where they should be collected. This demonstration takes you through the process of creating a diagnostic setting to collect resource logs for a resource in your Azure subscription and analyzing it with a log query.

In this demonstration, you learn how to:

- Create a Log Analytics workspace in Azure Monitor
- Create a diagnostic setting to collect resource logs
- Create a simple log query to analyze logs

Log in to the Azure portal at <https://portal.azure.com><sup>5</sup>.

## Create a workspace

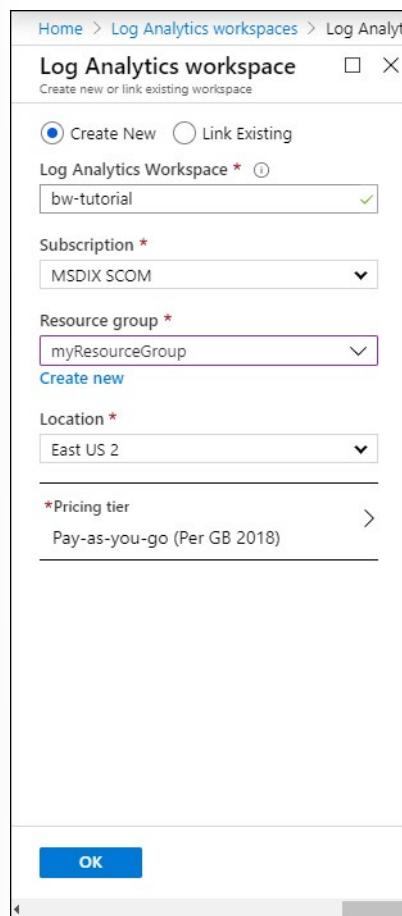
A Log Analytics workspace in Azure Monitor collects and indexes log data from a variety of sources and allows advanced analysis using a powerful query language. The Log Analytics workspace needs to exist before you create a diagnostic setting to send data into it. You can use an existing workspace in your Azure subscription or create one with the following procedure.

✓ **Note:**

While you can work with data in Log Analytics workspaces in the **Azure Monitor** menu, you create and manage workspaces in the **Log Analytics workspaces** menu.

1. From **All services**, select **Log Analytics workspaces**.
2. Click **Add** at the top of the screen and provide the following details for the workspace:
  - **Log Analytics workspace:** Name for the new workspace. This name must be globally unique across all Azure Monitor subscriptions.
  - **Subscription:** Select the subscription to store the workspace. This does not need to be the same subscription same as the resource being monitored.
  - **Resource Group:** Select an existing resource group or click Create new to create a new one. This does not need to be the same resource group same as the resource being monitored.
  - **Location:** Select an Azure region or create a new one. This does not need to be the same location same as the resource being monitored.
  - **Pricing tier:** Select *Pay-as-you-go* as the pricing tier. You can change this pricing tier later. Click the **Log Analytics pricing** link to learn more about different pricing tiers.

<sup>5</sup> <https://portal.azure.com/>



3. Click **OK** to create the workspace.

## Create a diagnostic setting

**Diagnostic settings** define where resource logs should be sent for a particular resource. A single diagnostic setting can have multiple destinations, but we'll only use a Log Analytics workspace in this tutorial.

1. Under the **Monitoring** section of your resource's menu, select **Diagnostic settings**.
2. You should have a message "No diagnostic settings defined". Click **Add diagnostic setting**.

The screenshot shows the 'Diagnostic settings' page for a Logic App named 'myLogicApp'. The left sidebar includes sections for 'Settings' (Workflow settings, Access keys, Identity, Properties, Locks, Export template), 'Monitoring' (Alerts, Metrics, Diagnostic settings, Logs, Diagnostics), and 'Support + troubleshooting' (New support request). The main content area shows a table titled 'Diagnostics settings' with columns: Name, Storage account, Event hub, Log Analytics workspace, and Edit setting. A note states 'No diagnostic settings defined' and provides a link to '+ Add diagnostic setting'. Below this, instructions say 'Click 'Add Diagnostic setting' above to configure the collection of the following data:' followed by a list: 'WorkflowRuntime' and 'AllMetrics'.

3. Each diagnostic setting has three basic parts:
  - **Name:** This has no significant effect and should simply be descriptive to you.
  - **Destinations:** One or more destinations to send the logs. All Azure services share the same set of three possible destinations. Each diagnostic setting can define one or more destinations but no more than one destination of a particular type.
  - **Categories:** Categories of logs to send to each of the destinations. The set of categories will vary for each Azure service.
4. Select **Send to Log Analytics workspace** and then select the workspace that you created.
5. Select the categories that you want to collect. See the documentation for each service for a definition of its available categories.

The screenshot shows the 'Diagnostics settings' page for a logic app named 'myLogicApp'. At the top, there are 'Save', 'Discard', and 'Delete' buttons. Below them is a 'Name \*' field containing 'Collect in Log Analytics workspace' with a green checkmark. There are three unchecked options: 'Archive to a storage account', 'Stream to an event hub', and 'Send to Log Analytics'. Under 'Subscription', 'Contoso IT - demo' is selected. In the 'Log Analytics workspace' dropdown, 'bw-tutorial (eastus2)' is chosen. The 'log' section has 'WorkflowRuntime' checked. The 'metric' section has 'AllMetrics' checked. The URL of the page is 'Home > Logic Apps > myLogicApp - Diagnostic settings > Diagnostics settings'.

6. Click **Save** to save the diagnostic settings.

## Use a log query to retrieve logs

Data is retrieved from a Log Analytics workspace using a log query written in Kusto Query Language (KQL). Insights and solutions in Azure Monitor will provide log queries to retrieve data for a particular service, but you can work directly with log queries and their results in the Azure portal with Log Analytics.

1. Under the **Monitoring** section of your resource's menu, select **Logs**.
2. Log Analytics opens with an empty query window with the scope set to your resource. Any queries will include only records from that resource.

**✓ Note**

If you opened Logs from the Azure Monitor menu, the scope would be set to the Log Analytics workspace. In this case, any queries will include all records in the workspace.

- The service shown in the example writes resource logs to the **AzureDiagnostics** table, but other services may write to other tables.

**✓ Note**

Multiple services write resource logs to the AzureDiagnostics table. If you start Log Analytics from the Azure Monitor menu, then you would need to add a `where` statement with the `ResourceProvider` column to specify your particular service. When you start Log Analytics from a resource's menu, then the scope is set to only records from this resource so this column isn't required. See the service's documentation for sample queries.

- Type in a query and click **Run** to inspect results.

TimeGenerated [UTC]	resource_originRundId_s	resource_actionName_s	correlation_actionTrackingId_g	workflowId_s	Level	_schema_s
12/13/2019, 12:54:21.577 AM					Information	/SUBSCRIPTIONS/4E56605E-4B16-4BAA-9358-DB88D6FAEDFE/RESO...
12/13/2019, 12:54:22.538 AM					Information	/SUBSCRIPTIONS/4E56605E-4B16-4BAA-9358-DB88D6FAEDFE/RESO...
12/13/2019, 12:54:22.525 AM	08586254084239710681729204791CU57				Information	/SUBSCRIPTIONS/4E56605E-4B16-4BAA-9358-DB88D6FAEDFE/RESO...
	TenantId	83dc2523-0480-4aae-b9b1-6acd6f599654				
	SourceSystem	Azure				
	TimeGenerated [UTC]	2019-12-13T00:54:22.525Z				
	resource_originRundId_s	08586254084239710681729204791CU57				
	workflowId_s	/SUBSCRIPTIONS/4E56605E-4B16-4BAA-9358-DB88D6FAEDFE/RESOURCEGROUPS/MYRESOURCEGROUP/PROVIDERS/MICROSOFT.LOGIC/WORKFLOWS/MYLOGICAPP				
	Level	Information				
	_schema_s	2016-06-01				
	status_s	Running				
	resource_resourceGroupName_s	myResourceGroup				
	resource_workflowName_s	myLogicApp				
	resource_rundId_s	08586254084239710681729204791CU57				
	resource_location_s	eastus2				
	correlation_actionId_s	08586254084239710681729204791CU57				

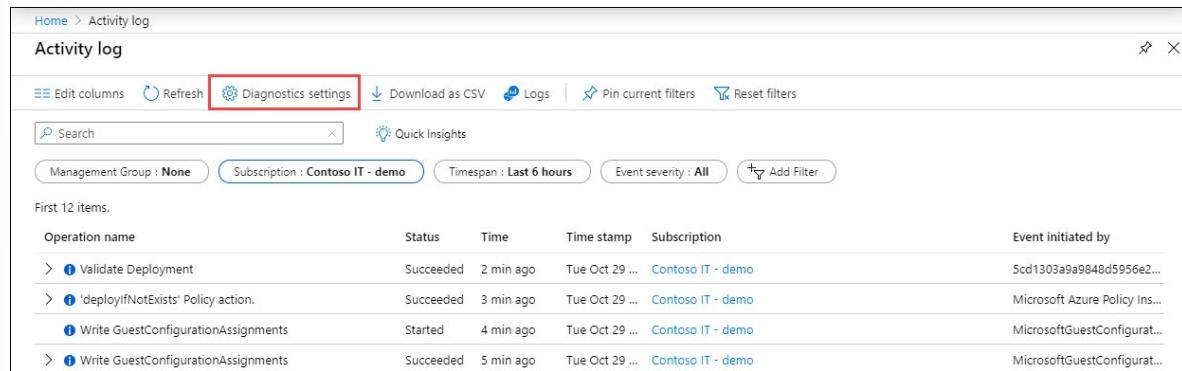
# Demonstration - Collect and Analyze Activity Log in Azure Monitor

The Azure Activity log is a platform log that provides insight into subscription-level events that have occurred in Azure. While you can view the Activity log in the Azure portal, you should configure it to send to a Log Analytics workspace to enable additional features of Azure Monitor.

## Collecting Activity log

The Activity log is collected automatically for viewing in the Azure portal. To collect it in a Log Analytics workspace or to send it to Azure storage or event hubs, create a diagnostic setting. This is the same method used by resource logs making it consistent for all platform logs.

To create a diagnostic setting for the Activity log, select **Diagnostic settings** from the **Activity log** menu in Azure Monitor. If you have any legacy settings, make sure you disable them before creating a diagnostic setting. Having both enabled may result in duplicate data.



The screenshot shows the 'Activity log' page in the Azure portal. At the top, there's a navigation bar with 'Home > Activity log'. Below it is a toolbar with 'Edit columns', 'Refresh', 'Diagnostics settings' (which is highlighted with a red box), 'Download as CSV', 'Logs', 'Pin current filters', and 'Reset filters'. There are also 'Search' and 'Quick Insights' buttons. Below the toolbar, there are filter buttons for 'Management Group : None', 'Subscription : Contoso IT - demo', 'Timespan : Last 6 hours', 'Event severity : All', and an 'Add Filter' button. The main area is titled 'First 12 items.' and contains a table with columns: Operation name, Status, Time, Time stamp, Subscription, and Event initiated by. The table lists four recent events:

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> ❶ Validate Deployment	Succeeded	2 min ago	Tue Oct 29 ...	Contoso IT - demo	5cd1303a9a9848d5956e2...
> ❶ 'deployIfNotExists' Policy action.	Succeeded	3 min ago	Tue Oct 29 ...	Contoso IT - demo	Microsoft Azure Policy Ins...
❶ Write GuestConfigurationAssignments	Started	4 min ago	Tue Oct 29 ...	Contoso IT - demo	MicrosoftGuestConfigurat...
❶ Write GuestConfigurationAssignments	Succeeded	5 min ago	Tue Oct 29 ...	Contoso IT - demo	MicrosoftGuestConfigurat...

## Legacy settings

While diagnostic settings are the preferred method to send the Activity log to different destinations, legacy methods will continue to work if you don't choose to replace with a diagnostic setting. Diagnostic settings have the following advantages over legacy methods, and it's recommended that you update your configuration:

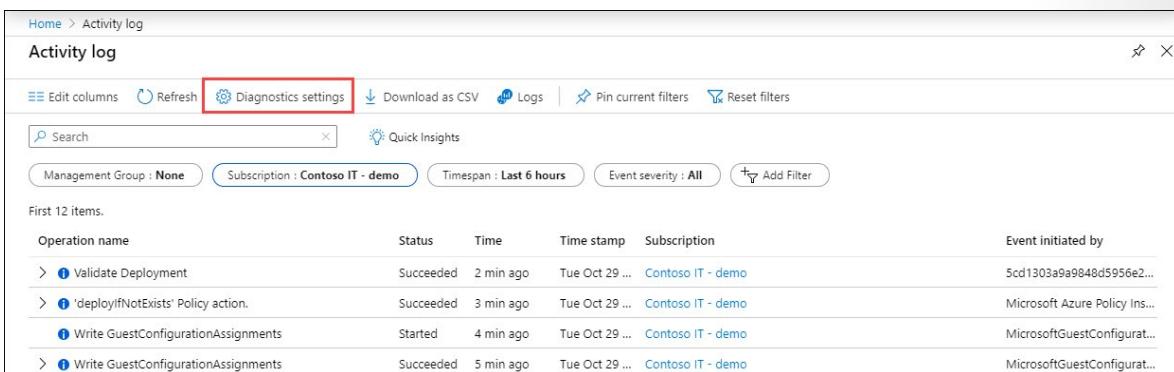
- Consistent method for collecting all platform logs.
- Collect Activity log across multiple subscriptions and tenants.
- Filter collection to only collect logs for particular categories.
- Collect all Activity log categories. Some categories are not collected using legacy method.
- Faster latency for log ingestion. The previous method has about 15 minutes latency while diagnostic settings adds only about 1 minute.

## Log profiles

Log profiles are the legacy method for sending the Activity log to Azure storage or event hubs. Use the following procedure to continue working with a log profile or to disable it in preparation for migrating to a diagnostic setting.

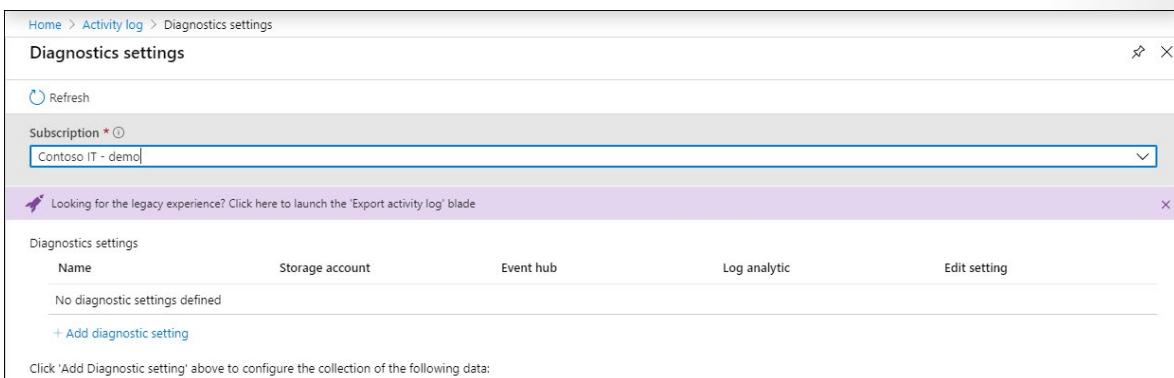
1. From the **Azure Monitor** menu in the Azure portal, select **Activity log**.

2. Click **Diagnostic settings**.



The screenshot shows the Azure Activity log interface. At the top, there are buttons for 'Edit columns', 'Refresh', 'Diagnostics settings' (which is highlighted with a red box), 'Download as CSV', 'Logs', 'Pin current filters', and 'Reset filters'. Below these are search and filter fields: 'Management Group : None', 'Subscription : Contoso IT - demo', 'Timespan : Last 6 hours', 'Event severity : All', and 'Add Filter'. The main area displays a table of activity logs with columns: Operation name, Status, Time, Time stamp, Subscription, and Event initiated by. The table lists several entries, such as 'Validate Deployment' and 'Write GuestConfigurationAssignments', with details like status (Succeeded or Started), time, and initiator.

3. Click the purple banner for the legacy experience.



The screenshot shows the 'Diagnostics settings' page. At the top, there is a 'Subscription' dropdown set to 'Contoso IT - demo'. A purple banner at the bottom left reads: 'Looking for the legacy experience? Click here to launch the "Export activity log" blade.' Below the banner, there is a table titled 'Diagnostics settings' with columns: Name, Storage account, Event hub, Log analytic, and 'Edit setting'. A note below the table says: 'Click "Add Diagnostic setting" above to configure the collection of the following data:' followed by a link '+ Add diagnostic setting'.

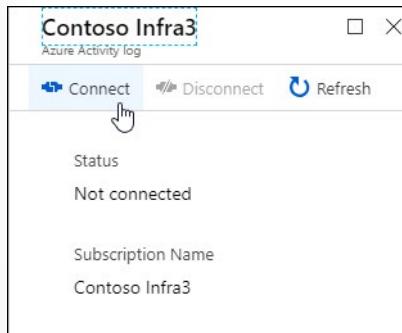
## Log Analytics workspace

The legacy method for collecting the Activity log into a Log Analytics workspace is connecting the log in the workspace configuration.

1. From the **Log Analytics workspaces** menu in the Azure portal, select the workspace to collect the Activity Log.
2. In the **Workspace Data Sources** section of the workspace's menu, select **Azure Activity log**.
3. Click the subscription you want to connect.

The screenshot shows the Log Analytics workspace interface. On the left, a list of workspaces is displayed, with 'contosoretail-IT' selected and highlighted with a red box. In the center, a sidebar lists various logs and resources, with 'Azure Activity log' also highlighted with a red box. On the right, a main pane displays a table of subscriptions and their connection status to the selected workspace. The table includes columns for 'Subscription' and 'LOG ANALYTICS CONNECTION'. Several subscriptions are listed as 'Not connected', while others like 'Contoso Dev' and 'Contoso IT - demo' are 'Connected'. A specific row for 'Contoso Infra3' is highlighted with a blue dashed border.

4. Click **Connect** to connect the Activity log in the subscription to the selected workspace. If the subscription is already connected to another workspace, click **Disconnect** first to disconnect it.



To disable the setting, perform the same procedure and click **Disconnect** to remove the subscription from the workspace.

## Analyze Activity log in Log Analytics workspace

When you connect an Activity Log to a Log Analytics workspace, entries will be written to the workspace into a table called *AzureActivity* that you can retrieve with a log query. The structure of this table varies depending on the category of the log entry.

### Data structure changes

Diagnostic settings collect the same data as the legacy method used to collect the Activity log with some changes to the structure of the *AzureActivity* table.

The columns in the following table have been deprecated in the updated schema. They still exist in *AzureActivity* but they will have no data. The replacement for these columns are not new, but they contain the same data as the deprecated column. They are in a different format, so you may need to modify log queries that use them.

Deprecated column	Replacement column
ActivityStatus	ActivityStatusValue
ActivitySubstatus	ActivitySubstatusValue
OperationName	OperationNameValue
ResourceProvider	ResourceProviderValue

✓ **Important**

In some cases, the values in these columns may be in all uppercase. If you have a query that includes these columns, you should use the `=~ operator` to do a case insensitive comparison.

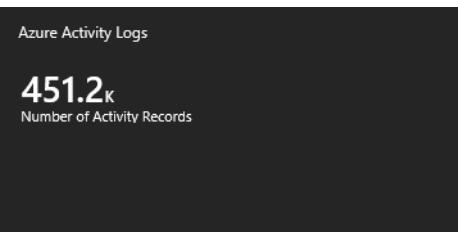
The following column have been added to `AzureActivity` in the updated schema:

- Authorization\_d
- Claims\_d
- Properties\_d

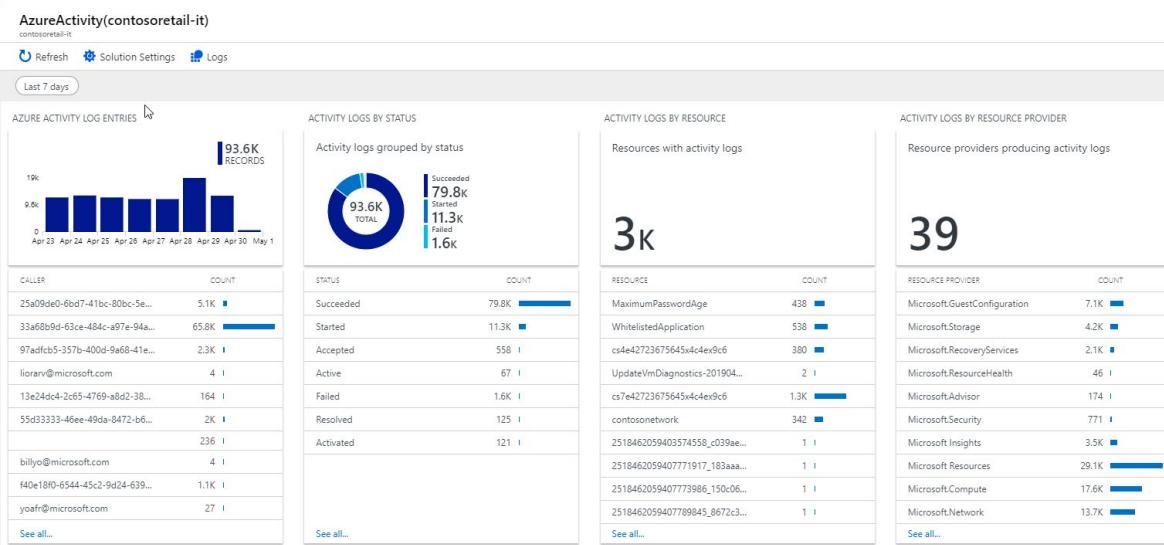
## Activity Logs Analytics monitoring solution

The Azure Log Analytics monitoring solution will be deprecated soon and replaced by a workbook using the updated schema in the Log Analytics workspace. You can still use the solution if you already have it enabled, but it can only be used if you're collecting the Activity log using legacy settings.

Monitoring solutions are accessed from the **Monitor** menu in the Azure portal. Select **More** in the **Insights** section to open the **Overview** page with the solution tiles. The **Azure Activity Logs** tile displays a count of the number of **AzureActivity** records in your workspace.



Click the **Azure Activity Logs** tile to open the **Azure Activity Logs** view. The view includes the visualization parts in the following table. Each part lists up to 10 items matching that part's criteria for the specified time range. You can run a log query that returns all matching records by clicking **See all** at the bottom of the part.



## Module 9 Review Questions

### Module 9 Review Questions



#### Review Question 1

You are asked to recommend a solution to generate a monthly report on all the recent Azure Resource Manager resource deployments in a subscription.

Which two solutions below should you include in your recommendation?

- Azure Advisor
- Azure Activity Log
- Application Insights
- Azure Log Analytics
- Azure Monitor action groups

#### Review Question 2

You are asked to recommend a solution that supports multiple Azure subscriptions and third-party hosting providers.

You are designing a central monitoring solution that will provide the following services:

- Collect log and diagnostic data from all subscriptions and third-party providers into a central repository.
- Also, services that analyze log data, detect threats, and provide automatic responses to known events.

Which Azure service should you include in the recommended solution?

- Azure Activity Log
- Application Insights
- Azure Sentinel
- Azure Log Analytics
- Azure Monitor

## Review Question 3

You are asked to recommend the implementation of an retail order processing web service that will contain microservices hosted in an Azure Service Fabric cluster.

You need to recommend a solution to developers that can actively identify and resolve performance issues. The developers need to have the ability to simulate user connections to the order processing web service from the Web and simulate user transactions.

The developers want to be notified if thresholds of the transaction response times are not met.

What should you recommend for the solution?

- Azure Network Watcher
- Azure Sentinel
- Azure Log Analytics
- Application Insights

# Answers

## Review Question 1

You are asked to recommend a solution to generate a monthly report on all the recent Azure Resource Manager resource deployments in a subscription.

Which two solutions below should you include in your recommendation?

- Azure Advisor
- Azure Activity Log
- Application Insights
- Azure Log Analytics
- Azure Monitor action groups

### Explanation

Azure Activity Log allows you to monitor operations on resources in a subscription. Also, Activity logs can be queried and reviewed in Log Analytics (AzureActivity). Azure Advisor does not provide deployment reviews. It provides best practices guidance. Action Groups are a set of actions to be taken in response to an alert but not to view all the recent Azure Resource Manager resource deployments.

## Review Question 2

You are asked to recommend a solution that supports multiple Azure subscriptions and third-party hosting providers.

You are designing a central monitoring solution that will provide the following services:

Which Azure service should you include in the recommended solution?

- Azure Activity Log
- Application Insights
- Azure Sentinel
- Azure Log Analytics
- Azure Monitor

### Explanation

**Correct Answer:** Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) tool. Azure Sentinel is using intelligent security analytics and threat intelligence.

Azure Sentinel assists with alert detection, threat visibility, proactive hunting, and threat response automatically. Also, it works with multiple tenants and there are currently more than 40 connectors for other systems available (3rd party providers).

Azure Monitor allows monitoring Azure and on-premises services. It aggregates and analyzes metrics, logs, and traces. However, it is not the solution because this service does not automatically analyze log data and detect threats.

**Review Question 3**

You are asked to recommend the implementation of an retail order processing web service that will contain microservices hosted in an Azure Service Fabric cluster.

You need to recommend a solution to developers that can actively identify and resolve performance issues. The developers need to have the ability to simulate user connections to the order processing web service from the Web and simulate user transactions.

The developers want to be notified if thresholds of the transaction response times are not met.

What should you recommend for the solution?

- Azure Network Watcher
- Azure Sentinel
- Azure Log Analytics
- Application Insights

*Explanation*

*Correct Answer: Application Insights allows you to gather the application information from inside apps regardless of where they are running and to analyze internal bottlenecks.*

## Module 10 Design a Solution for Backup and Recovery

### Architectural Best Practices for Reliability

#### Architectural Best Practices for Reliability

Building a reliable application in the cloud is different from traditional application development. While historically you may have purchased levels of redundant higher-end hardware to minimize the chance of an entire application platform failing. In the cloud, we acknowledge up front that failures will happen. Instead of trying to prevent failures altogether, the goal is to minimize the effects of a single failing component.

Reliable applications are:

- **Resilient** and recover gracefully from failures, and they continue to function with minimal downtime and data loss before full recovery.
- **Highly available (HA)** and run as designed in a healthy state with no significant downtime.

Understanding how these elements work together, and how they affect cost, is essential to building a reliable application. It can help you determine how much downtime is acceptable, the potential cost to your business, and which functions are necessary during a recovery.

This lesson provides a brief overview of building reliability into each step of the Azure application design process.

### Build for Reliability

This section describes six steps for building a reliable Azure application.

1. **Define Requirements.** Develop availability and recovery requirements based on decomposed workloads and business needs.
2. **Use Architectural Best Practices.** Follow proven practices, identify possible failure points in the architecture, and determine how the application will respond to failure.

3. **Test with Simulations and Forced Failovers.** Simulate faults, trigger forced failovers, and test detection and recovery from these failures.
4. **Deploy the Application Consistently.** Release to production using reliable and repeatable processes.
5. **Monitor Application Health.** Detect failures, monitor indicators of potential failures, and gauge the health of your applications.
6. **Respond to Failures and Disasters.** Identify when a failure occurs and determine how to address it based on established strategies.

## Define Requirements

Identify your business needs and build your reliability plan to address them. Consider the following:

- **Identify workloads and usage.** A *workload* is a distinct capability or task that is logically separated from other tasks, in terms of business logic and data storage requirements. Each workload has different requirements for availability, scalability, data consistency, and disaster recovery.
  - **Plan for usage patterns.** *Usage patterns* also play a role in requirements. Identify differences in requirements during critical and non-critical periods. For example, a tax-filing application can't fail during a filing deadline. To ensure uptime, plan redundancy across several regions in case one fails. Conversely, to minimize costs during non-critical periods, you can run your application in a single region.
  - **Establish availability metrics — mean time to recovery (MTTR) and mean time between failures (MTBF).** MTTR is the average time it takes to restore a component after a failure. MTBF is how long a component can reasonably expect to last between outages. Use these measures to determine where to add redundancy and to determine service-level agreements (SLAs) for customers.
  - **Establish recovery metrics — recovery time objective and recovery point objective (RPO).** RTO is the maximum acceptable time an application can be unavailable after an incident. RPO is the maximum duration of data loss that is acceptable during a disaster. To derive these values, conduct a risk assessment and make sure you understand the cost and risk of downtime or data loss in your organization.
- ✓ **Note** If the MTTR of any critical component in a highly available setup exceeds the system RTO, a failure in the system might cause an unacceptable business disruption. That is, you can't restore the system within the defined RTO.
- **Determine workload availability targets.** To ensure that application architecture meets your business requirements, define target SLAs for each workload. Account for the cost and complexity of meeting availability requirements, in addition to application dependencies.
  - **Understand service-level agreements.** In Azure, the SLA describes the Microsoft commitments for uptime and connectivity. If the SLA for a particular service is 99.9 percent, you should expect the service to be available 99.9 percent of the time.

Define your own target SLAs for each workload in your solution, so you can determine whether the architecture meets the business requirements. For example, if a workload requires 99.99 percent uptime but depends on a service with a 99.9 percent SLA, that service can't be a single point of failure in the system.

## Use Architectural Best Practices

During the architectural phase, focus on implementing practices that meet your business requirements, identify failure points, and minimize the scope of failures.

- **Perform a failure mode analysis (FMA).** FMA builds resiliency into an application early in the design stage. It helps you identify the types of failures your application might experience, the potential effects of each, and possible recovery strategies.
- **Create a redundancy plan.** The level of redundancy required for each workload depends on your business needs and factors into the overall cost of your application.
- **Design for scalability.** A cloud application must be able to scale to accommodate changes in usage. Begin with discrete components and design the application to respond automatically to load changes whenever possible. Keep scaling limits in mind during design so you can expand easily in the future.
- **Plan for subscription and service requirements.** You might need additional subscriptions to provision enough resources to meet your business requirements for storage, connections, throughput, and more.
- **Use load-balancing to distribute requests.** Load-balancing distributes your application's requests to healthy service instances by removing unhealthy instances from rotation.
- **Implement resiliency strategies.** Resiliency is the ability of a system to recover from failures and continue to function. Implement resiliency design patterns, such as isolating critical resources, using compensating transactions, and performing asynchronous operations whenever possible.
- **Build availability requirements into your design.** Availability is the proportion of time your system is functional and working. Take steps to ensure that application availability conforms to your service-level agreement. For example, avoid single points of failure, decompose workloads by service-level objective, and throttle high-volume users.
- **Manage your data.** How you store, backup, and replicate data is critical.
  - **Choose replication methods for your application data.** Your application data is stored in various data stores and might have different availability requirements. Evaluate the replication methods and locations for each type of data store to ensure that they satisfy your requirements.
  - **Document and test your failover and fallback processes.** Clearly document instructions to fail over to a new data store and test them regularly to make sure they are accurate and easy to follow.
  - **Protect your data.** Backup and validate data regularly, and make sure no single user account has access to both production and backup data.
  - **Plan for data recovery.** Make sure that your backup and replication strategy provides for data recovery times that meet your service-level requirements. Account for all types of data your application uses, including reference data and databases.

## Azure Service Dependencies

Microsoft Azure services are available globally to drive your cloud operations at an optimal level. You can choose the best region for your needs based on technical and regulatory considerations: service capabilities, data residency, compliance requirements, and latency.

Azure services deployed to Azure regions are listed on the **Azure global infrastructure products<sup>1</sup>** page. To better understand regions and Availability Zones in Azure, see **Regions and Availability Zones in Azure<sup>2</sup>**.

Azure services are built for resiliency including high availability and disaster recovery. There are no services that are dependent on a single logical data center (to avoid single points of failure). Non-regional services listed on **Azure global infrastructure products<sup>3</sup>** are services for which there is no dependency on a specific Azure region. Non-regional services are deployed to two or more regions and if there is a regional failure, the instance of the service in another region continues servicing customers. Certain non-regional services enable customers to specify the region where the underlying virtual machine (VM) on which service runs will be deployed. For example, Windows Virtual Desktop enables customers to specify the region location where the VM resides. All Azure services that store customer data allow the customer to specify the specific regions in which their data will be stored. The exception is Azure Active Directory (Azure AD), which has geo placement (such as Europe or North America). For more information about data storage residency, see the **Data residency map<sup>4</sup>**.

## Test with Simulations and Forced Failovers

Testing for reliability requires measuring how the end-to-end workload performs under failure conditions that only occur intermittently.

- **Test for common failure scenarios by triggering actual failures or by simulating them.** Use fault injection testing to test common scenarios (including combinations of failures) and recovery time.
- **Identify failures that occur only under load.** Test for peak load, using production data or synthetic data that is as close to production data as possible, to see how the application behaves under real-world conditions.
- **Run disaster recovery drills.** Have a disaster recovery plan in place, and test it periodically to make sure it works.
- **Perform failover and fallback testing.** Ensure that your application's dependent services fail over and fail back in the correct order.
- **Run simulation tests.** Testing real-life scenarios can highlight issues that need to be addressed. Scenarios should be controllable and non-disruptive to the business. Inform management of simulation testing plans.
- **Test health probes.** Configure health probes for load balancers and traffic managers to check critical system components. Test them to make sure that they respond appropriately.
- **Test monitoring systems.** Be sure that monitoring systems are reliably reporting critical information and accurate data to help identify potential failures.
- **Include third-party services in test scenarios.** Test possible points of failure due to third-party service disruption, in addition to recovery.

Testing is an iterative process. Test the application, measure the outcome, analyze and address any failures, and repeat the process.

<sup>1</sup> <https://azure.microsoft.com/global-infrastructure/services/?products=all>

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/availability-zones/az-overview>

<sup>3</sup> <https://azure.microsoft.com/global-infrastructure/services/?products=all>

<sup>4</sup> <https://azuredatcentermap.azurewebsites.net/>

## Deploy Applications Consistently

*Deployment* includes provisioning Azure resources, deploying application code, and applying configuration settings. An update may involve all three tasks or a subset of them.

After an application is deployed to production, updates are a possible source of errors. Minimize errors with predictable and repeatable deployment processes.

- **Automate your application deployment process.** Automate as many processes as possible.
- **Design your release process to maximize availability.** If your release process requires services to go offline during deployment, your application is unavailable until they come back online. Take advantage of platform staging and production features. Use blue-green or canary releases to deploy updates, so if a failure occurs, you can quickly roll back the update.
- **Have a rollback plan for deployment.** Design a rollback process to return to a last known good version and to minimize downtime if a deployment fails.
- **Log and audit deployments.** If you use staged deployment techniques, more than one version of your application is running in production. Implement a robust logging strategy to capture as much version-specific information as possible.
- **Document the application release process.** Clearly define and document your release process and ensure that it's available to the entire operations team.

## Monitor Application Health

Implement best practices for monitoring and alerts in your application so you can detect failures and alert an operator to fix them.

- **Implement health probes and check functions.** Run them regularly from outside the application to identify degradation of application health and performance.
- **Check long-running workflows.** Catching issues early can minimize the need to roll back the entire workflow or to execute multiple compensating transactions.
- **Maintain application logs.**
  - Log applications in production and at service boundaries.
  - Use semantic and asynchronous logging.
  - Separate application logs from audit logs.
- **Measure remote call statistics and share the data with the application team.** To give your operations team an instantaneous view into application health, summarize remote call metrics, such as latency, throughput, and errors in the 99 and 95 percentiles. Perform statistical analysis on the metrics to uncover errors that occur within each percentile.
- **Track transient exceptions and retries over an appropriate time frame.** A trend of increasing exceptions over time indicates that the service is having an issue and may fail.
- **Set up an early warning system.** Identify the key performance indicators (KPIs) of an application's health, such as transient exceptions and remote call latency, and set appropriate threshold values for each of them. Send an alert to operations when the threshold value is reached.
- **Operate within Azure subscription limits.** Azure subscriptions have limits on certain resource types, such as the number of resource groups, cores, and storage accounts. Watch your use of resource types.

- **Monitor third-party services.** Log your invocations and correlate them with your application's health and diagnostic logging using a unique identifier.
- **Train multiple operators to monitor the application and to perform manual recovery steps.** Make sure there is always at least one trained operator active.

## Respond to Failures and Disasters

Create a recovery plan, and make sure that it covers data restoration, network outages, dependent service failures, and region-wide service disruptions. Consider your VMs, storage, databases, and other Azure platform services in your recovery strategy.

- **Plan for Azure support interactions.** Before the need arises, establish a process for contacting Azure support.
- **Document and test your disaster recovery plan.** Write a disaster recovery plan that reflects the business impact of application failures. Automate the recovery process as much as possible and document any manual steps. Regularly test your disaster recovery process to validate and improve the plan.
- **Fail over manually when required.** Some systems can't fail over automatically and require a manual failover. If an application fails over to a secondary region, perform an operational readiness test. Verify that the primary region is healthy and ready to receive traffic again before failing back. Determine what the reduced application functionality is and how the app informs users of temporary problems.
- **Prepare for application failure.** Prepare for a range of failures, including faults that are handled automatically, those that result in reduced functionality, and those that cause the application to become unavailable. The application should inform users of temporary issues.
- **Recover from data corruption.** If a failure happens in a data store, check for data inconsistencies when the store becomes available again, especially if the data was replicated. Restore corrupt data from a backup.
- **Recover from a network outage.** You might be able to use cached data to run locally with reduced application functionality. If not, consider application downtime or fail over to another region. Store your data in an alternate location until connectivity is restored.
- **Recover from a dependent service failure.** Determine which functionality is still available and how the application should respond.
- **Recover from a region-wide service disruption.** Region-wide service disruptions are uncommon, but you should have a strategy to address them, especially for critical applications. You might be able to redeploy the application to another region or redistribute traffic.

# Recommend an Azure Site Recovery Solution

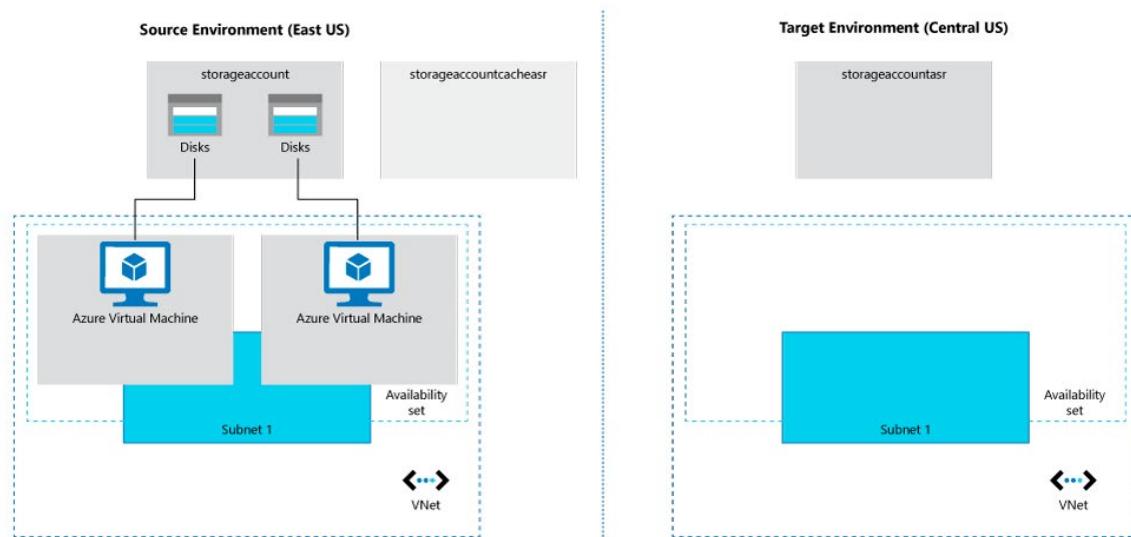
## Azure to Azure Disaster Recovery Architecture

This lesson describes the architecture, components, and processes used when you deploy disaster recovery for Azure virtual machines (VMs) using the Azure Site Recovery service. With disaster recovery set up, Azure VMs continuously replicate from 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.

### Architectural components

The components involved in disaster recovery for Azure VMs are summarized in the following table.

Component	Requirements
<b>VMs in source region</b>	One of more Azure VMs in a supported source region. VMs can be running any supported operating system.
<b>Source VM storage</b>	Azure VMs can be managed, or have non-managed disks spread across storage accounts.
<b>Source VM networks</b>	VMs can be located in one or more subnets in a virtual network (VNet) in the source region.
<b>Cache storage account</b>	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. Cache storage accounts must be Standard.
<b>Target resources</b>	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.

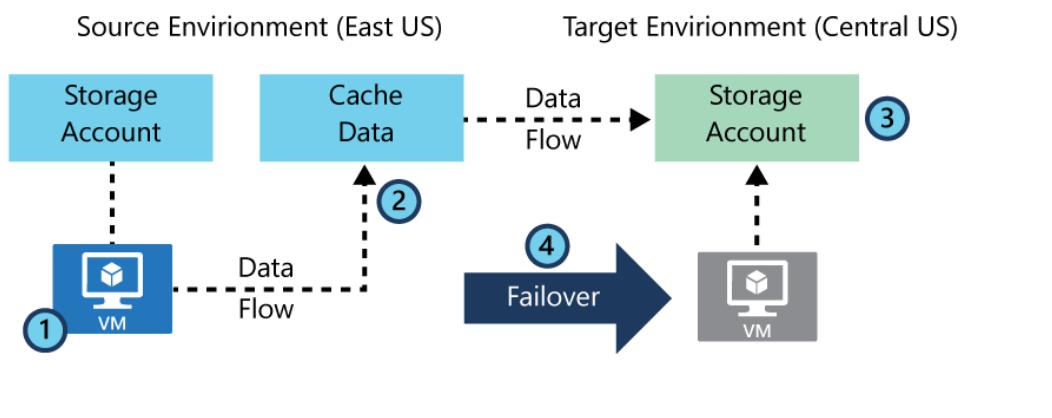


## Target Resources

When you enable replication for a VM, Site Recovery gives you the option of creating target resources automatically.

Target resource	Default setting
<b>Target subscription</b>	Same as the source subscription.
<b>Target resource group</b>	The resource group to which VMs belong after failover. It can be in any Azure region except the source region. Site Recovery creates a new resource group in the target region, with an "asr" suffix.
<b>Target VNet</b>	The virtual network (VNet) in which replicated VMs are located after failover. A network mapping is created between source and target virtual networks, and vice versa. Site Recovery creates a new VNet and subnet, with the "asr" suffix.
<b>Target storage account</b>	If the VM doesn't use a managed disk, this is the storage account to which data is replicated. Site Recovery creates a new storage account in the target region, to mirror the source storage account.
<b>Replica managed disks</b>	If the VM uses a managed disk, this is the managed disks to which data is replicated. Site Recovery creates replica managed disks in the storage region to mirror the source.

Target resource	Default setting
<b>Target availability sets</b>	Availability set in which replicating VMs are located after failover. Site Recovery creates an availability set in the target region with the suffix "asr", for VMs that are located in an availability set in the source location. If an availability set exists, it's used and a new one isn't created.
<b>Target availability zones</b>	If the target region supports availability zones, Site Recovery assigns the same zone number as that used in the source region.



## Managing target resources

You can manage target resources as follows:

- You can modify target settings as you enable replication.
- You can modify target settings after replication is already working. Please note that the default SKU for the target region VM is the same as the SKU of the source VM (or the next best available SKU in comparison to the source VM SKU). The target region VM SKU can also be updated after replication is in progress.

## Replication Policy

When you enable Azure VM replication, by default Site Recovery creates a new replication policy with the default settings summarized in the table.

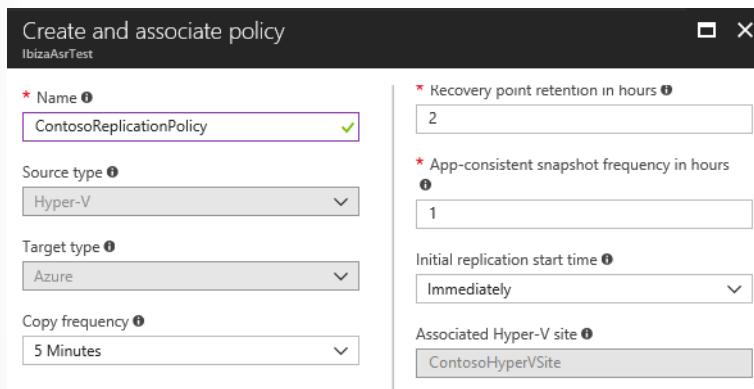
Policy setting	Details	Default
Recovery point retention	Specifies how long Site Recovery keeps recovery points	24 hours
App-consistent snapshot frequency	How often Site Recovery takes an app-consistent snapshot.	Every four hours

## Managing replication policies

You can manage and modify the default replication policies settings as follows:

- You can modify the settings as you enable replication.
- You can create a replication policy at any time, and then apply it when you enable replication.

After selecting what you want to replicate you will create a replication policy. Pay attention to the copy frequency, recovery point retention, app-consistent snapshot, and initial replication start time settings. You can create different replication scenarios.



- **Copy frequency.** Specify how often you want to replicate delta data after the initial replication.
- **Recovery point retention.** Specify in hours how long the retention window will be for each recovery point.
- **App-consistent snapshot.** Specify the frequency that recovery points containing app-consistent snapshots will be created. Hyper-V application-consistent snapshot takes a point-in-time snapshot of the application data inside the virtual machine.
- **Initial replication start time.** Specify when to start the initial replication. The replication occurs over your internet bandwidth, so you might want to schedule it outside your busy hours.

## Multi-VM consistency

If you want VMs to replicate together and have shared crash-consistent and app-consistent recovery points at failover, you can gather them together into a replication group. Multi-VM consistency impacts workload performance and should only be used for VMs running workloads that need consistency across all machines.

## Snapshots and Recovery Points

Recovery points are created from snapshots of VM disks taken at a specific point in time. When you fail over a VM, you use a recovery point to restore the VM in the target location.

When failing over, we generally want to ensure that the VM starts with no corruption or data loss, and that the VM data is consistent for the operating system, and for apps that run on the VM. This depends on the type of snapshots taken.

Site Recovery takes snapshots as follows:

1. Site Recovery takes crash-consistent snapshots of data by default, and app-consistent snapshots if you specify a frequency for them.

2. Recovery points are created from the snapshots, and stored in accordance with retention settings in the replication policy.

## Consistency

The following tables explain different types of consistency.

### Crash-consistent

A crash consistent snapshot captures data that was on the disk when the snapshot was taken. It doesn't include anything in memory.

It contains the equivalent of the on-disk data that would be present if the VM crashed or the power cord was pulled from the server at the instant that the snapshot was taken.

A crash-consistent doesn't guarantee data consistency for the operating system, or for apps on the VM.

✓ **Note:** Site Recovery creates crash-consistent recovery points every five minutes by default. This setting can't be modified.

✓ **Recommendation:** Crash-consistent recovery points are usually sufficient for the replication of operating systems, and apps such as DHCP servers and print servers.

### App-consistent

App-consistent recovery points are created from app-consistent snapshots.

An app-consistent snapshot contain all the information in a crash-consistent snapshot, plus all the data in memory and transactions in progress.

App-consistent snapshots use the Volume Shadow Copy Service (VSS):

1. When a snapshot is initiated, VSS perform a copy-on-write (COW) operation on the volume.
2. Before it performs the COW, VSS informs every app on the machine that it needs to flush its memory-resident data to disk.
3. VSS then allows the backup/disaster recovery app (in this case Site Recovery) to read the snapshot data and proceed.

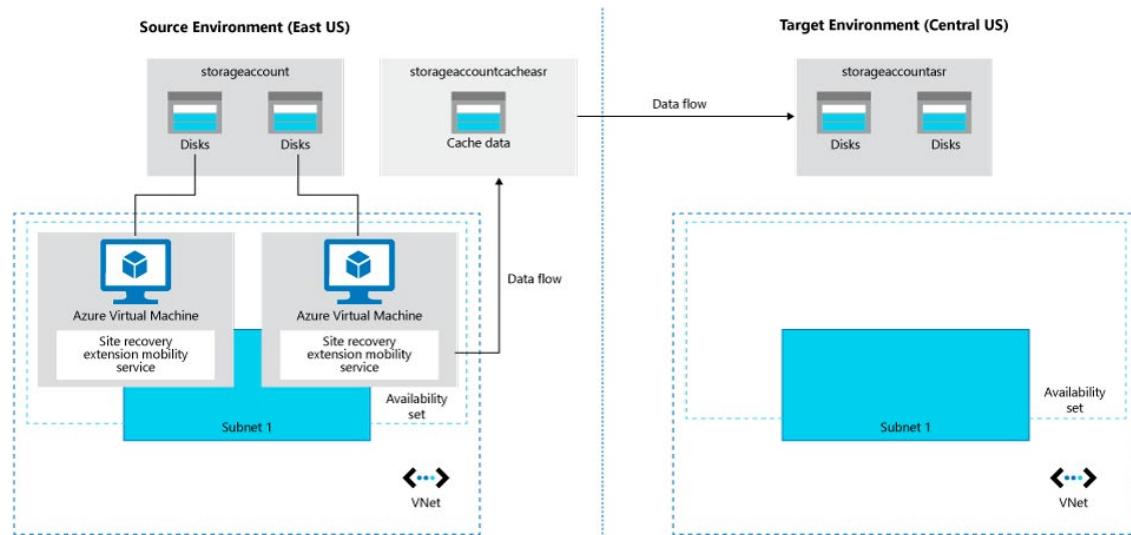
✓ **Recommendation:** App-consistent snapshots are taken in accordance with the frequency you specify. This frequency should always be less than you set for retaining recovery points. For example, if you retain recovery points using the default setting of 24 hours, you should set the frequency at less than 24 hours.

## Replication Process

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

1. The Site Recovery Mobility service extension is automatically installed on the VM.
2. The extension registers the VM with Site Recovery.
3. Continuous replication begins for the VM. Disk writes are immediately transferred to the cache storage account in the source location.
4. Site Recovery processes the data in the cache, and sends it to the target storage account, or to the replica managed disks.

5. After the data is processed, crash-consistent recovery points are generated every five minutes. App-consistent recovery points are generated according to the setting specified in the replication policy.



## Connectivity Requirements

The Azure VMs you replicate need outbound connectivity. Site Recovery never needs inbound connectivity to the VM.

### Outbound connectivity (URLs)

If outbound access for VMs is controlled with URLs, allow these URLs.

Name	Commercial	Government	Description
Storage	.blob.core.windows.net	.blob.core.usgovcloudapi.net	Allows data to be written from the VM to the cache storage account in the source region.
Azure Active Directory	login.microsoftonline.com	login.microsoftonline.us	Provides authorization and authentication to Site Recovery service URLs.
Replication	.hypervrecoverymanager.windowsazure.com	.hypervrecoverymanager.windowsazure.com	Allows the VM to communicate with the Site Recovery service.
Service Bus	.servicebus.windows.net	.servicebus.usgovcloudapi.net	Allows the VM to write Site Recovery monitoring and diagnostics data.

Name	Commercial	Government	Description
Key Vault	.vault.azure.net	.vault.usgovcloudapi.net	Allows access to enable replication for ADE-enabled virtual machines via portal
Azure Automation	.automation.ext.azure.com	.azure-automation.us	Allows enabling auto-upgrade of mobility agent for a replicated item via portal

## Outbound connectivity for IP address ranges

To control outbound connectivity for VMs using IP addresses, allow these addresses.

### Source region rules

Rule	Details	Service tag
Allow HTTPS outbound: port 443	Allow ranges that correspond to storage accounts in the source region	Storage.region-name
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Active Directory (Azure AD)	AzureActiveDirectory
Allow HTTPS outbound: port 443	Allow ranges that correspond to Events Hub in the target region.	EventsHub.region-name
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Site Recovery	AzureSiteRecovery
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Key Vault (This is required only for enabling replication of ADE-enabled virtual machines via portal)	AzureKeyVault
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Automation Controller (This is required only for enabling auto-upgrade of mobility agent for a replicated item via portal)	GuestAndHybridManagement

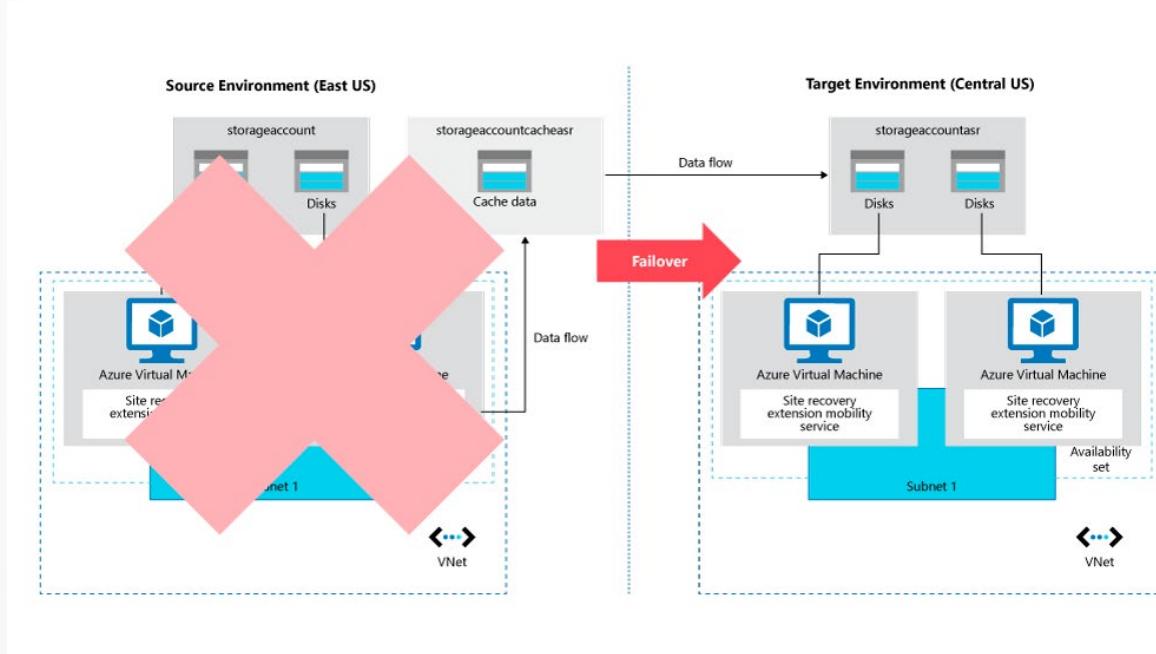
### Target region rules

Rule	Details	Service tag
Allow HTTPS outbound: port 443	Allow ranges that correspond to storage accounts in the target region	Storage.region-name
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure AD	AzureActiveDirectory

Rule	Details	Service tag
Allow HTTPS outbound: port 443	Allow ranges that correspond to Events Hub in the source region.	EventsHub.region-name
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Site Recovery	AzureSiteRecovery
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Key Vault (This is required only for enabling replication of ADE-enabled virtual machines via portal)	AzureKeyVault
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Automation Controller (This is required only for enabling auto-upgrade of mobility agent for a	GuestAndHybridManagement

## Failover Process

When you initiate a failover, the VMs are created in the target resource group, target virtual network, target subnet, and in the target availability set. During a failover, you can use any recovery point.



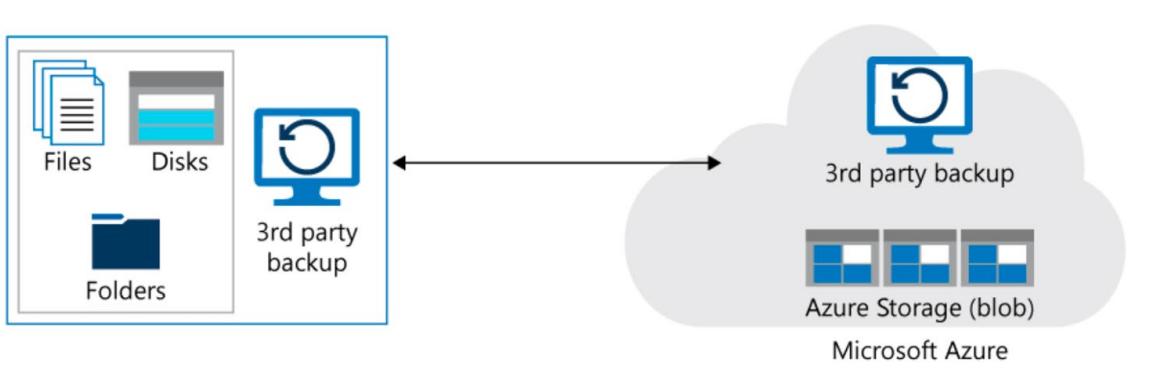
# Design a Solution for Data Archiving and Retention

## Archive On-Premises Data to Cloud

Archive your on-premises data to Azure Blob storage.

This solution is built on the Azure managed services: StorSimple and Blob Storage. These services run in a high-availability environment, patched and supported, allowing you to focus on your solution instead of the environment they run in.

### Architecture



### Components

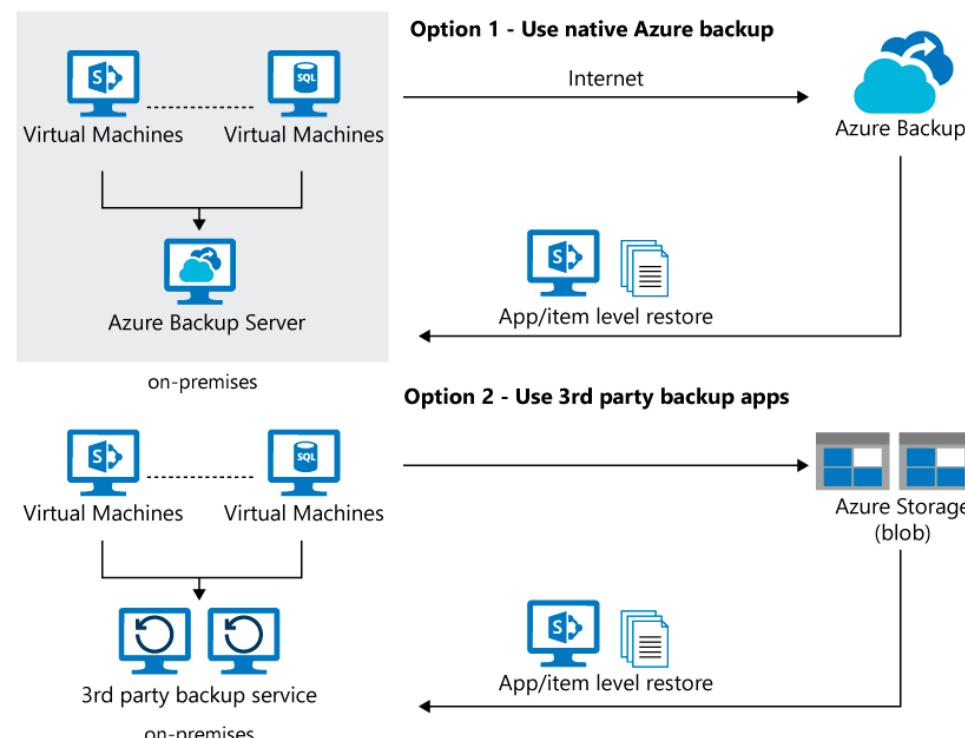
- **Azure StorSimple** appliance running on-premises that can tier data to Azure Blob storage (both hot and cool tier). StorSimple can be used to archive data from on-premises to Azure.
- **Blob Storage:** A cool or archive tier on Azure Blob storage is used to backup data that's less frequently accessed, while a hot tier is used to store data that's frequently accessed.

## Backup On-Premises Applications and Data to the Cloud

Backup data and applications from an on-premises system to Azure using Azure Backup or a partner solution. An Internet connection to Azure is used to connect to Azure Backup or Azure Blob storage. Azure Backup Server can write backups directly to Azure Backup. Alternatively, a partner solution such as Commvault Simpana or Veeam Availability Suite, hosted on-premises, can write backups to Blob storage directly or via a cloud endpoint such as Veeam Cloud Connect.

This solution is built on the Azure managed services: Backup Server and Blob Storage. These services run in a high-availability environment, patched and supported, allowing you to focus on your solution instead of the environment they run in.

## Architecture



### Components

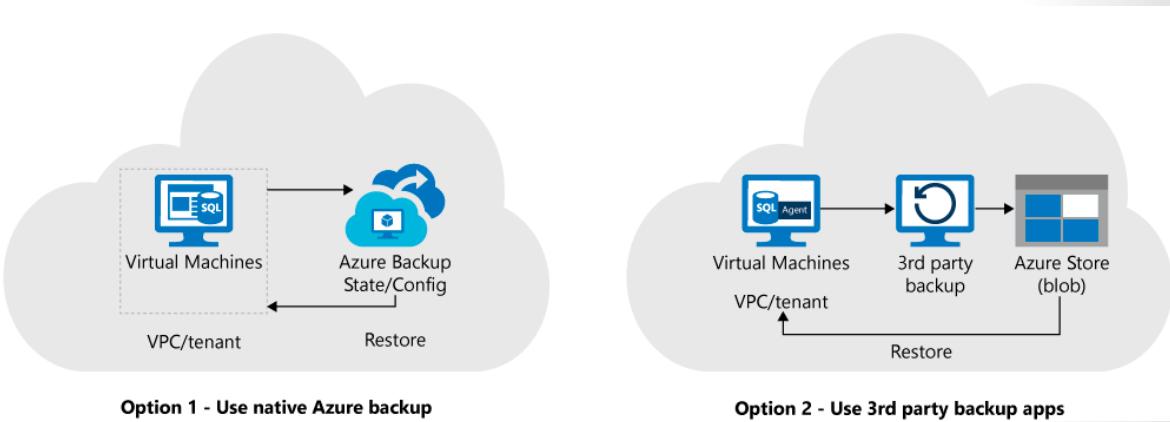
- **Azure Backup Server** orchestrates the backup of machines and manages the configuration of the restore procedures. It also has two days of backup data for operational recovery.
- **Azure Backup service** runs on the cloud and holds the recovery points, enforces policies, and enables you to manage data and application protection. You don't need to create or manage an Azure Blob storage account when using Azure Backup.
- **Blob Storage:** Blob storage that partner solutions such as Commvault connect to for backing up data and applications. You need to create and manage Azure Blob storage when using partner solutions.

## Backup Cloud Applications and Data to Cloud

Backup data and applications running in Azure to another Azure location by using Azure Backup or a partner solution.

This solution is built on the Azure managed services: Azure Backup and Blob Storage. These services run in a high-availability environment, patched and supported, allowing you to focus on your solution instead of the environment they run in.

### Architecture



## Components

- **Azure Backup** service runs on the cloud and holds the recovery points, enforces policies, and enables you to manage data and application protection. You don't need to create or manage an Azure Blob storage account when using Azure Backup.
- **Blob Storage:** Blob storage that partner solutions such as Commvault connect to for backing up data and applications. You need to create and manage Azure Blob storage when using partner solutions.

## Module 10 Review Questions

### Module 10 Review Questions



#### Review Question 1

You have been asked to design a business continuity solution for the deployment of a payment processing system to Azure for an auto parts wholesaler.

The payment processing system will use Azure VMs running SUSE Linux Enterprise Server and Windows.

You need to recommend a solution for a business continuity solution that fulfill the following:

- Provide business continuity if an Azure region fails.
- Minimize costs.
- Provide an RTO of 90 minutes.
- Provide an RPO of 5 minutes.

What should you recommendation?

- Azure Backup
- Azure Site Recovery
- Premium managed disks
- Azure Data Lake Analytics with Azure Monitor Logs

#### Review Question 2

You are asked to design a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Your solution is to include StorSimple as a part of your design.

Does your design recommendation provide on-premises storage with replication to Azure?

- Yes
- No

# Answers

## Review Question 1

You have been asked to design a business continuity solution for the deployment of a payment processing system to Azure for an auto parts wholesaler.

The payment processing system will use Azure VMs running SUSE Linux Enterprise Server and Windows. You need to recommend a solution for a business continuity solution that fulfill the following:

What should you recommendation?

- Azure Backup
- Azure Site Recovery
- Premium managed disks
- Azure Data Lake Analytics with Azure Monitor Logs

*Explanation*

*Correct Answer: Azure Site Recovery. Azure Site Recovery enables failover and would move the affected VMs to another region.*

## Review Question 2

You are asked to design a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Your solution is to include StorSimple as a part of your design.

Does your design recommendation provide on-premises storage with replication to Azure?

- Yes
- No

*Explanation*

*Correct Answer: Yes. StorSimple is an appliance that can be used both on-premises and in Azure to provide immediate replication between the two sites.*



## Module 11 Design for High Availability

### High Availability

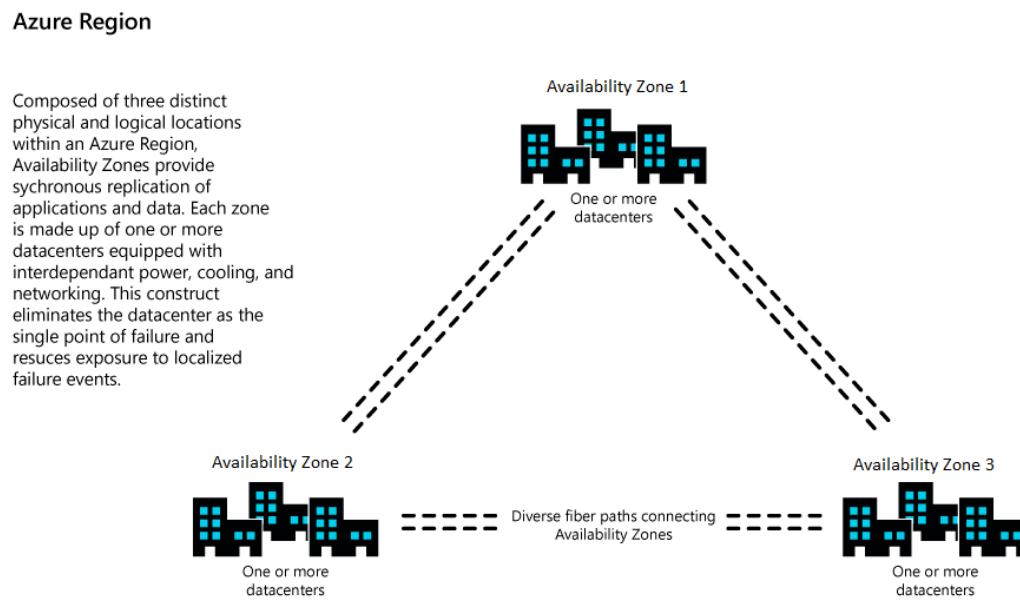
#### Building Solutions for High Availability using Availability Zones

Microsoft Azure global infrastructure is designed and constructed at every layer to deliver the highest levels of redundancy and resiliency to its customers. Azure infrastructure is composed of geographies, regions, and Availability Zones, which limit the blast radius of a failure and therefore limit potential impact to customer applications and data. The Azure Availability Zones construct was developed to provide a software and networking solution to protect against datacenter failures and to provide increased high availability (HA) to our customers.

Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters with independent power, cooling, and networking. The physical separation of Availability Zones within a region limits the impact to applications and data from zone failures, such as large-scale flooding, major storms and superstorms, and other events that could disrupt site access, safe passage, extended utilities uptime, and the availability of resources. Availability Zones and their associated datacenters are designed such that if one zone is compromised, the services, capacity, and availability are supported by the other Availability Zones in the region.

Availability Zones can be used to spread a solution across multiple zones within a region, allowing for an application to continue functioning when one zone fails. With Availability Zones, Azure offers industry best 99.99% **Virtual Machine (VM) uptime service-level agreement (SLA)**<sup>1</sup>. Zone-redundant services replicate your services and data across Availability Zones to protect from single points of failure.

<sup>1</sup> [https://azure.microsoft.com/support/legal/sla/virtual-machines/v1\\_9/](https://azure.microsoft.com/support/legal/sla/virtual-machines/v1_9/)



This lesson covers the following topics for building solutions for high availability using Availability Zones:

- Delivering Reliability in Azure
- Zonal vs. Zone-Redundant Architecture
- SLA Offered by Availability Zones

## Delivering Reliability in Azure

Designing solutions that continue to function in spite of failure is key to improving the reliability of a solution. In cloud-based solutions, building to survive failure is a shared responsibility. This can be viewed at three levels:

- Resilient foundation
- Resilient services
- Resilient applications

The **foundation** is the Microsoft investment in the platform, including Availability Zones.

On top of this foundation are the **Azure services** that customers can enable to support high availability, such as zone-redundant storage (ZRS), which replicates data across zones. The customer builds applications upon the enabled services supported by the foundation.

The **applications** should be architected to support resiliency.

When architecting for resilience, all three layers—foundation, services, and applications—should be considered to achieve the highest level of reliability. Since a solution can be made up of many components, each component should be designed for reliability.

## Zonal vs. Zone-Redundant Architecture

An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to take care that VMs in different zones are not updated at the same time.

Azure services supporting Availability Zones fall into two categories: zonal and zone redundant. Customer workloads can be categorized to utilize either architecture scenario to meet application performance and durability requirements.

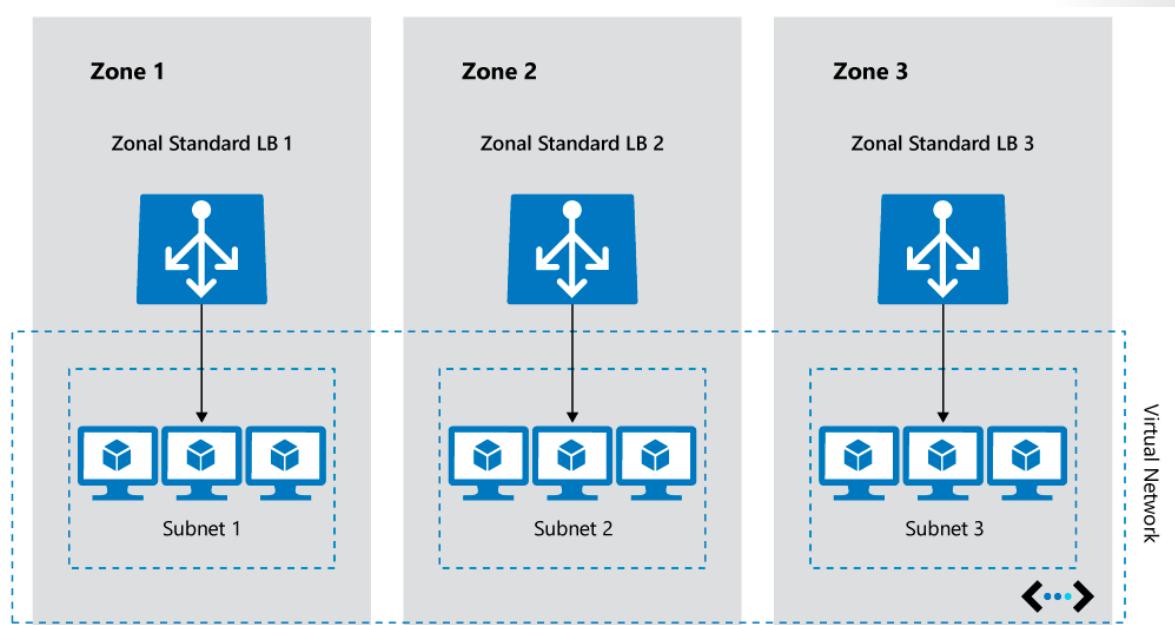
With **zonal architecture**, a resource can be deployed to a specific, self-selected Availability Zone to achieve more stringent latency or performance requirements. Resiliency is self-architected by replicating applications and data to one or more zones within the region. You can choose specific Availability Zones for synchronous replication, providing high availability, or asynchronous replication, providing backup or cost advantage. You can pin resources—for example, virtual machines, managed disks, or standard IP addresses—to a specific zone, allowing for increased resilience by having one or more instances of resources spread across zones.

With **zone-redundant architecture**, the Azure platform automatically replicates the resource and data across zones. Microsoft manages the delivery of high availability since Azure automatically replicates and distributes instances within the region.

A failure to a zone affects zonal and zone-redundant services differently. In the case of a zone failure, the zonal services in the failed zone become unavailable until the zone has recovered. By architecting your solutions to use replicated VMs in zones, you can protect your applications and data from a zone becoming unavailable—for example, due to a power outage. If one zone is compromised, replicated apps and data are instantly available in another zone.

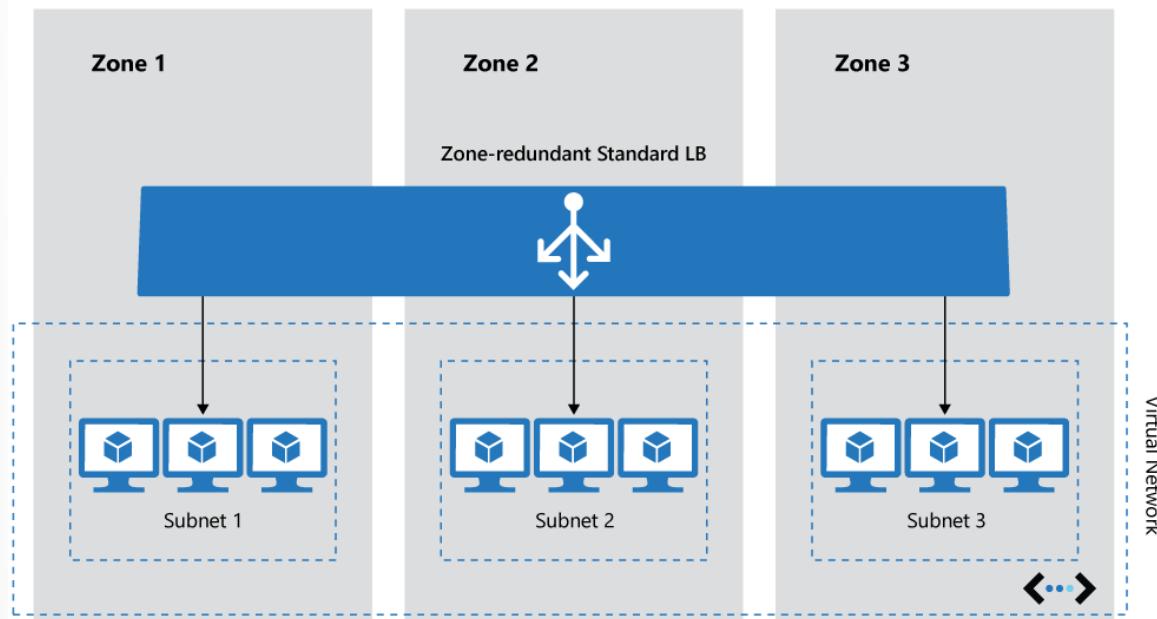
Zonal architecture applies to a specific resource, typically an infrastructure as a service (IaaS) resource, like a VM or managed disk, as illustrated.

In the illustration below, each VM and load balancer (LB) are deployed to a specific zone.



With zone-redundant services, the distribution of the workload is a feature of the service and is handled by Azure. Azure automatically replicates the resource across zones without requiring your intervention. ZRS, for example, replicates the data across three zones so a zone failure does not impact the HA of the data.

The following illustration is of a zone-redundant load balancer.



For example, zone-redundant load balancer, Azure Application Gateway, Azure Service Bus, virtual private network (VPN), zone-redundant storage, Azure ExpressRoute, Azure Event Hubs, Azure Cosmos DB.

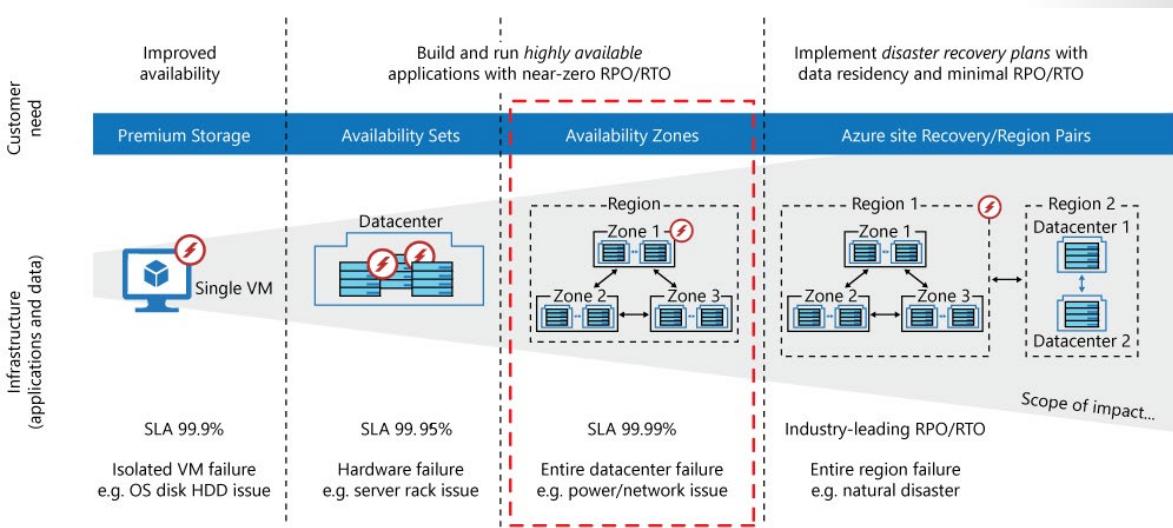
A few resources, like the load balancer and subnets, support both zonal and zone-redundant deployments. An important consideration in HA is distributing the traffic effectively across resources in the different Availability Zones.

## SLA Offered by Availability Zones

With Availability Zones, Azure offers industry best 99.99% VM uptime SLA. The full [Azure SLA<sup>2</sup>](#) explains the guaranteed availability of Azure as a whole.

The following diagram illustrates the different levels of HA offered by a single VM, Availability Sets, and Availability Zones.

<sup>2</sup> [https://azure.microsoft.com/support/legal/sla/virtual-machines/v1\\_9/](https://azure.microsoft.com/support/legal/sla/virtual-machines/v1_9/)



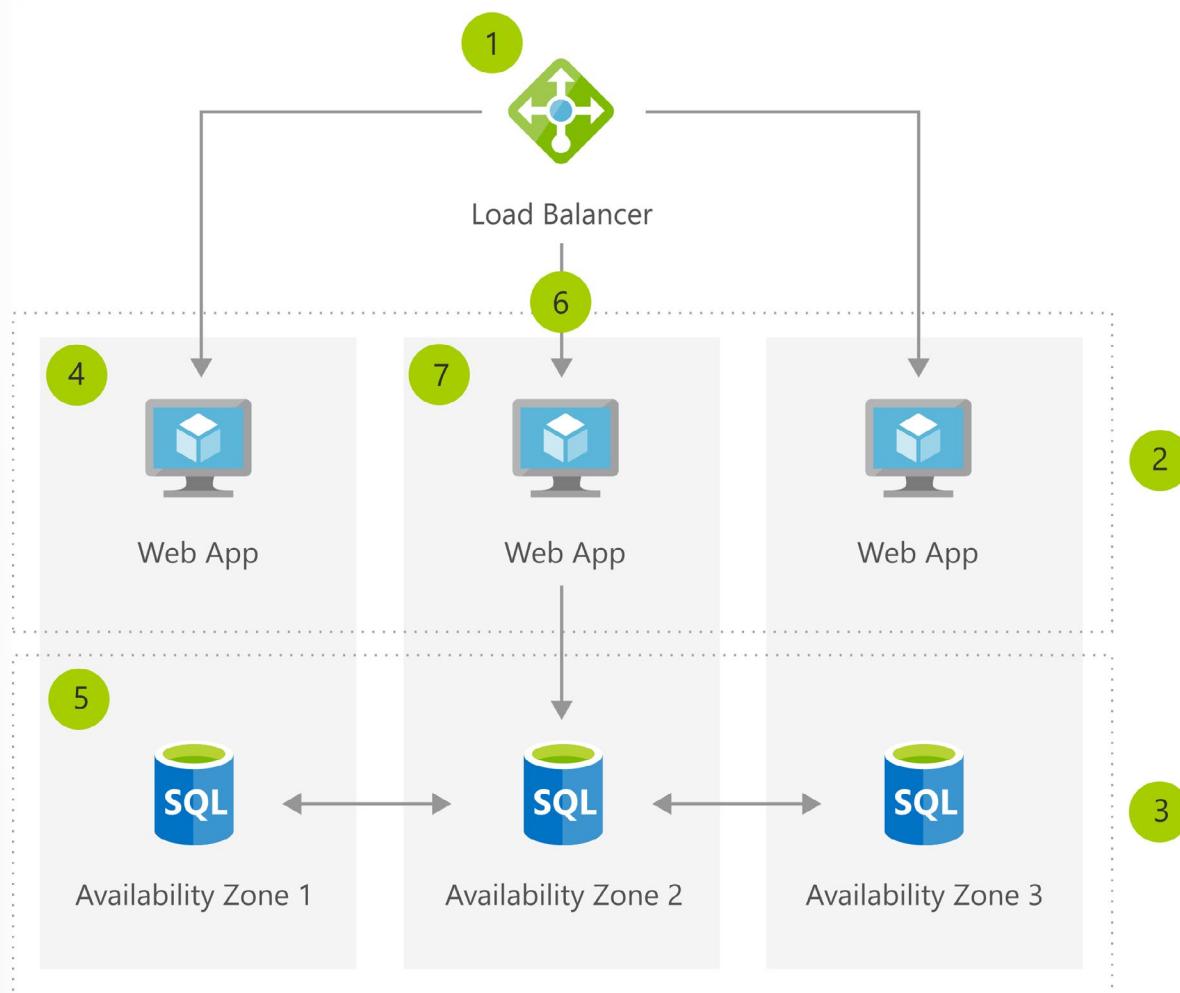
Using a VM workload as an example, a single VM has an SLA of 99.9%. This means the VM will be available 99.9% of the time. Within a single datacenter, the use of Availability Sets can increase the level of SLA to 99.95% by protecting a set of VMs, ensuring they will not all be on the same hardware. Within a region, VM workloads can be distributed across Availability Zones to increase the SLA to 99.99%. Every organization has unique requirements, and you should design your applications to best meet your complex business needs. Defining a target SLA will make it possible to evaluate whether the architecture meets your business requirements. Some things to consider include:

- What are the availability requirements?
- How much downtime is acceptable?
- How much will potential downtime cost your business?
- How much should you invest in making the application highly available?
- What are the data backup requirements?
- What are the data replication requirements?
- What are the monitoring requirements?
- Does your application have specific latency requirements?

## High Availability for Business Continuity and Disaster Recovery

Virtual machines (VMs) are physically separated across zones, and a virtual network is created using load balancers at each site. These locations are close enough for high availability replication, so your applications stay running, despite any issues at the physical locations.

## Architecture



## Data Flow

1. Create zone-redundant Load Balancer.
2. Create front-end subnet.
3. Create DB subnet.
4. Create VMs in three Availability Zones.
5. Configure zone-redundant SQL DB.
6. Add VMs to the load balancer's back-end pool.
7. Deploy your application on VMs for redundancy and high availability.

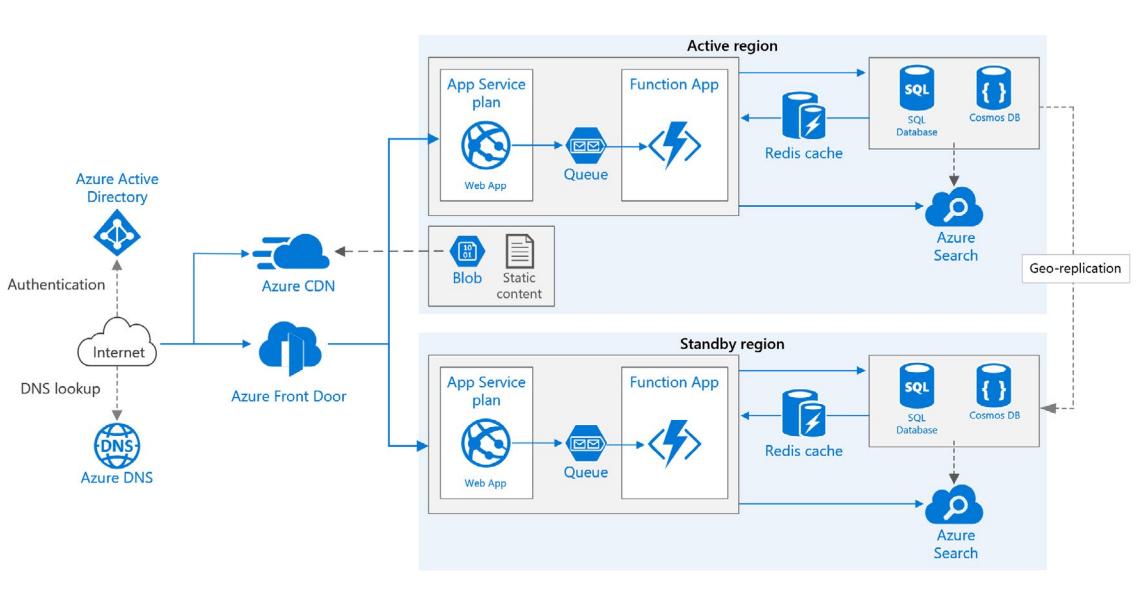
## Components

- **Virtual Machines:** Provision Windows and Linux virtual machines in seconds
- **Azure SQL Database:** Managed, intelligent SQL in the cloud
- **Load Balancer:** Deliver high availability and network performance to your applications

# Applications in Multiple Azure Regions for High Availability

## Multiple Azure Regions for High Availability

This reference architecture shows how to run an Azure App Service application in multiple regions to achieve high availability.



## Architecture

This architecture builds on the following:

- **Primary and secondary regions.** This architecture uses two regions to achieve higher availability. The application is deployed to each region. During normal operations, network traffic is routed to the primary region. If the primary region becomes unavailable, traffic is routed to the secondary region.
- **Front Door.** Front Door routes incoming requests to the primary region. If the application running that region becomes unavailable, Front Door fails over to the secondary region.
- **Geo-replication** of SQL Database and/or Cosmos DB.

A multi-region architecture can provide higher availability than deploying to a single region. If a regional outage affects the primary region, you can use Front Door to fail over to the secondary region. This architecture can also help if an individual subsystem of the application fails.

There are several general approaches to achieving high availability across regions:

- **Active/passive with hot standby.** Traffic goes to one region, while the other waits on hot standby. Hot standby means the VMs in the secondary region are allocated and running at all times.
- **Active/passive with cold standby.** Traffic goes to one region, while the other waits on cold standby. Cold standby means the VMs in the secondary region are not allocated until needed for failover. This approach costs less to run, but will generally take longer to come online during a failure.

- **Active/active.** Both regions are active, and requests are load balanced between them. If one region becomes unavailable, it is taken out of rotation.

This reference architecture focuses on active/passive with hot standby, using Front Door for failover.

## Recommendations

Your requirements might differ from the architecture described here. Use the recommendations in this section as a starting point.

### Regional pairing

Each Azure region is paired with another region within the same geography. In general, choose regions from the same regional pair (for example, East US 2 and Central US). Benefits of doing so include:

- If there is a broad outage, recovery of at least one region out of every pair is prioritized.
- Planned Azure system updates are rolled out to paired regions sequentially to minimize possible downtime.
- In most cases, regional pairs reside within the same geography to meet data residency requirements.

However, make sure that both regions support all of the Azure services needed for your application.

### Resource groups

Consider placing the primary region, secondary region, and Traffic Manager into separate resource groups. This lets you manage the resources deployed to each region as a single collection.

### Front Door configuration



**Routing.** Front Door supports several routing mechanisms. For the scenario described in this lesson use priority routing. With this setting, Front Door sends all requests to the primary region unless the endpoint for that region becomes unreachable. At that point, it automatically fails over to the secondary region. Set the backend pool with different priority values, 1 for the active region and 2 or higher for the standby or passive region.

**Health probe.** Front Door uses an HTTP (or HTTPS) probe to monitor the availability of each back end. The probe gives Front Door a pass/fail test for failing over to the secondary region. It works by sending a request to a specified URL path. If it gets a non-200 response within a timeout period, the probe fails.

As a best practice, create a health probe path in your application backend that reports the overall health of the application. This health probe should check critical dependencies such as the App Service apps, storage queue, and SQL Database. Otherwise, the probe might report a healthy backend when critical parts of the application are actually failing. On the other hand, don't use the health probe to check lower priority services.

## SQL Database

Use Active Geo-Replication to create a readable secondary replica in a different region. You can have up to four readable secondary replicas. Fail over to a secondary database if your primary database fails or needs to be taken offline. Active Geo-Replication can be configured for any database in any elastic database pool.

## Cosmos DB

Cosmos DB supports geo-replication across regions with multi-master (multiple write regions). Alternatively, you can designate one region as the writable region and the others as read-only replicas. If there is a regional outage, you can fail over by selecting another region to be the write region. The client SDK automatically sends write requests to the current write region, so you don't need to update the client configuration after a failover.

## Storage

For Azure Storage, use read-access geo-redundant storage (RA-GRS). With RA-GRS storage, the data is replicated to a secondary region. You have read-only access to the data in the secondary region through a separate endpoint. If there is a regional outage or disaster, the Azure Storage team might decide to perform a geo-failover to the secondary region. There is no customer action required for this failover.

For Queue storage, create a backup queue in the secondary region. During failover, the app can use the backup queue until the primary region becomes available again. That way, the application can still process new requests.

## RA-GRS Storage



RA-GRS storage provides durable storage, but it's important to understand what can happen during an outage:

- If a storage outage occurs, there will be a period of time when you don't have write-access to the data. You can still read from the secondary endpoint during the outage.
- If a regional outage or disaster affects the primary location and the data there cannot be recovered, the Azure Storage team may decide to perform a geo-failover to the secondary region.
- Data replication to the secondary region is performed asynchronously. Therefore, if a geo-failover is performed, some data loss is possible if the data can't be recovered from the primary region.
- Transient failures, such as a network outage, will not trigger a storage failover. Design your application to be resilient to transient failures. Mitigation options include:
  - Read from the secondary region.
  - Temporarily switch to another storage account for new write operations (for example, to queue messages).
  - Copy data from the secondary region to another storage account.
  - Provide reduced functionality until the system fails back.

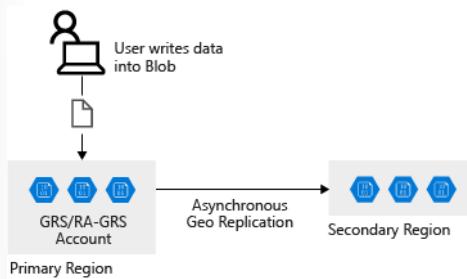
# Design HA Applications to Handle Disaster Recovery

## Design HA Applications to Handle Disaster Recovery

In this lesson, you look at how to design and configure an application that can handle disaster recovery and failover. You also explore the considerations that apply when you design applications for high availability.

### How an account failover works

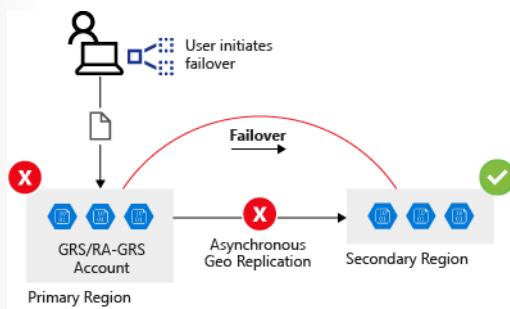
When you configure a storage account GRS or RA-GRS, the client writes data to the primary endpoint or region. The data is then automatically replicated across to the secondary region, as shown in the following image:



If the primary region that hosts your geo-redundant storage becomes unavailable, you can fail over to the secondary region.

When failover occurs, the secondary region becomes your new primary region, and all data is then accessible from this new primary region. All DNS records, which relate to your storage account, have their DNS endpoints updated to point to the new primary region. This redirection requires no changes to your application code.

A failure in the primary region is shown in the following image:



- Important Failover is automatic and controlled by Microsoft. A manual failover of an Azure storage account isn't possible in a majority of the Azure regions. However, Microsoft has made a new feature available in WestUS2 and CentralUS regions, with which you can manually failover the storage account by using the following command:

```
az storage account failover --name "storageaccountname"
```

## Implications of a storage account failover

When a storage account failover occurs, you could lose data. Data from the current primary region might not replicate across to the secondary region at the time of the failover. To determine whether there's likely to be data loss, you can check the Last Sync Time property. You used the command for finding this value in the previous exercise to review the storage account replication status.

# Best Practices for Cloud-based Applications with RA-GRS

When you develop applications for the cloud, consider the guidelines in the next sections.

## Retry transient failures

Transient failures can be caused by a number of conditions from a disconnected database, temporary loss of network, or latency issues that cause slow response times from services. Applications must detect the faults and determine whether it's merely a blip in the service or a more severe outage. The application must have the capability to retry a service if it believes the fault is likely to be transient, before listing it as failed.

## Handle failed writes

RA-GRS replicates writes across locations. If the primary location fails, you can direct read operations toward the secondary location. However, this secondary location is read-only. If a long-lasting outage (more than a few seconds) occurs at the primary location, your application must run in read-only mode. You can achieve read-only mode in several ways:

- Temporarily return an error from all write operations until write capability is restored.
- Buffer write operations, perhaps by using a queue, and enact them later when the write location becomes available.
- Write updates to a different storage account in another location. Merge these changes into the storage account at the primary location when it becomes available.
- Trigger the application to disable all write operations, and inform the user that the application is running in read-only mode. You can also use this mechanism if you need to upgrade the application and ensure that no-one is using the primary location while the upgrade is taking place.

An application that uses the Azure Storage client library can set the LocationMode of a read request to one of the following values:

- **PrimaryOnly**: The read request fails if the primary location is unavailable. This failure is the default behavior.
- **PrimaryThenSecondary**: Try the primary location first, and then try the secondary location if the primary location is unavailable. Fail if the secondary location is also unavailable.
- **SecondaryOnly**: Try only the secondary location, and fail if it's not available.
- **SecondaryThenPrimary**: Try the secondary location first, and then try the primary location.

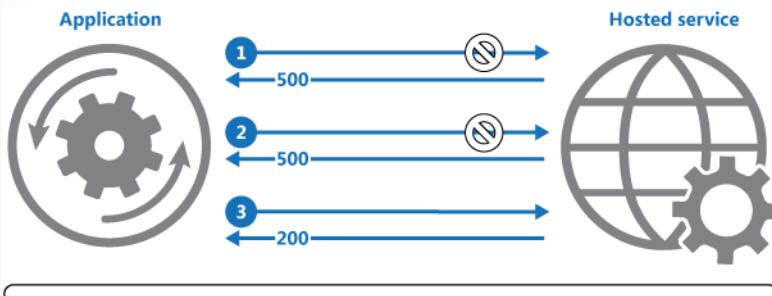
## Retry Pattern

Transient faults aren't uncommon and an application should be designed to handle them elegantly and transparently. This minimizes the effects faults can have on the business tasks the application is performing.

If an application detects a failure when it tries to send a request to a remote service, it can handle the failure using the following strategies:

- **Cancel.** If the fault indicates that the failure isn't transient or is unlikely to be successful if repeated, the application should cancel the operation and report an exception. For example, an authentication failure caused by providing invalid credentials is not likely to succeed no matter how many times it's attempted.
- **Retry.** If the specific fault reported is unusual or rare, it might have been caused by unusual circumstances such as a network packet becoming corrupted while it was being transmitted. In this case, the application could retry the failing request again immediately because the same failure is unlikely to be repeated and the request will probably be successful.
- **Retry after delay.** If the fault is caused by one of the more commonplace connectivity or busy failures, the network or service might need a short period while the connectivity issues are corrected or the backlog of work is cleared. The application should wait for a suitable time before retrying the request.

The following diagram illustrates invoking an operation in a hosted service using this pattern. If the request is unsuccessful after a predefined number of attempts, the application should treat the fault as an exception and handle it accordingly.



- 1: Application invokes operation on hosted service. The request fails, and the service host responds with HTTP response code 500 (internal server error).
- 2: Application waits for a short interval and tries again. The request still fails with HTTP response code 500.
- 3: Application waits for a longer interval and tries again. The request succeeds with HTTP response code 200 (OK).

## Handle eventual consistency

Be prepared to handle stale data if it's read from a secondary region. As previously described, it takes time to replicate data between regions, and an outage can occur between the time when data is written to the primary location and it's replicated to each secondary location.

## The Circuit Breaker Pattern

In some situations, when an outage is severe, it makes sense for the application to stop retrying the operation and instead start failover to a secondary site.

To prevent an application from retrying operations that have failed, you can implement the Circuit Breaker pattern.

The Circuit Breaker pattern forces the application to fail over to the secondary site, which allows the application to resume its normal service. At the same time, the circuit breaker continues to check on whether the resources on the primary site are back online. And when they do come online, it allows the application to reconnect to the primary site. The circuit breaker acts as a proxy. It monitors the service, and if there's a failure in the service, it prevents the application from retrying that endpoint and forces it to go to an alternative endpoint.

The difference between the Circuit Breaker pattern and the Retry pattern is that the Retry pattern allows an application to keep retrying a connection to a resource, which might be offline. The Circuit Breaker pattern prevents this behavior and fails over the application to the secondary connection.

The purpose of implementing a Circuit Breaker pattern is to provide stability to your application while the system recovers from a failure.

Use the Circuit Breaker pattern to prevent an application from trying connections to resources that have failed and, instead, to minimize disruption by redirecting the connection to working resources. Don't use the Circuit Breaker pattern for accessing local or in-memory data structures, because circuit breakers would add overhead to the system.

When you implement the Circuit Breaker pattern, set the *LocationMode* of read requests appropriately. Most of the time, you should set this mode to *PrimaryThenSecondary*. If the read from the primary location times out, the secondary location is used. However, this process can slow down an application if it's done repeatedly. After the circuit breaker has detected that the primary location is unavailable, it should switch the mode to *SecondaryOnly*. This action ensures that read operations don't wait for a timeout from the primary location before trying the secondary location.

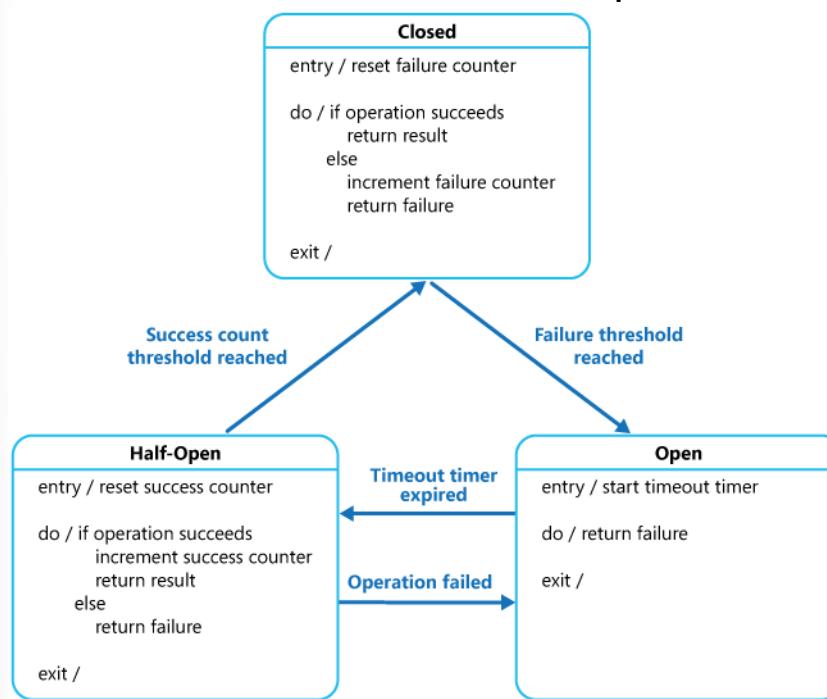
A circuit breaker acts as a proxy for operations that might fail. The proxy should monitor the number of recent failures that have occurred, and use this information to decide whether to allow the operation to proceed, or simply return an exception immediately.

The proxy can be implemented as a state machine with the following states that mimic the functionality of an electrical circuit breaker:

- **Closed:** The request from the application is routed to the operation.
- **Open:** The request from the application fails immediately and an exception is returned to the application.
- **Half-Open:** A limited number of requests from the application are allowed to pass through and invoke the operation

In the figure below, the failure counter used by the **Closed** state is time based. It's automatically reset at periodic intervals. This helps to prevent the circuit breaker from entering the **Open** state if it experiences occasional failures. The failure threshold that trips the circuit breaker into the **Open** state is only reached when a specified number of failures have occurred during a specified interval. The counter used by the **Half-Open** state records the number of successful attempts to invoke the operation. The circuit breaker reverts to the **Closed** state after a specified number of consecutive operation invocations have been successful. If any invocation fails, the circuit breaker enters the Open state immediately and the success

counter will be reset the next time it enters the **Half-Open** state.



# Module 11 Review Questions

## Module 11 Review Questions



### Review Question 1

You need recommend a strategy for moving a Web app named WebApp4 from an on-premises data center to Azure.

WebApp4 is dependent on an extension that is installed on the host server.

You need to recommend a solution for hosting WebApp4 in Azure. The recommendation should fulfill the following:

- WebApp4 must be available to users if an Azure data center becomes unavailable.
- Cost should be minimized.

What should your recommendation include?

- In two Azure regions, deploy a load balancer and a virtual machine scale set.
- Deploy a load balancer and a virtual machine scale set across two availability zones.
- In two Azure regions, deploy a load balancer and a web app.
- In two Azure regions, deploy a Traffic Manager profile and a web app.

### Review Question 2

You are recommending a plan for deploying 15 applications to Azure.

The applications will be deployed to two Azure Kubernetes Service clusters. Each cluster will be deployed to a separate Azure region.

The application deployment must meet the following requirements:

- Ensure that the applications remain available if a single AKS cluster fails.
- Ensure that the connection traffic over the internet is encrypted by using SSL without having to configure SSL on each container instance.

Which Azure service should you include in your recommendation?

- AKS ingress controller
- Azure Front Door
- Azure Traffic Manager
- Azure Load Balancer

## Review Question 3

You advise a company that plans to deploy multiple instances of an Azure web app across multiple regions. You need to recommend an access solution for the Azure web app.

The recommendation must fulfill the following

- Include rate limiting
- Balance all requests between all instances
- Allow that users to access the Azure web app even during a regional outage

You recommend using Azure Front Door to provide access to the Azure web app.

Does your recommendation meet the requirements?

- Yes  
 No

# Answers

## Review Question 1

You need recommend a strategy for moving a Web app named WebApp4 from an on-premises data center to Azure.

WebApp4 is dependent on an extension that is installed on the host server.

You need to recommend a solution for hosting WebApp4 in Azure. The recommendation should fulfill the following:

What should your recommendation include?

- In two Azure regions, deploy a load balancer and a virtual machine scale set.
- Deploy a load balancer and a virtual machine scale set across two availability zones.
- In two Azure regions, deploy a load balancer and a web app.
- In two Azure regions, deploy a Traffic Manager profile and a web app.

### Explanation

*Correct Answer: Deploy a load balancer and a virtual machine scale set across two availability zones. Using a virtual machine scale set across two or more zones in a single region meets the requirement. Using a single load balancer to allow traffic to reach the endpoints is the most cost-effective solution.*

## Review Question 2

You are recommending a plan for deploying 15 applications to Azure.

The applications will be deployed to two Azure Kubernetes Service clusters. Each cluster will be deployed to a separate Azure region.

The application deployment must meet the following requirements:

Which Azure service should you include in your recommendation?

- AKS ingress controller
- Azure Front Door
- Azure Traffic Manager
- Azure Load Balancer

### Explanation

*Correct Answer: Azure Front Door. Azure Front Door Service enables you to define, manage, and monitor the global routing for web traffic by optimizing for performance and instant global failover for high availability. Azure Front Door can also terminate Secure Sockets Layer (SSL) sessions.*

## Review Question 3

You advise a company that plans to deploy multiple instances of an Azure web app across multiple regions.

You need to recommend an access solution for the Azure web app.

The recommendation must fulfill the following

You recommend using Azure Front Door to provide access to the Azure web app.  
Does your recommendation meet the requirements?

- Yes
- No

*Explanation*

*Correct answer: Yes. Front Door. Front Door routes incoming requests to the primary region. If the application running that region becomes unavailable, Front Door fails over to the secondary region.*

## Module 12 Design for Cost Optimization

### Recommend Solutions for Cost Management

#### Azure Cost Management

Cost management is the process of effectively planning and controlling costs involved in your business. Cost management tasks are normally performed by finance, management, and app teams. Azure **Cost Management + Billing** helps organizations plan with cost in mind. It also helps to analyze costs effectively and take action to optimize cloud spending.

Subscription name	Subscription ID	Status	Last billed amount	Due date
Azure Pass - Sponsorship		Active	Not available	Not available

Cost Management shows organizational cost and usage patterns with advanced analytics. Reports in Cost Management show the usage-based costs consumed by Azure services and third-party Marketplace offerings. Costs are based on negotiated prices and factor in reservation and Azure Hybrid Benefit discounts. Collectively, the reports show your internal and external costs for usage and Azure Marketplace charges. Other charges, such as reservation purchases, support, and taxes are not yet shown in reports.

The reports help you understand your spending and resource use and can help find spending anomalies. Predictive analytics are also available. Cost Management uses Azure management groups, budgets, and recommendations to show clearly how your expenses are organized and how you might reduce costs.

## Plan and control expenses

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

The screenshot shows the Microsoft Azure Cost Management + Billing Overview page. The left sidebar includes sections for Cost Management (Cost analysis, Cost alerts, Budgets, Advisor recommendations, Cloudyn), Settings (Exports, Connectors for AWS (Preview)), and Support + troubleshooting (New support request). The main content area features a heading 'Analyze and optimize cloud costs' with a sub-section 'Visualize and monitor your cloud costs and trends, improve your organizational accountability, and optimize your cloud efficiency. Learn more'. Below this are three cards: 'Analyze cloud costs' (Break down and analyze costs to identify anomalies and drive a deeper understanding of cost and usage patterns. Learn more), 'Monitor with budgets' (Create a budget to control costs and configure alerts to warn teams about impending budget overages. Learn more), and 'Optimize with recommendations' (View Advisor recommendations to identify unused or underutilized resources. Take action to reduce waste. Learn more).

You use **cost analysis** to explore and analyze your organizational costs. You can view aggregated costs by organization to understand where costs are accrued and to identify spending trends. And you can see accumulated costs over time to estimate monthly, quarterly, or even yearly cost trends against a budget.

**Budgets** help you plan for and meet financial accountability in your organization. They help prevent cost thresholds or limits from being surpassed. Budgets can also help you inform others about their spending to proactively manage costs. And with them, you can see how spending progresses over time.

**Recommendations** show how you can optimize and improve efficiency by identifying idle and underutilized resources. Or, they can show less expensive resource options. When you act on the recommendations, you change the way you use your resources to save money. To act, you first view cost optimization recommendations to view potential usage inefficiencies. Next, you act on a recommendation to modify your Azure resource use to a more cost-effective option. Then you verify the action to make sure that the change you make is successful.

If you use external systems to access or review cost **management data**, you can easily export the data from Azure. And you can set a daily scheduled export in CSV format and store the data files in Azure storage. Then, you can access the data from your external system.

## Optimize with Azure Cost Management



Azure Cost Management gives you the tools to plan for, analyze and reduce your spending to maximize your cloud investment.

This topic provides an approach to cost management and highlights the tools available to you as you address your organization's cost challenges.

It's important that solutions are optimized to minimize the cost to your organization. Following the principles outlined in this section and using our tools will help to make sure your organization is prepared for success.

## Methodology

Cost management is an organizational problem and should be an ongoing practice that begins before you spend money on cloud resources.

To successfully implement cost management and optimize costs, your organization must:

- Be prepared with the proper tools for success
- Be accountable for costs
- Take appropriate action to optimize spending

Three key groups, outlined below, must be aligned in your organization to make sure that you successfully manage costs.

- **Finance** - People responsible for approving budget requests across the organization based on cloud spending forecasts. They pay the corresponding bill and assign costs to various teams to drive accountability.
- **Managers** - Business decision makers in an organization that need to understand cloud spending to find the best spending results.
- **App teams** - Engineers managing cloud resources on a day-to-day basis, developing services to meet the organization's needs. These teams need the flexibility to deliver the most value in their defined budgets.

## Cost Design Principles

Use the principles outlined below to position your organization for success in cloud cost management.

### Planning

Comprehensive, up-front planning allows you to tailor cloud usage to your specific business requirements. Ask yourself:

- What business problem am I solving?
- What usage patterns do I expect from my resources?

Your answers will help you select the offerings that are right for you. They determine the infrastructure to use and how it's used to maximize your Azure efficiency.

### Visibility

When structured well, Cost Management helps you to inform people about the Azure costs they're responsible for or for the money they spend. Azure has services designed to give you insight into where your money is spent. Take advantage of these tools. They can help you find resources that are underused, remove waste, and maximize cost-saving opportunities.

## Accountability

Attribute costs in your organization to make sure that people responsible are accountable for their team's spending. To fully understand your organization's Azure spending, you should organize your resources to maximize insight into cost attribution. Good organization helps to manage and reduce costs and hold people accountable for efficient spending in your organization.

## Optimization

Act to reduce your spending. Make the most of it based on the findings gathered through planning and increasing cost visibility. You might consider purchase and licensing optimizations along with infrastructure deployment changes that are discussed in detail later in this lesson.

## Iteration

Everyone in your organization must engage in the cost management lifecycle. They need to stay involved on an ongoing basis to optimize costs. Be rigorous about this iterative process and make it a key tenet of responsible cloud governance in your organization.

Publisher type	Charge type	Service name	Service tier	Cost
azure	usage	log analytics	all	\$11,053.43
azure	usage	virtual machines	dv2/dsv2 series	\$7,509.44
azure	usage	storage	premium ssd managed disks	\$4,302.19
azure	usage	virtual machines	dv2/dsv2 series windows	\$2,698.49
azure	usage	storage	premium page blob	\$2,570.43
azure	usage	azure firewall	all	\$1,932.05
azure	usage	azure app service	standard plan	\$1,545.60
azure	usage	azure cosmos db	all	\$1,410.79
azure	usage	virtual machines	dv3/dsv3 series windows	\$1,333.03
azure	usage	virtual machines	a series windows	\$816.66
azure	usage	vnet gateway	high performance gateway	\$757.17
azure	usage	storage	standard hdd managed disks	\$735.51

## Design with Cost in Mind

Before you deploy cloud resources, assess the following items:

- The Azure offer that best meets your needs
- The resources you plan to use
- How much they might cost

Azure provides tools to assist you in the assessment process. The tools can give you a good idea of the investment required to enable your workloads. Then you can select the best configuration for your situation.

## Azure onboarding options

The first step in maximizing your experience within Cost Management is to investigate and decide which Azure offer is best for you. Think about how you plan to use Azure in the future. Also consider how you want your billing model configured.

Below is a quick review of the common billing models.

### Pay as you go

- No minimums or commitments
- Competitive Pricing
- Pay only for what you use
- Cancel anytime

### Enterprise Agreement

- Options for up-front monetary commitments
- Access to reduced Azure pricing

### Azure in CSP

- CSP partners are the first point of contact for their customers' needs and the center of the customer relationship
- CSP partners provision new customers, order subscriptions, manage subscriptions, and perform admin tasks on behalf of their customers
- CSP partners bundle services with unique solutions or resell Azure while controlling the pricing, terms and billing

## Estimate the cost of the solution

Before you deploy any infrastructure, assess how much your solution will cost. The assessment will help you create a budget for your organization for the workload, up-front. Then you can use a budget over time to benchmark the validity of your initial estimation. And you can compare it with the actual cost of your deployed solution.

## Azure pricing calculator

The Azure pricing calculator allows you to mix and match different combinations of Azure services to see an estimate of the costs. You can implement your solution using different ways in Azure - each might influence your overall spending. Thinking early about all of the infrastructure needs of your cloud deployment helps you use the tool most effectively. It can help you get a solid estimate of your estimated spending in Azure.

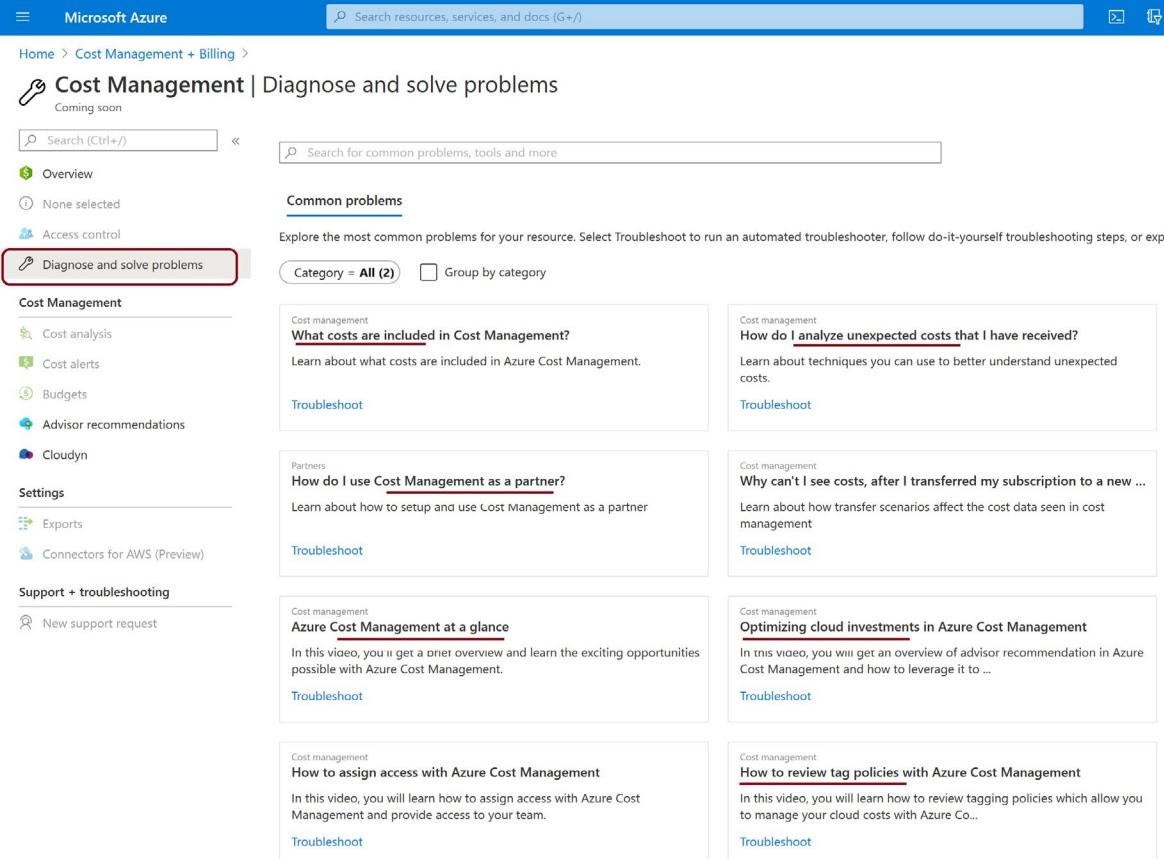
## Azure Migrate

Azure Migrate is a service that assesses your organization's current workloads in on-premises data-centers. It gives you insight into what you might need from an Azure replacement solution. First, Migrate analyzes your on-premises machines to determine whether migration is feasible. Then, it recommends VM sizing in Azure to maximize performance. Finally, it also creates a cost estimate for an Azure-based solution.

## Analyze and Manage Costs

Keep informed about how your organization's costs evolve over time. Use the following techniques to properly understand and manage your spending.

One way to understand where costs are associated with subscriptions, partners, and unexpected costs, see **Diagnose and solve problems**.



The screenshot shows the Microsoft Azure Cost Management interface. The top navigation bar includes 'Microsoft Azure', a search bar, and various icons. Below the navigation is a breadcrumb trail: Home > Cost Management + Billing > Cost Management | Diagnose and solve problems. A message 'Coming soon' is displayed above the main content area. On the left, a sidebar lists sections: Cost Management (Cost analysis, Cost alerts, Budgets, Advisor recommendations, Cloudyn), Settings (Exports, Connectors for AWS (Preview)), and Support + troubleshooting (New support request). The main content area is titled 'Common problems' and contains several cards. One card for 'Cost management' has its title 'What costs are included in Cost Management?' highlighted with a red box. Other cards include 'How do I analyze unexpected costs that I have received?', 'How do I use Cost Management as a partner?', 'Optimizing cloud investments in Azure Cost Management', and 'How to review tag policies with Azure Cost Management'. Each card has a 'Troubleshoot' link at the bottom.

## Organize and tag resources

Organize your resources with cost in mind. As you create subscriptions and resource groups, think about the teams that are responsible for associated costs. Make sure your reporting keeps your organization in mind. Subscriptions and resource groups provide good buckets to organize and attribute spending across your organization. Tags provide a good way to attribute cost. You can use tags as a filter. And you can use them to group by when you analyze data and investigate costs. Enterprise Agreement customers can also create departments and place subscriptions under them. Cost-based organization in Azure helps keep the relevant people in your organization accountable for reducing their team's spending.

## Use cost analysis

Cost analysis allows you to analyze your organizational costs in-depth by slicing and dicing your costs using standard resource properties. Consider the following common questions as a guide for your

analysis. Answering these questions on a regular basis will help you stay more informed and enable more cost-conscious decisions.

- Estimated costs for the current month – How much have I incurred so far this month? Will I stay under my budget?
- Investigate anomalies – Do routine checks to make sure that costs stay within a reasonable range of normal usage. What are the trends? Are there any outliers?
- Invoice reconciliation - Is my latest invoiced cost more than the previous month? How did spending habits change month-over-month?
- Internal chargeback - Now that I know how much I'm being charged, how should those charges be broken down for my organization?

## Export billing data on a schedule

Do you need to import your billing data into an external system, like a dashboard or financial system? Set up automated exports to Azure Storage and avoid manually downloading files every month. You can then easily set up automatic integrations with other systems to keep your billing data in sync.

## Create budgets

After you've identified and analyzed your spending patterns, it's important to begin setting limits for yourself and your teams. Azure budgets give you the ability to set either a cost or usage-based budget with many thresholds and alerts. Make sure to review the budgets that you create regularly to see your budget burn-down progress and make changes as needed. Azure budgets also allow you to configure an automation trigger when a given budget threshold is reached. For example, you can configure your service to shut down VMs. Or you can move your infrastructure to a different pricing tier in response to a budget trigger.

## Act to Optimize

Use the following ways to optimize spending.

## Cut out waste

After you've deployed your infrastructure in Azure, it's important to make sure it is being used. The easiest way to start saving immediately is to review your resources and remove any that aren't being used. From there, you should determine if your resources are being used as efficiently as possible.

## Azure Advisor

Azure Advisor is a service that, among other things, identifies virtual machines with low utilization from a CPU or network usage standpoint. From there, you can decide to either shut down or resize the machine based on the estimated cost to continue running the machines. Advisor also provides recommendations for reserved instance purchases. The recommendations are based on your last 30 days of virtual machine usage. When acted on, the recommendations can help you reduce your spending.

## Size VMs properly

VM sizing has a significant impact on your overall Azure cost. The number of VMs needed in Azure might not equate to what you currently have deployed in an on-premises datacenter. Make sure you choose the right size for the workloads that you plan to run.

## Use purchase discounts

Azure has many discounts that your organization should take advantage of to save money.

## Azure Reservations

Azure Reservations allow you to prepay for one-year or three-years of virtual machine or SQL Database compute capacity. Pre-paying will allow you to get a discount on the resources you use. Azure reservations can significantly reduce your virtual machine or SQL database compute costs — up to 72 percent on pay-as-you-go prices with one-year or three-year upfront commitment. Reservations provide a billing discount and don't affect the runtime state of your virtual machines or SQL databases.

## Use Azure Hybrid Benefit

If you already have Windows Server or SQL Server licenses in your on-premises deployments, you can use the Azure Hybrid Benefit program to save in Azure. With the Windows Server benefit, each license covers the cost of the OS (up to two virtual machines), and you only pay for base compute costs. You can use existing SQL Server licenses to save up to 55 percent on vCore-based SQL Database options. Options include SQL Server in Azure Virtual Machines and SQL Server Integration Services.

For more information, see [Azure Hybrid Benefit savings calculator<sup>1</sup>](#).

## Demonstration - Optimize Costs from Recommendations

This demonstration walks you through an example where you identify underutilized Azure resources and then you take action to reduce costs.

- View cost optimization recommendations to view potential usage inefficiencies
- Act on a recommendation to resize a virtual machine to a more cost-effective option
- Verify the action to ensure that the virtual machine was successfully resized
- Subscription
- Resource group

## View cost optimization recommendations

Sign in to the Azure portal at <https://portal.azure.com<sup>2</sup>>.

To view cost optimization recommendations for a subscription, open the desired scope in the Azure portal and select **Advisor**.

---

<sup>1</sup> <https://azure.microsoft.com/pricing/hybrid-benefit/>

<sup>2</sup> <https://portal.azure.com/>

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a search bar and a navigation bar with 'Microsoft Azure' and 'All services'. Below the search bar, there are two tabs: 'Overview' (selected) and 'Featured'. The 'Featured' tab includes icons for various services like Virtual machines, App Services, Storage accounts, etc., with 'Advisor' being the one highlighted by a red box. To the right of the featured services is a 'Free training from Microsoft' section with three cards: 'Core Cloud Services - Azure architecture and service guarantees', 'Core Cloud Services - Manage services with the Azure portal', and 'Cloud Concepts - Principles of cloud computing'. On the left, there's a sidebar titled 'Categories' with a long list of service names.

To view recommendations for a management group, open the desired scope in the Azure portal and select **Cost** in the menu.

The screenshot shows the 'Advisor' service page in the Azure portal. The URL is 'All services > Advisor'. The left sidebar has a 'Recommendations' section with 'Cost' selected (highlighted by a red box). Other options in this section include Security, High Availability, Operational Excellence, Performance, and All recommendations. Below this are sections for Monitoring, Alerts (Preview), and Recommendation digests. The main content area shows five cards: 'Cost' (You are following all of our cost recommendations), 'Security' (You are following all of our security recommendations), 'High Availability' (3 Recommendations: 0 High impact, 3 Medium impact, 0 Low impact), 'Operational Excellence' (You are following all of our operational excellence recommendations), and 'Performance' (You are following all of our performance recommendations).

The list of recommendations identifies usage inefficiencies or shows purchase recommendations that can help you save additional money. The totaled **Potential yearly savings** shows the total amount that you can save if you shut down or deallocate all of your VMs that meet recommendation rules.

The **Impact** category, along with the **Potential yearly savings**, are designed to help identify recommendations that have the potential to save as much as possible.

## Act on a recommendation

Azure Advisor monitors virtual machine usage for seven days and then identifies underutilized virtual machines. Virtual machines whose CPU utilization is five percent or less and network usage is seven MB or less for four or more days are considered low-utilization virtual machines.

The 5% or less CPU utilization setting is the default, but you can adjust the settings.

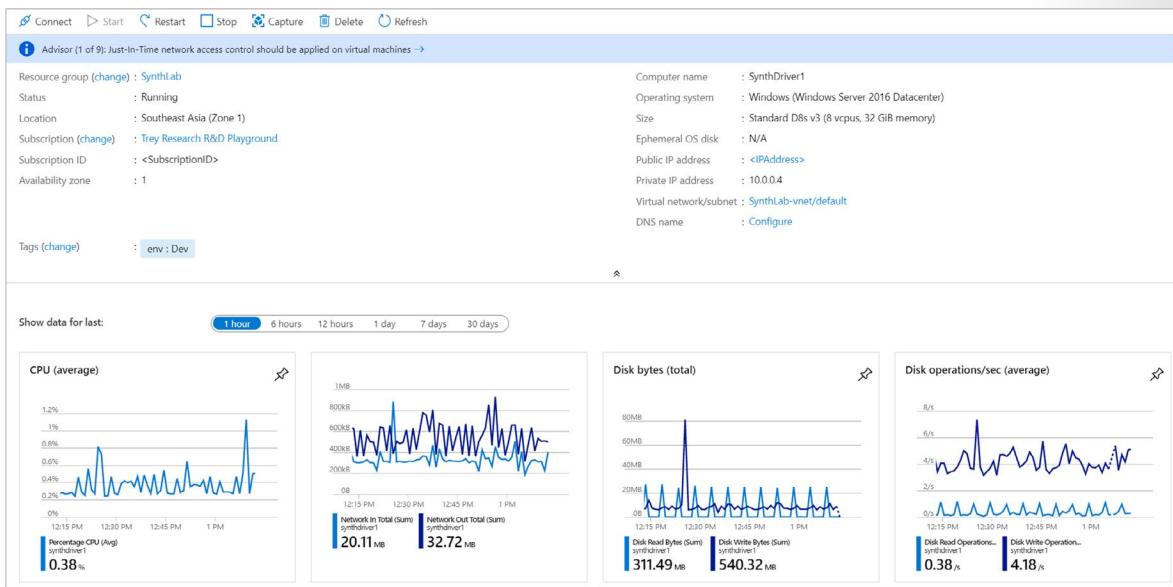
Although some scenarios can result in low utilization by design, you can often save money by changing the size of your virtual machines to less expensive sizes. Your actual savings might vary if you choose a resize action. Let's walk through an example of resizing a virtual machine.

In the list of recommendations, click the **Right-size or shutdown underutilized virtual machines** recommendation. In the list of virtual machine candidates, choose a virtual machine to resize and then click the virtual machine.

The screenshot shows the Azure Advisor interface for managing virtual machine recommendations. At the top, there are download and alert configuration options. Below that, a summary section indicates potential yearly savings of **5,972.83 USD**. The main table lists two virtual machines:

SELECT	VIRTUAL MACHINE	RECOMMENDED ACTIONS	POTENTIAL SAVINGS*	SUBSCRIPTION	RECOMMENDATION RULE	UPDATED AT	ACTION
<input type="checkbox"/>	SynthDriver1	Resize Standard_D8s_v3 to Standard_D2s_v3 View Usage Patterns	<b>3,348.00 USD</b> (75%)	Trey Research R&D Playground	CPU utilization < 20%	10/24/2019, 9:23:23 AM	<a href="#">Postpone</a>   <a href="#">Dismiss</a>
<input type="checkbox"/>	testAvi	Resize Standard_DS12_v2 to Standard_DS2_v2 View Usage Patterns	<b>2,624.83 USD</b> (63%)	Trey Research R&D Playground	CPU utilization < 20%	10/24/2019, 9:30:48 AM	<a href="#">Postpone</a>   <a href="#">Dismiss</a>

In the VM details, check the utilization of the virtual machine to confirm that it's a suitable resize candidate.



Note the current virtual machine's size. After you've verified that the virtual machine should be resized, close the VM details so that you see the list of virtual machines.

In the list of candidates to shut down or resize, select **ResizeFromVirtualMachineSKU** to **ToVirtualMachineSKU**.

Next, you're presented with a list of available resize options. Choose the one that will give the best performance and cost-effectiveness for your scenario.

After you choose a suitable size, click **Resize** to start the resize action.

The screenshot shows a list of available VM sizes for resizing. At the top, there are filters: 'Search by VM size...', 'Clear all filters', 'Size : Small (0-6)', 'Generation : 2 selected', 'Family : General purpose', 'Premium disk : Supported', and 'Add filter'. Below these, it says 'Showing 11 of 101 VM sizes.' and lists the following table:

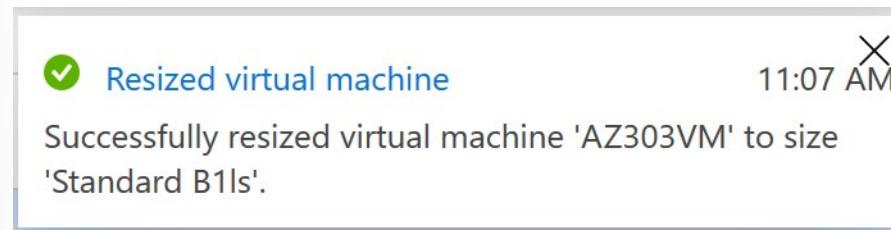
VM Size ↑	Offering ↑	Family ↑	vCPUs ↑	RAM (GiB) ↑	Data disks ↑	Max IOPS ↑	Temporary storage (GiB) ↑	Premium disk support ↑	Cost/month (estimated) ↑
B1ls	Standard	General purpose	1	0.5	2	160	4	Yes	\$7.15
B1ms	Standard	General purpose	1	2	2	640	4	Yes	\$17.96
B1s	Standard	General purpose	1	1	2	320	4	Yes	\$10.22
B2ms	Standard	General purpose	2	8	4	1920	16	Yes	\$66.58
B2s	Standard	General purpose	2	4	4	1280	8	Yes	\$36.21
B4ms	Standard	General purpose	4	16	8	2880	32	Yes	\$132.86
D2s_v3	Standard	General purpose	2	8	4	3200	16	Yes	\$137.24
D4s_v3	Standard	General purpose	4	16	8	6400	32	Yes	\$274.48
DS1_v2	Standard	General purpose	1	3.5	4	3200	7	Yes	\$91.98
DS2_v2	Standard	General purpose	2	7	8	6400	14	Yes	\$183.96
DS3_v2	Standard	General purpose	4	14	16	12800	28	Yes	\$367.92

At the bottom left, there's a red-bordered button labeled 'Resize'. A note below the table states: 'Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. [View Azure pricing calculator](#)'.

Resizing requires an actively running virtual machine to restart.

## Verify the action

When the VM resizing completes successfully, an Azure notification is shown.



# Recommendations for Minimizing Costs

## View Cost Breakdown by Azure Service

Viewing costs by an Azure service can help you to better understand the parts of an infrastructure that cost the most. For example, VM compute costs might be small. Yet you might accrue significant networking costs because of the amount of information emitting from the VMs.

1. In the Azure portal, navigate to cost analysis for your scope. For example: **Cost Management + Billing > Cost Management > Cost analysis**.
2. Select **Cost by service** and then group by **Service tier**.
3. Change the view to **Table**.

The screenshot shows the Azure portal's Cost analysis blade for the scope 'Contoso IT - demo'. The 'Cost by service' view is selected. The table is grouped by 'Service tier'. The 'Table' view is highlighted with a red box.

Publisher type	Charge type	Service name	Service tier	Cost
azure	usage	log analytics	all	\$11,053.43
azure	usage	virtual machines	dv2/dsv2 series	\$7,509.44
azure	usage	storage	premium ssd managed disks	\$4,302.19
azure	usage	virtual machines	dv2/dsv2 series windows	\$2,698.49
azure	usage	storage	premium page blob	\$2,570.43
azure	usage	azure firewall	all	\$1,932.05
azure	usage	azure app service	standard plan	\$1,545.60
azure	usage	azure cosmos db	all	\$1,410.79
azure	usage	virtual machines	dv3/dsv3 series windows	\$1,333.03
azure	usage	virtual machines	a series windows	\$816.66
azure	usage	vnet gateway	high performance gateway	\$757.17
azure	usage	storage	standard hdd managed disks	\$735.51

## Review Invoiced Charges in Cost Analysis

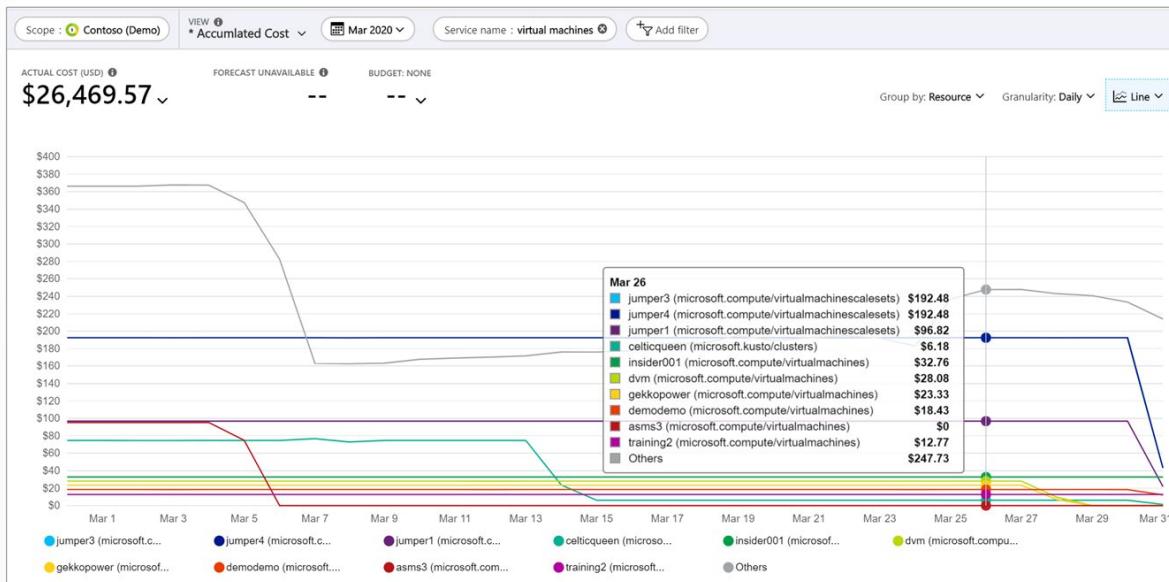
To view invoice details in the Azure portal, navigate to Cost analysis for the scope associated with the invoice that you're analyzing. Select the **Invoice details** view. Invoice details show you the charges as seen on the invoice.

The screenshot shows the Azure portal's Cost analysis blade for the scope 'Contoso (Demo)'. The 'Invoice details' view is selected. The table is grouped by 'Meter'. The 'Table' view is highlighted with a red box.

Publisher type	Charge type	Service name	Service tier	Meter	Part Number	Cost
azure	usage	virtual machines	fsv2 series windows vm	f72s v2	aad-10036	\$11,634.61
azure	usage	azure stack hub	azure stack-windows vm	1 core	aaa-56070	\$9,432.73
azure	usage	hdinsight	hdinsight d series	d4	n7h-01995	\$7,455.47
azure	usage	expressroute	expressroute	premium metered data 10 gbp...	j2q-00792	\$6,398.39
azure	usage	virtual machines licenses	sql server ent	16 vcpu vm license	n7h-07116	\$3,936.78
azure	usage	virtual machines	dv2 series windows vm	d15 v2/dsv15 v2	aaa-14527	\$2,926.18
azure	usage	sql database	sql db single/elastic pool gen ...	vcore	aad-17849	\$2,832.64

Viewing invoice details, you can identify the service that has unexpected costs and determine which resources are directly associated with the resource in Cost analysis. For example, if you want to analyze

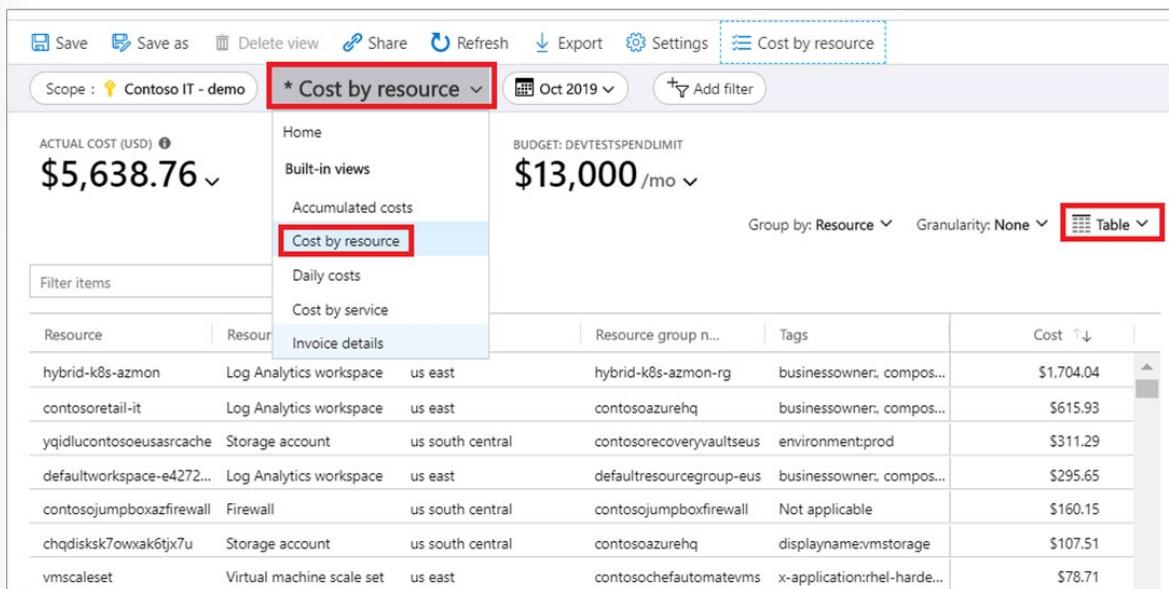
charges for the Virtual Machines service, navigate to the **Accumulated cost** view. Then, set the granularity to **Daily** and filter charges **Service name: Virtual machines** and group charges by **Resource**.



## View Cost Breakdown by Azure Resource

Services are built with Azure resources. Reviewing costs based on resources can help you quickly identify the primary cost contributors. If a service has resources that are too expensive, consider making changes to reduce costs.

- In the Azure portal, navigate to cost analysis for scope. For example: **Cost Management + Billing > Cost Management > Cost analysis**.
- Select **Cost by resource**.
- Change the view to **Table**.



## View Cost Breakdown by Selected Dimensions

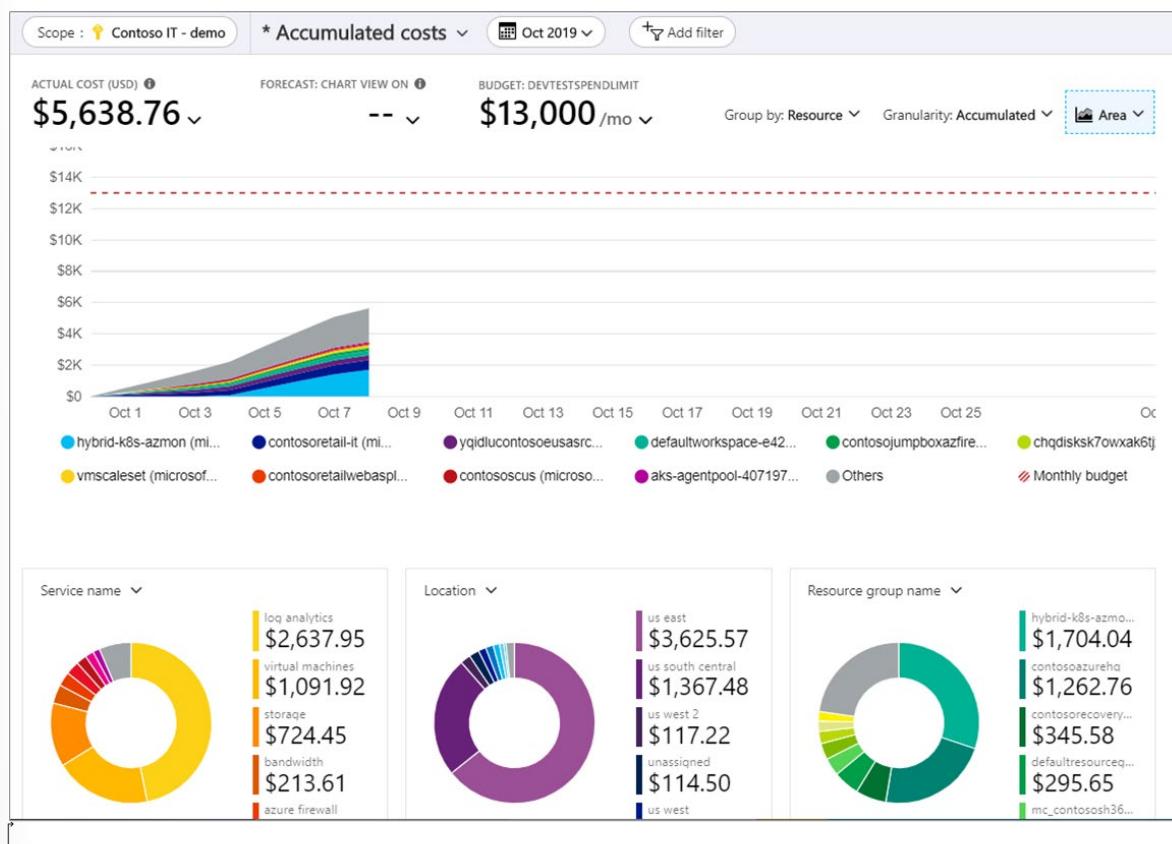
Dimensions allow you to organize costs based on various metadata values shown in charges. For example, you could group costs by location.

1. In the Azure portal, navigate to cost analysis for your scope. For example: **Cost Management + Billing > Cost Management > Cost analysis**.
2. Select the **Group by** filter.

The screenshot shows the Azure Cost Analysis blade. At the top, it displays "ACTUAL COST (USD) \$5,638.76", "FORECAST: CHART VIEW ON --", and "BUDGET: DEVTESTSPENDLIMIT \$13,000 /mo". Below this is a table with 469 rows, showing columns for Resource, Resource type, and Location. To the right of the table is a "Group by" filter dropdown menu. The menu is open and shows a list of dimensions: None, Billing period, Charge type, Frequency, InvoiceNumber, Location, Meter, Meter category, and Meter subcategory. The "Group by: Resource" option is highlighted with a red box.

Resource	Resource type	Location
hybrid-k8s-azmon	Log Analytics workspace	us east
contosoretail-it	Log Analytics workspace	us east
yqidlucontosoeusasrcac...	Storage account	us south central
defaultworkspace-e427...	Log Analytics workspace	us east
contosojumpboxazfirew...	Firewall	us south central
chqdisksk7owxak6tjx7u	Storage account	us south central

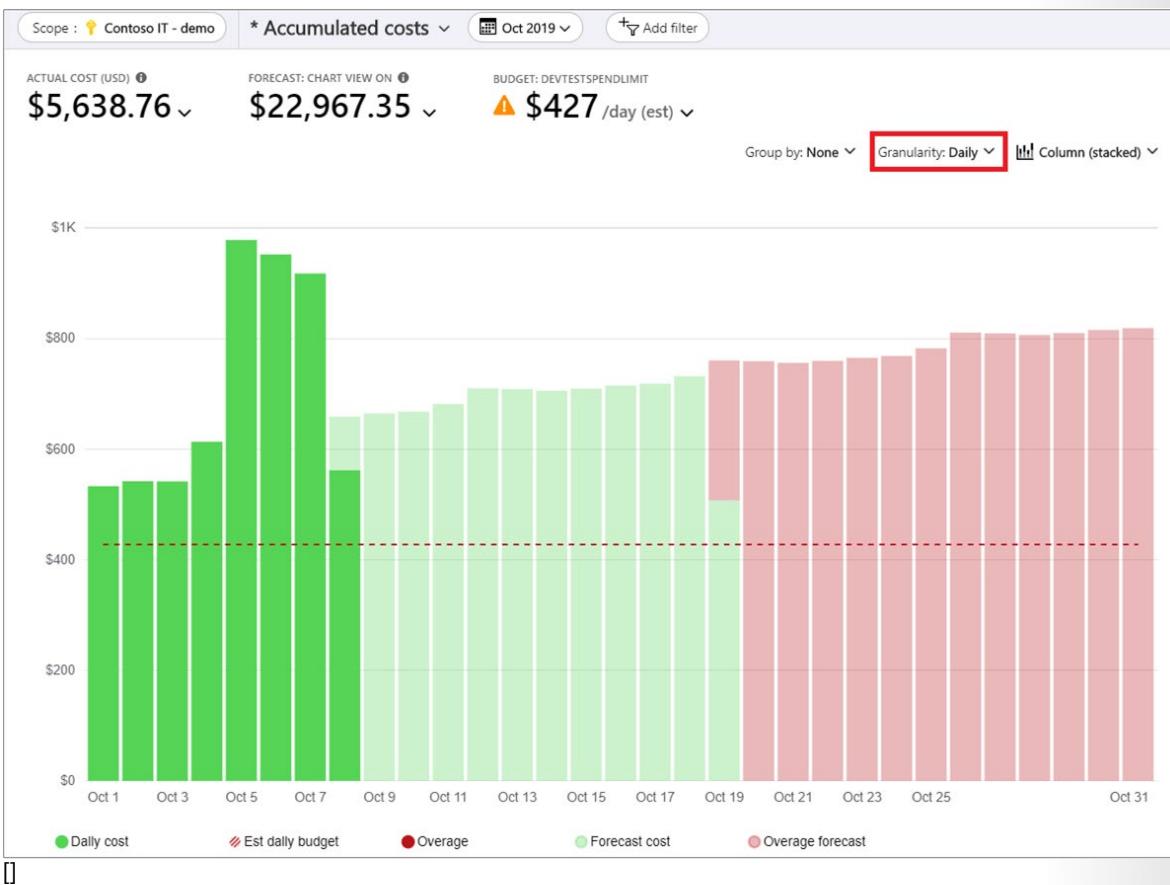
3. Optionally, you save the view for later use.
4. Click a pie chart below the graph to view more detailed data.



## View Costs by Day or Month

Looking at daily and monthly costs can help you to better understand if there's a time of the week or year where costs are higher. If you have more customer traffic in a holiday period, does that lead to a corresponding increase in Azure costs? Is Friday a more costly day than Monday?

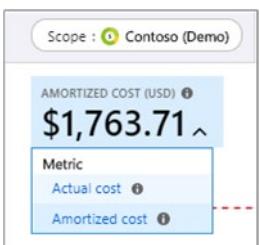
1. In the Azure portal, navigate to cost analysis for your scope. For example: **Cost Management + Billing > Cost Management > Cost analysis**.
2. Set the **Granularity** to **Monthly** or **Daily**.



## View Reservation Charges

Reserved instances provide a way for you to save money with Azure. With reservations, you spend money up front for a given number of resources over time. Cost analysis shows the charges as they appear on the bill. The charges are shown as actual costs or amortized over the course of the reservation period.

1. In the Azure portal, navigate to cost analysis for your scope. For example, **Cost Management + Billing > Cost Management > Cost analysis**.
2. Add a filter for **Pricing Model: Reservation**.
3. Under **Scope** and next to the cost shown, click the down arrow symbol, select either **Actual cost** or **Amortized cost metric**.



Each metric affects how data is shown for reservation charges.

**Actual cost** - Shows the purchase as it appears on the bill. For example, if you bought a one-year reservation for \$1200 in January, cost analysis shows a \$1200 cost in the month of January for the

reservation. It doesn't show a reservation cost for other months of the year. If you group actual costs by VM, then a VM that received the reservation benefit for a given month would have zero cost for the month.

**Amortized cost** - Shows a reservation purchase split as an amortized cost over the duration of the reservation term. Using the same example above, cost analysis shows a \$100 cost for each month throughout the year if you purchased a one-year reservation for \$1200 in January. If you group costs by VM in this example, you'd see cost attributed to each VM that received the reservation benefit.

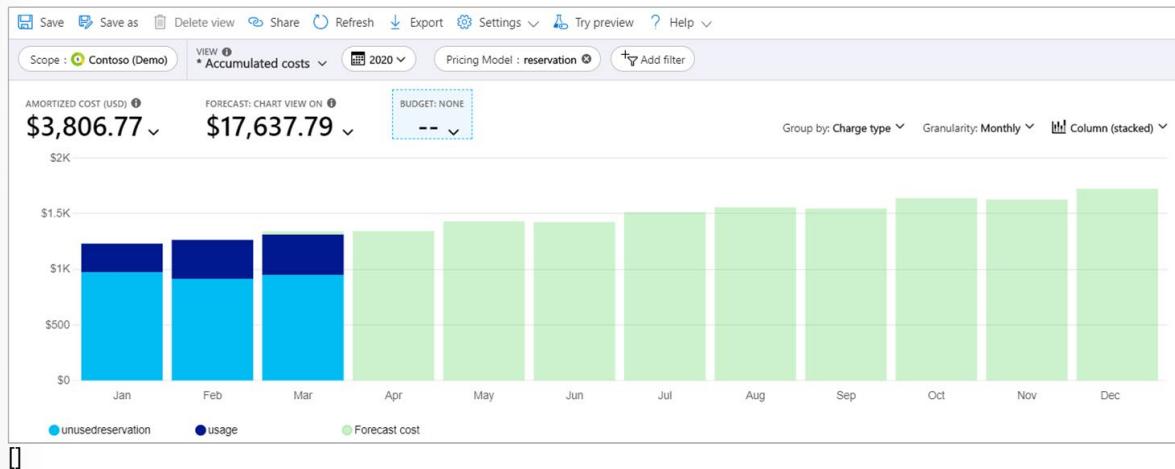
## View Reservation Utilization

After you buy a reservation, it's important to track its utilization so that you get what you paid for.

### View unused RI costs in cost analysis

To identify how much cost is currently being wasted each month for reservation purchase, follow the steps below.

1. In the Azure portal, navigate to cost analysis for the scope where the reservation is applied. For example, **Cost Management + Billing > Cost Management > Cost analysis**.
2. Add a filter for **Pricing Model: Reservation**.
3. Select the **Amortized Cost** view.
4. Set the granularity to **Monthly**.
5. Set the time period to the current year or reservation term.
6. Set the chart type to **Column (stacked)**.
7. Group charges by **Charge Type**.
8. Review the results for unused reservation values.



## View Costs for a Specific Tag

Many Azure users apply tags to their resources such as a cost center or development environment (production and test) to better categorize charges. Tags appear as a dimension in cost analysis. You can use the dimension to gain insights into your custom tagging categorizations.

Support for tags applies to usage reported after the tag was applied to the resource. Tags aren't applied retroactively for cost rollups.

1. In the Azure portal, navigate to cost analysis for your scope. For example: **Cost Management + Billing > Cost Management > Cost analysis**.
2. Select **Group by** for your tag.

The screenshot shows the Azure Cost Management + Billing interface. At the top, it displays 'Scope : Contoso IT - demo', 'Accumulated costs', 'Oct 2019', and an 'Add filter' button. Below this, there are three main cost summary sections: 'ACTUAL COST (USD) \$5,638.76', 'FORECAST: CHART VIEW ON --', and 'BUDGET: DEVTESTSPENDLIMIT \$13,000/mo'. A 'Filter items...' input field shows '3 rows'. On the right, a 'Group by:' dropdown menu is open, listing various grouping options like 'environment', 'Publisher type', 'Reservation', etc., with 'Tag' highlighted with a red box. The 'Granularity: None' dropdown is also visible.

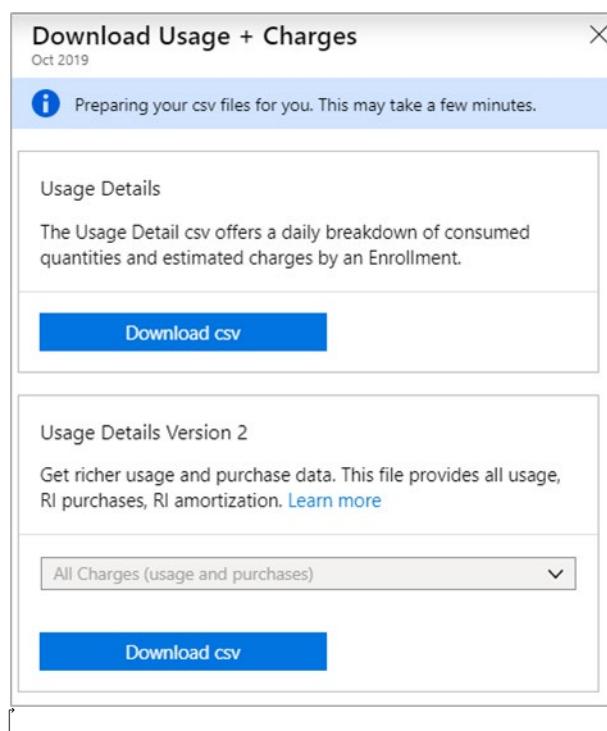
## Download Usage Details

The Usage details report file, in CSV format, provides a breakdown of all the charges that accrued towards an invoice. You can use the report to compare it to, and better understand, the invoice. Each billed charge on the invoice corresponds to broken-down charges in the usage report.

1. In the Azure portal, navigate to the Usage and Charges tab for a billing account or subscription. For example: **Cost Management + Billing > Billing > Usage + charges**.
2. Select the line item to download from and then click the download symbol.

The screenshot shows the Azure Cost Management + Billing interface with the 'Usage + charges' tab selected. The left sidebar includes links for 'Create a resource', 'Dashboard', 'All services', 'FAVORITES', 'Resource groups', 'Subscriptions', 'All resources', 'Reservations', 'Cost Management + Billing', 'Recent', 'App Services', 'SQL databases', 'Virtual machines (classic)', 'Virtual machines', 'Cloud services (classic)', 'Azure Active Directory', 'Monitor', 'Security Center', 'Help + support', and 'Log Analytics workspaces'. The main area shows a table of usage data for the last 12 months. The table has columns for Month, Charges against credits, Service overage, Billed separately, Azure marketplace, Total charges, and a 'Download' column with a downward arrow icon. A red box highlights the 'Download' icon in the first row. At the bottom, there's a 'Total' section with summary statistics: 'Charges against credits 0 usd', 'Service overage 889.29 K usd', 'Billed separately 172.71 usd', 'Azure marketplace 18.88 K usd', and 'Total charges 908.35 K usd'.

3. Select the usage file to download.

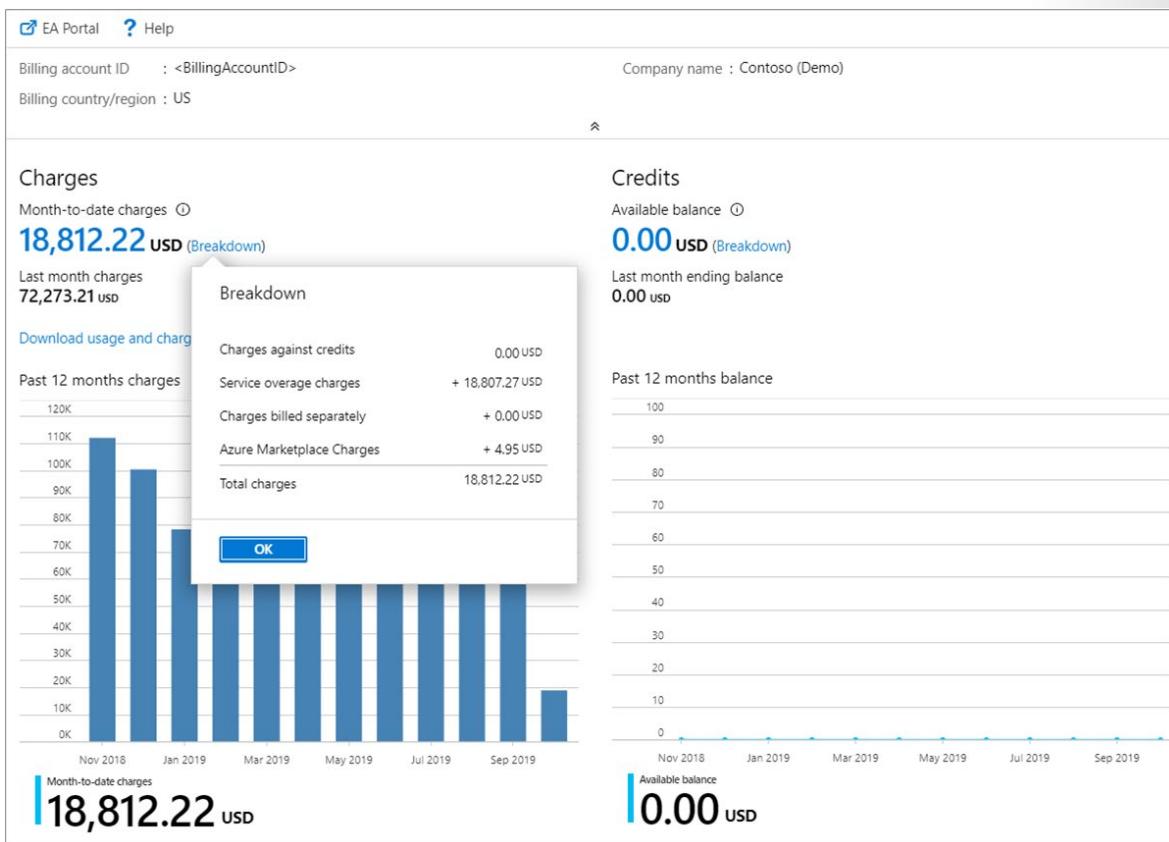


## View Monthly EA Cost Breakdown

The EA enrollment accrues costs for an entire organization. Understanding how costs accrue and are invoiced over time helps to engage the appropriate stakeholders to ensure that costs are managed responsibly.

Costs are only shown for an active enrollment. If you transferred an enrollment (inactive) to a new one (active), costs for the previous enrollment aren't shown in Cost Management.

1. In the Azure portal, navigate to **Cost Management + Billing > Overview**.
2. Click **Breakdown** for the current month and view the monetary commitment burn down.



3. Click the Usage and Charges tab and view the prior month's breakdown in the chosen timespan.

This screenshot shows the 'Cost Management + Billing - Usage + charges' page. The left sidebar includes links for Overview, All billing scopes, Management groups, Access control (IAM), Cost Management (Cost analysis, Budgets, Cloudyn), Billing (Usage + charges, Credits, Reservation transactions, Departments, Accounts, Subscriptions), Settings, and Properties. The main area displays a table of monthly charges from Oct 2019 to Nov 2018. The 'Usage + charges' tab is selected. At the bottom, there's a summary of total charges by category.

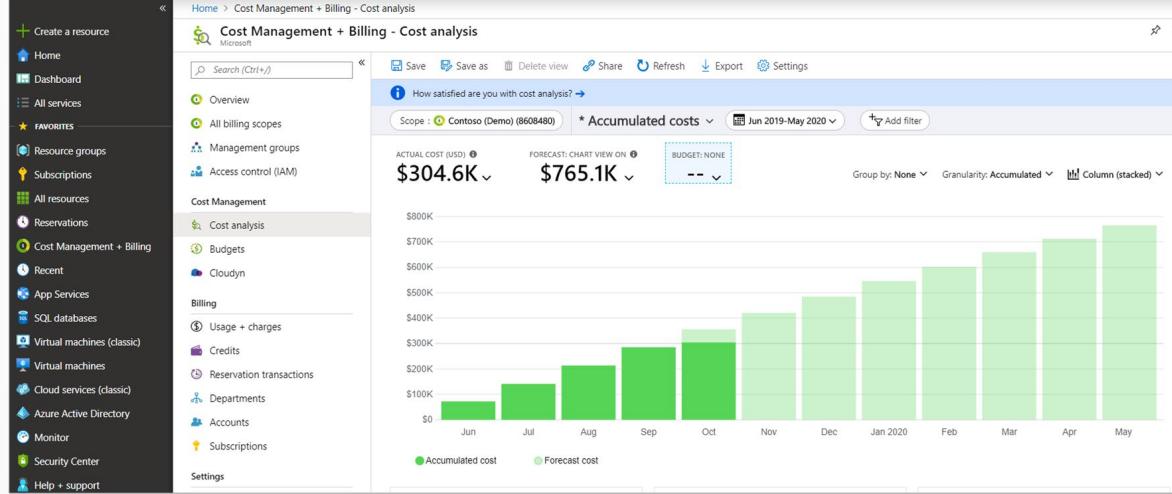
Category	Value
Charges against credits	<b>0 USD</b>
Service overage	<b>889.29 K USD</b>
Billed separately	<b>172.71 USD</b>
Azure marketplace	<b>18.88 K USD</b>
Total charges	<b>908.35 K USD</b>

## View Enrollment Monthly Cost by Term

Use a graphical view of the enrollment's monthly costs to understand the cost trends and invoiced amounts for a given period.

1. In the Azure portal, navigate to cost analysis for your scope. For example: **Cost Management + Billing > Cost Management > Cost**.
2. Select your enrollment and set the enrollment term.
3. Set the granularity to monthly and then set the view to Column (stacked).

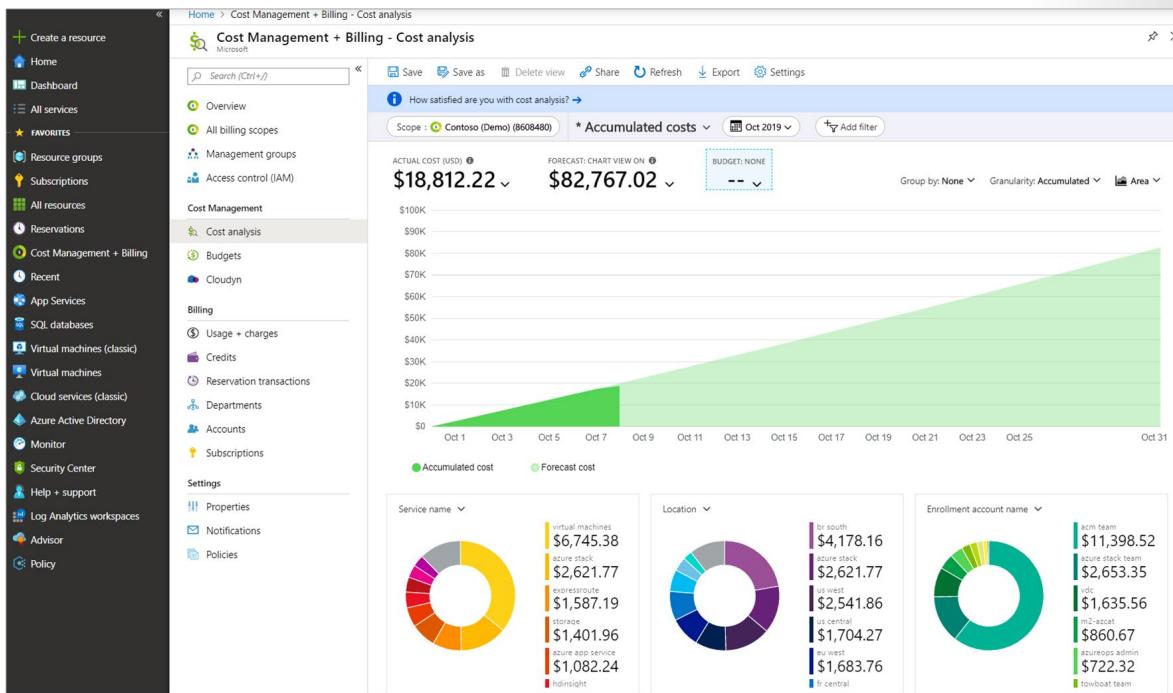
You can group by and filter data for a more detailed analysis.



## View EA Enrollment Accumulated Costs

View the net accumulated charges over time to understand overall expenditures for an organization for a given period.

1. In the Azure portal, navigate to cost analysis for your scope. For example: **Cost Management + Billing > Cost Management > Cost analysis**.
2. Select the enrollment and then view the current accumulated costs.



AUTHORIZED TRAINER USE ONLY. STUDENT USE PROHIBITED

# Cost Optimization Checklists

## Checklist - Design for Cost

Use this checklist when designing a cost-effective workload.

### Cost model

- **Capture clear requirements.** Gather detailed information about the business workflow, regulatory, security, and availability.
  - **Capture requirements<sup>3</sup>**
- **Estimate the initial cost.** Use tools such as **Azure pricing calculator<sup>4</sup>** to assess cost of the services you plan to use in the workload. Use **Azure Migrate<sup>5</sup>** and **Microsoft Azure Total Cost of Ownership (TCO) Calculator<sup>6</sup>** for migration projects. Accurately reflect the cost associated with right storage type. Add hidden costs, such as networking cost for large data download.
  - **Estimate the initial cost<sup>7</sup>**
- **Define policies for the cost constraints defined by the organization.** Understand the constraints and define acceptable boundaries for quality pillars of scale, availability, security.
  - **Consider the cost constraints<sup>8</sup>**
- **Identify shared assets.** Evaluate the business areas where you can use shared resources. Review the billing meters build chargeback reports per consumer to identify metered costs for shared cloud services.
  - **Create a structured view of the organization in the cloud<sup>9</sup>**
- **Plan a governance strategy.** Plan for cost controls through Azure Policy. Use resource tags so that custom cost report can be created. Define budgets and alerts to send notifications when certain thresholds are reached.
  - **Governance<sup>10</sup>**

### Architecture

- **Check the cost of resources in various Azure geographic regions.** Check your egress and ingress cost, within regions and across regions. Only deploy to multiple regions if your service levels require it for either availability or geo-distribution.
  - **Azure regions<sup>11</sup>**
- **Choose a subscription that is appropriate for the workload.** Azure Dev/Test subscription types are suitable for experimental or non-production workloads and have lower prices on some Azure services

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-capture-requirements>

<sup>4</sup> <https://azure.microsoft.com/pricing/calculator>

<sup>5</sup> <https://docs.microsoft.com/en-us/azure/migrate/migrate-services-overview>

<sup>6</sup> <https://azure.microsoft.com/pricing/tco/calculator/>

<sup>7</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-initial-estimate>

<sup>8</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-model>

<sup>9</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-model>

<sup>10</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-governance>

<sup>11</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-regions>

such as specific VM sizes. If you can commit to one or three years, consider subscriptions and offer types that support Azure Reservations.

- **Subscription and offer type<sup>12</sup>**
- **Choose the right resources to handle the performance.** Understand the usage meters and the number of meters for each resource in the workload. Consider tradeoffs over time. For example, cheaper virtual machines may initially indicate a lower cost but can be more expensive over time to maintain a certain performance level. Be clear about the billing model of third-party services.
  - **Azure resources<sup>13</sup>**
  - **Use cost alerts to monitor usage and spending<sup>14</sup>**
- **Compare consumption-based pricing with pre-provisioned cost.** Establish baseline cost by considering the peaks and the frequency of peaks when analyzing performance.
  - **Consumption and fixed cost models<sup>15</sup>**
- **Use proof-of-concept deployments.** The **Azure Architecture Center<sup>16</sup>** has many reference architectures and implementations that can serve as a starting point. The **Azure Tech Community<sup>17</sup>** has architecture and services forums.
- **Choose managed services when possible.** With PaaS and SaaS options, the cost of running and maintaining the infrastructure is included in the service price.
  - **Managed services<sup>18</sup>**

## Checklist - Provisioning Cloud Resources to Optimize Cost

Use the **Azure Pricing calculator<sup>19</sup>** to estimate the cost of your SKU choices.

Below is a list with pointers for cost considerations.

- **AI + Machine Learning<sup>20</sup>**
- **Big data analytics<sup>21</sup>**
- **Networking<sup>22</sup>**
- **Data stores<sup>23</sup>**

---

<sup>12</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-resources>

<sup>13</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-resources>

<sup>14</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending>

<sup>15</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-price>

<sup>16</sup> <https://docs.microsoft.com/en-us/azure/architecture>

<sup>17</sup> <https://techcommunity.microsoft.com/t5/azure/ct-p/Azure>

<sup>18</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-paas>

<sup>19</sup> <https://azure.microsoft.com/pricing/calculator/>

<sup>20</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/provision-ai-ml>

<sup>21</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/provision-analytics>

<sup>22</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/provision-networking>

<sup>23</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/provision-datastores>

## Checklist - Monitor Cost

Use this checklist to monitor the cost of the workload.

- **Gather cost data from diverse sources to create reports.** Start with tools like **Azure Advisor<sup>24</sup>** and **Azure Cost Management<sup>25</sup>**. Build custom reports relevant for the business by using **Consumption APIs<sup>26</sup>**.
  - **Cost reports<sup>27</sup>**
  - **Review costs in cost analysis<sup>28</sup>**
- **Use resource tag policies to build reports.** Tags can be used to identify the owners of systems or applications and create custom reports.
  - **Video: How to review tag policies with Azure Cost Management<sup>29</sup>**
- **Use RBAC built-in roles for cost.** Only give access to users who are intended to view and analyze cost reports. The roles are defined per scope. For example, use the Cost Management Reader role to enable users to view costs for their resources in subscriptions or resource groups.
  - **Azure RBAC scopes<sup>30</sup>**
- **Respond to alerts and have a response plan according to the constraints.** Respond to alerts quickly and identify possible causes and any required action.
  - **Budget and alerts<sup>31</sup>**
  - **Use cost alerts to monitor usage and spending<sup>32</sup>**
- **Adopt both proactive and reactive approaches for cost reviews.** Conduct cost reviews at a regular cadence to determine the cost trend. Also review reports that are created because of alerts.
  - **Conduct cost reviews<sup>33</sup>**
- **Analyze the cost at all scopes** by using Cost analysis. Identify services that are driving the cost through different dimensions, such as location, usage meters, and so on. Review whether certain optimizations are bringing results. For example, analyze costs associated with reserved instances and Spot VMs against business goals.
  - **Quickstart: Explore and analyze costs with cost analysis<sup>34</sup>**
- **Detect anomalies** and identify changes in business or applications that might have contributed changes in cost. Focus on these factors:
  - Traffic pattern as the application scales.
  - Budget for the usage meters on resources.
  - Performance bottle necks.
  - CPU utilization and network throughput.

<sup>24</sup> <https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations>

<sup>25</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/>

<sup>26</sup> <https://docs.microsoft.com/en-us/rest/api/consumption/>

<sup>27</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/monitor-reports>

<sup>28</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/quick-acm-cost-analysis>

<sup>29</sup> <https://www.youtube.com/watch?v=nHQYcGKuyw>

<sup>30</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/understand-work-scopes>

<sup>31</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/monitor-alert>

<sup>32</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending>

<sup>33</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/monitor-reviews>

<sup>34</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/quick-acm-cost-analysis>

- Storage footprint for blobs, backups, archiving.
- **Use Visualization tools to analyze cost information.**
  - **Create visuals and reports with the Azure Cost Management connector in Power BI Desktop**<sup>35</sup>
  - **Cost Management App**<sup>36</sup>

## Checklist - Optimize Cost

Use this checklist to optimize a workload.

- **Review the underutilized resources.** Evaluate CPU utilization and network throughput over time to check if the resources are used adequately. Azure Advisor identifies underutilized virtual machines. You can choose to decommission, resize, or shut down the machine to meet the cost requirements.
  - **Resize virtual machines**<sup>37</sup>
  - **Shutdown the under utilized instances**<sup>38</sup>
- **Continuously take action on the cost reviews.** Treat cost optimization as a process, rather than a point-in-time activity. Use tooling in Azure that provides recommendations on usage or cost optimization. Review the cost management recommendations and take action. Make sure that all stakeholders are in agreement about the implementation and timing of the change.
  - **Recommended tab in the Azure portal**<sup>39</sup>
  - Recommendations in the **Cost Management Power BI app**<sup>40</sup>
  - Recommendations in **Azure Advisor**<sup>41</sup>
  - Recommendations using **Reservation REST APIs**<sup>42</sup>
- **Use reserved instances on long running workloads.** Reserve a prepaid capacity for a period, generally one or three years. With reserved instances, there's a significant discount when compared with pay-as-you-go pricing.
  - **Reserved instances**<sup>43</sup>
- **Use discount prices.** These methods of buying Azure resources can lower costs.
  - **Azure Hybrid Use Benefit**<sup>44</sup>
  - **Azure Reservations**<sup>45</sup>

There are also payment plans offered at a lower cost:

- **Microsoft Azure Enterprise Agreement**<sup>46</sup>
- **Enterprise Dev Test Subscription**<sup>47</sup>

---

<sup>35</sup> <https://docs.microsoft.com/en-us/power-bi/desktop-connect-azure-cost-management>

<sup>36</sup> <https://appsource.microsoft.com/product/power-bi/costmanagement.azurecostmanagementapp>

<sup>37</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/optimize-vm>

<sup>38</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/optimize-vm>

<sup>39</sup> <https://portal.azure.com/>

<sup>40</sup> <https://appsource.microsoft.com/product/power-bi/costmanagement.azurecostmanagementapp>

<sup>41</sup> <https://portal.azure.com/>

<sup>42</sup> <https://docs.microsoft.com/en-us/rest/api/consumption/reservationrecommendations/list>

<sup>43</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/optimize-reserved>

<sup>44</sup> <https://azure.microsoft.com/pricing/hybrid-benefit>

<sup>45</sup> <https://azure.microsoft.com/reservations>

<sup>46</sup> <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/ea-portal-get-started>

<sup>47</sup> <https://azure.microsoft.com/offers/ms-azr-0148p/>

- **Cloud Service Provider (Partner Program)**<sup>48</sup>
- **Have a scale-in and scale-out policy.** In a cost-optimized architecture, costs scale linearly with demand. Increasing customer base shouldn't require more investment in infrastructure. Conversely, if demand drops, scale-down of unused resources. Autoscale Azure resources when possible.
  - **Autoscale instances**<sup>49</sup>
- **Reevaluate design choices.** Analyze the cost reports and forecast the capacity needs. You might need to change some design choices.
  - **Choose the right storage tier.** Consider using hot, cold, archive tier for storage account data. Storage accounts can provide automated tiering and lifecycle management. For more information, see [Review your storage options](#)<sup>50</sup>
  - **Choose the right data store.** Instead of using one data store service, use a mix of data store depending on the type of data you need to store for each workload. For more information, see [Choose the right data store](#)<sup>51</sup>.
  - **Choose Spot VMs for low priority workloads.** Spot VMs are ideal for workloads that can be interrupted, such as highly parallel batch processing jobs.
  - [Spot VMs](https://docs.microsoft.com/en-us/azure/architecture/framework/cost/optimize-vm)
  - **Optimize data transfer.** Only deploy to multiple regions if your service levels require it for either availability or geo-distribution. Data going out of Azure datacenters can add cost because pricing is based on Billing Zones.
  - **Traffic across billing zones and regions**<sup>52</sup>
  - **Reduce load on servers.** Use Azure Content Delivery Network (CDN) and caching service to reduce load on front-end servers. Caching is suitable for servers that are continually rendering dynamic content that doesn't change frequently.
  - **Use managed services.** Measure the cost of maintaining infrastructure and replace it with Azure PaaS or SaaS services.
  - **Managed services**<sup>53</sup>

---

<sup>48</sup> <https://partner.microsoft.com/membership/cloud-solution-provider>

<sup>49</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/optimize-autoscale>

<sup>50</sup> <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/storage-options>

<sup>51</sup> <https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/data-store-overview>

<sup>52</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-regions>

<sup>53</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/cost/design-paas>

## Module 12 Review Questions

### Module 12 Review Questions



#### Review Question 1

You are designing an Azure solution for your organization that has five departments. Every department will deploy Azure app services and Azure SQL databases. You are asked to recommend a solution that reports costs for each department deploying the databases and app services and there needs to be a combined view for the cost reporting.

Your solution: Create an individual resource group for each department and place the separate resources for each department in their individual groups.

Does this fulfill your objective?

- Yes
- No

#### Review Question 2

You manage an Azure subscription that contains 250 Linux virtual machines.

You need to evaluate CPU utilization and network throughput over time to check if the resources are used adequately.

You want to identify and choose to decommission, resize, or shut down unused machines to meet the cost requirements.

What should you do next?

- Modify the inventory settings for all VMs.
- Use Azure Advisor to identify underutilized virtual machines.
- From Azure Advisor, modify the Advisor configuration.
- Assign tags to the VMs.

## Review Question 3

*You are responsible for identifying and managing costs for your organization.*

*You have been tasked to report on the parts of your infrastructure that cost the most for a monthly review meeting.*

*You notice that VM compute costs are relatively small. Yet you accrue significant networking costs because of the amount of information emitting from the VMs.*

*What should you do?*

- Use Azure Advisor to view a dashboard identify costs.
- Use Azure activity log for an audit log of resource activities.
- Use Cost Management and review cost analysis to view the costs by service.
- Use Query Performance Insight to view the query text and history of resource utilization.

# Answers

## Review Question 1

You are designing an Azure solution for your organization that has five departments. Every department will deploy Azure app services and Azure SQL databases. You are asked to recommend a solution that reports costs for each department deploying the databases and app services and there needs to be a combined view for the cost reporting.

Your solution: Create an individual resource group for each department and place the separate resources for each department in their individual groups.

Does this fulfill your objective?

- Yes
- No

*Explanation*

*Cost Management can track by Resource Group. Allows you to report by resource group.*

## Review Question 2

You manage an Azure subscription that contains 250 Linux virtual machines.

You need to evaluate CPU utilization and network throughput over time to check if the resources are used adequately.

You want to identify and choose to decommission, resize, or shut down unused machines to meet the cost requirements.

What should you do next?

- Modify the inventory settings for all VMs.
- Use Azure Advisor to identify underutilized virtual machines.
- From Azure Advisor, modify the Advisor configuration.
- Assign tags to the VMs.

*Explanation*

*To evaluate CPU utilization and network throughput over time to check if the resources are used adequately. Azure Advisor identifies underutilized virtual machines. You can choose to decommission, resize, or shut down the machine to meet the cost requirements*

**Review Question 3**

You are responsible for identifying and managing costs for your organization.

You have been tasked to report on the parts of your infrastructure that cost the most for a monthly review meeting.

You notice that VM compute costs are relatively small. Yet you accrue significant networking costs because of the amount of information emitting from the VMs.

What should you do?

- Use Azure Advisor to view a dashboard identify costs.
- Use Azure activity log for an audit log of resource activities.
- Use Cost Management and review cost analysis to view the costs by service.
- Use Query Performance Insight to view the query text and history of resource utilization.

*Explanation*

*Use Cost Management + Billing > Cost Management > Cost analysis to view costs by an Azure service can help you to better understand the parts of an infrastructure that cost the most. For example, VM compute costs might be small. Yet you might accrue significant networking costs because of the amount of information emitting from the VMs.*

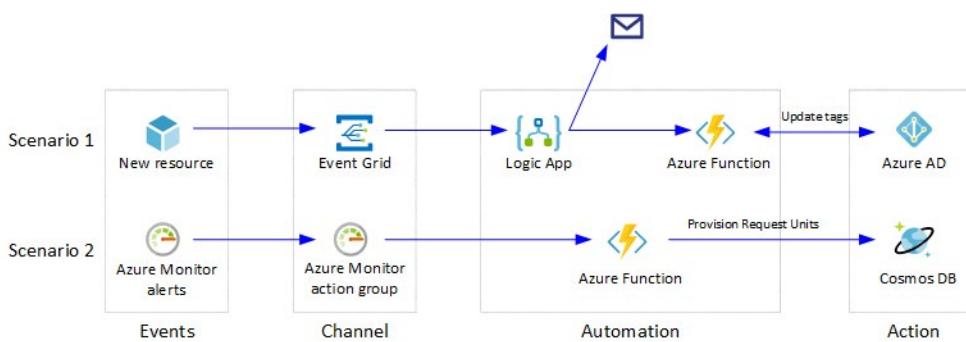
## Module 13 Design an Application Architecture

### Recommend Event-Based Cloud Automation on Azure

#### Event-Based Cloud Automation on Azure

A serverless model is best suited for automation scenarios that fit an event driven approach. This reference architecture illustrates two such cloud automation scenarios:

1. **Cost center tagging:** This implementation tracks the cost centers of each Azure resource. The **Azure Policy** service tags all new resources in a group with a default cost center ID. The Event Grid monitors resource creation events, and then calls an **Azure function**. The function interacts with Azure Active Directory, and validates the cost center ID for the new resource. If different, it updates the tag and sends out an email to the resource owner. The REST queries for Azure Active Directory are mocked out for simplicity.
2. **Throttling response:** This implementation monitors a Cosmos DB database for throttling. **Azure Monitor alerts** are triggered when data access requests to CosmosDB exceed the capacity in Request Units (or RUs). An Azure Monitor action group is configured to call the automation function in response to these alerts. The function scales the RUs to a higher value, increasing the capacity and in turn stopping the alerts.



✓ **NOTE:** The reference implementations for this architecture are available on [GitHub<sup>1</sup>](#).

The functions in these implementations are written in PowerShell and Python. They are deployed using **Azure Functions Core Tools** in Azure CLI.

## Patterns in Event-Based Automation



Event-based automation scenarios are best implemented using Azure Functions. They follow these common patterns:

- **Respond to events on resources.** These are responses to events such as an Azure resource or resource group getting created, deleted, changed, and so on. This pattern uses **Event Grid** to trigger the function for such events. The cost center tagging implementation is an example of this pattern. Other common scenarios include:
  - Granting the DevOps teams access to newly created resource groups.
  - Sending notification to the DevOps when a resource is deleted.
- **Scheduled tasks.** These are typically maintenance tasks executed using **timer-triggered functions**. Examples of this pattern are:
  - Stopping a VM at night and starting in the morning.
  - Reading Blob Storage content at regular intervals.
- **Process Azure alerts.** This pattern leverages the ease of integrating Azure Monitor alerts and action groups with Azure Functions. The function typically takes remedial actions in response to metrics, log analytics, and alerts originating in the applications as well as the infrastructure. The throttling response implementation is an example of this pattern. Other common scenarios are:
  - Restarting a service in a VM when it is erroneously stopped.
  - Sending notifications if a function is failing.
- **Orchestrate with external systems.** This pattern enables integration with external systems, using **Logic Apps** to orchestrate the workflow. **Logic Apps connectors** can integrate with third-party services as well as Microsoft services such as Office 365. Azure Functions can be used for the actual automation. The cost center tagging implementation demonstrates this pattern. Other common scenarios include:
  - Monitoring IT processes such as change requests or approvals.
  - Sending email notification when automation task is completed.
- **Expose as a web hook or API.** Automation tasks using Azure Functions can be integrated into third-party applications or even command-line tools, by exposing the function as a web hook/API using **HTTP trigger**. Multiple authentication methods are available in both PowerShell and Python to

---

<sup>1</sup> <https://github.com/mspnp/serverless-automation>

secure external access to the function. The automation happens in response to the app-specific external events, for example, integration with power apps or GitHub. Common scenarios include:

- Triggering automation for a failing service.
- Onboarding users to the organization's resources.
- **Create ChatOps interface.** This pattern enables customers to create a chat-based operational interface and run development and operations functions and commands in-line with human collaboration. This can integrate with the Azure Bot Framework and use Microsoft Teams commands for deployment, monitoring, common questions, and so on. A ChatOps interface creates a real-time system for managing production incidents, with each step documented automatically on the chat.
- **Hybrid automation.** This pattern uses the **Azure App Service Hybrid Connections** to install a software component on your local machine. This component allows secure access to resources on that machine. The ability to manage hybrid environments is currently available on Windows-based systems using PowerShell functions. Common scenarios include:
  - Managing your on-premises machines.
  - Managing other systems behind the firewall (for example, an on-premises SQL Server) through a jump server.

## Architecture

The architecture consists of the following blocks:



**Azure Functions.** Azure Functions provide the event-driven, serverless compute capabilities in this architecture. A function performs automation tasks, when triggered by events or alerts. In the reference implementations, a function is invoked with an HTTP request. Code complexity should be minimized, by developing the function that is **stateless**, and **idempotent**.

Multiple executions of an idempotent function create the same results. To maintain idempotency, the function scaling in the throttling scenario is kept simplistic. In real world automation, make sure to scale up or down appropriately.



**Logic Apps.** Logic Apps can be used to perform simpler tasks, easily implemented using the built-in connectors. These tasks can range from email notifications, to integrating with external management applications.

Logic Apps provides a *no code* or *low code* visual designer, and may be used alone in some automation scenarios.



**Event Grid.** Event Grid has built-in support for events from other Azure services, as well as custom events (also called *custom topics*). Operational events such as resource creation can be easily propagated to the automation function, using the Event Grid's built-in mechanism.

Event Grid simplifies the event-based automation with a **publish-subscribe model**, allowing reliable automation for events delivered over HTTP.



**Azure Monitor.** Azure Monitor alerts can monitor for critical conditions, and take corrective action using Azure Monitor action groups. These action groups are easily integrated with Azure Functions. This is useful to watch for and fix any error conditions in your infrastructure, such as database throttling.



**Automation action.** This broad block represents other services that your function can interact with, to provide the automation functionality. For example, Azure Active Directory for tag validation as in the first scenario, or a database to provision as in the second scenario.

## Resiliency

### Azure Functions

#### Handle HTTP timeouts

To avoid HTTP timeouts for a longer automation task, queue this event in a Service Bus, and handle the actual automation in another function. The throttling response automation scenario illustrates this pattern, even though the actual Cosmos DB RU provisioning is fast.



**Durable functions**, which maintain state between invocations, provide an alternative to the above approach. These are currently supported only in JavaScript and C#.

#### Log failures

As a best practice, the function should log any failures in carrying out automation tasks. This allows for proper troubleshooting of the error conditions. The reference implementations use the **Application Insights** as the telemetry system.

#### Concurrency

Verify the concurrency requirement for your automation function. Concurrency is limited by setting the variable `maxConcurrentRequests` in the file `host.json`. This setting limits the number of concurrent function instances running in your function app. Since every instance consumes CPU and memory, this value needs to be adjusted for CPU-intensive operations. Lower the `maxConcurrentRequests` if your function calls appear to be too slow or aren't able to complete.

#### Idempotency

Make sure your automation function is idempotent. Both Azure Monitor and Event Grid may emit alerts or events that indicate progression such as your subscribed event is *resolved*, *fired*, *in progress*, etc., your resource is being *provisioned*, *created successfully*, etc., or even send false alerts due to a misconfiguration. Make sure your function acts only on the relevant alerts and events, and ignores all others, so that false or misconfigured events do not cause unwanted results.

## Event Grid

If your workflow uses Event Grid, check if your scenario could generate a high volume of events, enough to clog the grid. The cost center workflow does not implement additional checks for this, since it only watches for resource creation events in a resource group. Monitoring resources created in an entire subscription, can generate larger number of events, requiring a more resilient handling.

## Azure Monitor

If a sufficiently large number of alerts are generated, and the automation updates Azure resources, throttling limits of the Azure Resource Manager might be reached. This can negatively affect the rest of the infrastructure in that subscription. Avoid this situation by limiting the *frequency* of alerts getting generated by the Azure Monitor.

## Security



### Control access to the function

Restrict access to an HTTP-triggered function by setting the authorization level. With *anonymous* authentication, the function is easily accessible with a URL such as `http://<APP_NAME>.azurewebsites.net/api/<FUNCTION_NAME>`. Function level authentication can obfuscate the http endpoint, by requiring function keys in the URL. This level is set in the file `function.json`:

```
{
  "bindings": [
    {
      "authLevel": "function",
      "type": "httpTrigger",
      "direction": "in",
      "name": "Request",
      "methods": [
        "get",
        "post"
      ]
    },
    {
      "type": "http",
      "direction": "out",
      "name": "Response"
    }
  ]
}
```

For production environments, additional strategies might be required to secure the function. In the reference implementations, the functions are executed within the Azure platform by other Azure services, and will not be exposed to the internet. Function authorization is sufficient for functions accessed as webhooks.

Consider adding security layers on top of function authentication, such as:

- Authenticating with client certificates.
- Making sure the caller is part of or has access to the directory that hosts the function, by using Easy Auth integration.

Note that function-level authentication is the only option available to Azure Monitor action groups.

If the calling service supports service endpoints, the following costlier options could be considered:

- Use a dedicated App Service plan, where you can lock down the functions in a virtual network to limit access to it. This is not possible in a consumption-based serverless model.
- Use the **Azure Functions Premium plan**, which includes a dedicated virtual network to be used by your function apps.

## Control function access

**Managed identities for Azure resources**, an Azure Active Directory feature, simplifies how the function authenticates and accesses other Azure resources and services. The code does not need to manage the authentication credentials, since it is managed by Azure AD.

There are two types of managed identities:

- **System-assigned managed identities**: These are created as part of the Azure resource, and cannot be shared among multiple resources. These get deleted when the resource is deleted.
- **User-assigned managed identities**: These are created as stand-alone Azure resources. These can be shared across multiple resources and need to be explicitly deleted.

## Costs

Use the Azure pricing calculator to estimate costs. Here are some considerations for lowering cost.

## Azure Logic Apps

Logic apps have a pay-as-you-go pricing model. Triggers, actions, and connector executions are metered each time a logic app runs. All successful and unsuccessful actions, including triggers, are considered as executions.

Logic apps have also a fixed pricing model.

In this architecture, logic apps are used in the cost center tagging scenario to orchestrate the workflow.

Built-in connectors are used to connect to Azure Functions and send email notification and when an automation task is completed. The functions are exposed as a web hook/API using an HTTP trigger. Logic apps are triggered only when an HTTPS request occurs. This is a cost-effective way when compared to a design where functions continuously poll and check for certain criteria. Every polling request is metered as an action.

## Azure Functions

Azure Functions are available with the following three pricing plans.

- **Consumption plan**. This is the most cost-effective, serverless plan available, where you only pay for the time your function runs. Under this plan, functions can run for up to 10 minutes at a time.

- **Premium plan.** Consider using Azure Functions Premium plan for automation scenarios with additional requirements, such as a dedicated virtual network, a longer execution duration, and so on. These functions can run for up to an hour, and should be chosen for longer automation tasks such as running backups, database indexing, or generating reports.
- **App Service plan.** Hybrid automation scenarios that use the Azure App Service Hybrid Connections, will need to use the App Service plan. The functions created under this plan can run for unlimited duration, similar to a web app.

## Azure Cosmos DB

Azure Cosmos DB bills for provisioned throughput and consumed storage by hour. Provisioned throughput is expressed in Request Units per second (RU/s), which can be used for typical database operations, such as inserts, reads. Storage is billed for each GB used for your stored data and index.

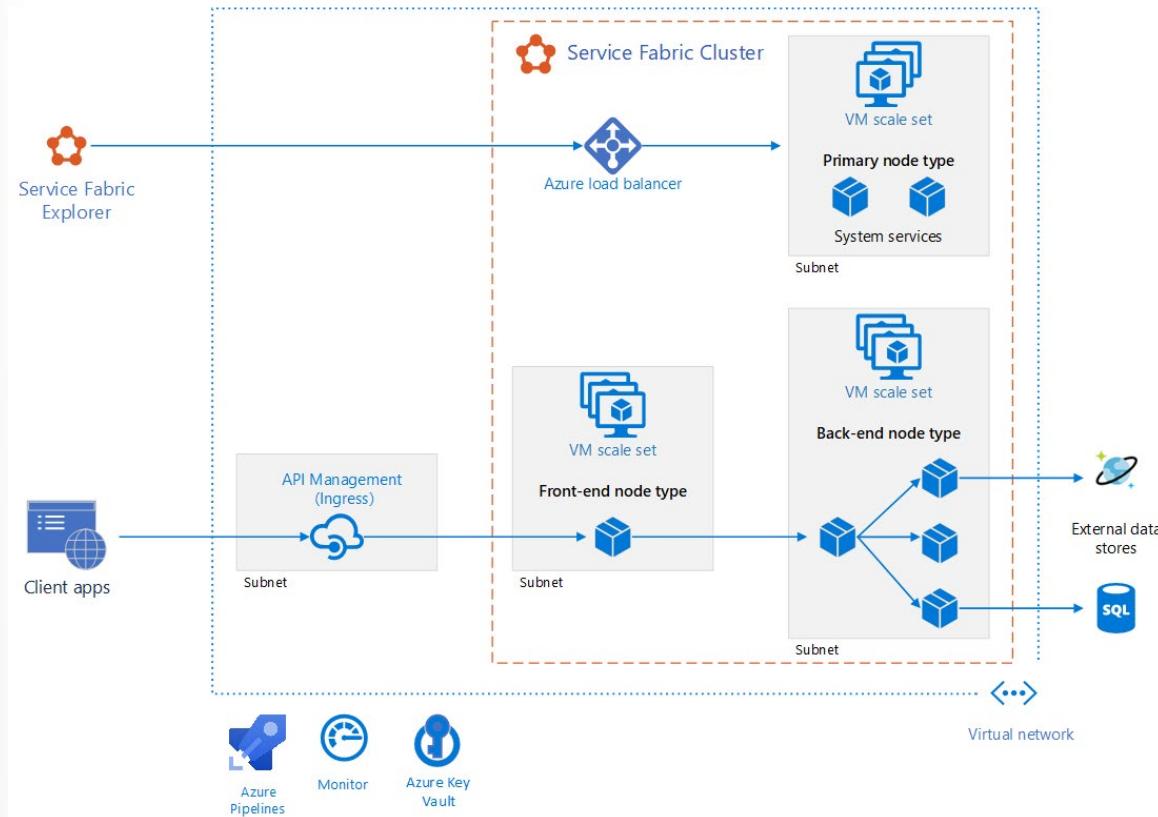
In this architecture, when data access requests to Cosmos DB exceed the capacity in Request Units (or RUs), Azure Monitor triggers alerts. In response to those alerts, an Azure Monitor action group is configured to call the automation function. The function scales the RUs to a higher value. This helps to keep the cost down because you only pay for the resources that your workloads need on a per-hour basis.

# Microservices Architecture on Azure Service Fabric

## Microservices Architecture on Azure Service Fabric

This reference architecture shows a microservices architecture deployed to Azure Service Fabric. It shows a basic cluster configuration that can be the starting point for most deployments.

✓ **NOTE:** The reference implementation of this architecture is available on [GitHub<sup>2</sup>](#).



## Architecture

The architecture consists of the following components.

**Service Fabric cluster.** A network-connected set of virtual machines (VMs) into which your microservices are deployed and managed.

**Virtual machine scale sets.** Virtual machine scale sets allow you to create and manage a group of identical, load balanced, and autoscaling VMs. It also provides the fault and upgrade domains.

**Nodes.** The nodes are the VMs that belong to the Service Fabric cluster.

**Node types.** A node type represents a virtual machine scale set that deploys a collection of nodes. A Service Fabric cluster has at least one node type. In a cluster with multiple node types, one must be

<sup>2</sup> <https://github.com/mspnp/microservices-reference-implementation-servicefabric>

declared the **Primary node type**. The primary node type in the cluster runs the Service Fabric system services. These services provide the platform capabilities of Service Fabric. The primary node type also acts as the **seed nodes** for the cluster, which are the nodes that maintain the availability of the underlying cluster.

**Services.** A service performs a standalone function that can start and run independently of other services. Instances of services get deployed to nodes in the cluster. There are two varieties of service in Service Fabric:

- **Stateless service.** A stateless service does not maintain state within the service. If state persistence is required, then state is written to and retrieved from an external store, such as Azure Cosmos DB.
- **Stateful service.** The service state is kept within the service itself. Most stateful services implement this through Service Fabric's Reliable Collections.

**Service Fabric Explorer.** Service Fabric Explorer is an open-source tool for inspecting and managing Service Fabric clusters.

**Azure Pipelines.** Pipelines is part of Azure DevOps Services and runs automated builds, tests, and deployments. You can also use third-party CI/CD solutions such as Jenkins.

**Azure Monitor.** Azure Monitor collects and stores metrics and logs, including platform metrics for the Azure services in the solution and application telemetry. Use this data to monitor the application, set up alerts and dashboards, and perform root cause analysis of failures. Azure Monitor integrates with Service Fabric to collect metrics from controllers, nodes, and containers, as well as container logs and master node logs.

**Azure Key Vault.** Use Key Vault to store any application secrets used by the microservices, such as connection strings.

**Azure API Management.** In this architecture, API Management acts as an API gateway that accepts requests from clients and routes them to your services.

## Design

This reference architecture is focused on microservices architectures. It is discoverable through service discovery mechanisms and can communicate with other services over APIs. Each service is self-contained and should implement a single business capability.

Service Fabric provides an infrastructure to build, deploy, and upgrade microservices efficiently. It also provides options for auto scaling, managing state, monitoring health, and restarting services in case of failure.

Service Fabric follows an application model where an application is a collection of microservices. The application is described in an application manifest file that defines the different types of service contained in that application, and pointers to the independent service packages. The application package also usually contains parameters that serve as overrides for certain settings used by the services.

## Choose an application-to-service packaging model

A tenet of microservices is that each service can be independently deployed. In Service Fabric, if you group all of your services into a single application package, and one service fails to upgrade, the entire application upgrade gets rolled back, which prevents other service from being upgraded.

In a microservices architecture, we recommend using multiple application packages. Put one or more closely related service types into a single application type

## Service Fabric programming models

When you add a microservice to a Service Fabric application, decide whether it has state or data that needs to be made highly available and reliable. If so, can it store data externally or is the data contained as part of the service? Choose a stateless service if you don't need to store data or want to store data in external storage. If you want to maintain state or data as part of the service (for example, you need that data to reside in memory close to the code), or cannot tolerate a dependency on an external store, consider choosing a stateful service.

If you have existing code that you want to run on Service Fabric, you can run it as a guest executable, which is an arbitrary executable that runs as a service. Service Fabric models both containers and guest executables as stateless services.

## API gateway

An API gateway (ingress) sits between external clients and the microservices. It acts as a reverse proxy, routing requests from clients to microservices. It may also perform various cross-cutting tasks such as authentication, SSL termination, and rate limiting.

Azure API Management is recommended for most scenarios, but **Traefik** is a popular open-source alternative. Both technology options are integrated with Service Fabric.

- **API Management** exposes a public IP address and routes traffic to your services. It runs in a dedicated subnet in the same virtual network as the Service Fabric cluster. It can access services in a node type that is exposed through a load balancer with a private IP address. This option is only available in the Premium and Developer tiers of API Management. For production workloads, use the Premium tier.
- **Traefik** supports features such as routing, tracing, logs, and metrics. Traefik runs as a stateless service in the Service Fabric cluster. Service versioning can be supported through routing.

## Interservice Communication

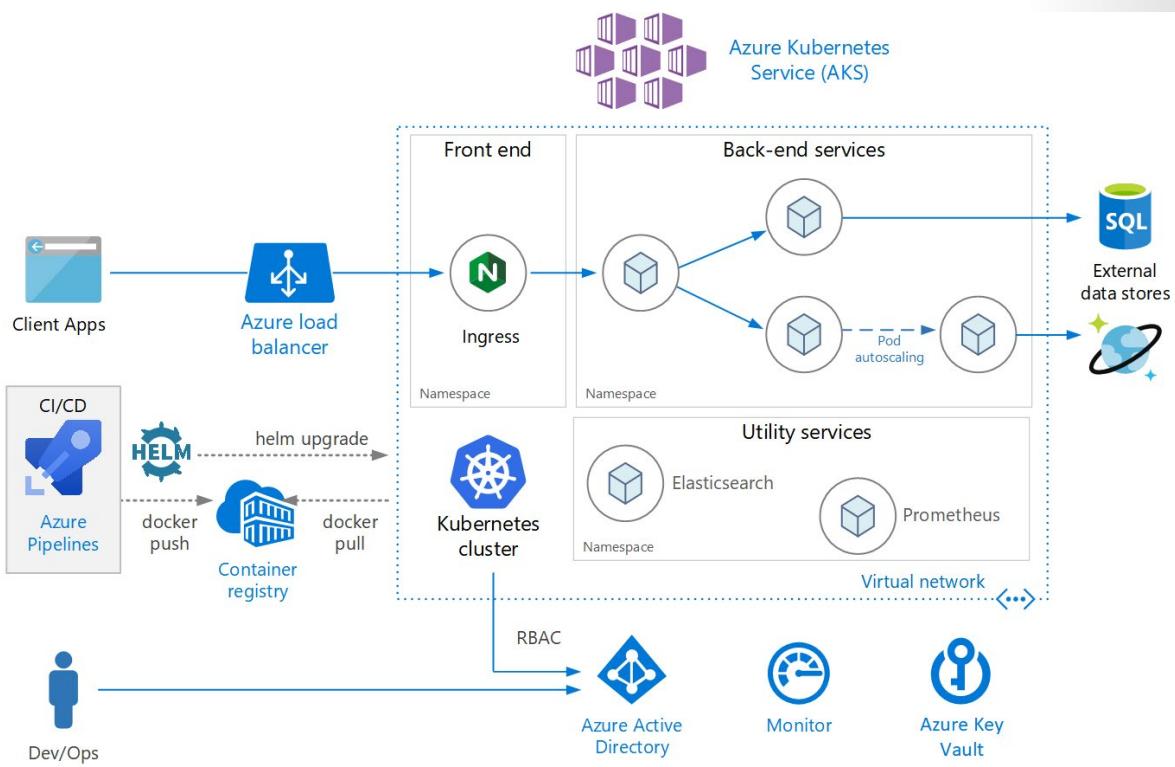
To facilitate service-to-service communication, consider using HTTP as the communication protocol. As a baseline for most scenarios, we recommend using the reverse proxy service for service discovery.

- **Communication protocol.** In a microservices architecture, services need to communicate with each other with minimum coupling at runtime. To enable language-agnostic communication, HTTP is an industry-standard with a wide range of tools and HTTP servers that are available in different languages, all supported by Service Fabric.
- **Service discovery.** To communicate with other services within a cluster, a client service needs to resolve the target service's current location. In Service Fabric, services can move between nodes, causing the service endpoints to change dynamically.

## Microservices Architecture on Azure Kubernetes Service

This reference architecture shows a microservices application deployed to Azure Kubernetes Service (AKS). It describes a basic AKS configuration that can be the starting point for most deployments. This article assumes basic knowledge of Kubernetes. The article focuses mainly on the infrastructure and DevOps considerations of running a microservices architecture on AKS.

A reference implementation of this architecture is available on [GitHub<sup>3</sup>](#).



## Architecture

The architecture consists of the following components.

**Azure Kubernetes Service (AKS).** AKS is an Azure service that deploys a managed Kubernetes cluster.

**Kubernetes cluster.** AKS is responsible for deploying the Kubernetes cluster and for managing the Kubernetes API server. You only manage the agent nodes.

**Virtual network.** By default, AKS creates a virtual network to deploy the agent nodes into. For more advanced scenarios, you can create the virtual network first, which lets you control things like how the subnets are configured, on-premises connectivity, and IP addressing.

**Ingress.** An ingress exposes HTTP(S) routes to services inside the cluster.

**Azure Load Balancer.** An Azure Load Balancer is created when the NGINX ingress controller is deployed. The load balancer routes internet traffic to the ingress.

**External data stores.** Microservices are typically stateless and write state to external data stores, such as Azure SQL Database or Cosmos DB.

**Azure Active Directory.** AKS uses an Azure Active Directory (Azure AD) identity to create and manage other Azure resources such as Azure load balancers. Azure AD is also recommended for user authentication in client applications.

**Azure Container Registry.** Use Container Registry to store private Docker images, which are deployed to the cluster. AKS can authenticate with Container Registry using its Azure AD identity. Note that AKS does not require Azure Container Registry. You can use other container registries, such as Docker Hub.

<sup>3</sup> <https://github.com/mspnp/microservices-reference-implementation>

**Azure Pipelines.** Pipelines is part of Azure DevOps Services and runs automated builds, tests, and deployments. You can also use third-party CI/CD solutions such as Jenkins.

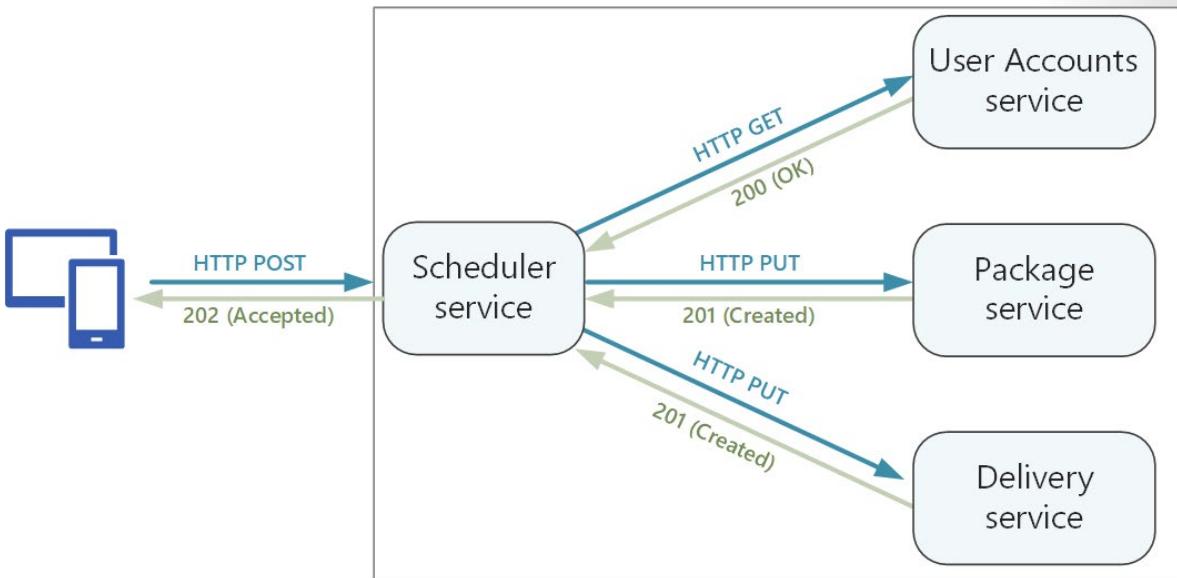
**Helm.** Helm is a package manager for Kubernetes — a way to bundle Kubernetes objects into a single unit that you can publish, deploy, version, and update.

**Azure Monitor.** Azure Monitor collects and stores metrics and logs, including platform metrics for the Azure services in the solution and application telemetry. Use this data to monitor the application, set up alerts and dashboards, and perform root cause analysis of failures. Azure Monitor integrates with AKS to collect metrics from controllers, nodes, and containers, as well as container and node logs.

# Designing APIs for Microservices

## Designing APIs for Microservices

All data exchange between services happens either through messages or API calls. APIs must be efficient to avoid creating chatty I/O. Because services are designed by teams working independently, APIs must have well-defined semantics and versioning schemes, so that updates don't break other services.



It's important to distinguish between two types of API:

- **Public APIs** that client applications call.
- **Backend APIs** that are used for interservice communication.

These two use cases have somewhat different requirements. A public API must be compatible with client applications, typically browser applications or native mobile applications. Most of the time, that means the public API will use REST over HTTP.

For the backend APIs, however, you need to take network performance into account. Depending on the granularity of your services, interservice communication can result in a lot of network traffic.

Services can quickly become I/O bound. For that reason, considerations such as serialization speed and payload size become more important. Some popular alternatives to using REST over HTTP include gRPC, Apache Avro, and Apache Thrift.

## Further Considerations

Here are some things to think about when choosing how to implement an API.

**REST versus RPC.** Consider the tradeoffs between using a REST-style interface versus an RPC-style interface.

- **REST models resources**, which can be a natural way to express your domain model. It defines a uniform interface based on HTTP verbs, which encourages evolvability. It has well-defined semantics in terms of idempotency, side effects, and response codes.
- **RPC** is more oriented around operations or commands. Because RPC interfaces look like local method calls, it may lead you to design overly chatty APIs.

For a RESTful interface, the most common choice is REST over HTTP using JSON. For an RPC-style interface, there are several popular frameworks, including gRPC, Apache Avro, and Apache Thrift.

**Efficiency.** Consider efficiency in terms of speed, memory, and payload size. Typically a gRPC-based interface is faster than REST over HTTP.

**Interface definition language (IDL).** An IDL is used to define the methods, parameters, and return values of an API. An IDL can be used to generate client code, serialization code, and API documentation. IDLs can also be consumed by API testing tools such as Postman.

**Serialization.** How are objects serialized over the wire? Options include text-based formats (primarily JSON) and binary formats such as protocol buffer. Binary formats are generally faster than text-based formats. However, JSON has advantages in terms of interoperability, because most languages and frameworks support JSON serialization.

**Framework and language support.** HTTP is supported in nearly every framework and language. gRPC, Avro, and Thrift all have libraries for C++, C#, Java, and Python.

**Compatibility and interoperability.** If you choose a protocol like gRPC, you may need a protocol translation layer between the public API and the back end. A gateway can perform that function. If you are using a service mesh, consider which protocols are compatible with the service mesh.

A good baseline recommendation is to choose REST over HTTP unless you need the performance benefits of a binary protocol. REST over HTTP requires no special libraries. It creates minimal coupling, because callers don't need a client stub to communicate with the service. There is rich ecosystems of tools to support schema definitions, testing, and monitoring of RESTful HTTP endpoints. Finally, HTTP is compatible with browser clients, so you don't need a protocol translation layer between the client and the backend.

However, if you choose REST over HTTP, you should do performance and load testing early in the development process, to validate whether it performs well enough for your scenario.

# Lab

## Lab: Implement Azure Logic Apps Integration with Azure Event Grid

✓ **Important:** To download the most recent version of this lab, please visit the AZ-304 [GitHub repository](#)<sup>4</sup>.

Direct link to the [Lab: Implement Azure Logic Apps Integration with Azure Event Grid](#)<sup>5</sup>.

### Lab scenario



Adatum Corporation has an extensive set of on-premises network monitoring framework that rely on the combination of agent-based and agentless solutions to provide visibility into any changes to its environment. The agentless solutions tend to be relatively inefficient since they rely on polling to determine state changes.

As Adatum is preparing to migrate some of its workloads to Azure, its Enterprise Architecture team wants to address these inefficiencies and evaluate the use of event driven architecture available in the cloud. The notion of using events in a solution or application is not new to the team. In fact, they have been promoting the idea of event-driven programming among its developers. One of the core tenets of an event-driven architecture is to reverse the dependencies that existing services may have with each other. Azure provides this functionality by relying on Event Grid, which is a fully managed service that supports the routing of events by utilizing a publisher-subscriber model. At its core, Event Grid is an event routing service that manages the routing and delivery of events from numerous sources and subscribers.

An event is created by a publisher such as a Blob Storage account, an Azure resource group, or even an Azure subscription. As events occur, they are published to an endpoint called a topic that the Event Grid service manages to digest all incoming messages. Event publishers are not limited to services on Azure. It is possible to use events that originate from custom applications or systems that can run from anywhere. This includes applications that are hosted on-premises, in a datacenter, or even on other clouds, if they can post an HTTP request to the Event Grid service.

Event handlers include several Azure services, including serverless technologies such as Functions, Logic Apps, or Azure Automation. Handlers are registered with Event Grid by creating an event subscription. If the event handler endpoint is publicly accessible and encrypted by Transport Layer Security, then messages can be pushed to it from Event Grid.

Unlike many other Azure services, there is no Event Grid namespace that needs to be provisioned or managed. Topics for native Azure resources are built in and completely transparent to users while custom topics are provisioned ad hoc and exist in a resource group. Event subscriptions are simply associated with a topic. This model simplifies management of topics as subscriptions and makes Event Grid highly multi-tenant, allowing for massive scale out.

Azure Event Grid is agnostic to any language or platform. While it integrates natively with Azure services, it can just as easily be leveraged by anything that supports the HTTP protocol, which makes it a very clever and innovative service.

<sup>4</sup> <https://github.com/MicrosoftLearning/AZ-304-Microsoft-Azure-Architect-Design>

<sup>5</sup> [https://aka.ms/304\\_Module\\_13\\_Lab\\_a](https://aka.ms/304_Module_13_Lab_a)

To explore this functionality, the Adatum Architecture team wants to test integration of Azure Logic Apps with Event Grid to:

- detect when the state of a designated Azure VM is changed
- automatically generate an email notification in response to the event

## Objectives

After completing this lab, you will be able to:

- Integrate Azure Logic Apps with Event Grid
- Trigger execution of Logic Apps in response to an event representing a change to a resource within a resource group

## 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\04\azuredeploy30304suba.json
- \AZ303\AllFiles\Labs\04\azuredeploy30304rga.json
- \AZ303\AllFiles\Labs\04\azuredeploy30304rga.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 authentication and authorization for an Azure logic app

1. Create an Azure Active Directory service principal
2. Assign the Reader role to the Azure AD service principal

## Exercise 2: Implement an Azure logic app

The main tasks for this exercise are as follows:

1. Create an Azure logic app
2. Add a trigger to the Azure logic app
3. Add a condition to the Azure logic app
4. Add an action to the Azure logic app

## Exercise 3: Implement an event subscription

The main tasks for this exercise are as follows:

1. Configure event subscription
2. Review the functionality of the Azure logic app
3. Remove Azure resources deployed in the lab

## Module 13 Review Questions

### Module 13 Review Questions



#### Review Question 1

*You are planning the implementation of an order processing web service that will contain microservices hosted in an Azure Service Fabric cluster.*

*You need to recommend a solution to provide developers with the ability to proactively identify and fix performance issues. The developers must be able to simulate user connections to the order processing web service from the internet, as well as simulate user transactions. The developers must be notified if the goals for the transaction response times are not met.*

*What should you recommend?*

- Azure Fabric Analytics
- Azure Network Watcher
- Source Network Address Translation (SNAT)
- Application Insights

#### Review Question 2

*You are designing a microservices architecture that will support a web application.*

*The solution must meet the following requirements:*

- Allow independent upgrades to each microservice.
- Deploy the solution on-premises and to Azure.
- Set policies for performing automatic repairs to the microservices.
- Support low-latency and hyper-scale operations.

*What should you recommend?*

- Azure Service Fabric
- Azure Logic App
- Azure Container Instance
- Azure Virtual Machine Scale Sets

# Answers

## Review Question 1

You are planning the implementation of an order processing web service that will contain microservices hosted in an Azure Service Fabric cluster.

You need to recommend a solution to provide developers with the ability to proactively identify and fix performance issues. The developers must be able to simulate user connections to the order processing web service from the internet, as well as simulate user transactions. The developers must be notified if the goals for the transaction response times are not met.

What should you recommend?

- Azure Fabric Analytics
- Azure Network Watcher
- Source Network Address Translation (SNAT)
- Application Insights

*Explanation*

*Correct Answer: Application Insights. Application Insights allows for the gathering of application information from inside apps irrespective of where they may be running as well as analysis of internal bottlenecks.*

## Review Question 2

You are designing a microservices architecture that will support a web application.

The solution must meet the following requirements:

What should you recommend?

- Azure Service Fabric
- Azure Logic App
- Azure Container Instance
- Azure Virtual Machine Scale Sets

*Explanation*

*Correct Answer: Azure Service Fabric. Azure Service Fabric is the only technology listed above that meets all requirements, especially running on-premises and in the cloud.*



## Module 14 Design Security for Applications

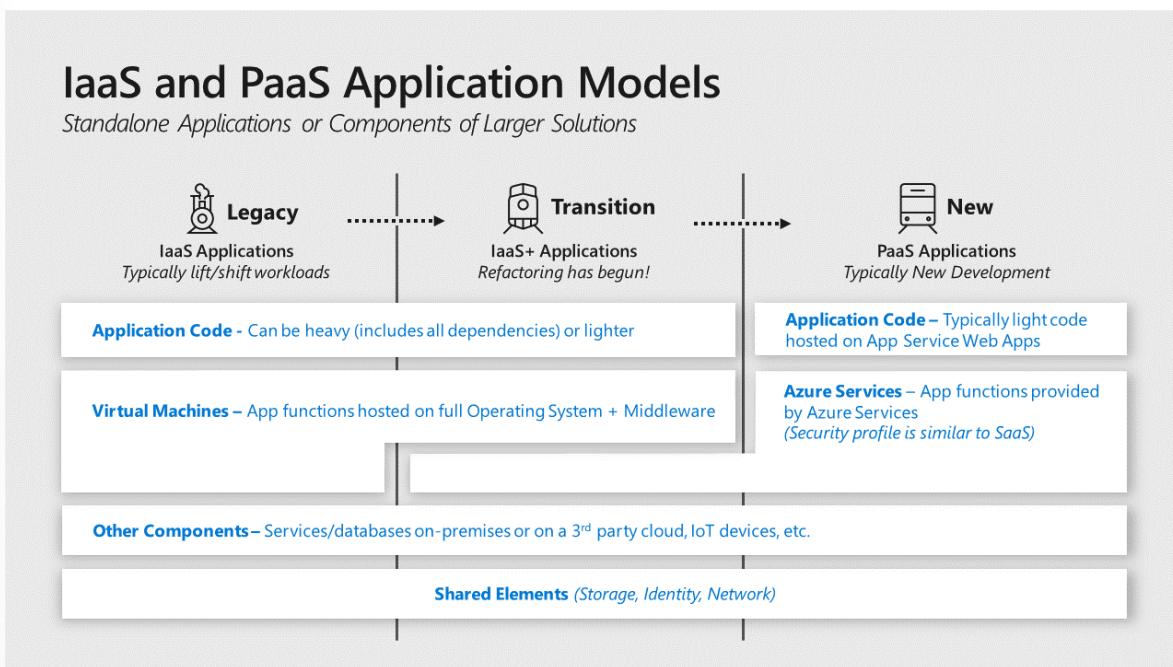
### Security for Applications and Services

#### Security for Applications and Services

Applications and the data associated with them ultimately act as the primary store of business value on a cloud platform. While the platform components like identity and storage are critical elements of the security environment, applications play an outsize role in risks to the business because:

- **Business Processes** are encapsulated and executed by applications and services need to be available and provided with high integrity.
- **Business Data** is stored and processed by application workloads and requires high assurances of confidentiality, integrity, and availability.

This lesson focuses on applications written by your organization or by others on behalf of your organization vs. SaaS or commercially available applications installed on IaaS VMs.



Modern cloud platforms like Azure can host both legacy and modern generations of applications

- **Legacy** applications are hosted on Infrastructure as a Service (IaaS) virtual machines that typically include all dependencies including OS, middleware, and other components.
- **Modern** Platform as a Service (PaaS) applications don't require the application owner to manage and secure the underlying server operating systems (OSes) and are sometimes fully "Serverless" and built primarily using functions as a service.
- **Hybrid:** While hybrid applications can take many forms, the most common is an "IaaS plus" state where legacy applications are transitioning to a modern architecture with modern services replacing legacy components or being added a legacy application.

Securing an application requires security assurances for three different component types:

- **Application Code:** This is the logic that defines the custom application that you write. The security of this code is the application owners' responsibility in all generations of application architecture including any open-source snippets or components included in the code.
- **Application Services:** These are the various standardized components that the application uses such as databases, identity providers, event hubs, IoT device management, and so on. For cloud services this is a shared responsibility:
  - **Cloud Provider** - The security of the underlying service is the responsibility of the cloud provider
  - **Application Owner** - The application owner is responsible for security implications of the configuration and operation of the service instance(s) used by the application including any data stored and processed on the service.
- **Application Hosting Platform** – This is the computing environment where the application actually executes and runs. In an enterprise with applications hosted on premises, in Azure and in third-party clouds like Amazon Web Services (AWS), this could take many forms with significant variations on who is responsible for security:
  - **Legacy Applications** typically require a full operating system (and any middleware) hosted on physical or virtualized hardware. The virtual hardware can be hosted on premises or on Infrastruc-

ture as a Service (IaaS) VMs. This operating system and installed middleware/other components are operated and secured by the application owner or their infrastructure team(s).

The responsibility for the physical hardware and OS virtualization components (virtualization hosts, operating systems, and management services) varies:

- **On premises** - The application owner or their organization is responsible for maintenance and security.
- **IaaS** – The cloud provider is responsible for maintenance and security of the underlying infrastructure and the application owner's organization is responsible for the VM configuration, operating system, and any components installed on it.
- **Modern Applications** are hosted on Platform as a Service (PaaS) environments such as an Azure application service. In most application service types, the underlying operating system is abstracted from the application owner and secured by the cloud provider. Application owners are responsible for the security of the application service configurations that are provided to them.
- **Containers** are an application packaging mechanism in which applications are abstracted from the environment in which they run. These containerized applications fit into either the legacy or modern models above depending on whether they are run on a container service by the cloud provider (Modern Applications) or on a server managed by the organization (on premises or in IaaS).

Topics covered in this lesson include the following:

- Identify and Classify Business Critical Applications
- Adopt the Devops Approach
- Use Cloud Services Instead of Custom Implementations
- Use Native Security Capabilities in Application Services
- Preference for Identity Authentication Over Keys
- Bottom-Up Approach to Reduce Security Bug Volume and Impact
- Top-Down Approach Through Threat Modeling

## Identify and Classify Business Critical Applications



Ensure you have identified and classified the applications in your portfolio that are critical to business functions.

Enterprise organizations typically have a large application portfolio, so prioritizing where to invest time and effort into manual and resource-intensive tasks like threat modeling can increase the effectiveness of your security program.

Identify applications that have a high potential impact and/or a high potential exposure to risk.

**High potential impact** – Identify application that would have a significant impact on the business if compromised. This could take the form of one or more of:

- **Business critical data** – Applications that process or store information, which would cause significant negative business or mission impact if an assurance of confidentiality, integrity, or availability is lost.
- **Regulated data** – Applications that handle monetary instruments and sensitive personal information regulated by standards. For example, payment card industry (PCI) and Health Information Portability and Accountability Act (HIPAA).
- **Business critical availability** – Applications whose functionality is critical to organizations business mission such as production lines generating revenue, devices, or services critical to life and safety, and other critical functions.
- **Significant Access** – Applications which have access to systems with a high potential impact through technical means such as:
  - *Stored Credentials* or keys/certificates that grant access to the data/service
  - Permissions\* granted via access control lists or other means

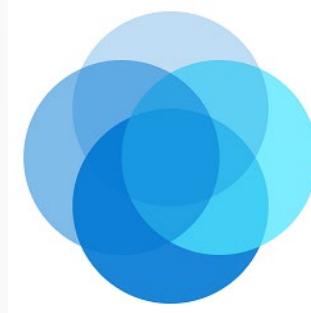
**High exposure to attacks** – Applications that are easily accessible to attackers such as web applications on the open internet. Legacy applications can also be higher exposure as attackers and penetration testers frequently target them because they know these legacy applications often have vulnerabilities that are difficult to fix.

## Adopt the DevOps Approach

Organizations should shift from a ‘Waterfall’ development cycle to DevOps lifecycle of continuous integration, continuous delivery (CI/CD) for applications as fast as is practical. DevOps is the union of people, processes, and tools that enable continuous delivery of value to end users. The contraction of Dev and Ops refers to combining the development and operations disciplines into multi-disciplinary teams that work together with shared and efficient practices and tools.

The DevOps model increases the organization’s ability to rapidly address security concerns without waiting for a longer planning and testing cycle of a waterfall model.

## Use Cloud Services Instead of Custom Implementations



Developers should use services available from your cloud provider for well-established functions like databases, encryption, identity directory, and authentication instead of writing custom versions of them.

These services provide better security, reliability, and efficiency because cloud providers operate and secure them with dedicated teams with deep expertise in those areas. Using these services also frees your

developer resources from reinventing the proverbial wheel so that they can focus development time on your unique requirements for your business. This practice should be followed to avoid risk during new application development as well as to reduce risk in existing applications either during planned update cycle or with a security-focused application update.

Several capabilities that should be prioritized first because of potential security impact:

- **Identity** – User directories and other authentication functions are complex to develop and critically important to security assurances. Avoid using homegrown authentication solutions and favor mature capabilities like Azure Active Directory (Azure AD), Azure AD B2B, Azure AD B2C, or third-party solutions to authenticate and grant permission to users, partners, customers, applications, services, and other entities.
- **Data Protection** – Developers should use established capabilities from cloud providers such as native encryption in cloud services to encrypt and protect data. The security world is littered with examples of failed attempts to protect data or passwords that didn't stand up to real world attacks. If direct use of cryptography is required, developers should call well-established cryptographic algorithms and not attempt to invent their own.
- **Key management** – Ideally use identity for authentication rather than directly handling keys. For situations where accessing services that require access to keys, leverage a key management service like Azure Key Vault or AWS Key Management Service to manage and secure these keys rather than attempting to safely handle keys in application code. You can use CredScan to discover potentially exposed keys in your application code.
- **Application Configurations** – Inconsistent configurations for applications can create security Risks. Azure App Configuration provides a service to centrally manage application settings and feature flags, which helps mitigate this risk.

## Preference for Identity Authentication Instead of Keys



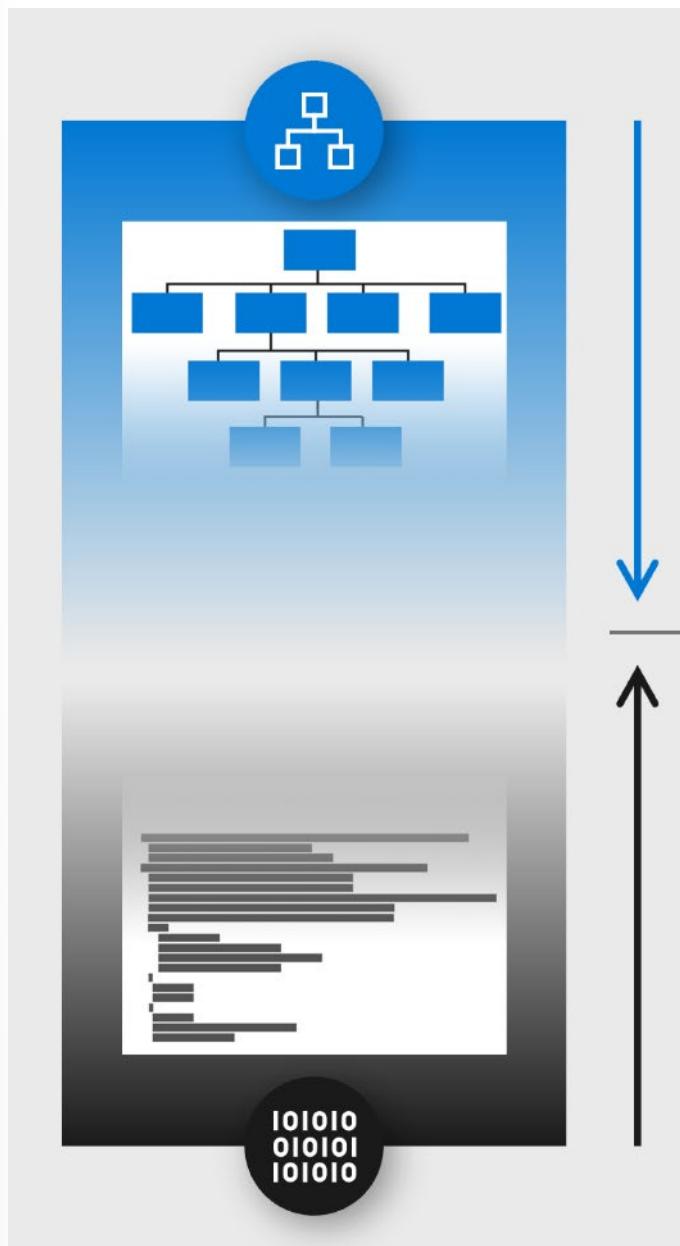
Always authenticate with identity services rather than cryptographic keys when available.

Managing keys securely with application code is difficult and regularly leads to mistakes like accidentally publishing sensitive access keys to code repositories like GitHub. Identity systems offer secure and usable experience for access control with built-in sophisticated mechanisms for key rotation, monitoring for anomalies, and more. Most organizations also have skilled teams dedicated to managing identity systems and few (if any) people actively managing key security systems.

For services that offer the Azure AD authentication like Azure Storage, Azure App Service, Azure Backup, use it for authentication and authorization. To further simplify using identities for developers, you can also take advantage of managed identities to assign identities to resources like VMs and App Services so that developers don't have to manage identities within the application.

## Bottom-Up Approach to Reduce Security Bug Volume and Impact

Reduce the count and potential severity of security bugs in your application by implementing security practices and tools during the development lifecycle.

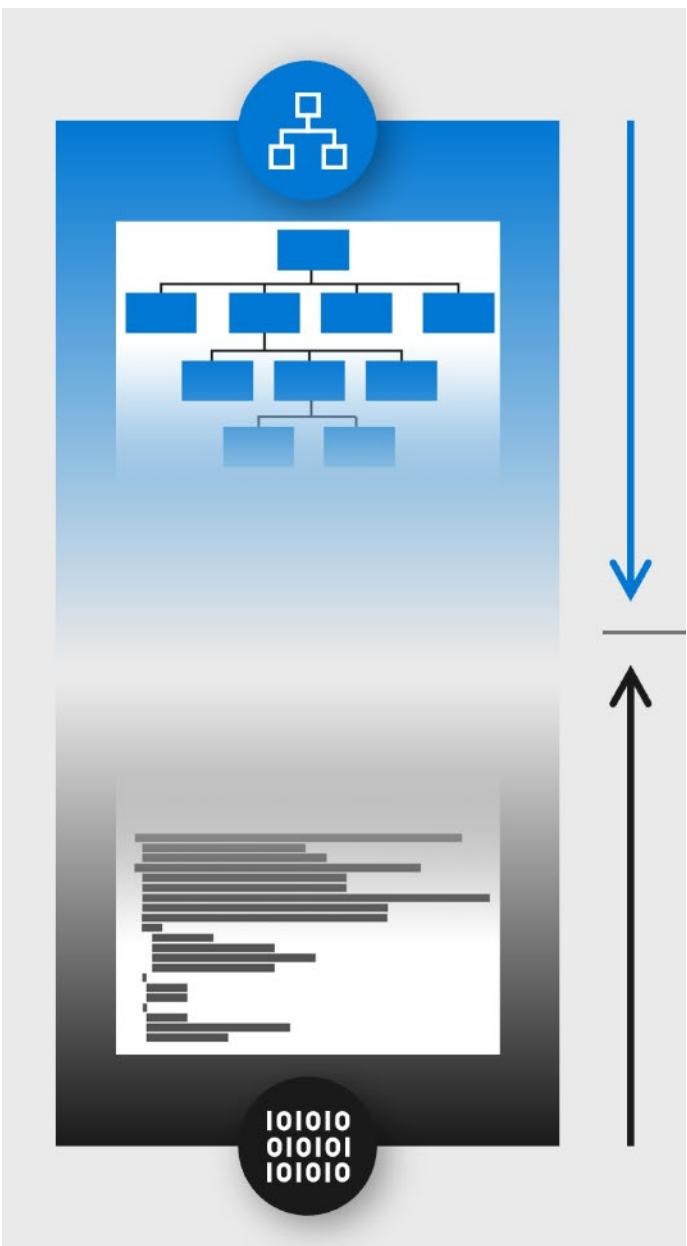


Security bugs can result in an application disclosing confidential data, allowing criminals to alter data/records, or the data/application becoming unavailable for use by customers and employees. Applications will always have some logic errors that can result in security risk, so it is important to discover, evaluate, and correct them to avoid damage to the organization's reputation, revenue, or margins.

Mitigating application risk is achieved by integrating security practices and tools into the development lifecycle, often called a secure development lifecycle (SDL or SDLC).

## Top-down Approach Through Threat Modeling

Perform threat modeling on your business-critical applications to discover and mitigate potential risks to your organization.



Threat modeling identifies risks to the application itself as well as risks that application may pose to your enterprise particularly when evaluating individual applications in a larger system.

Threat modeling can be used at any stage of application development or production, but it is uniquely effective for the design stages of new functionality because no real-world data yet exists for that application.

Because threat modeling is a skill intensive exercise, we recommend taking measures to minimize time investment while maximizing security value:

**Prioritize by risk** - Apply threat modeling first to business-critical applications that would have an outsize impact on the business if compromised

**Limit Scope** - Perform threat modeling in progressive stages of detail to quickly identify quick wins and actionable mitigations before spending a lot of manual effort:

- **Progressively evaluate Application Design** – as resource and expertise are available, move to a more advanced analysis using the STRIDE method **Advanced threat modeling techniques<sup>1</sup>** or another similar one already used by your team. Start with the architecture level design and progressively increase detail as time and resources allow:
  - **System level design** – includes applications and how they interact with each other
  - **Application level** – includes components of the application and how they interact with each other
  - **Component level** – includes how the individual component is composed and how each element of it interacts with each other

**Align with Development lifecycle** – Optimize your efforts by aligning threat modeling activities with your application development lifecycles.

- **Waterfall** – ensure major projects should include threat modeling during the design process and during significant updates to the application.
- **DevOps** – Trigger threat modeling activities at a frequency that adds security value without over-burdening the development teams. Good integration points are during the introduction of significant features or changes to the application and a regular recurring calendar schedule for example, every quarter for business-critical applications.
- **Legacy applications** – These applications typically lack support, source code access, and/or expertise in the organization, so perform threat modeling on a best effort basis with what application knowledge/expertise you have available.

---

<sup>1</sup> <https://docs.microsoft.com/en-us/azure/architecture/framework/security/applications-services>

# Recommend a Solution using Key Vault

## Azure Key Vault Overview



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>
```

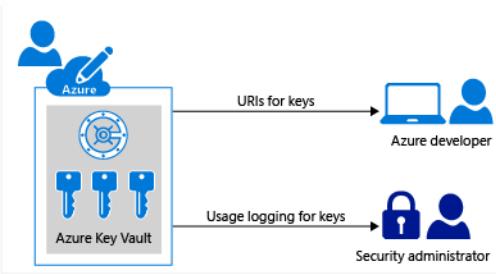
Here's the same command using Azure PowerShell:

```
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.

**Tip** For production use, it's recommended to use HSM-protected keys and use software-protected keys in only test/pilot scenarios. There is an additional charge for HSM-backed keys per-month if the key is used in that month. The summary page has a link to the pricing details for Azure Key Vault.

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 Authentication and Authorization



Key Vault access has two facets: the management of the Key Vault itself, and accessing the data contained in the Key Vault. Documentation refers to these facets as the *management plane* and the *data plane*.

These two areas are separated because the creation of the Key Vault (a management operation) is a different role than storing and retrieving a secret stored in the Key Vault. To access a key vault, all users or applications must have proper *authentication* to identify the caller, and *authorization* to determine the operations the caller can perform.

## Authentication

Azure Key Vault uses Azure Active Directory to authenticate users and applications that try to access a vault. Authentication is always performed by associating the Azure AD tenant of the subscription that the Key Vault is part of and every user or app making a request must be known to the AAD. There is no support for anonymous access to a Key Vault.

## Authorization

Management operations (creating a new Azure Key Vault) use role-based access control (RBAC). There is a built-in role **Key Vault Contributor** that provides access to management features of key vaults, but doesn't allow access to the key vault data. This is the recommended role to use. There's also a **Contributor** role that includes full administration rights - including the ability to grant access to the data plane.

Reading and writing data in the Key Vault uses a separate Key Vault *access policy*. A Key Vault access policy is a permission set assigned to a user or managed identity to read, write, and/or delete secrets and keys. You can create an access policy using the CLI, REST API, or Azure portal as shown below.

## Add access policy

Add access policy

Configure from template (optional)

Key, Secret, & Certificate Management

Key permissions

9 selected

Secret permissions

7 selected

Certificate permissions

15 selected

Select principal

\*

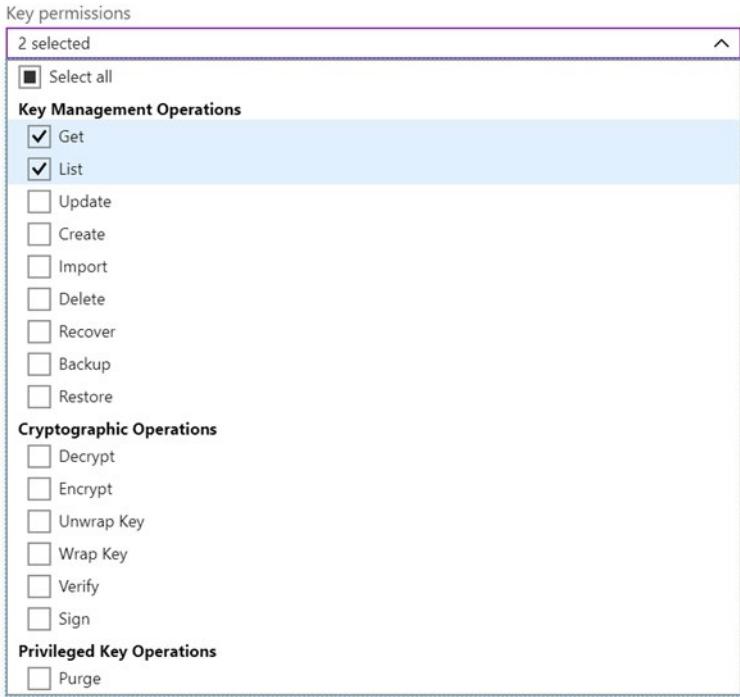
Microsoft Learning Partner >

Authorized application ⓘ

learn-app-dev >

**Add**

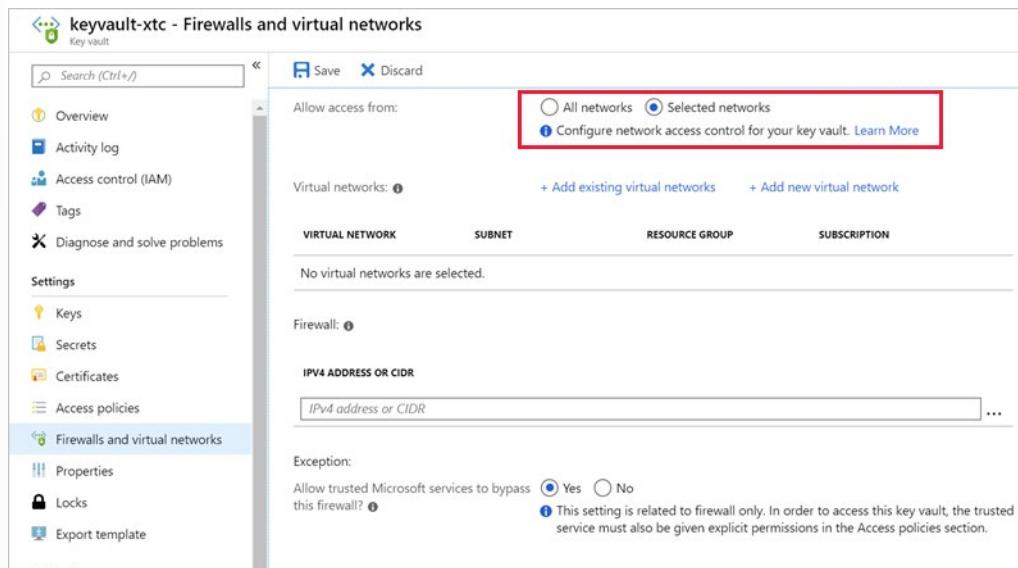
The system has a list of predefined management options that define the permissions allowed for this policy - here we have **Key, Secret, & Certificate Management** selected which is appropriate to manage secrets in the Key Vault. You can then customize the permissions as desired by changing the **Key permissions** entries. For example, we could adjust the permissions to only allow *read* operations:



Developers will only need Get and List permissions to a development-environment vault. A lead or senior developer will need full permissions to the vault to change and add secrets when necessary. Full permissions to production-environment vaults are typically reserved for senior operations staff. For applications, often only Get permissions are required as they will just need to retrieve secrets.

## Restricting network access

Another point to consider with Azure Key Vault is what services in your network can access the vault. In most cases, the network endpoints don't need to be open to the Internet. You should determine the minimum network access required - for example you can restrict Key Vault endpoints to specific Azure Virtual Network subnets, specific IP addresses, or trusted Microsoft services including Azure SQL, Azure App Service, and various data and storage services that use encryption keys.



## Azure Key Vault Availability and Redundancy

Azure Key Vault features multiple layers of redundancy to make sure that your keys and secrets remain available to your application even if individual components of the service fail.

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away but within the same geography. This maintains high durability of your keys and secrets.

✓ **Note:** See the [Azure paired regions<sup>2</sup>](#) document for details on specific region pairs.

If individual components within the key vault service fail, alternate components within the region step in to serve your request to make sure that there is no degradation of functionality. You do not need to take any action to trigger this. It happens automatically and will be transparent to you.

In the rare event that an entire Azure region is unavailable, the requests that you make of Azure Key Vault in that region are automatically routed (failed over) to a secondary region. When the primary region is available again, requests are routed back (failed back) to the primary region. Again, you do not need to take any action because this happens automatically.

Through this high availability design, Azure Key Vault requires no downtime for maintenance activities.

Below are a few things to keep in mind:

- In the event of a region failover, it may take a few minutes for the service to fail over. Requests that are made during this time may fail until the failover completes.
- After a failover is complete, your key vault is in read-only mode. Requests that are supported in this mode are:
  - List key vaults
  - Get properties of key vaults
  - List certificates
  - Get certificates
  - List secrets

<sup>2</sup> <https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions>

- Get secrets
  - List keys
  - Get (properties of) keys
  - Encrypt
  - Decrypt
  - Wrap
  - Unwrap
  - Verify
  - Sign
  - Backup
- After a failover is failed back, all request types (including read and write requests) are available.

## Recommend Solutions using Azure AD Managed Identities

### Azure Active Directory Managed Identities



Azure Key Vault provides a way to securely store credentials, secrets, and other keys, but your code has to authenticate to Key Vault to retrieve them.

Managed identities for Azure resources provides Azure services with an automatically managed identity in Azure AD.

You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

The managed identities for Azure resources feature is free with Azure AD for Azure subscriptions.

### Terminology

The following terms are used throughout the managed identities for Azure resources documentation set:

- **Client ID** - a unique identifier generated by Azure AD that is tied to an application and service principal during its initial provisioning.
- **Principal ID** - the object ID of the service principal object for your managed identity that is used to grant role-based access to an Azure resource.
- **Azure Instance Metadata Service (IMDS)** - a REST endpoint accessible to all IaaS VMs created via the Azure Resource Manager. The endpoint is available at a well-known non-routable IP address (169.254.169.254) that can be accessed only from within the VM.

### How Managed Identities for Azure Resources Works

There are two types of managed identities:

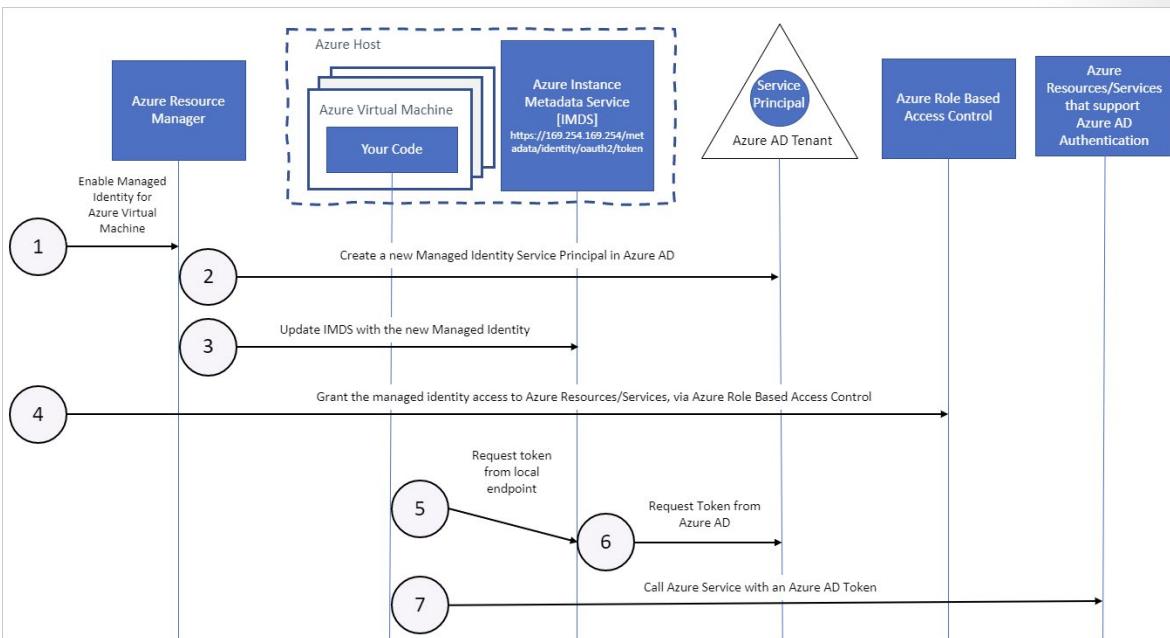
- A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The life cycle of a system-assigned identity is directly tied to the Azure service instance that it's enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.
- A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Azure AD tenant that's trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The

life cycle of a user-assigned identity is managed separately from the life cycle of the Azure service instances to which it's assigned.

Managed identities are service principals locked to be used with Azure resources. When the managed identity is deleted, the corresponding service principal is automatically removed. Also, when a User-Assigned or System-Assigned Identity is created, the Managed Identity Resource Provider (MSRP) issues a certificate internally to that identity.

## System-Assigned Managed Identity and Azure VMs

The following diagram shows how managed service identities work with Azure virtual machines (VMs):



1. Azure Resource Manager receives a request to enable the system-assigned managed identity on a VM.
2. Azure Resource Manager creates a service principal in Azure AD for the identity of the VM. The service principal is created in the Azure AD tenant that's trusted by the subscription.
3. Azure Resource Manager configures the identity on the VM by updating the Azure Instance Metadata Service identity endpoint with the service principal client ID and certificate.
4. After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
5. The code that's running on the VM can request a token from the Azure Instance Metadata service endpoint, accessible only from within the VM: <http://169.254.169.254/metadata/identity/oauth2/token>
  - The resource parameter specifies the service to which the token is sent. To authenticate to Azure Resource Manager, use `resource=https://management.azure.com/`.
  - API version parameter specifies the IMDS version, use `api-version=2018-02-01` or greater.

6. A call is made to Azure AD to request an access token (as specified in step 5) by using the client ID and certificate configured in step 3. Azure AD returns a JSON Web Token (JWT) access token.
7. The code sends the access token on a call to a service that supports Azure AD authentication.

Property	System-assigned managed identity	User-assigned managed identity
Creation	Created as part of an Azure resource (for example, an Azure virtual machine or Azure App Service)	Created as a stand-alone Azure resource
Life cycle	Shared life cycle with the Azure resource that the managed identity is created with. When the parent resource is deleted, the managed identity is deleted as well.	Independent life cycle. Must be explicitly deleted.
Sharing across Azure resources	Cannot be shared. It can only be associated with a single Azure resource.	Can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.
Common use cases	Workloads that are contained within a single Azure resource Workloads for which you need independent identities. For example, an application that runs on a single virtual machine	Workloads that run on multiple resources and which can share a single identity. Workloads that need pre-authorization to a secure resource as part of a provisioning flow. Workloads where resources are recycled frequently, but permissions should stay consistent. For example, a workload where multiple virtual machines need to access the same resource

✓ **Note:** For a list of Azure services that support managed identities for Azure resources feature, see [Services that support managed identities for Azure resources<sup>3</sup>](#).

<sup>3</sup> <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/services-support-msi>

# Module 14 Review Questions

## Module 14 Review Questions



### Review Question 1

You are asked to design a data protection solution for Azure VMs, where all of the VMs use managed disks. The requirements are as follows:

- All data is encrypted at rest
- The use of encryption keys is audited
- Microsoft does not manage the encryption keys, your organization does.

What do you recommend?

- Azure Disk Encryption
- Bitlocker
- Client-side encryption
- Azure Storage Service Encryption

### Review Question 2

Your organization has an Azure subscription with 210 virtual machines.

You have been asked to design a data protection strategy to encrypt the VMs. The requirements are as follows:

- Encrypt disks using by using Azur Disk Encryption
- The solution must allow for encrypting operating system disks and data disks.

What do you recommend?

- A secret
- Bitlocker
- A certificate
- A key

## Review Question 3

You are asked to recommend an identity solution for a customer who is planning to migrate several on-premises applications to Azure.

The requirements are as follows:

- You are working with an existing single-domain on-premises AD forest named tailwind.com with forest functional level at Windows Server 2016.
- Must eliminate the need for hybrid network connectivity.
- Must minimize the management overhead of Active Directory.

What do you recommend?

- Within Azure, deploy additional domain controllers for the tailwind.com domain
- Implement Azure AD DS
- Implement a new Active Directory forest in Azure
- Deploy an additional child domain in tailwind.com within Azure

## Review Question 4

Your company has a line-of-business application that uses a Key Vault named Key\_Vault\_Seattle\_3 for the West US Azure region.

- The company has an Azure Subscription and is located in Seattle.
- Key\_Vault\_Seattle\_3 is routinely backed up.
- You are asked to recommend a disaster recovery plan for Key\_Vault\_Seattle\_3.
- You need to identify where to restore the backup.

What needs to be identified?

- The same region only
- The same geography only
- Key\_Vault\_Seattle\_3 only
- The Azure subscription only

## Review Question 5

You are asked to create an Azure Storage account that uses a custom encryption key.

- The storage account is in the West US Azure region.

What do you need to implement encryption?

- An Azure key vault in the same region as the storage account
- Keys stored in Key Vault that are hardware-protected
- An asymmetric key used for SQL Server TDE (Transparent Data Encryption)
- An Azure subscription

# Answers

## Review Question 1

You are asked to design a data protection solution for Azure VMs, where all of the VMs use managed disks.

The requirements are as follows:

What do you recommend?

- Azure Disk Encryption
- Bitlocker
- Client-side encryption
- Azure Storage Service Encryption

*Explanation*

*Correct Answer: Azure Disk Encryption. Azure Disk Encryption uses Key Vault, performing encryption at rest using customer-managed keys. Key access in Key Vault is auditable.*

## Review Question 2

Your organization has an Azure subscription with 210 virtual machines.

You have been asked to design a data protection strategy to encrypt the VMs.

The requirements are as follows:

What do you recommend?

- A secret
- Bitlocker
- A certificate
- A key

*Explanation*

*Correct Answer: A key. Azure Disk encryption uses the Azure Key Vault this requires the encryption key to be stored in the key vault for use by Bitlocker or dm-crypt.*

## Review Question 3

You are asked to recommend an identity solution for a customer who is planning to migrate several on-premises applications to Azure.

The requirements are as follows:

What do you recommend?

- Within Azure, deploy additional domain controllers for the tailwind.com domain
- Implement Azure AD DS
- Implement a new Active Directory forest in Azure
- Deploy an additional child domain in tailwind.com within Azure

*Explanation*

*Correct Answer: Azure Active Directory Domain Services (Azure AD DS). This scenario is a managed Azure AD DS deployment in Azure, which does not require hybrid network connectivity.*

**Review Question 4**

Your company has a line-of-business application that uses a Key Vault named Key\_Vault\_Seattle\_3 for the West US Azure region.

What needs to be identified?

- The same region only
- The same geography only
- Key\_Vault\_Seattle\_3 only
- The Azure subscription only

*Explanation*

*Correct answer: The same geography only.*

**Review Question 5**

You are asked to create an Azure Storage account that uses a custom encryption key.

What do you need to implement encryption?

- An Azure key vault in the same region as the storage account
- Keys stored in Key Vault that are hardware-protected
- An asymmetric key used for SQL Server TDE (Transparent Data Encryption)
- An Azure subscription

*Explanation*

*Correct answer: An Azure key vault in the same region as the storage account.*