Microsoft

Microsoft Official Course

AZ-300T02

Implementing Workloads and Security

AZ-300T02
Implementing Workloads and Security

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

MICROSOFT LICENSE TERMS

MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. **DEFINITIONS.**
    1. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
    2. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
    3. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facility that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
    4. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of an MPN Member, or (iii) a Microsoft full-time employee.
    5. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
    6. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
    7. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.
    8. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.
    9. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
    10. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.
    11. "MPN Member" means an active Microsoft Partner Network program member in good standing.
    12. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

13. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
14. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.
15. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

2. **USE RIGHTS.** The Licensed Content is licensed not sold. The Licensed Content is licensed on a **one copy per user basis**, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

- 2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

1. **If you are a Microsoft IT Academy Program Member:**

1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
2. For each license you acquire on behalf of an End User or Trainer, you may either:

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**

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**

provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content, **provided you comply with the following:**

3. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
4. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
5. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

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

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

1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
2. For each license you acquire on behalf of an End User or MCT, you may either:

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**

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**

you will provide one (1) MCT with the unique redemption code and instructions on how they can access one (1) Trainer Content, **provided you comply with the following:**

3. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
4. you will ensure that each End User attending a Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
5. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
6. you will ensure that each Trainer teaching a Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
7. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,

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

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:

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**

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**

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. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
4. you will ensure that each End User attending a Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
5. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
6. you will ensure that each Trainer teaching a Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
7. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
8. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
9. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
10. you will only provide access to the Trainer Content to Trainers.

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

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

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

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

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

3. **LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("**Pre-release**"), then in addition to the other provisions in this agreement, these terms also apply:

   1. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.

2. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.
3. **Pre-release Term.** If you are a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("**Pre-release term**"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

4. **SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
   - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
   - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
   - modify or create a derivative work of any Licensed Content,
   - publicly display, or make the Licensed Content available for others to access or use,
   - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
   - work around any technical limitations in the Licensed Content, or
   - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.

5. **RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.
6. **EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www. microsoft. com/exporting.
7. **SUPPORT SERVICES.** Because the Licensed Content is "as is", we may not provide support services for it.

8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
9. **LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
11. **APPLICABLE LAW.**
    1. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
    2. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.
12. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED"AS-IS"AND"AS AVAILABLE. "YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
14. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US$5. 00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

    This limitation applies to

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

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

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

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

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection 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 contre-façon sont exclues.

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

Cette limitation concerne:

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

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

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

Revised November 2014

Contents

Module 0 Start Here

Welcome to Implementing Workloads and Security

Welcome to Understanding Implementing Workloads and Security

Course Overview: Implementing Workloads and Security

Welcome to *Implementing Workloads and Security*. This course is part of a series of five courses to help students prepare for Microsoft's Azure Solutions Architect technical certification exam AZ-300: Microsoft Azure Architect Technologies. These courses are designed for IT professionals and developers with experience and knowledge across various aspects of IT operations, including networking, virtualization, identity, security, business continuity, disaster recovery, data management, budgeting, and governance.

This course teaches IT professionals how to discover, assess, plan and implement a migration of on-premises resources and infrastructure to Azure. Students will learn how to use Azure Migrate to perform the discovery and assessment phase that is critical to a successful migration. They will also learn how to use Azure Site Recovery for performing an actual migration of workloads to Azure. This course focuses on using ASR on a Hyper-V infrastructure to prepare and complete the migration process.

Also, you will learn how to deploy serverless computing features like Azure Functions, Event Grid, and Service Bus. You will see how Azure multi-factor authentication facilitates safeguard access to data and applications, thus helping to meet customer demands for a simple sign-in process. Also, see how to use Azure Active Directory Privileged Identity Management to manage, control, and monitor access to Azure resources within an organization.

Additionally, learn how to manage and maintain infrastructure for core web apps and services that developers build and deploy. Discover how the Azure App Service is used as a Platform as a Service (PaaS) offering for deploying cloud apps for web and mobile environments.

Lastly, you will see how to implement advanced networking features, such as Application Gateway, and how to configure load balancing. See how to integrate on-premises networks with Azure virtual networks and use Network Watcher to monitor and troubleshoot issues.

The outline for this course is as follows:

Module 1 - Evaluating and Performing Server Migration to Azure

This module covers migrating workloads to a new environment, whether it be another datacenter, or to a public cloud, and setting clear goals for the migration. Goals include both technology-focused and business-focused goals for migrations, and how that benefits an organization's business. Activities include components of the Azure migration process: creating a project, creating a collector, assessing readiness, and estimating costs. Additionally, you will receive an overview of Azure Site Recovery (ASR) that includes end-to-end scenarios.

Module 2 - Implementing and Managing Application Services

This module includes the following topics:

-
  - Deploying Web Apps
  - Managing Web Apps
  - App Service Security
  - Serverless Computing Concepts
  - Managing Event Grid
  - Managing Service Bus
  - Managing Logic App

Module 3 - Implementing Advanced Virtual Networking

This module includes the following topics:

-
  - Azure Load Balancer
  - Azure Application Gateway
  - Site-to-Site VPN Connections

As well as an overview of ExpressRoute which allows companies to extend on-premises networks into the Microsoft cloud over a dedicated private connection facilitated by a connectivity provider.

Module 4 - Determining Azure Workload Requirements

A fictitious case study of Contoso, a US-based financial company based in Boston, where there are three additional local branches across the United States. The main datacenter is connected to the internet with a fiber metro Ethernet connection (500 Mbps). Each branch is connected locally to the internet using business class connections, with IPSec VPN tunnels back to the main datacenter. This allows the entire network to be permanently connected, and optimizes internet connectivity.

The module contains the following topics:

-
  - Overview of Customer Case Study
  - Step-by-Step: Determining Azure Workload Requirements
  - Checklist of Assessment Goals

What You'll Learn

-
  - Evaluating and Performing Server Migration to Azure
  - Implementing and Managing Application Services
  - Implementing Advanced Virtual Networking
  - Securing Identities using Azure

Prerequisites

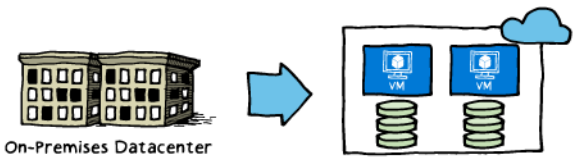
Successful Cloud Solutions Architects begin this role with practical experience with operating systems, virtualization, cloud infrastructure, storage structures, billing, and networking.

Module 1 Evaluating and Performing Server Migration to Azure

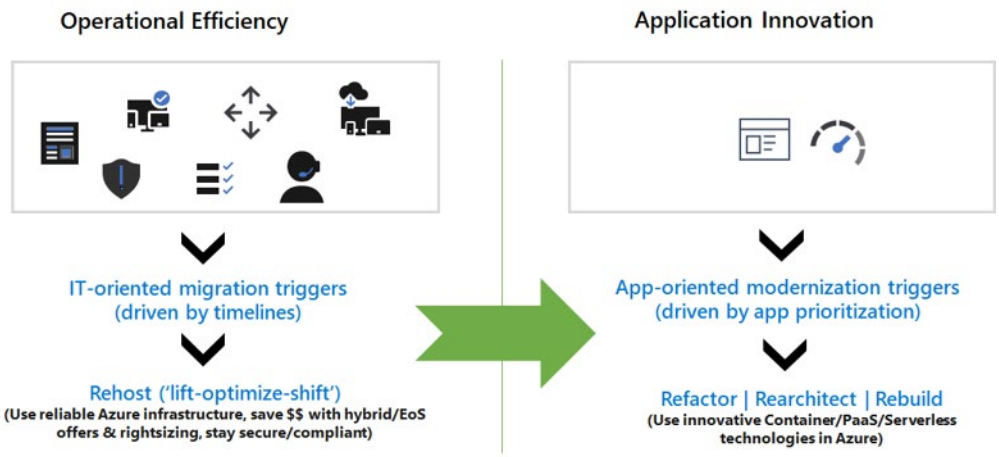
Migrate to Azure

Migration Goals

When migrating any workload to a new environment, whether it be another datacenter, or to a public cloud, you should have a clear set of goals for migration in mind. Note that there are both technology-focused and business-focused goals that motivate potential migrations, but any such effort should result in direct benefits to the organization's business.



Organizations consider a migration of their on-premises assets to the cloud for a variety of reasons, ranging from acquisition integration to application innovation. For IT organizations, the reasons fall broadly into two main patterns:



- A need for greater operational efficiency (followed by further enhancing and modernizing workloads)
- A desire to modernize their applications and take fuller advantage of the capabilities offered by the cloud

The two patterns are not necessarily mutually exclusive, and as the diagram shows, one pattern will often lead to another, or in some cases may happen in parallel. Organizations must consider both infrastructure and application dependencies when deciding to migrate.

Operational efficiency

This pattern is often characterized by urgency and deadlines. For example, the integration of an acquisition into an IT organization tends to come with legal contracts that are time-bound. Or perhaps the lease on a datacenter is expiring and organizations must decide whether or not to renew the lease. Additionally, datacenter capacity may be insufficient to support the business needs. This all contributes to the desire to get out of the datacenter by a certain date.

In such cases, a migration to the cloud is an appealing incentive to significantly improve operational efficiency. This leads to cost savings, increased security and compliance, and raises the level of availability and performance.

Application innovation

In this pattern, company leaders want to modernize those applications that are considered key to the future growth and success of the business. IT organizations will consider their traditional datacenter applications against the capabilities offered by the cloud for applications that are designed for the cloud. This involves deciding on the right model, whether to *refactor*, *rearchitect*, or *rebuild* those existing applications.

This differs from scenario 1 where the emphasis is on a *lift-optimize-shift* approach. Here, a more strategic approach will involve consideration of innovations such as containers and serverless technologies.

Migration benefits

Most businesses today already have one or more workloads running in the cloud. Although cloud environments are generally scalable, reliable, and highly available, organizations must take multiple factors into account when driving their decision to migrate their workloads. Balancing benefits and risks,

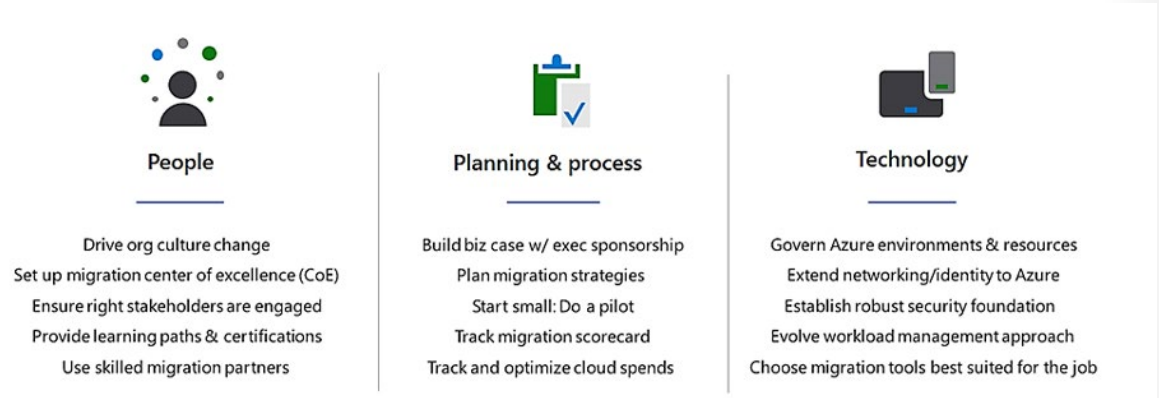
evaluating the cloud service model and type that is ideal for the business are critical in deriving business value. There are many problems that moving to the cloud can solve. The following list of business benefits is typical, but by no means all-inclusive.

- With cloud service providers managing thousands of clients at a time, security upgrades are equitably applied to the entire user base.
- Many security solutions can be managed on-premises and in the cloud – simplifies transition to a hybrid environment.
- Cloud-based solutions significantly enhance backup, disaster recovery, archiving, and management of data and applications.
- Moving to the cloud enables businesses to modernize Network-Attached Storage (NAS) with scalable file sharing and global access.
- Continuous innovation cycles (DevOps) move beyond periodic refresh and allow innovation to keep up with the business. Today's cloud solutions accommodate and optimize legacy applications across any operating system or business function — ensuring continued benefits from previous investments.
- Companies can manage and protect data and applications regardless of location (including hybrid scenario, with minimal latency, optimized security and essentially limitless scalability.)
- Significant reduction in TCO by cutting out big hardware and infrastructure investments, while increasing efficiency and functionality.
- Access to new tools to enhance the customer experience — media streaming, web hosting, API management, big data and more.

Migration Approach - Best Practices

✓ See **Azure migration center**[1] for details of best practices.

Let's consider some important best practices under the familiar framework of *people*, *process* and *technology*.



People

It's imperative to ensure that your organization is properly skilled to successfully adopt Azure. This includes organizational change management, setting up a dedicated migration center of excellence,

1 https://azure.microsoft.com/en-us/migration/resources/

setting up training and certification paths, and even if you have a great in-house team, finding a skilled migration partner as an outside balancing voice for your organization.

Process and planning

Strong planning ensures successful migration. This includes strong executive sponsorship, a compelling business case, and clear success metrics. Having a strong app portfolio evaluation process which identifies the right mix of migration strategies is crucial – this is where you would need to make decisions like which workloads to migrate versus. modernize.

The recommended guidance is that whenever you are up against a time bound IT trigger, use the rehost strategy and then modernize after you move the workload to Azure. Conversely, refactor or rearchitect strategies might be appropriate when the trigger comes from the business or app development teams. It is also important to start with a migration pilot and go through the full migration journey. This enables organizations to harvest learnings and adjust their approach before scaling migration efforts.

Technology

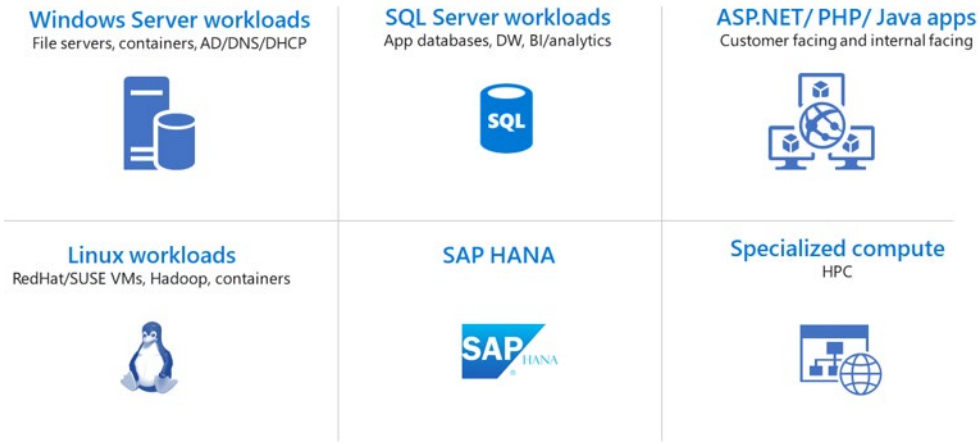
You need to consider investing in a few critical capabilities as you look to scale your Azure migration efforts:

- **Choosing the right Azure migration tools** – As described above, Microsoft has a comprehensive set of Azure and third party migration tools. Choose the one that best meets your requirements – **Azure migration center**[2] provides specific guidance to help you make the best choice. The goal should be to ensure a successful migration experience versus regardless of the tool used.
- **Azure resource governance** - Without a standard governance model, you run the risk of inefficiency or losing control around your cloud resources. Defining standardized cloud environments provides a governance model that provides you with the needed control while allowing app teams to move quickly. As described above, Azure Blueprints helps solve this challenge with a templatized approach that includes the artifacts needed to deploy a fully compliant target environment on Azure.
- **Extending identity / networking to Azure** - Identity and networking are critical issues to plan and solve for. You need a common identity infrastructure which can help you quickly establish single sign-on access to your migrated workloads. For apps/workloads that are distributed across Azure and on-premises, you need secure, dedicated connectivity to ensure workload needs are met. Azure AD Connect can help you replicate on-premises AD to Azure AD, while Azure ExpressRoute connectivity sets you up to extend your on-premises AD into Azure.
- **Integrated Security / Management tools** - You will have assets in both Azure and on-premises environments as you migrate. Organizations often have questions about how to operate across these hybrid environments. In the near term, this means you need to integrate your existing management tools and approach with Azure-native security and management tools. You can then plan the transition to Azure-native tools over time, as your workload profile shifts to Azure.

Common Migration and Modernization Projects

As a previous topic explained, organizations may choose to migrate as part of a *lift-optimize-shift* approach, or migrate workloads in order to modernize their applications, implementing a *refactor*, *rearchitect*, or *rebuild* approach. As mentioned, some migration and modernization projects may also happen in parallel.

2 https://azure.microsoft.com/en-us/migration/resources/

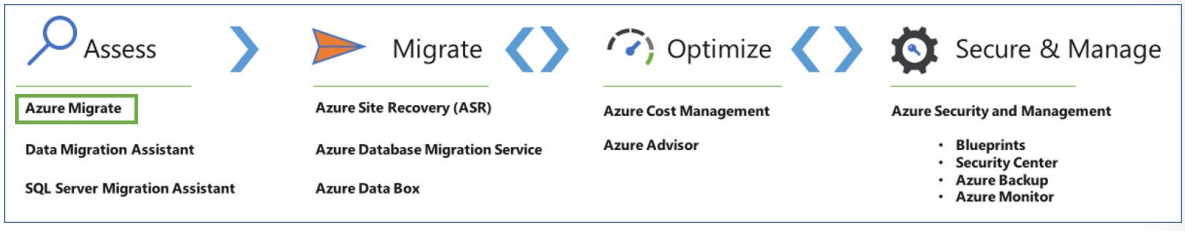


What are some common migration and modernization projects?

- **Windows Server workloads.** For example a set of file servers that can simply be moved to the cloud in bulk. Or containers in an existing Windows Server on-premises environment that need to be provisioned. Also, core infrastructure functionality, where you have roles and servers that can be easily migrated.
- **SQL Server workloads.** Examples include application-serving databases, analytics and Data Warehouse solutions.
- **ASP.NET applications**, obviously related to Windows Server, but commonly PHP and Java apps are common examples of workloads suitable for migration and modernization.
- **Linux Workloads** Virtual machines and special purpose applications. interestingly, Linux workloads that start in RedHat and SUSE can scale to become Hadoop clusters.
- **Specialized projects.** For example, projects involving SAP and specialized compute scenarios, such as HPC.

Migration Phases

When planning for migration of workloads to Azure, consider the following phases: assess, migrate, optimize and secure and manage.



Assess. In the Assess phase you work to get better visibility of applications, workloads, and data in your environment, and assess the optimal resource level to run them in Microsoft Azure. Use this information to help decide which workloads to move. Azure Migrate is the primary tool for this, and includes:

- Automated server, app, and database discovery.
- Intelligent workload right-sizing and costing for maximum ROI.
- Workload configuration analyses and recommendations.

 The next lesson and lab will go into more detail about Azure Migrate for assessing and discovering your on-premises workloads and resources.

Migrate. In the Migrate phase you move selected workloads to Azure. There are a variety of sources including physical servers and virtualized workloads hosted in Hyper-V or VMware environments. Azure Site Recovery is the primary tool in this area and includes:

- Lifting and shifting of servers, apps, databases, and data.
- Containerization of existing applications and infrastructure.
- Modernization options for apps and databases.

Optimize. In the Optimize phase you fine tune your Azure-based workloads and maximize your ROI. In this course, you will learn how you can use Azure Migrate to assess your on-premises environment, but partner tools are also available if you need some richer assessment capabilities.

Secure and Manage In the Secure and Manage phase, you use Azure services to protect and manage your virtual machines, applications, and data.

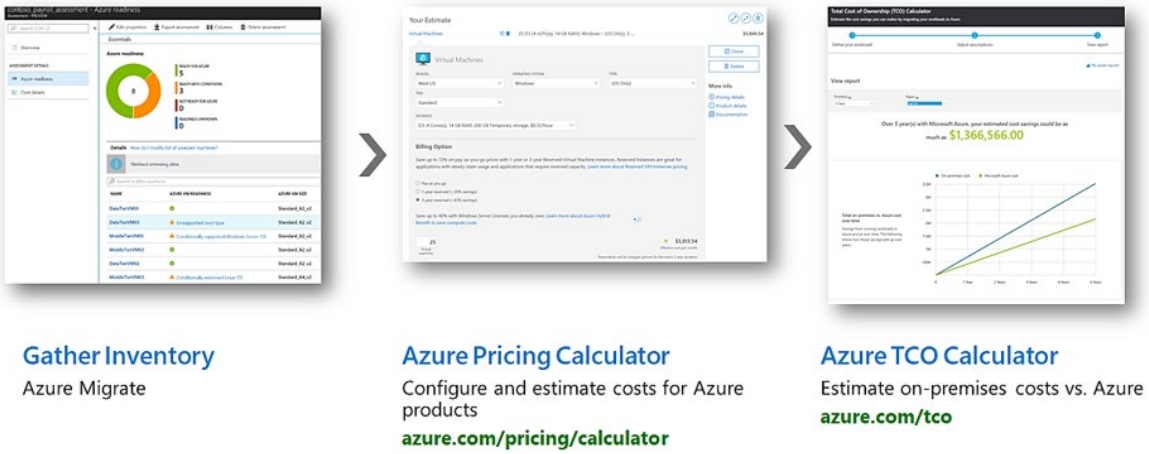
- Azure Security Center for security management across your hybrid cloud workloads.
- Secure your cloud application data against ransomware and human error with Azure Backup
- Azure Monitor, Log Analytics, and Application Insights for tracking health and performance of your cloud apps, infrastructure, and data

 Individual Partners can also assist with the other phases of the migration journey. For example, with security and management, there are many Microsoft partners to help you with backup, monitoring, security assessments, and cost management.

For more information, you can see:

Azure migration partners - **https://azure.microsoft.com/en-us/migration/partners/**

Best Practice Example - Building a Cloud Business Case



✓ Make sure to look at licensing and leverage Hybrid Use Benefits for Windows and SQL Server as well as Reserved Instance to save up to 80 percent on cloud spend.

Migration Tools and Services

Tools for managing different stages of an Azure migration

Once the workloads are running in Azure, there is a set of native Azure services to assist with each of the migration phases, some of which were introduced in the previous topic. For example, Azure Migrate for assessment and discovery, Azure Site Recovery for migrating workloads, and Azure Security Center for ongoing security and management.

In addition, there is a set of independent software vendor (ISV) tools that are available to help with each stage of the migration journey, as shown in the following illustration:

Microsoft solution providers

In addition to third party tools and ISV solutions, there are skilled migration partners available in most regions, who can provide additional expertise as needed for your Azure migration project. In the reference link below, you can search for a partner based on organization size and location.

For more information, see:

Find a Microsoft Solution Provider - **https://azure.microsoft.com/en-us/migration/partners/**

Assessment and Discovery – Azure Migrate

Overview of the Azure Migrate Service

Azure Migrate provides a hub of tools that help you to discover, assess, and migrate apps, infrastructure, and workloads to Microsoft Azure. The hub includes Azure Migrate tools, and third-party independent software vendor (ISV) offerings.

When planning for assessment of large number of Hyper-V VMs, there are a couple of things to think about:

- Plan Azure Migrate projects: Figure out how to deploy Azure Migrate projects. For example, if your data centers are in different geographies, or you need to store discovery, assessment or migration-related metadata in a different geography, you might need multiple projects.
- Plan appliances: Azure Migrate uses an on-premises Azure Migrate appliance, deployed as a Hyper-V VM, to continually discover VMs for assessment and migration. The appliance monitors environment changes such as adding VMs, disks, or network adapters. It also sends metadata and performance data about them to Azure. You need to figure out how many appliances to deploy.

Use the limits summarized in this table for planning.

Planning	Limits
Azure Migrate projects	Assess up to 35,000 VMs in a project.
Azure Migrate appliance	An appliance can discover up to 5000 VMs. An appliance can connect to up to 300 Hyper-V hosts. An appliance can only be associated with a single Azure Migrate project. Any number of appliances can be associated with a single Azure Migrate project.
Group	You can add up to 35,000 VMs in a single group.
Azure Migrate assessment	You can assess up to 35,000 VMs in a single assessment.

For more information, you can see:

Assess large numbers of Hyper-V VMs for migration to Azure - **https://docs.microsoft.com/en-us/azure/migrate/scale-hyper-v-assessment**

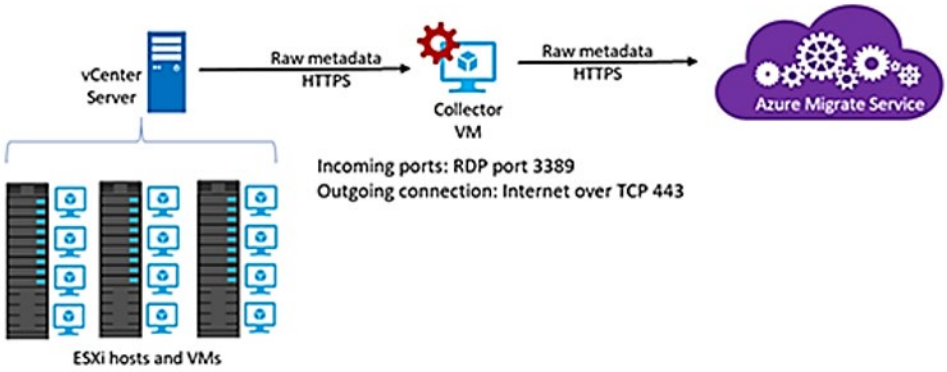
Create a project - **https://docs.microsoft.com/en-us/azure/migrate/create-manage-projects**

Azure Migrate - Process Overview

We've talked about the concepts and use cases for Azure Migrate. Now let's look at the process of using Azure Migrate to discover and assess on-premises workloads for migration to Azure. We'll begin by looking at a basic architectural illustration of that process.

Architecture

The basic architecture of the Azure Migration service is shown in the following diagram. Azure Migrate service works to discover information about ESXi hosts and VMs in a VMware vCenter server. An assessment is created as an outcome of the discovery process.



Process

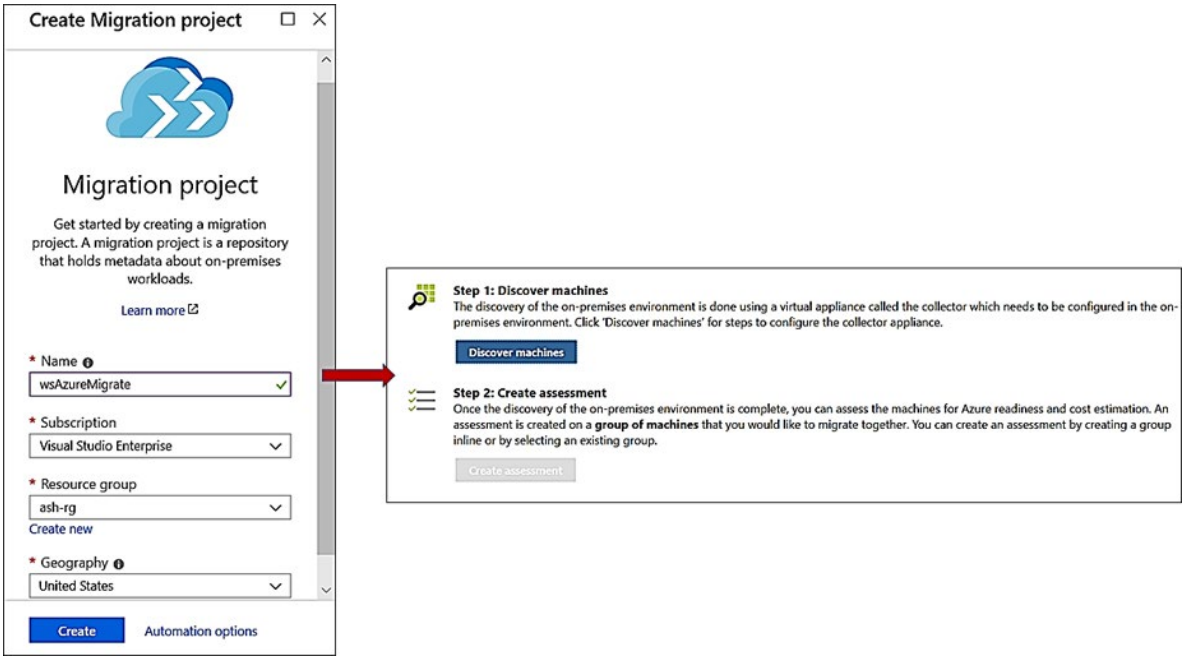
Here are the basic steps.

- **Create a project**. In Azure, create an Azure Migrate project.
- **Discover the machines**. Azure Migrate uses an on-premises VM called the collector appliance, to discover information about your on-premises machines. To create the appliance, you download a setup file in Open Virtualization Appliance (.ova) format and import it as a VM on your on-premises vCenter Server. You connect to the VM using console connection in vCenter Server, and then run the collector application in the VM to initiate discovery.
- **Collect the information**. The collector collects VM metadata using VMware PowerCLI cmdlets. Discovery is agentless and doesn't install anything on VMware hosts or VMs. The collected metadata includes VM information (cores, memory, disks, disk sizes, and network adapters). It also collects performance data for VMs, including CPU and memory usage, disk IOPS, disk throughput (MBps), and network output (MBps).
- **Assess the project**. The metadata is pushed to the Azure Migrate project. You can view it in the Azure portal. For the purposes of assessment, you can gather the discovered VMs into groups. For example, you might group VMs that run the same application. For more precise grouping, you can use dependency visualization to view dependencies of a specific machine, or for all machines in a group and refine the group. Once your group is formed, you create an assessment for the group. After the assessment finishes, you can view it in the portal, or download it in Excel format.

Discovery of On-premises Environment

Create a project

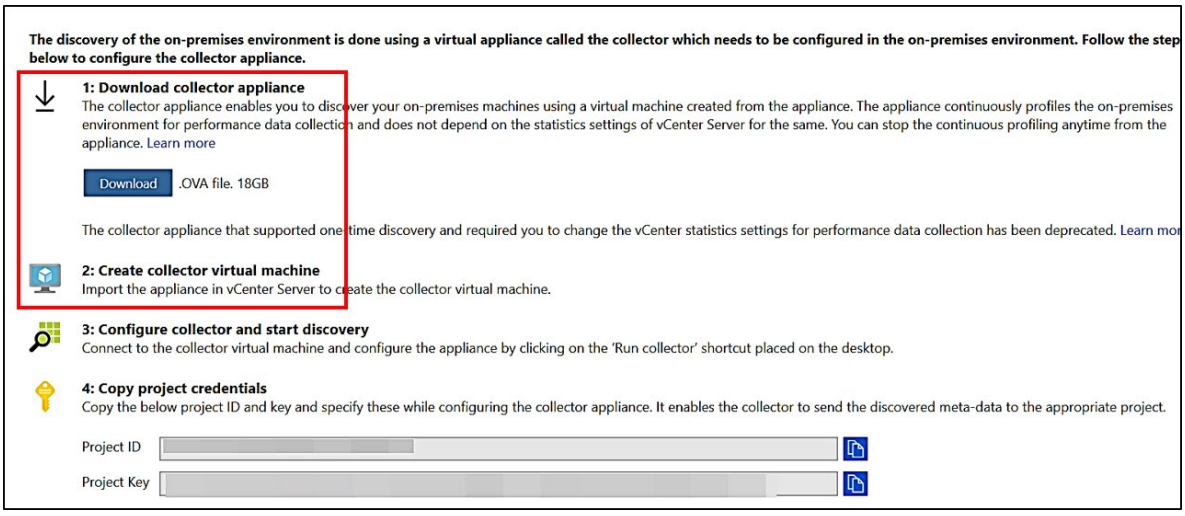
You can create the Azure Migrate project from the portal. It is as simple as filling out Name, Subscription, Resource Group, and Location. The Azure Migrate project holds the metadata of your on-premises machines and enables you to assess migration suitability.



 Azure supports discovery of up to 35,000 servers in an Azure Migrate project. If you have a larger environment with more than 35,000 servers, you can scale out by splitting the discovery into and creating multiple projects.

Creating a Collector

The discovery of the on-premises environment is done using a virtual appliance called the Collector. The Collector is configured in the on-premise environment. There are four basic steps, as shown in the screenshot:



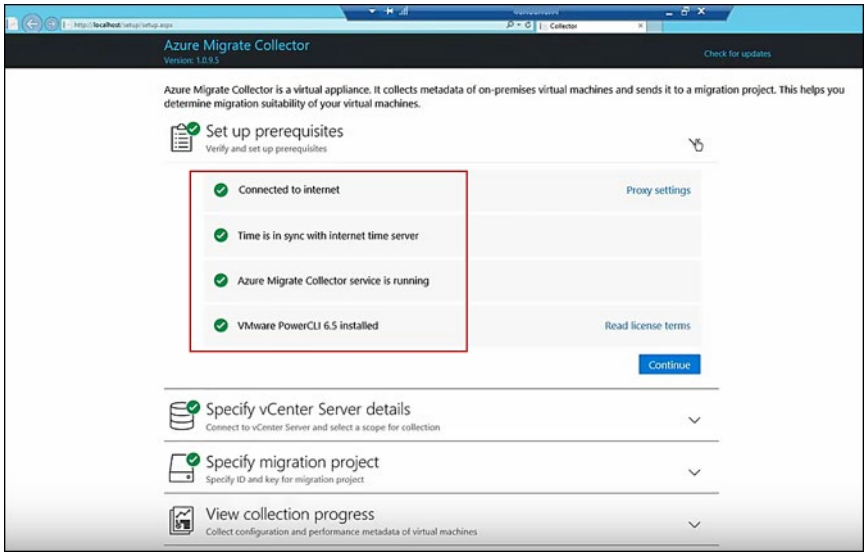
1. **Download the Collector Appliance**. The Collector appliance is a complete, preconfigured single file in Open Virtualization Appliance (.ova) format that you download from the Azure Migrate project on the Discovered Machines blade.
2. **Create the Collector Virtual Machine**. After the download is complete, you then import the appliance into the on-premises environment. For example, for a VMware environment you can use a vCenter Server to import the .ova file and create the Collector machine.

Configuring the Collector

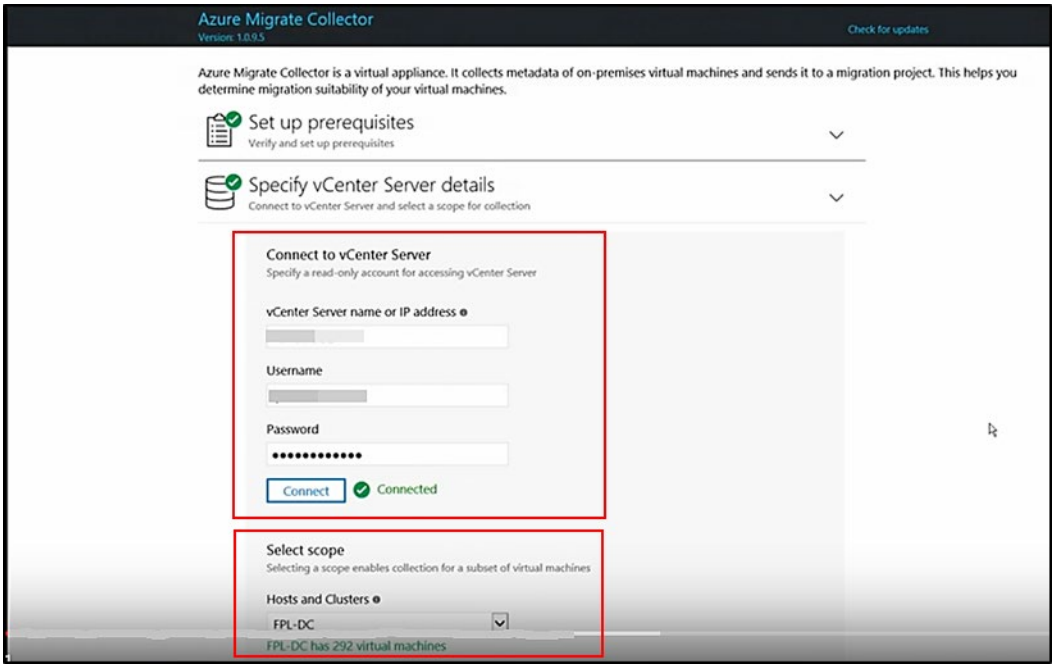
Once you have downloaded the collector appliance and imported it into a virtual machine that's now running your collector, you then log into the virtual machine for the first time. You are presented with a very simple four step process that helps you configure your Azure Migrate project to get started with assessments.

In the following example, we are using a vCenter environment.

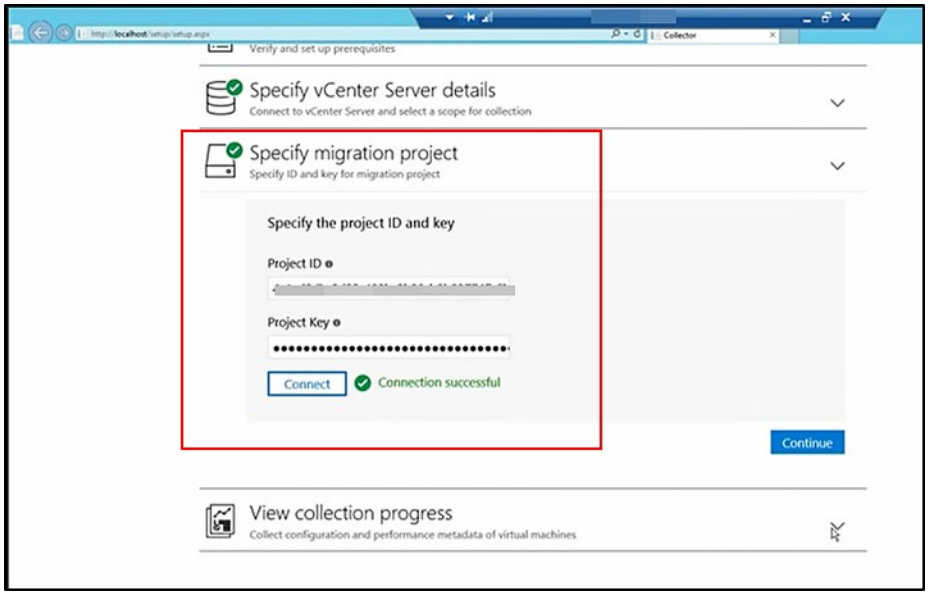
1. **Configure the Collector and Start Discovery**. Once the machine is created you can connect to collector and run the appliance using the shortcut on the desktop. Again, using a VMware environment as an example, you will be asked to set up prerequisites, which includes:
   - Accept licensing terms
   - Check your connection to the internet
   - Make sure your time is in sync with the internet time server
   - Ensure you have a current version of the VMware PowerShellCLI installed. (If not, the tool automatically installs it.)



2. **Specify the vCenter server**. You then specify the vCenter server that you are going to use along with the credentials and the location for that vCenter environment.You can also scope your discovery based on the hosts and the clusters that you want to discover. This is particularly helpful if you are running a multi-tenanted environment and you don't want to discover everything at the same time in one project.



3. **Obtain Project Credentials**. In addition to the credentials for the vCenter server to which you are attaching, the Collector will need the Azure Migrate project ID and key that was generated in Azure when you created the migration project. This enables the Collector to send the discovered metadata to the appropriate Azure Migrate project. Once the Collector is running you can view the metadata being collected from the VMs. Typically, for 100 VMs, the collector takes around an hour for discovery to finish.

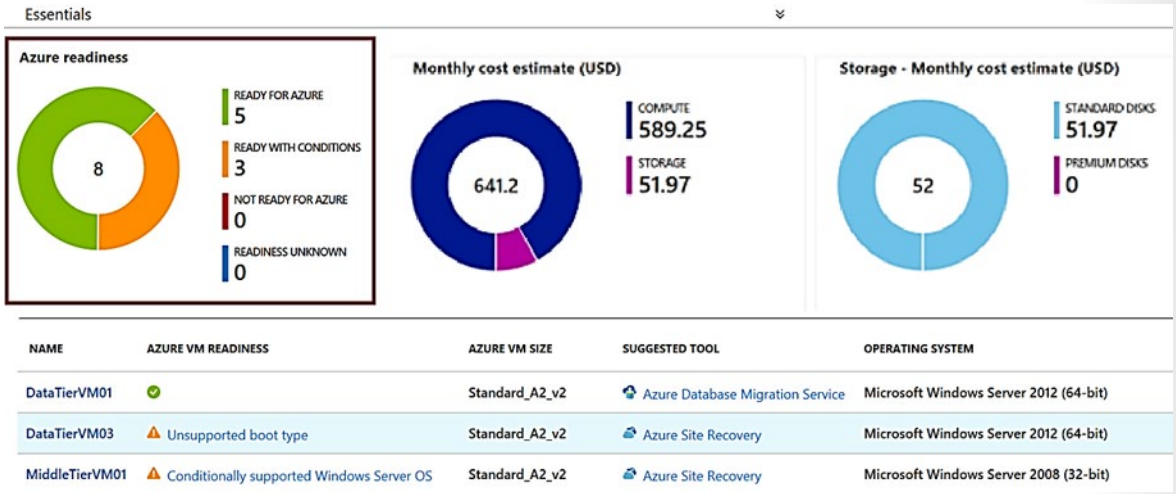


 Keep in mind that the discovery process is a read-only inspection of your VMs and their metadata, including performance history, which you will use for right-sizing those VMs in Azure.

Assessing Readiness

The discovery process results in an assessment, which provides a dashboard view of the discovery results. The assessment details highlight two key areas:

- Readiness status for the Azure environment
- Monthly estimates for compute and storage costs



The Azure readiness view in the assessment shows the readiness status of each VM. The Azure readiness view in the assessment shows the readiness status of each VM, whether or not each VM is compatible with Azure, and a recommended VM SKU for each machine. Depending on the properties of the VM, each VM can be marked as:

- **Ready for Azure (green)**. For VMs that are ready, Azure Migrate recommends a VM size in Azure. The next topic covers how the recommended size is determined.
- **Ready with conditions (Orange)** and **Not ready for Azure (Red)**. For these VMs, Azure Migrate explains the readiness issues and provides remediation steps. Several things are considered in making this determination: boot type, cores, memory, storage disks, networking components, and operating system. For example, a machine with an older version of Windows Server OS might be not ready for Azure. Read more at the reference link.
- **Readiness unknown (Blue)**. The VMs for which Azure Migrate cannot identify Azure readiness (due to data unavailability) are marked as readiness unknown. For example, a VM that was offline.

Assessing VM Sizing

Performance-based assessment

You can choose to migrate all your VMs directly as to Azure or optimize your workloads as part of the migration using performance-based assessment. The performance-based assessment profiles the workload over a specified duration and allows you to select the percentile utilization, accounting for the peaks and valleys inherent in the workload utilization.

After a machine is marked ready for Azure, Azure Migrate sizes the VM and its disks for Azure and uses the performance-based sizing method by default. This is the best method when you may have over-allocated the on-premises VM, the utilization is low, and you would like to right-size the VMs in Azure to save cost.

Mapping Azure VMs to on-premises VM requirements

For performance-based sizing, Azure Migrate starts with the disks attached to the VM, followed by network adapters, and then maps an Azure VM based on the compute requirements of the on-premises VM.

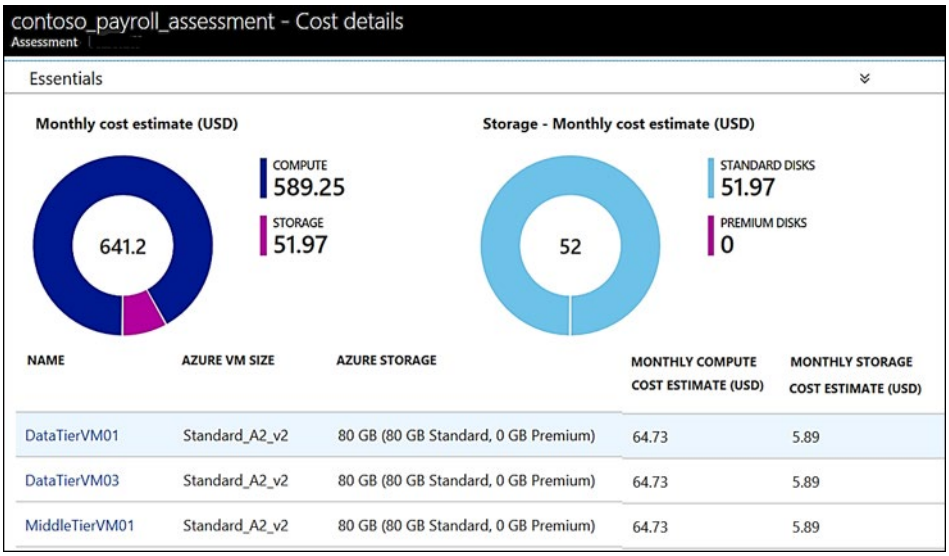
- **Storage**. Azure Migrate tries to map every disk attached to the machine to a disk in Azure.
- **Network**. Azure Migrate tries to find an Azure VM that can support the number of network adapters attached to the on-premises machine and the performance required by these network adapters.
- **Compute**. After storage and network requirements are calculated, Azure Migrate considers CPU and memory requirements to find a suitable VM size in Azure.

Using a VMware environment, for example, Azure Migrate collects performance history of on-premises VMs from the vCenter Server. To ensure accurate right-sizing, you should ensure that the statistics setting in vCenter Server is set to level 3 and wait for at least a day before initiating discovery of the on-premises VMs. If the statistics setting in vCenter Server is below level 3, performance data for disk and network is not collected.

✓ The alternative to performance based sizing is **As on-premises** sizing. Azure Migrate allocates a VM SKU in Azure based on the size allocated on-premises. Similarly, for disk sizing, it looks at the Storage type and recommends the disk type accordingly. The default storage type is Premium disks.

Estimating Cost

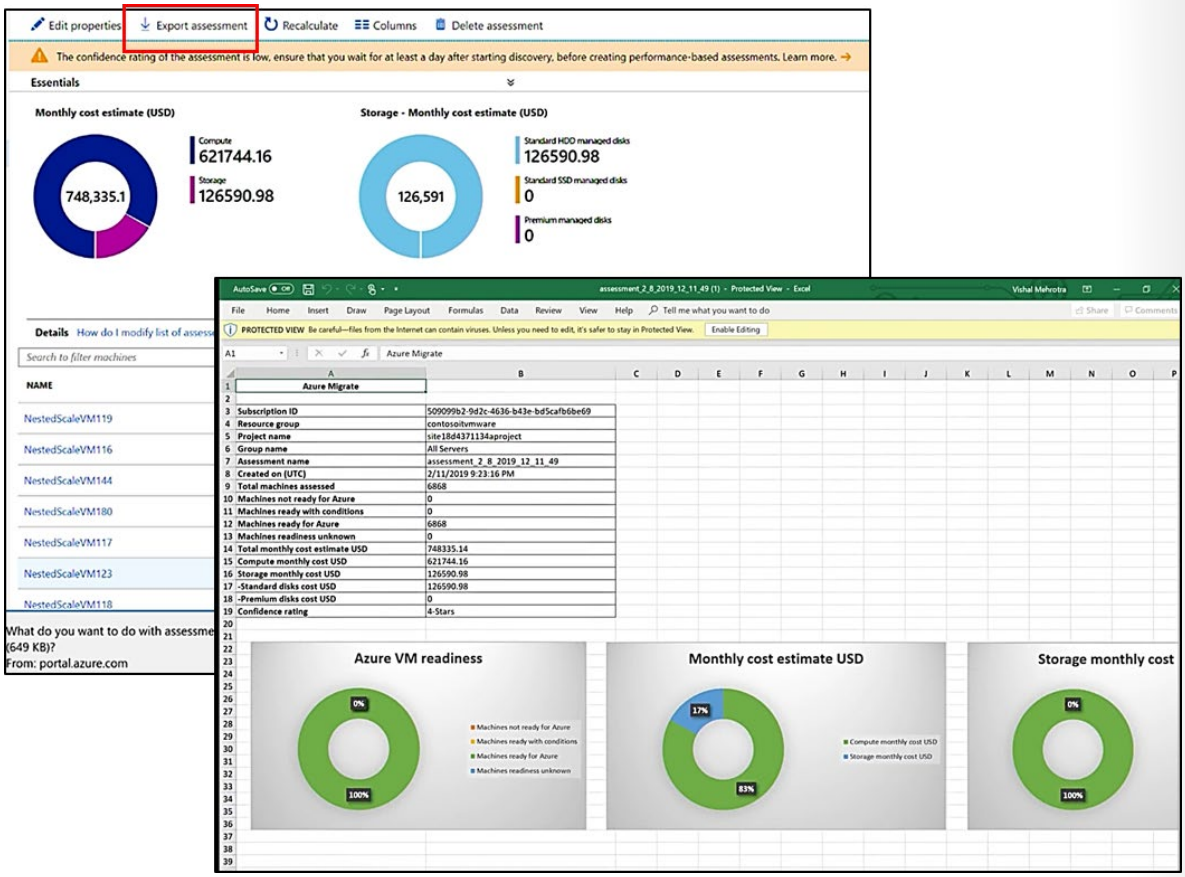
The Cost assessment view shows the total compute and storage cost of running the VMs in Azure along with the details for each machine. Cost estimates are calculated considering the size recommendations done by Azure Migrate for a machine, its disks, and the assessment properties. Estimated monthly costs for compute and storage are aggregated for all VMs in the group.



Compute cost. Using the recommended Azure VM size, Azure Migrate uses the Billing API to calculate the monthly cost for the VM. The calculation takes the operating system, software assurance, reserved instances, VM uptime, location, and currency settings into account. It aggregates the cost across all machines, to calculate the total monthly compute cost.

Storage cost. The monthly storage cost for a machine is calculated by aggregating the monthly cost of all disks attached to the machine. Azure Migrate calculates the total monthly storage costs by aggregating the storage costs of all machines. Currently, the calculation doesn't take offers specified in the assessment settings into account.

Azure Migrate also provides an export of the data captured as part of the assessment as a CSV file to allow further data manipulation.



Subscription ID	509099b2-9d2c-4636-b43e-bd5cafb6be69
Resource group	contosoitvmware
Project name	site18d4371134aproject
Group name	All Servers
Assessment name	assessment_2_8_2019_12_11_49
Created on (UTC)	2/11/2019 9:23:16 PM
Total machines assessed	6868
Machines not ready for Azure	0
Machines ready with conditions	0
Machines ready for Azure	6868
Machines readiness unknown	0
Total monthly cost estimate USD	748335.14
Compute monthly cost USD	621744.16
Storage monthly cost USD	126590.98
-Standard disks cost USD	126590.98
-Premium disks cost USD	0
Confidence rating	4-Stars

✓ The cost estimation provided by Azure Migrate is for running the on-premises VMs as Azure Infrastructure as a service (IaaS) VMs. Azure Migrate does not consider any Platform as a service (PaaS) or Software as a service (SaaS) costs.

Customize the Assessment

What-if analysis

Azure Migrate also provides the capability to do a more detailed *what-if* analysis with a property assessment. For example, you can select a particular target region and determine the cost of running your workloads in one region versus another. Or you can calculate the cost of using reserved instances versus no reserved instances.

As mentioned in a previous discussion of VM sizing, Azure Migrate provides for a performance-based versus As on-premises sizing assessment. Additionally, you can prevent Azure Migrate from automatically mapping to the best SKU option if you have organizational requirements that you want to ensure are maintained. For example, you may have a requirement to use only General purpose compute SKUs. And finally, for those workloads that are not running all the time, you can model how those workloads perform using Azure Hybrid Benefit.

By customizing different assessments, you can perform different what-if analyses, to help select the best way for your organization to migrate to Azure.

Editing assessment properties

In addition to the options listed in the table below, you can customize other options like currency, discounts, VM uptime, and performance history duration, making it a straightforward task to create an assessment or set of assessments that give you the best migration solution based on your particular needs.

Setting	Details	Default
Target location	The Azure location to which you want to migrate. Azure Migrate currently supports 30 regions.	West US 2 is the default location.
Pricing tier	You can specify the **pricing tier (Basic/Standard)** *(https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general)* for the target Azure VMs.	By default the **Standard** *(https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general)* tier is used.
Storage type	You can specify the type of disks you want to allocate in Azure.	The default value is Premium managed disks.
Comfort factor	Azure Migrate considers a buffer (comfort factor) during assessment. This buffer is applied on top of machine utilization data for VMs.	Default setting is 1.3x.

For more information, you can see:

What's in an assessment? - **https://docs.microsoft.com/en-us/azure/migrate/migrate-overview#whats-in-an-assessment**[3]

Products available by region - **https://azure.microsoft.com/en-us/global-infrastructure/services/**

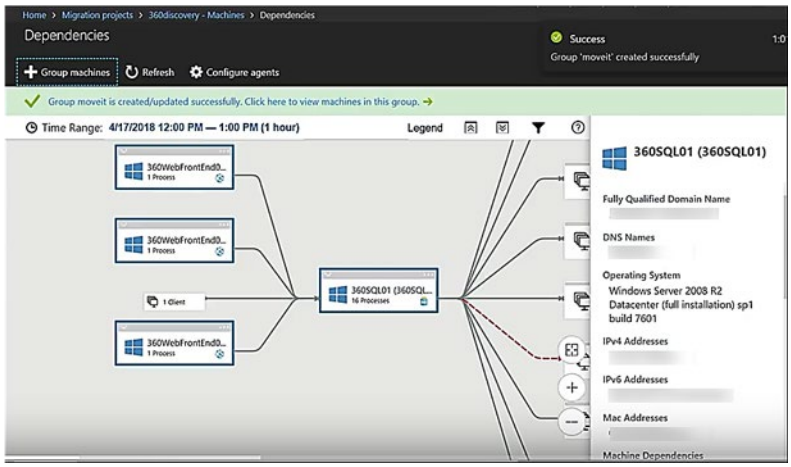
Grouping VMs for Assessment

App dependency mapping

The Azure Migrate services assesses groups of on-premises machines for migration to Azure. You can use the dependency visualization functionality in Azure Migrate to create groups of related machines that need to be migrated together to Azure. By viewing the view network dependencies of machines to group related machines, you can ensure that you migrate all the machines and dependencies that make up an application and therefore need to be migrated together.

The SQL Server application in the diagram has been mapped out and shows relationships to some frontend web servers. These machines can now be assembled into a group representing the application.

3 https://docs.microsoft.com/en-us/azure/migrate/migrate-overview



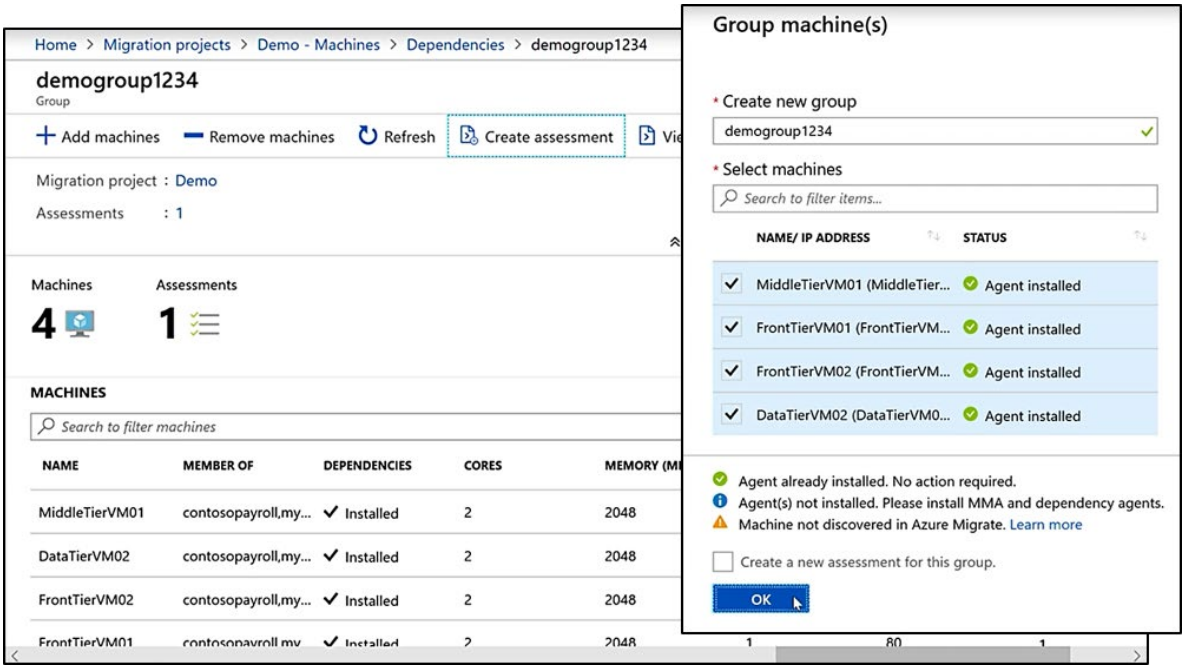
Using a dependency map to create groups

Having discovered the machines in your environment, you can now start creating assessments on those machines. An assessment is created on a group of machines that are moved to Azure as a unit.

There are two ways in which you can do this:

1. If an organization already has a complete understanding of their on-premises environment, it can simply create the group(s) manually in Azure Migrate and create an assessment the group.
2. However, if an organization does not have complete clarity about their environment, they can use the dependency visualization in Azure Migrate to create the groups. Using the dependency map, you can select the machines you want to group and create a move group.

Leveraging this functionality does require the installation of an agent for each machine on which you want to view dependencies. The dependency view shows all the inbound and outbound connections of the server graphically. You can also look at an expanded view of each VM and the processes running inside the VM, as well as the port and IP address details of the client and server connections. You can use this dependency application to identify connections which are relevant to your applications, and remove any connections which are not required.



Troubleshooting Azure Migrate

Most issues with Azure Migrate involve collecting information. Here are a few of the most common issues and errors.

- **Migration project creation failed**. This issue can happen when users do not have access to the Azure Active Directory (Azure AD) tenant of the organization. When a user is added to an Azure AD tenant for the first time, he/she receives an email invite to join the tenant. Users need to go to the email and accept the invitation to be added to the tenant. Once the invite is accepted, the user needs to sign out of Azure portal and sign-in again, as refreshing the browser will not work. The user can then try creating the migration project again.
- **No performance data**. This can occur if the statistics setting level on a vCenter server is set to less than three. At level three or higher, vCenter stores VM performance history for compute, storage, and network. For less than level three, vCenter doesn't store storage and network data, but CPU and memory data only.
- **Collector is not able to connect to the internet**. This can happen when the machine you are using is behind a proxy. Make sure you provide the authorization credentials if the proxy needs one, or import the required proxy certificate on to the Collector VM.
- **Date and time synchronization error**. The server clock might be out-of-synchronization with the current time by more than five minutes. Change the clock time on the collector VM to match the current time.
- **Error UnableToConnectToServer**. There was no endpoint listening at https://Servername.com:9443/sdk that could accept the message. Check if you are running the latest version of the collector appliance, if not, upgrade the appliance.

✓ If you have an error code, you can look it up at the reference link. The link also has information on collecting logs.

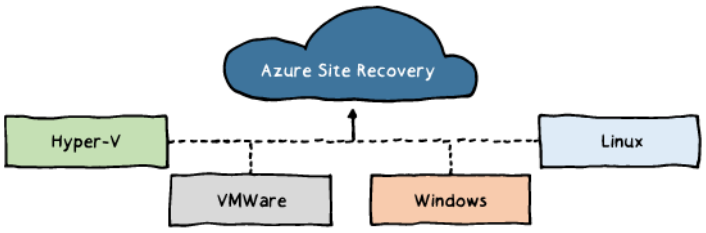
For more information you can see:

Troubleshoot common errors - **https://docs.microsoft.com/en-us/azure/migrate/troubleshooting-general#troubleshoot-common-errors**[4]

Azure Migrate forum - **https://social.msdn.microsoft.com/Forums/en-US/home?forum=AzureMigrate**

Azure Site Recovery (ASR) Scenarios

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



Azure Site Recovery works in the following three scenarios:

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

✓ Are you considering using Azure Site Recovery?

Azure Site Recovery (ASR) Features

Here are some reasons to use Azure Site Recovery.

- **Eliminate the need for disaster recovery sites**. Your environment can be protected by automating the replication of the virtual machines based on policies that you set and control. Site Recovery is heterogeneous and can protect Hyper-V, VMware, and physical servers.
- **Reduce infrastructure costs**. Lower your on-premises infrastructure costs by using Azure as a secondary site for conducting business during outages. Or, eliminate datacenter costs altogether by moving to Azure and setting up disaster recovery between Azure regions. You can pre-assess network, storage, and compute resources needed to replicate applications from on-premises to Azure—and pay only for compute and storage resources needed to run apps in Azure during outages.

4 https://docs.microsoft.com/en-us/azure/migrate/troubleshooting-general

- **Automatically replicate to Azure**. Automate the orderly recovery of services in the event of a site outage at the primary datacenter. Automate the orderly recovery of services in the event of a site outage at the primary datacenter.
- **Safeguard against outages of complex workloads**. Protect applications in SQL Server, SharePoint, SAP, and Oracle.
- **Extend or boost capacity**. Applications can be Migrated to Azure with just a few clicks or burst to Azure temporarily when you encounter a surge in demand.
- **Continuous health monitoring**. Site Recovery monitors the state of your protected instances continuously and remotely from Azure. When replicating between two sites you control, your virtual machines' data and replication remains on your networks. All communication with Azure is encrypted.

✓ Are you interested in any of these specific features? Which one is most important to you?

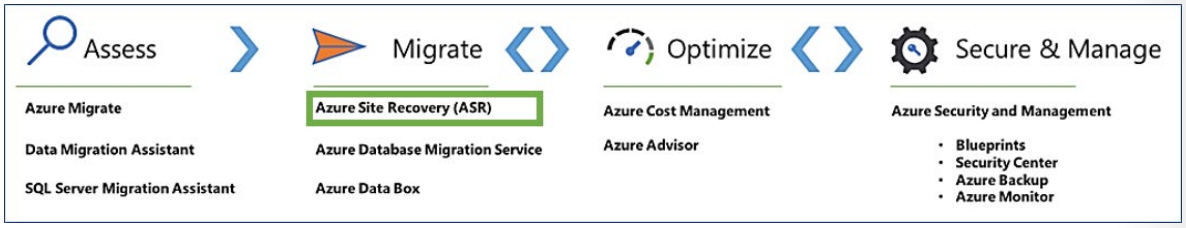
For more information, you can see:

Site Recovery - **https://azure.microsoft.com/en-us/services/site-recovery/**

Site Recovery Pricing - **https://azure.microsoft.com/en-us/pricing/details/site-recovery/**

Implementing a Migration (Azure Site Recovery)

Overview of Azure Site Recovery (ASR)



In the previous module, we reviewed the Assess process. In this module we are focusing on the Migrate phase using Azure Site Recovery (ASR).

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads up and running, when planned and unplanned outages occur.

Azure Recovery Services contributes to your BCDR strategy:

- **Site Recovery service**: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- **Backup service**: The Azure Backup service keeps your data safe and recoverable by backing it up to Azure.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs and physical servers.

After you've assessed on-premises machines, you can use a couple of tools to perform the migration:

- **Azure Site Recovery**: You can use Azure Site Recovery to migrate to Azure. To do this, you **prepare the Azure components**[5] you need, including a storage account and virtual network. On-premises, you prepare your Hyper-V or VMware environment. When everything's prepared, you set up and enable replication to Azure, and migrate the VMs. Learn more.
- **Azure Database Migration**: If on-premises machines are running a database such as SQL Server, MySQL, or Oracle, you can use the **Azure Database Migration Service**[6] to migrate them to Azure. Which you will learn in the next Module.

Reference material: **https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview**

5 https://docs.microsoft.com/en-us/azure/site-recovery/tutorial-prepare-azure
6 https://docs.microsoft.com/en-us/azure/dms/dms-overview

Azure Site Recovery At-A-Glance

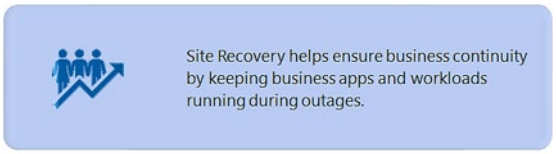
Automated Protection	Continuous Health Monitoring	Orchestrated Recovery
• Delivers on-going replication of virtual machines • Integrates with Hyper-V Replica and System Center Virtual Machine Manager technologies • Integrates with VMware	• Continuously and remotely monitors application availability • Only Virtual Machine Manager servers communicate directly with Azure	• Orchestrates orderly recovery of virtual machines that compose multi-tier services • Offers customizable recovery plans • Simplifies recovery plan testing

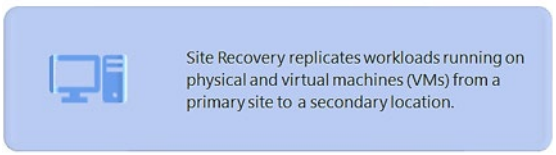
Additional ASR features:

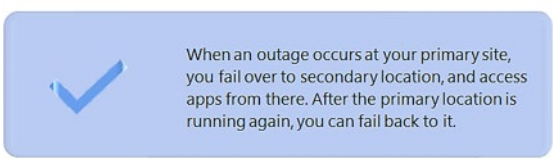
- Eliminating the need for disaster recovery sites
- Reducing infrastructure costs
- Automatically replicating to Azure
- Safeguarding against outages of complex workloads
- Extending or boosting capacity
- Continuous health monitoring

Azure Site Recovery Features

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



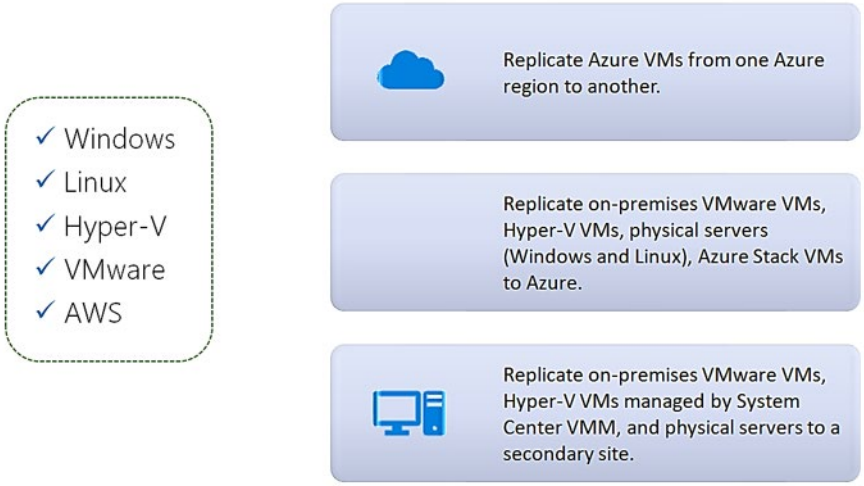




The Site Recovery service contributes to a robust BC/DR solution that protects your on-premises physical servers and virtual machines by orchestrating and automating replication and failover to Azure, or to a secondary on-premises datacenter.

- **Simplify** - Site Recovery helps simplify your BC/DR strategy by making it easy to configure replication and run failover and recovery for your on-premises workloads and applications.
- **Replication** - You can replicate on-premises workloads to Azure storage, or to a secondary data-center.
- **Vault** - To manage replication, you set up a Site Recovery vault in an Azure region you select. All metadata remains within that region.
- **Metadata** - Unless you are using Azure as the storage location for your replicas, no application data is sent to Azure. Site Recovery only needs metadata such as virtual machine and VMM cloud names, to orchestrate replication and failover.
- **Connection to Azure** - Management servers communicate with Azure depending on your deploy-ment scenario. For example, if you're replicating virtual machines located in an on-premises VMM cloud, the VMM server communicates with Site Recovery over an encrypted outbound HTTPS connec-tion. No connection is required from the virtual machines or Hyper-V hosts.
- **Hyper-V Replica** - Azure Site Recovery leverages Hyper-V Replica for the replication process and can also use SAN replication if you're replicating between two on-premises VMM sites. Site Recovery uses smart replication, replicating only data blocks and not the entire VHD for the initial replication. For ongoing replication only delta changes are replicated. Site Recovery supports offline data transfer and works with WAN optimizers.

Replication Scenarios



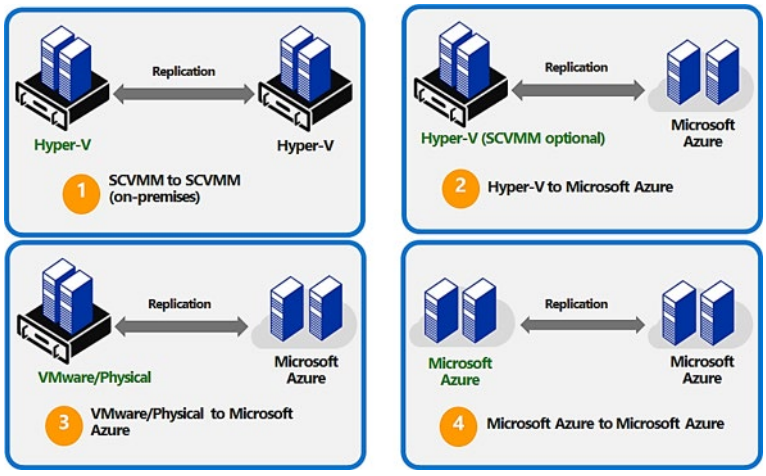
You can use Azure Site Recovery to replicate on-premises physical or virtual machines running Windows or Linux. Azure Site Recovery includes support for both Hyper-V and VMware virtual machines. You can replicate data from your on-premises datacenter to Azure or to a secondary site. Orchestration is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

Supported replication

The following table provides some more details about supported replication scenarios:

Supported	Details
Replication scenarios	Replicate Azure VMs from one Azure region to another.
	Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure.
	Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site.
Regions	Review **supported regions** *(https://azure.microsoft.com/en-us/global-infrastructure/services/?products=site-recovery)* for Site Recovery.
Replicated Machines	Review the replication requirements for **Azure VM** *(https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix#replicated-machine-operating-systems)* replication, **on-premises VMware VMs and physical servers** *(https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix#replicated-machines)*, and on-premises **Hyper-V VMs** *(https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix#replicated-vms)*.
Workloads	You can replicate any workload running on a machine that's supported for replication. In addition, the Site Recovery team have performed app-specific testing for a **number of apps** *(https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-workload#workload-summary)*. An example of a workload is taking an entire on-premise SharePoint farm and migrating it into Azure.

Azure Site Recovery – Key Infrastructure Scenarios



What are the different infrastructures that Azure Site Recovery can provide a solution for?

1. **Hyper-V to Hyper-V (On Premises)** - For customers who have multiple sites, or work with a service provider as a secondary site, and Hyper-V is running on both sites, they can take advantage of Azure Site Recovery to orchestrate the replication and recovery between those sites. In that example, the engine of replication will be Hyper-V Replica, an inbox VM replication technology that is built into Windows Server 2012 and Windows Server 2012 R2.
2. **SAN Replication (On-Premises)** - For customers with an investment in SAN technology, that includes replication in the box, through integration with Hyper-V, System Center and Azure Site Recovery, customers can orchestrate the replication and recovery of their key workloads between those sites, this time, harnessing the power of the SAN, through asynchronous or synchronous replication, to transfer data between sites.
3. **Hyper-V to Microsoft Azure** - For customers who do not have a second site, and are running Hyper-V on their primary site, using Azure Site Recovery, customers can orchestrate the replication and recovery of their on-premises workloads into the Azure datacenters, enabling this as a target for failover in the event of a disaster. The engine of replication in this example is Hyper-V Replica.

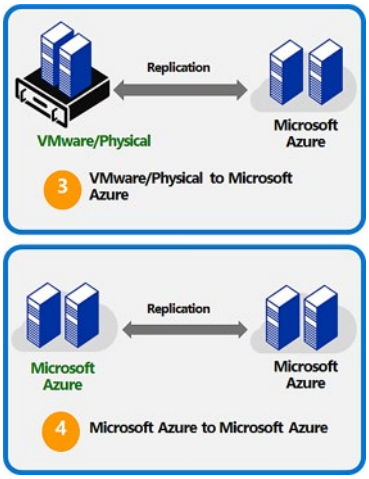
✓ **Note**: In each of the previous three scenarios, we can replace Hyper-V with a VMM cloud.

4. **VMWare/Physical to VMWare (On Premises)** – Using Azure Site Recovery, customers can orchestrate the replication and recovery of key workloads from physical, or VMware-based sites, over to a secondary site, running VMware.
5. **VMWare/Physical to Microsoft Azure** – ASR also allows you to replicate and recover VMware-based VMs into Microsoft Azure.
6. **Microsoft Azure to Microsoft Azure** - you can use Site Recovery to manage migration of Azure VMs to a secondary region. To migrate Azure VMs, you enable replication for them, and fail them over from the primary region to the secondary region of your choice.

Infrastructure Scenarios

You can use Azure Site Recovery to replicate on-premises physical or virtual machines running Windows or Linux. Azure Site Recovery includes support for both Hyper-V and VMware virtual machines. You can

replicate data from your on-premises datacenter to Azure or to a secondary site. Orchestration is built in with Azure Site Recovery, which means that the management of replication, failover, and recovery is included. For example, should a virtual machine or service fail in your datacenter, you can use Azure Site Recovery to failover to the replicated resource in either Azure or your secondary site.



Server Migration Scenarios

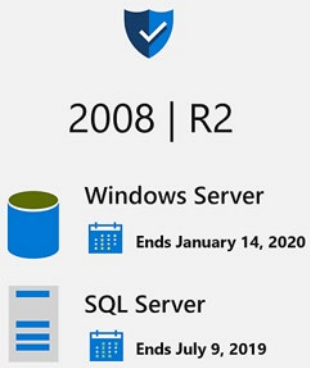
There are some specific scenarios that make good candidates for consideration as migration projects.

Amazon Web Services (AWS) VMs

You can use ASR to migrate virtual machines from AWS to Azure. When you migrate AWS EC2 instances to Azure, the VMs are treated like physical, on-premises computers.

End of support scenarios

With Windows Server 2008 and SQL Server end of support are good server migration opportunities to use ASR to migrate into Azure.



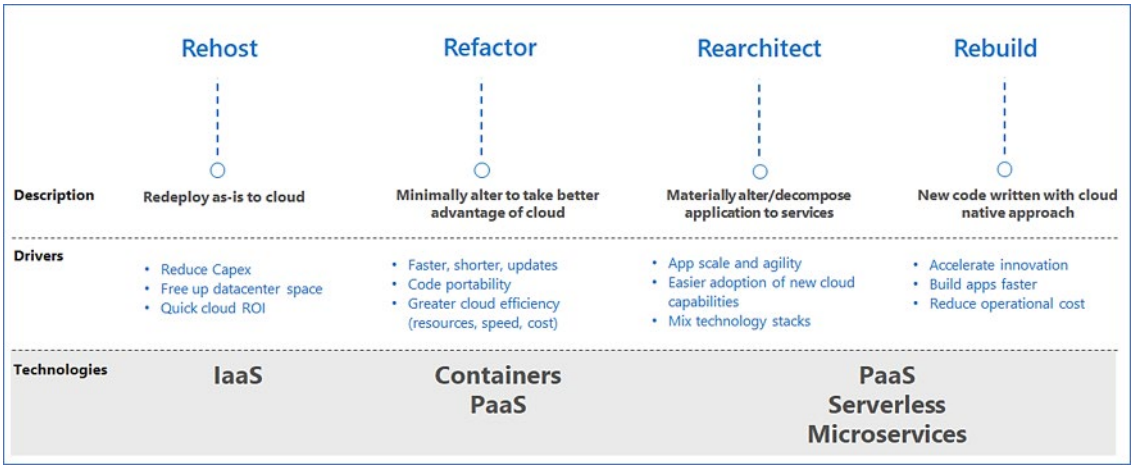
You can migrate these 2008 servers to Azure and extend the security updates for free if migrated to Azure:

- 3 years of security updates after support ends
- 75% of the license cost to buy standalone
- Reuse existing licenses with Azure Hybrid Benefit

Migration and Modernization scenarios

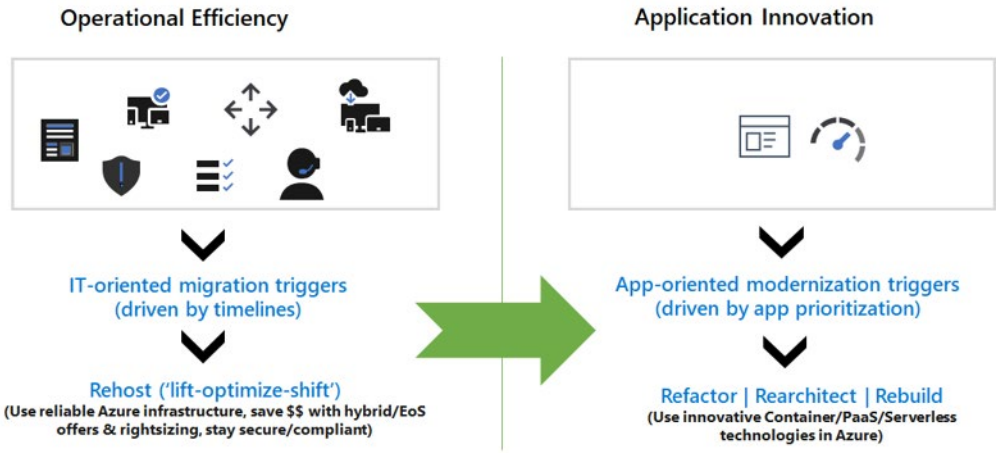
These are the Azure migration scenarios and associated technologies. These scenarios are based on an industry standard framework.

- **Rehost**: Redeploy as-is to cloud; this is used for a quick return on investment (ROI), freeing up space in the datacenter, with the least effort. Key technology in this scenario: Infrastructure as a Service (IaaS).
- **Refactor**: Minimally alter applications to take better advantage of cloud capabilities; used for code portability and quick updates. Key technologies: Containers and Platform as a Service (PaaS).
- **Rearchitect**: Materially alter or decompose applications into services, thus enhancing app scale and agility. Key technologies: PaaS, Serverless, and Microservices.
- **Rebuild**: New code written with a cloud native approach; to accelerate innovation and build apps faster. Key technologies: PaaS, Serverless, and Microservices.



Migration - Transformational Journey

When organizations are contemplating a cloud migration, they must often balance short-term needs against somewhat longer-term goals. If we think of migration to the cloud as a transformational journey, and because organizations understand the business benefits of moving to the cloud, there are two generally distinct paths to achieving the desired business outcome.



First path – Time-driven triggers

In this scenario, an organization has a need to quickly discontinue their reliance and investment in their on-premises datacenter, often due to lease expiration, running out of capacity, or similar factors. This is a good opportunity for the organization to *rehost* or *lift-optimize-shift* their entire datacenter resources to Azure. They can now can take advantage of the reliable Azure infrastructure, associated cost savings, increased scale and availability, and improved security. Most importantly, organizations can now repurpose their IT staff from having to do undifferentiated work and instead participate more directly in driving business priorities.

✓ Here, it works best to define migration projects with deadlines that address the organization's urgency trigger. A recommendation is to then group 3-5 related apps in each project and avoid lengthy assessments, but move forward with migrating successive batches of workloads.

Second path – cloud adoption but not ready to migrate everything

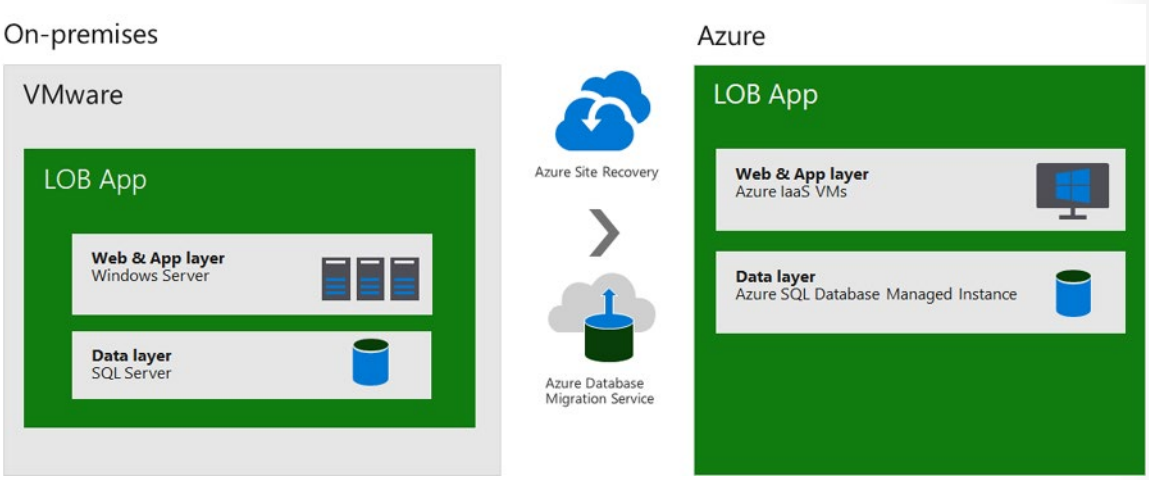
In this scenario, an organization desires to accelerate their cloud adoption, but is also dealing with time-bound triggers. The organization wants to migrate to Azure, but are not to invest all of their resources in a complete *rehost* or *lift-optimize-shift* strategy. In this case, there are two approaches the organization can take, and those can occur in parallel.

1. Decide which workloads can use the lift-optimize-shift approach, applying the same timeline vector based on the trigger.
2. Identify a small number of strategic apps and refactor or rebuild those apps

✓ In this scenario, it works best to define migration projects with clear timelines and move forward with smaller groups of related apps in each project.

Application Migration Scenarios

The example in the diagram shows the architecture for a basic migration scenario where a hospitality company named SmartHotel360 wants to move to the cloud. As part of modernizing their services and streamlining infrastructure support, SmartHotel360 to planning to re-host the application that is used by the front desk to check customers in or out and manage details of their stay. This app is critical to the business, but as it's really a back office capability, SmartHotel360 has not made the app a priority for investment and transformation. The company wants to quickly get value from Azure by rehosting this application.



This app is running on traditional Windows Server 2008 R2 and SQL Server 2008 R2 platforms virtualized in VMWare. As you can see from the diagram, it includes dedicated app and data tiers running in a load balanced environment. Let's now walk you through an assessment with Azure Migrate and rehost the application layer to Azure IaaS virtual machines and the data layer to a fully managed database target of Azure SQL Managed Instance.

Application Migration Scenarios can be more complex

Strategies for migration to the cloud fall into four broad categories: rehost, refactor, rearchitect, or rebuild. The strategy you adopt depends upon your business drivers, and migration goals. You might adopt multiple strategies. For example, you could choose to rehost (lift-and-shift) simple apps, or apps

that aren't critical to your business, but rearchitect those that are more complex and business-critical. Let's look at the strategies.

Choosing the migration strategy that's right for you

Strategies for migration to the cloud fall into four broad categories: rehost, refactor, rearchitect, or rebuild. The strategy you adopt depends upon your business drivers, and migration goals. You might adopt multiple strategies. For example, you could choose to rehost (lift-and-shift) simple apps, or apps that aren't critical to your business, but rearchitect those that are more complex and business-critical. Let's look at the strategies.

The following table describes the four categories in more detail:

Strategy	Definition	When to use
Rehost	Often referred to as a *lift-and-shift* migration. This option doesn't require code changes, and let's you migrate your existing apps to Azure quickly. Each app is migrated as is, to reap the benefits of the cloud, without the risk and cost associated with code changes.	When you need to move apps quickly to the cloud. When you want to move an app without modifying it. When your apps are architected so that they can leverage **Azure IaaS** *(https://azure.microsoft.com/en-us/overview/what-is-iaas/)* scalability after migration. When apps are important to your business, but you don't need immediate changes to app capabilities.
Refactor	Often referred to as *repackaging*, refactoring requires minimal changes to apps, so that they can connect to **Azure PaaS** *(https://azure.microsoft.com/en-us/overview/what-is-paas/)*, and use cloud offerings. For example, you could migrate existing apps to Azure App Service or Azure Kubernetes Service (AKS).Or, you could refactor relational and non-relational databases into options such as Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB.	If your app can easily be repackaged to work in Azure If you want to apply innovative DevOps practices provided by Azure, or you're thinking about DevOps using a container strategy for workloads. For refactoring, you need to think about the portability of your existing code base, and available development skills

Strategy	Definition	When to use
Rearchitect	Rearchitecting for migration focuses on modifying and extending app functionality and the code base to optimize the app architecture for cloud scalability. For example, you could break down a monolithic application into a group of microservices that work together and scale easily.Or, you could rearchitect relational and non-relational databases to a fully managed DBaaS solutions, such as Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB.	When your apps need major revisions to incorporate new capabilities, or to work effectively on a cloud platform. When you want to use existing application investments, meet scalability requirements, apply innovative Azure DevOps practices, and minimize use of virtual machines.
Rebuild	Rebuild takes things a step further by rebuilding an app from scratch using Azure cloud technologies. For example, you could build green field apps with **cloud-native** *(https://azure.microsoft.com/en-us/overview/cloudnative/)* technologies like Azure Functions, Azure AI, Azure SQL Database Managed Instance, and Azure Cosmos DB.	When you want rapid development, and existing apps have limited functionality and lifespan. When you're ready to expedite business innovation (including DevOps practices provided by Azure), build new applications using cloud-native technologies, and take advantage of advancements in AI, Blockchain, and IoT.

Documentation: **https://aka.ms/rehostapp_model1**

Video - ASR End to End

Video: Azure Site Recovery End to End

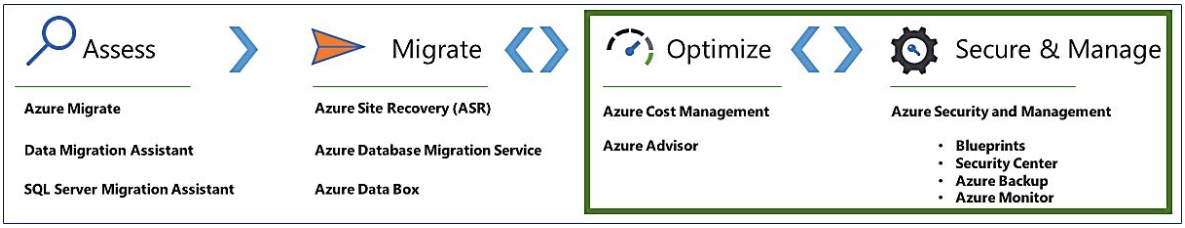
In the following video, from the Azure Friday Series on Channel 9,

Scott Hanselman discusses Azure Site Recovery with Kelly Anderson:

https://channel9.msdn.com/Shows/Azure-Friday/Azure-Site-Recovery/player

Preparing the Infrastructure (Azure Site Recovery)

ASR Migration - Optimize and Secure Phase



As a reminder of where we are in the process:

1. After you've assessed on-premises machines, you use Azure Site Recovery to migrate to Azure.
2. To do this, you prepare the Azure components you need, including a storage account and virtual network.
3. On-premises, you prepare your VMware or Hyper-V environment.
4. When everything's prepared, you set up and enable replication to Azure, and migrate the VMs.

Best practices

After migration, the most critical task is to secure migrated workloads from internal and external threats. This lesson discusses best practices for making sure you can do that. This lesson also focuses on optimizing your resources on an ongoing basis, with particular emphasis on strategies for modernizing those resources. That section may be of particular interest to the app developement teams in your organization.

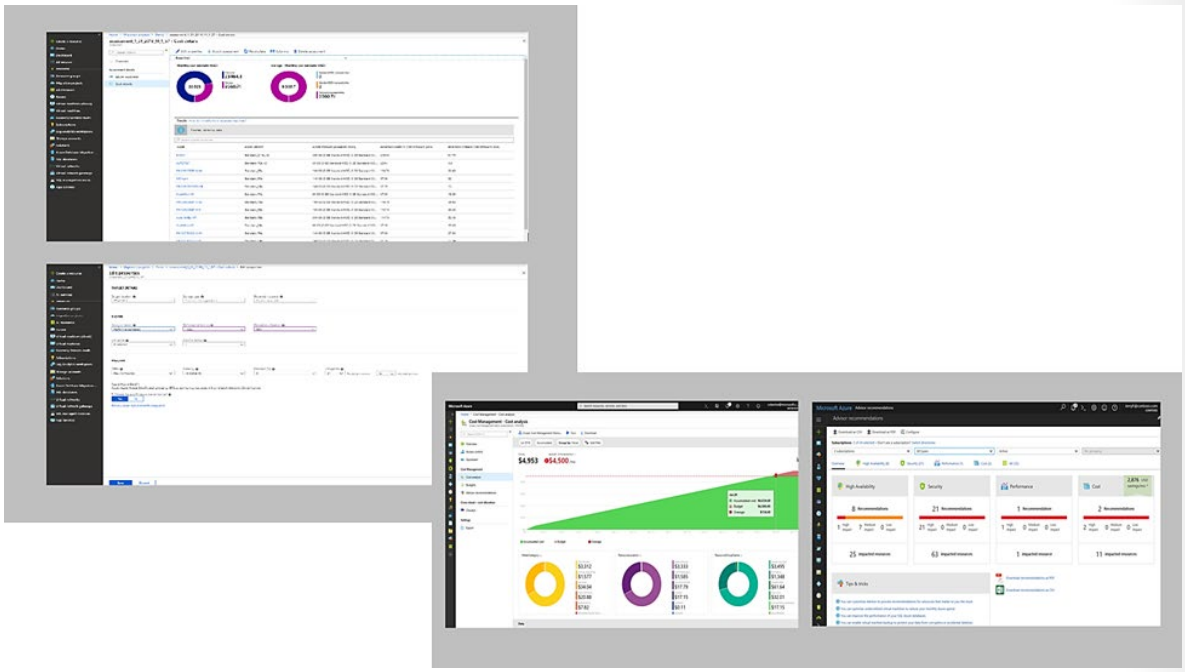
You can also review the best practices for security in the following links:

- **Work with Azure Security Center**[7]: Learn how to work with the monitoring, assessments, and recommendations provided by Azure Security Center
- **Encrypt your data**[8]: Get best practices for encrypting your data in Azure.
- **Set up antimalware**[9]: Protect your VMs from malware and malicious attacks.
- **Secure web apps**[10]: Keep sensitive information secure in migrated web apps.
- **Review subscriptions**[11]: Verify who can access your Azure subscriptions and resources after migration.
- **Work with logs**[12]: Review your Azure auditing and security logs on a regular basis.

7 https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-security-management
8 https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-security-management#best-practice-encrypt-data
9 https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-security-management#best-practice-protect-vms-with-antimalware
10 https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-security-management#best-practice-secure-web-apps
11 https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-security-management#best-practice-review-subscriptions-and-resource-permissions
12 https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-security-management#best-practice-review-audit-and-security-logs

- **Review other security features**[13]: Understand and evaluate advanced security features that Azure offers.

Continuous Optimization



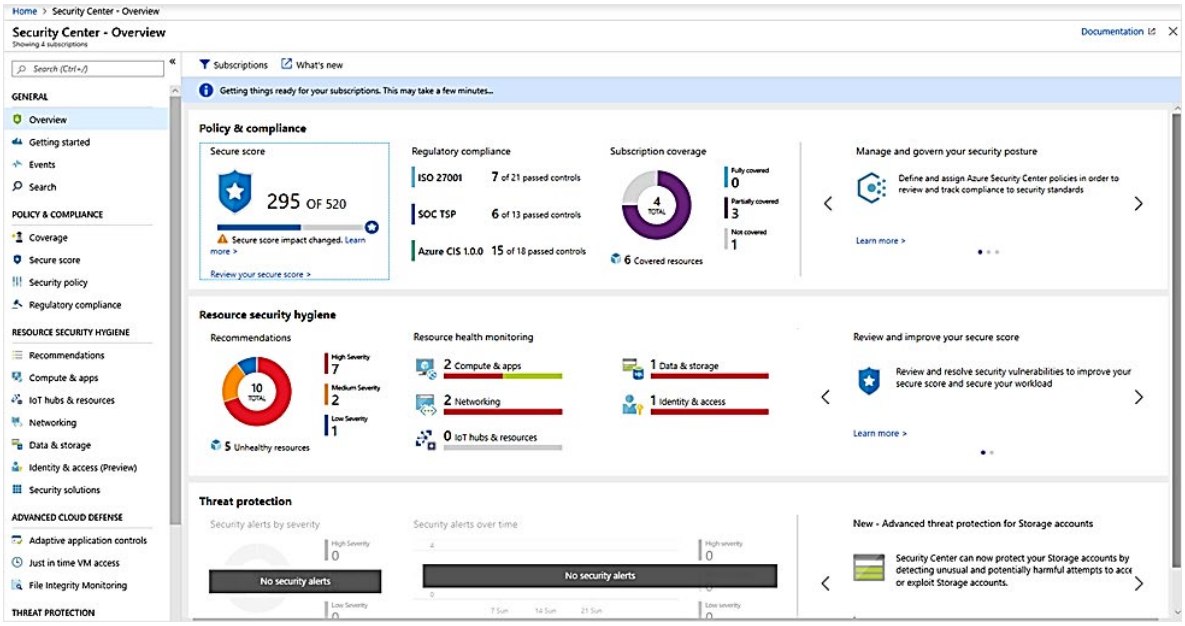
Let's also consider the *Optimize* phase in the Azure migration journey.

Many organizations look to the cloud to gain operational efficiencies and cost savings. With Azure Cost Management, organizations can now manage their cloud spend in a unified experience, and leverage built-in best practice recommendations, such as turning off idle VMs, to drive operational efficiency. They can also apply the Azure Hybrid Benefit and Azure Reserved Instances during or after migration for significant savings.

✓ Don't forget to consider the fact that for a migration project, you can optimize the migration efforts during and after by modernizing your resources for longer term value.

13 https://docs.microsoft.com/en-us/azure/migrate/migrate-best-practices-security-management#best-practice-evaluate-other-security-features

Best Practice - Secure Migrated Workloads to Azure



Azure Security Center provides unified security management. From the Security Center, you can apply security policies across workloads, limit threat exposure, and detect and respond to attacks. Security Center analyzes resources and configurations across Azure tenants and makes security recommendations, including:

Centralized policy management – Ensure compliance with company or regulatory security requirements by centrally managing security policies across all your hybrid cloud workloads.

Continuous security assessment – Monitor the security posture of machines, networks, storage and data services, and applications to discover potential security issues.

Actionable recommendations – Remediate security vulnerabilities before they can be exploited by attackers with prioritized and actionable security recommendations.

Prioritized alerts and incidents - Focus on the most critical threats first with prioritized security alerts and incidents.

In addition to assessments and recommendations, the Security Center provides a number of other security features that can be enabled for specific resources.

Just In Time (JIT) access: Reduce your network attack surface with just in time, controlled access to management ports on Azure VMs.

- Having VM RDP port 3389 open on the internet exposes VMs to continual bad actor activity. Azure IP addresses are well-known, and hackers continually probe them for attacks on open 3389 ports.
- Just in time uses network security groups (NSGs) and incoming rules that limit the amount of time that a specific port is open.
- With just in time enabled, Security Center checks that a user has role-based access control (RBAC) write access permissions for a VM. In addition, specify rules for how users can connect to VMs. If permissions are OK, an access request is approved and Security Center configures NSGs to allow

inbound traffic to the selected ports for the amount of time you specify. NSGs are return to their previous state when the time expires.

Adaptive application controls: Keep software and malware off VMs by controlling which apps run on them using dynamic app whitelisting.

- Adaptive application controls allow you to white list apps, and prevent rogue users or administrators from installing unapproved or vetting software apps on your VMs.
- You can block or alert attempts to run malicious apps, avoid unwanted or malicious apps, and ensure compliance with your organization's app security policy.

File Integrity Monitoring: Ensure the integrity of files running on VMs.

You don't need to install software to cause VM issues. Changing a system file can also cause VM failure or performance degradation. File integrity Monitoring examines system files and registry settings for changes, and notifies you if something is updated. Security Center recommends which files you should monitor.

Learn more:

Learn more[14] about Azure Security Center.

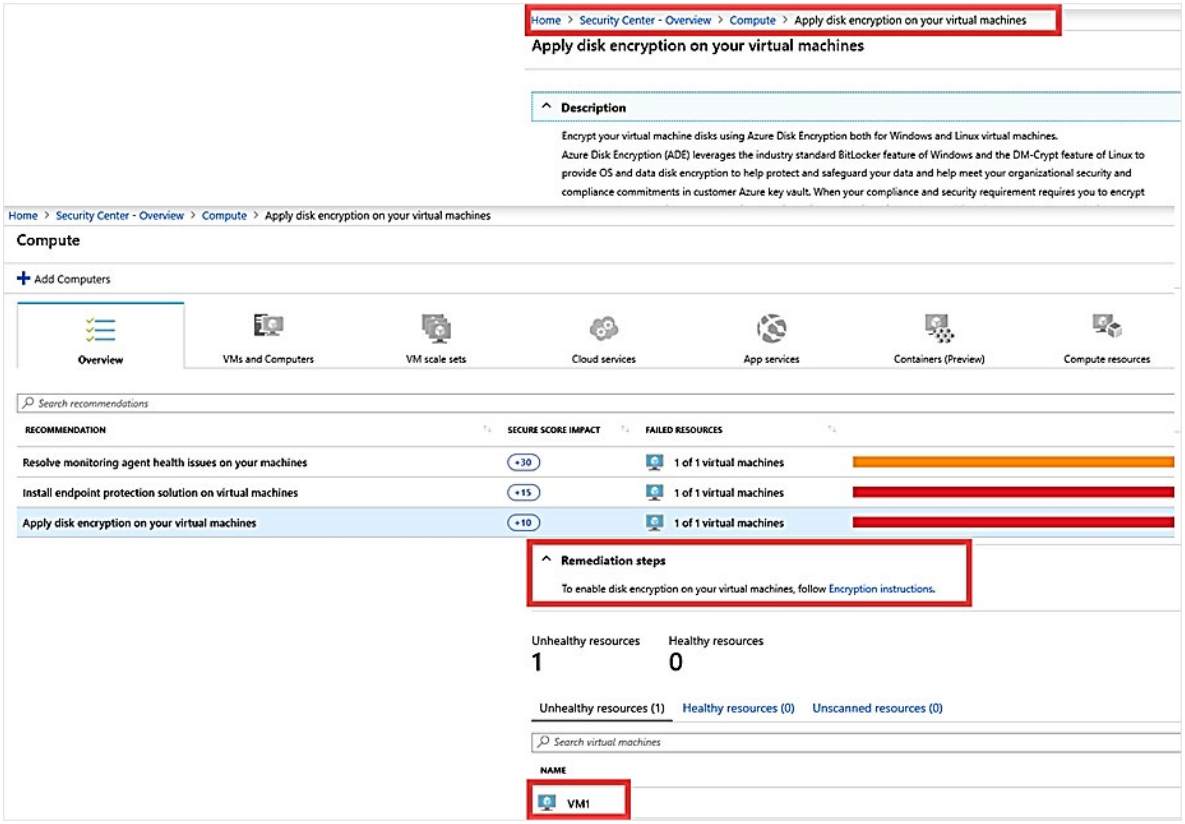
Learn more[15] about just in time VM access.

Learn more[16] applying adaptive application controls.

Get started[17] with File Integrity Monitoring.

14 https://docs.microsoft.com/en-us/azure/security-center/security-center-intro
15 https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time
16 https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application
17 https://docs.microsoft.com/en-us/azure/security-center/security-center-file-integrity-monitoring

Best Practice - Encrypt Data



Encryption is an important part of Azure security practices. Ensuring that encryption is enabled at all levels helps prevent unauthorized parties from gaining access to sensitive data, including data in transit and at rest.

Encryption for IaaS

VMs: For VMs you can use Azure Disk Encryption to encrypt your Windows and Linux IaaS VM disks.

- Disk encryption leverages BitLocker for Windows, and DM-Crypt for Linux to provide volume encryption for the OS and data disks.
- You can use an encryption key created by Azure, or you can supply your own encryption keys, safeguarded in Azure Key Vault.
- With Disk Encryption, IaaS VM data is secured at rest (on the disk) and during VM boot.
- Azure Security Center alerts you if you have VMs that aren't encrypted.

Storage: Protect at rest data stored in Azure storage.

- Data stored in Azure storage accounts can be encrypted using Microsoft-generated AES keys that are FIPS 140-2 compliant, or you can use your own keys.
- Storage Service Encryption is enabled for all new and existing storage accounts and can't be disabled.

Encryption for PaaS

Unlike IaaS where you manage your own VMs and infrastructure, in a PaaS model platform and infrastructure is managed by the provider, leaving you to focus on core app logic and capabilities. With so many different types of PaaS services, each service will be evaluated individually for security purposes. As an example, let's see how we might enable encryption for Azure SQL Database.

- **Always Encrypted**: Use the Always Encrypted Wizard in SQL Server Management Studio to protect data at rest.You create Always Encrypted key to encrypt individual column data.Always Encrypted keys can be stored as encrypted in database metadata, or stored in trusted key stores such as Azure Key Vault.App changes will probably be needed to use this feature.
- **Transparent data encryption (TDE)**: Protect the Azure SQL Database with real-time encryption and decryption of the database, associated backups, and transaction log files at rest.TDE allows encryption activities to take place without changes at the app layer.TDE can use encryption keys provided by Microsoft, or you can provide your own keys using Bring Your Own Key support.

Learn more:

Learn about[18] Azure Disk Encryption for IaaS VMs.

Enable encryption[19] for IaaS Windows VMs.

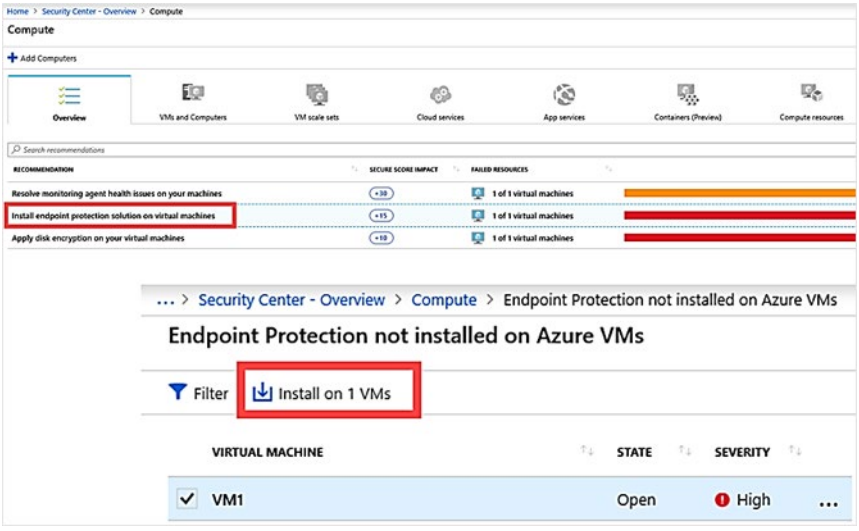
Learn about[20] Azure Storage Service Encryption for data at rest.

Read[21] an overview of Always Encrypted.

Read about[22] TDE for Azure SQL Database.

Learn about[23] TDE with Bring Your Own Key.

Best Practice - Protect VMs with Antimalware



Best practice: Protect VMs with antimalware

18 https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview
19 https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-windows
20 https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
21 https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault
22 https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql?view=sql-server-2017
23 https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-byok-azure-sql

In particular, older Azure migrated VMs may not have the appropriate level of antimalware installed. Azure provides a free endpoint solution that helps protect VMs from viruses, spyware, and other malware.

Microsoft Antimalware for Azure generates alerts when known malicious or unwanted software tries to install itself.

It's a single agent solution that runs in the background without human intervention.

In Azure Security Center, you can easily identify VMs that don't have endpoint protection running, and install Microsoft Antimalware as needed.

Learn more:

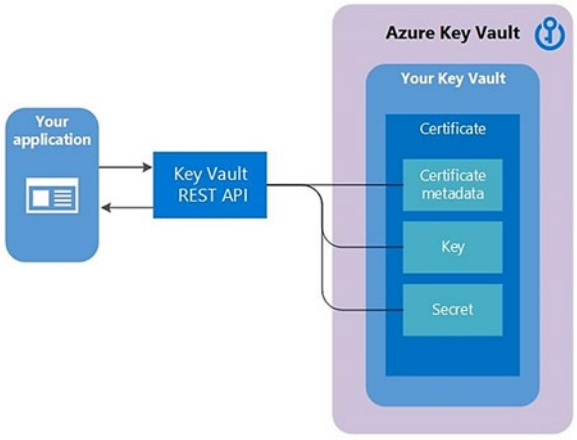
Learn about[24] Microsoft Antimalware.

Best Practice – Secure Web Apps

Best practice: Secure web apps

Migrated web apps face a couple of issues:

- Most legacy web applications tend to have sensitive information inside configuration files. Files containing such information can present security issues when apps are backed up, or when app code is checked into or out of source control.
- In addition, when you migrate web apps residing in a VM, you are likely moving that machine from an on-premises network and firewall-protected environment to an environment facing the internet. You need to make sure that you set up a solution that does the same work as your on-premises protection resources.



Azure provides a couple of solutions:

Azure Key Vault

Today web app developers are taking steps to ensure that sensitive information isn't leaked from these files. One method to secure information is to extract it from files and put it into an Azure Key Vault.

- You can use Key Vault to centralize storage of app secrets, and control their distribution. It avoids the need to store security information in app files.
- Apps can security access information in the vault using URIs, without needing custom code.

24 https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware

- Azure Key Vault allows you to lock down access via Azure security controls and to seamlessly implement 'rolling keys'. Microsoft does not see or extract your data.

App Service Environment

If an app you migrate needs extra protection, you can consider adding an App Service Environment and Web Application Firewall to protect the app resources.

- The Azure App Service Environment provides a fully isolated and dedicated environment in which to running App Service apps such as Windows and Linux web apps, Docker containers, mobile apps, and functions.
- It's useful for apps that are very high scale, require isolation and secure network access or have high memory utilization

Web Application Firewall

A feature of Application Gateway that provides centralized protection for web apps.

- It protects web apps without requiring backend code modifications.
- It protects multiple web apps at the same time behind an application gateway.
- Web application firewall can be monitored using Azure Monitor, and is integrated into Azure Security Center.

Learn more:

Get an overview[25] of Azure Key Vault.

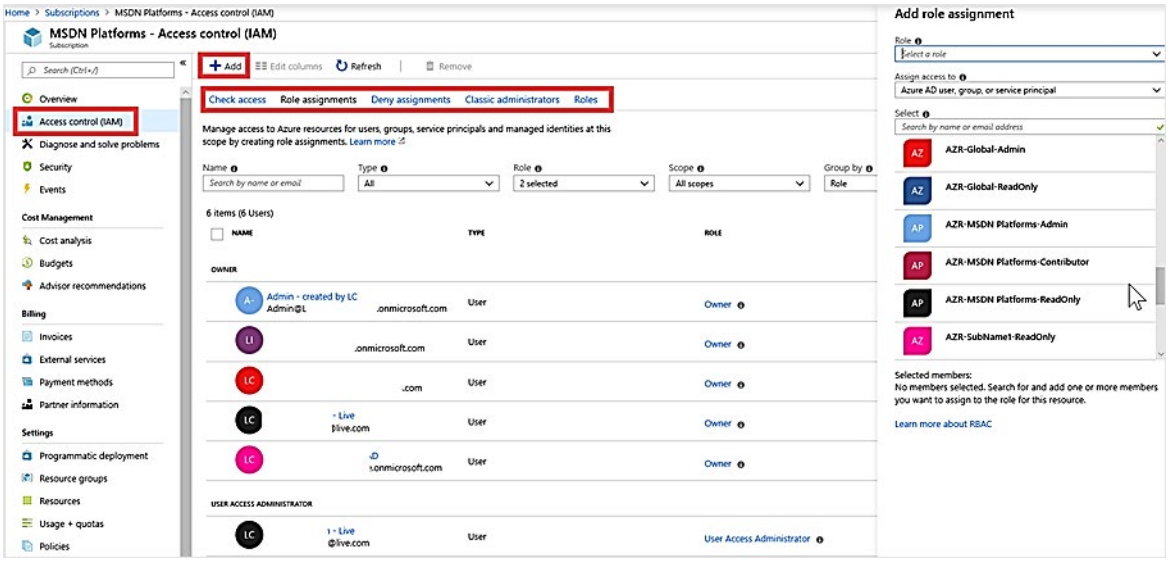
Learn about[26] Web application firewall.

Get an introduction[27] to App Service Environments.

Learn how to[28] configure a web app to read secrets from Key Vault.

25 https://docs.microsoft.com/en-us/azure/key-vault/key-vault-overview
26 https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview
27 https://docs.microsoft.com/en-us/azure/app-service/environment/intro
28 https://docs.microsoft.com/en-us/azure/key-vault/tutorial-net-create-vault-azure-web-app

Best Practice - Review Subscriptions and Resource Permissions



Best practice: Review subscriptions and resource permissions

As you migrate your workloads and run them in Azure, staff with workload access move around. Your security team should review access to your Azure tenant and resource groups on a regular basis. Azure provides a number of offerings for identity management and access control security, including role-based access control (RBAC) to authorize permissions to access Azure resources.

RBAC assigns access permissions for *security principals*. Security principals represent users, groups (a set of users), *service principals* (identity used by apps and services), and *managed identities* (an Azure Active Directory identity automatically managed by Azure).

RBAC can assign roles to security principles, such as owner, contributor and reader, and *role definitions* (a collection of permissions) that define the operations that can be performed by the roles.

RBAC can also set *scopes* that set the boundary for a role. Scope can be set at a number of levels, including a management group, subscription, resource group, or resource

Ensure that admins with Azure access are only able to access resources that you want to allow. If the predefined roles in Azure aren't granular enough, you can create custom roles to separate and limit access permissions.

Learn more:

About[29] RBAC.

Learn[30] to manage access using RBAC and the Azure portal.

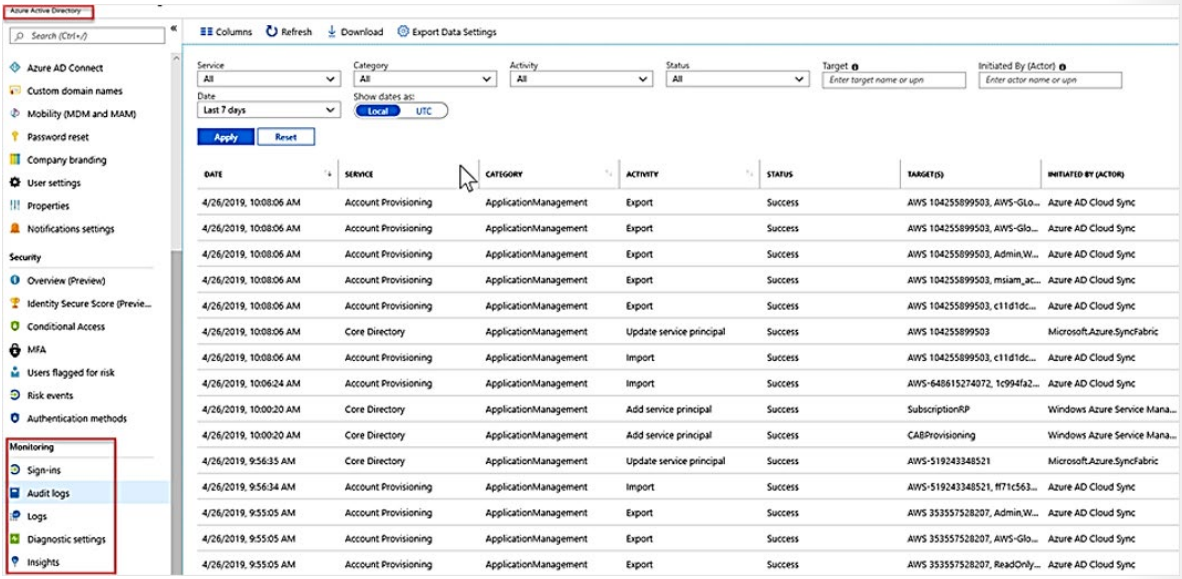
Learn[31] about custom roles.

Best Practice - Review Audit and Security Logs

Best practice: Review audit and security logs

29 https://docs.microsoft.com/en-us/azure/role-based-access-control/overview
30 https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
31 https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

Azure Active Directory (AD) provides activity logs that appear in Azure Monitor. The logs capture the operations performed in Azure tenancy, when they occurred, and who performed them.



Audit logs show the history of tasks in the tenant. Sign-in activity logs show who carried out the tasks.

Access to security reports depends on your Azure AD license. In Free and Basic you get a list of risky users and sign-ins. In Premium 1 and Premium 2 editions you get underlying event information.

You can route activity logs to a number of endpoints for long-term retention and data insights.

Make it a common practice to review the logs or integrate your security information and event management (SIEM) tools to automatically review abnormalities. If you're not using Premium 1 or 2, you'll need to do a lot of analysis yourself or using your SIEM system. Analysis includes looking for risky sign-ins and events, and other user attack patterns.

Learn more:

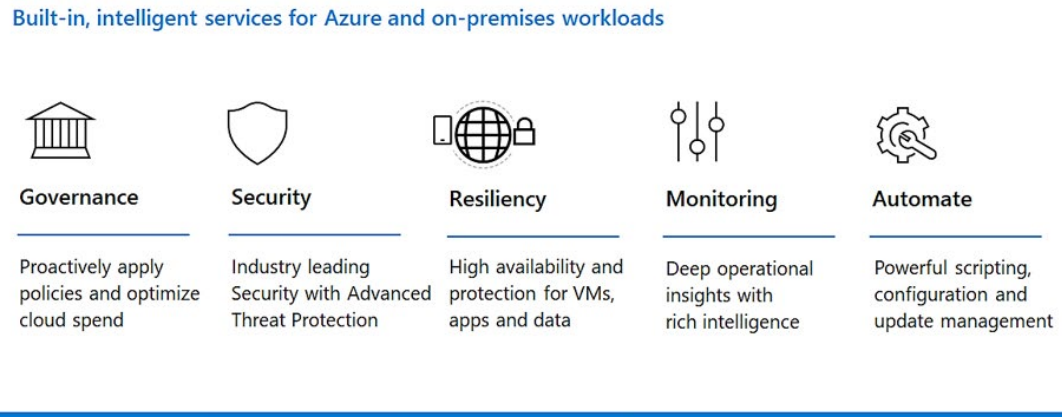
Learn about[32] Azure AD activity logs in Azure Monitor.

Learn how to[33] audit activity reports in the Azure AD portal.

Secure and Manage Migrated Workloads

At this point, it's important to consider strategies and planning for how you will keep your migrated workloads secure and continually well-managed.

32 https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor
33 https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs



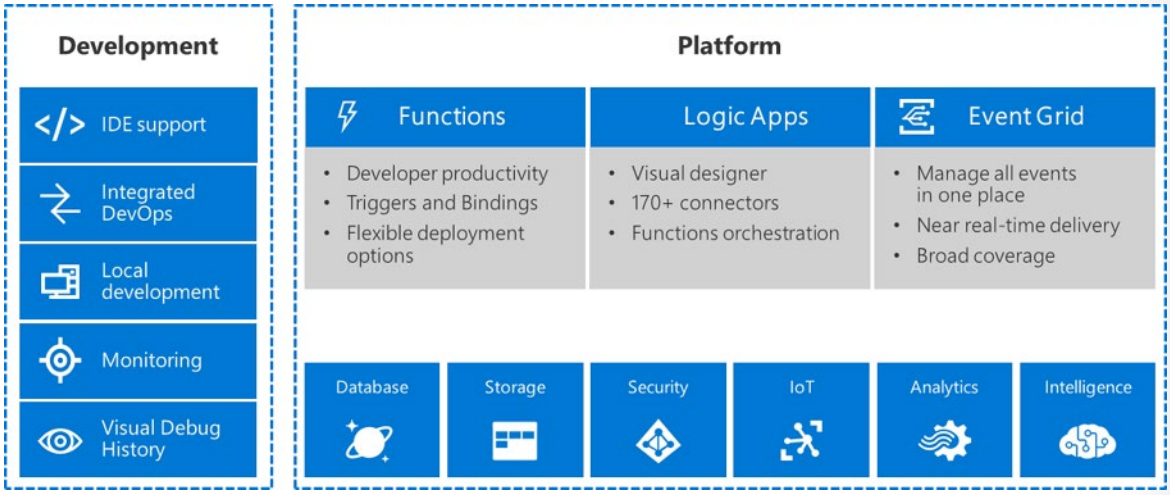
Securing and managing migrated resources is critical, both during migration and on an ongoing basis. With Azure security and management , organizations can take advantage of built-in intelligent services for their Azure and on-premises workloads. It's highly recommend that you turn on Azure Security Center, Azure Backup, and Azure Log Analytics immediately after the resource is migrated, followed by fine-tuning over time.

Enterprise organizations are looking to Azure for speed and control. **Azure Blueprints**[34] , a new governance capability, makes it simple to set up compliant subscriptions with the resources, policies and access controls already pre-defined. This ensures that you get to the control you need to be compliant, accelerates the creation of new environments, and enables compliant developer self-service.

Serverless Application Platform Components in Azure

Let's talk about what constitutes MSFT's Serverless platform: At the center of the Serverless platform are the compute offerings: Azure Functions and Azure Logic Apps. Azure Functions is an event-based Serverless compute experience that helps you accelerate your development. Logic Apps is a powerful orchestration tool that enables you to build a Serverless app in minutes. You simply orchestrate multiple functions using a visual workflow tool.

34 https://azure.microsoft.com/en-us/services/blueprints/



Serverless – core components

For example, consider as a first step that your apps are up and running using Serverless. You now need to collect intelligence from different apps across platforms upon which to take actions. There are a few essential components that are core to building Serverless applications:

Data/Storage. - Functions has triggers and bindings with Azure Cosmos DB and Azure Blob storage:

- **Triggers**. Triggers are event responses used to trigger your custom code. They allow you to respond to events across the Azure platform or on premise.
- **Bindings**. Bindings represent the necessary meta data used to connect your code to the desired trigger or associated input or output data.

Messaging - such as queues and topics using Azure Service Bus and Azure Event Hubs.

Integration - includes core LOB apps and SaaS apps integration via Azure Logic Apps.

Intelligence on data and sentiment/ predictive analysis - using Cognitive services and Machine learning.

Conversation as a service - How can developers be equipped to build apps that offer an end-to-end experience for their end users? Azure Bot Service offers a Serverless interactive bot experience.

Increasingly, developers are spending more time writing code that allows them to add huge business impact with Serverless. Microsoft offers numerous development tools such as IDE Support for Visual Studio in functions and Logic Apps, enables local development (versus a web browser coding environment), visual debugging capability, all with the tools of choice.

Serverless - use cases

The following list highlights the top scenarios and use cases for Serverless:

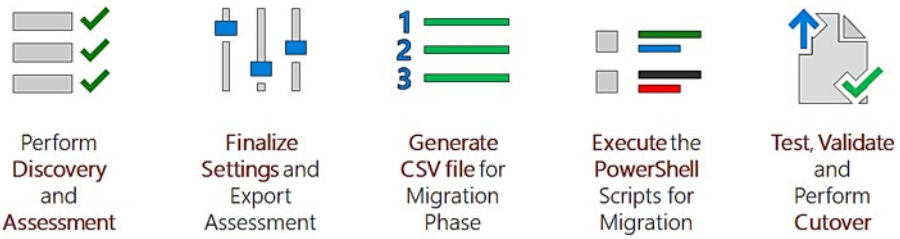
- **Real-time Stream analytics**: Customers can use Functions to feed real-time streams of data from application tracking into structured data and store it in SQL online.
- **SaaS event processing**: Customers can use Functions and Logic Apps to analyze data from an excel file in OneDrive and perform validation, filtration, sorting and convert data into consumable business charts

- **Web app architecture**: Used a lot in creating targeted marketing collaterals – when a customer clicks on a webpage, it triggers a webhook, that uses a function to create an ad that matches the customer profile and displays a completed webpage.
- **Real-time bot messaging**: When customers send a message to a chatbox, Functions calls Cortana analytics to generate appropriate answers and sends a response back.

Datacenter Migration using Migration Factory

Large Scale Migrations to Azure

Implementing large-scale migrations, those involving hundreds of applications or servers, to the cloud is challenging, but organizations want to take advantage of the benefits, such as significant cost savings and to position themselves for modernization. As discussed previously, some organizations want to migrate their entire datacenter to the cloud, while others want to maintain a hybrid solution and make the transition more gradually.



Microsoft Consulting Services (MCS) has been performing large migrations with a custom "factory" approach for several years. This allowed them to help customers quickly migrate out of entire datacenters before their renewal deadlines.

Microsoft took MCS's approach and created and published PowerShell scripts on GitHub that automate the migration steps to perform in Azure Site Recovery after the ASR Infrastructure is configured, as covered in the previous Lessons.

Using Automation for Migration Factory, you can now move multiple VMs at scale from on-premises to Azure. This topic describes the high level process of executing a large scale migration.

✓ The next few topics will look at individual parts of the process in a little more detail.

Automating a large scale migration: the process

- Discovery and assessment is essential before migrating. In Azure, begin with server assessment, and finalize the settings of your assessment. For example, whether you will use reserved instances, or which region you will migrate to.
- Once all the settings have been finalized, export the assessment.
- Generate a CSV file which will provide the inputs to the automation scripts you will use to perform the migration.
- Execute the PowerShell scripts and perform the migration.
- Test the performance of the applications in Azure, validate the migration results, and when satisified with performance and functionality perform the cutover to production.

Limitations

- Support for specifying the static IP address is only for the primary NIC of the target VM
- The scripts do not take Azure Hybrid Benefit related inputs, you need to manually update the properties of the replicated VM in the portal

Documentation: **https://aka.ms/migrate/migration_factory**

GitHub repository: **https://aka.ms/migrate/migration_factory_scripts**

Prerequisites for Scripted Large-Scale Migration

These are the pre-requisites for using the scripted large-scale migration approach.

It is important to note that while we are showing you how you can migrate at scale with some automation, you should still perform the on-premise and ASR configurations and perform some manual replications through the ASR portal. Also, use the Test Failover, and other features to verify networking is correct, and to understand your options.

1. Ensure that the Site Recovery vault is created in your Azure subscription.
2. Ensure that the Configuration Server and Process Server are installed in the source environment and the vault is able to discover the environment.
3. Ensure that a Replication Policy is created and associated with the Configuration Server.
4. Ensure that you have added the VM admin account to the config server (that will be used to replicate the on premises VMs).
5. Ensure that the target artifacts in Azure are created:
   - Target Resource Group
   - Target Storage Account (and its Resource Group) - Create a premium storage account if you plan to migrate to premium-managed disks
   - Cache Storage Account (and its Resource Group) - Create a standard storage account in the same region as the vault
   - Target Virtual Network for failover (and its Resource Group)
   - Target Subnet
   - Target Virtual Network for Test failover (and its Resource Group)
   - Availability Set (if needed)
   - Target Network Security Group and its Resource Group
6. Ensure that you have decided on the properties of the target VM:
   - Target VM name
   - Target VM size in Azure (can be decided using Azure Migrate assessment)
   - Private IP Address of the primary NIC in the VM
7. Download the scripts from **Azure PowerShell Samples**[35] repo on GitHub

Automating the Process (1 of 2)

Generate the CSV for large scale migrations

For a large scale migration, begin with the CSV file which provides the inputs for all the PowerShell scripts. The CSV is a simple template that lists every VM that you intend to migrate, where you provide information such as which Azure subscription you want to migrate to, storage account, resource group, network/subnet, availability set, desired SKU, and so on.

35 https://github.com/Azure/azure-docs-powershell-samples/tree/master/azure-migrate/migrate-at-scale-with-site-recovery

All the scripts are designed to work on the same CSV file. A sample CSV template is available in the scripts folder for your reference.

A	B	C	D	E	F	G	H	I	J
VAULT_SUBSCRIPTION_ID	VAULT_NAME	SOURCE_MACHINE_NAME	TARGET_MACHINE_NAME	CONFIGURATION_SERVER	PROCESS_SERVER	TARGET_RESOURCE_GROUP	TARGET_STORAGE_ACCOUNT	TARGET_VNET	REPLICATION_POLICY
8c3c936a-c09b-4de3-830b-3f5f244d72e9	ContosoScale	Contoso-DataTier1	Contoso-DataTier1	ContosoCS	ContosoCS	ScaleDemo	storageaccountscale	VirtualNetworkScale	Scalemigration
8c3c936a-c09b-4de3-830b-3f5f244d72e9	ContosoScale	Contoso-DataTier2	Contoso-DataTier2	ContosoCS	ContosoCS	ScaleDemo	storageaccountscale	VirtualNetworkScale	Scalemigration
8c3c936a-c09b-4de3-830b-3f5f244d72e9	ContosoScale	Contoso-DataTier3	Contoso-DataTier3	ContosoCS	ContosoCS	ScaleDemo	storageaccountscale	VirtualNetworkScale	Scalemigration
8c3c936a-c09b-4de3-830b-3f5f244d72e9	ContosoScale	Contoso-FrontTier3	Contoso-FrontTier3	ContosoCS	ContosoCS	ScaleDemo	storageaccountscale	VirtualNetworkScale	Scalemigration
8c3c936a-c09b-4de3-830b-3f5f244d72e9	ContosoScale	Contoso-MiddleTier1	Contoso-MiddleTier1	ContosoCS	ContosoCS	ScaleDemo	storageaccountscale	VirtualNetworkScale	Scalemigration

Execute *ASR_StartMigration.ps1* to start replicating servers to Azure

asr_startmigration.ps1 enables replication for all the VMs listed in the csv, the script creates a CSV output with the job details for each VM.

Once the CSV is complete, execute *ASR_StartMigration.ps1* against the CSV to start replicating servers to Azure. All the migration jobs are initiated at scale against every row in the CSV.

Jobs are executed at scale but there is built-in batching available for large jobs to mitigate throttling issues while so many VMs are being processed for the cutover. For example, we recommend inserting a 2 minute pause between every 50 cutovers.

The replication progress is tracked by executing *ASR_ReplicationStatus_ps1*. Logging aspects are also built in so that the script will generate a log output, in case of a need to open a support ticket.

```
23      $vaultName = $csvItem.VAULT_NAME
24      $sourceAccountName = $csvItem.ACCOUNT_NAME
25      $sourceProcessServer = $csvItem.PROCESS_SERVER
26      $sourceConfigurationServer = $csvItem.CONFIGURATION_SERVER
27      $targetPostFailoverResourceGroup = $csvItem.TARGET_RESOURCE_GROUP
28      $targetPostFailoverStorageAccountName = $csvItem.TARGET_STORAGE_ACCOUNT
29      $targetPostFailoverLogStorageAccountName = $csvItem.TARGET_LOGSTORAGE_ACCOUNT
30      $targetPostFailoverVNET = $csvItem.TARGET_VNET
31      $targetPostFailoverSubnet = $csvItem.TARGET_SUBNET
32      $sourceMachineName = $csvItem.SOURCE_MACHINE_NAME
33      $replicationPolicy = $csvItem.REPLICATION_POLICY
34      $targetMachineName = $csvItem.TARGET_MACHINE_NAME
35      $targetStorageAccountRG = $csvItem.TARGET_STORAGE_ACCOUNT_RG
36      $targetLogStorageAccountRG = $csvItem.TARGET_LOGSTORAGE_ACCOUNT_RG
37      $targetVNETRG = $csvItem.TARGET_VNET_RG
```

GitHub repository: **https://aka.ms/migrate/migration_factory_scripts**

Automating the Process (2 of 2)

Evaluate migration and modify additional settings

Asr_updateproperties.ps1 updates the target properties of the VM (Compute and Network properties), and it verifies if the properties are appropriately updated.

Execute *ASR_PropertiesUpdate.ps1* to modify settings that you may not have considered when you initiated replication, or any changes you decide to make after the fact.

For example, you may want to increase the size of the VMs, so you update the compute SKU, or you may want to make changes to the network configuration. Or possibly an organiztion may not have finalized the availability set design, even after initiating replication. In this example, *ASR_PropertiesUpdate.ps1* can continue to be updated while the replication is in progress. In fact, you have the option to modify settings any time up to the point of the cutover.

The automation factory includes a complementary script to do a properties check (*ASR_PropertiesCheck.ps1*).

```
$updatePropertiesJob = Set-AzRecoveryServicesAsrReplicationProtectedItem `
    -InputObject $protectedItem `
    -PrimaryNic $nicDetails.NicId `
    -RecoveryNicStaticIPAddress $targetPrivateIP `
    -RecoveryNetworkId $nicdetails.RecoveryVMNetworkId `
    -RecoveryNicSubnetName $targetSubnet `
    -UseManagedDisk $True `
    -RecoveryAvailabilitySet $targetAvailabilitySetObj.Id `
    -Size $targetMachineSize
```

Test the migration

Asr_TestMigration.ps1 starts the test failover of the VMs listed in the csv, the script creates a CSV output with the job details for each VM.

Execute *Asr_TestMigration.ps1* to perform migration testing for replicated servers. This is the most important step in the migration. There is also a complementary script (*ASR_CleanupTestMigration.ps1*) that automatically cleans up all the artifacts that were created as part of the testing and restores the subscription to its original state.

```
#Start the test failover operation
$testFailoverJob = Start-AzRecoveryServicesAsrTestFailoverJob `
    -ReplicationProtectedItem $protectedItem `
    -AzureVMNetworkId $targetTestFailoverVNETObj.Id `
    -Direction PrimaryToRecovery
$reportItem.TestFailoverJobId = $testFailoverJob.ID
```

Perform a cutover

Finally, when testing is complete and you are satisfied that everything is ready, bring everything over into the cloud with *ASR_Migration.ps1*. *ASR_Migration.ps1* performs an unplanned failover for the VMs listed in the csv, the script creates a CSV output with the job details for each VM. The script does not shut down the on premises VMs before triggering the failover, for application consistency, it is recommended that you manually shut down the VMs before executing the script. It then performs the commit operation on the VMs and delete the Azure Site Recovery entities.

Use *ASR_CompleteMigration.ps1* to finalize the cutover, getting the ASR process out of the way and the deployment into Azure.

```
$protectedItem = $asrCommon.GetProtectedItemFromVault($vaultName, $sourceMachineName, $sourceConfigurationServer)
if ($protectedItem -ne $null) {
if ($protectedItem.AllowedOperations.Contains('UnplannedFailover')) {
$processor.Logger.LogTrace("Starting UnplannedFailover operation for item '$($sourceMachineName)'")
$targetFailoverJob = Start-AzRecoveryServicesAsrUnplannedFailoverJob `
-ReplicationProtectedItem $protectedItem `
-Direction PrimaryToRecovery

$reportItem.FailoverJobId = $targetFailoverJob.ID
        } else {
$processor.Logger.LogTrace("UnplannedFailover operation not allowed for item '$($sourceMachineName)'")
        }
    } else {
$processor.Logger.LogTrace("'$($sourceMachineName)' item is not in a protected state ready for replication")
    }
}
```

ASR_PostMigration.ps1 is also available to assign NSG rules post migration. Execute *ASR_PostMigration.ps1* if you plan to assign network security groups to the NICs post-failover. This script assigns an NSG to any one NIC in the target VM.

The script, by default, migrates the VMs to managed disks in Azure. If the target storage account provided is a premium storage account, premium-managed disks are created post migration. The cache storage account can still be a standard account. If the target storage account is a standard storage account, standard disks are created post migration.

```
$processor.Logger.LogTrace("Setting Network Security Group to Network Interface '$($networkInterfaceResourceObj.Name)'")
$networkInterfaceObj.NetworkSecurityGroup = $targetNsgObj
Set-AzNetworkInterface -NetworkInterface $networkInterfaceObj
```

Online Lab - Implementing Azure to Azure Migration

Lab Steps

Online Lab: Implementing Azure to Azure Migration

NOTE: For the most recent version of this online lab, see: **https://github.com/MicrosoftLearning/AZ-300-MicrosoftAzureArchitectTechnologies**

Scenario

Adatum Corporation wants to migrate their existing Azure VMs to another region

Objectives

After completing this lab, you will be able to:

- Implement Azure Site Recovery Vault
- Migrate Azure VMs between Azure regions

Lab Setup

Estimated Time: 45 minutes

User Name: **Student**

Password: **Pa55w.rd**

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

The main tasks for this exercise are as follows:

1. Deploy an Azure VM to be migrated
2. Create an Azure Recovery Services vault

Task 1: Deploy an Azure VM to be migrated

1. From the lab virtual machine, start Microsoft Edge and browse to the Azure portal at **http://portal.azure.com** and sign in by using the Microsoft account that has the Owner role in the target Azure subscription.
2. In the Azure portal, in the Microsoft Edge window, start a **PowerShell** session within the **Cloud Shell**.
3. If you are presented with the **You have no storage mounted** message, configure storage using the following settings:
   - Subsciption: the name of the target Azure subscription
   - Cloud Shell region: the name of the Azure region that is available in your subscription and which is closest to the lab location
   - Resource group: the name of a new resource group **az3000600-LabRG**
   - Storage account: a name of a new storage account
   - File share: a name of a new file share
4. From the Cloud Shell pane, create a resource group by running (replace the `<Azure region>` placeholder with the name of the Azure region that is available in your subscription and which is closest to the lab location)

   ```
   New-AzResourceGroup -Name az3000601-LabRG -Location <Azure region>
   ```

5. From the Cloud Shell pane, upload the Azure Resource Manager template **\allfiles\AZ-300T02\Module_01\azuredeploy06.json** into the home directory.
6. From the Cloud Shell pane, upload the parameter file **\allfiles\AZ-300T02\Module_01\azuredeploy06.parameters.json** into the home directory.
7. From the Cloud Shell pane, deploy an Azure VM hosting Windows Server 2016 Datacenter by running:

   ```
   New-AzResourceGroupDeployment -ResourceGroupName az3000601-LabRG -Template-
   File azuredeploy06.json -TemplateParameterFile azuredeploy06.parameters.
   json
   ```

Note: Do not wait for the deployment to complete but instead proceed to the next task.

Note: If you are getting azuredeploy06.json not found, use -TemplateFile $HOME/azuredeploy06.json and -TemplateParameterFile $HOME/azuredeploy06.parameters.json

Task 2: Implement an Azure Site Recovery vault

1. From Azure Portal, create an instance of **Backup and Site Recovery (OMS)** Recovery Services vault with the following settings:
   - Name: **vaultaz3000602**
   - Subscription: the name of the target Azure subscription

- Resource group: the name of a new resource group **az3000602-LabRG**
- Location: the name of an Azure region that is available in your subscription and which is **different** from the region you deployed an Azure VM in the previous task

2. Wait until the vault is provisioned. This will take about a minute.

Result: After you completed this exercise, you have created an Azure VM to be migrated and an Azure Site Recovery vault that will host the migrated disk files of the Azure VM.

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

The main tasks for this exercise are as follows:

1. Configure Azure VM replication
2. Review Azure VM replication settings
3. Disable replication of an Azure VM and delete the Azure Recovery Services vault

Task 1: Configure Azure VM replication

1. In the the Azure portal, navigate to the blade of the newly provisioned Azure Recovery Services vault.
2. On the Recovery Services vault blade, click the **+ Replicate** button.
3. Enable replication by specifying the following settings:
   - Source: **Azure**
   - Source location: the same Azure region into which you deployed the Azure VM in the previous exercise of this lab
   - Azure virtual machine deployment model: **Resource Manager**
   - Source resource group: **az3000601-LabRG**
   - Virtual machines: **az300061-vm**
   - Target location: the name of an Azure region that is available in your subscription and which is different from the region you deployed an Azure VM in the previous task
   - Target resource group: **(new) az3000601-LabRG-asr**
   - Target virtual network: **(new) az3000601-vnet-asr**
   - Cache storage account: accept the default setting
   - Replica managed disks: **(new) 1 premium disk(s), 0 standard disk(s)**
   - Target availability sets: **Not Applicable**
   - Replication policy: **Create new**
   - Name: **12-hour-retention-policy**

- Recovery point retention: **12 Hours**
- App consistent snapshot frequency: **6 Hours**
- Multi-VM consistency: **No**

4. Initiate creation of target resources.
5. Enable the replication.

Note: Wait for the operation of enabling the replication to complete. Then proceed to the next task.

Task 2: Review Azure VM replication settings

1. In the Azure portal, from the Azure Site Recovery vault blade, navigate to the replicated item blade representing the Azure VM **az3000601-vm**.
2. On the replicated item blade, review the **Health and status**, **Latest available recovery points**, and **Failover readiness** sections. Note the **Failover** and **Test Failover** entries in the toolbar. Scroll down to the **Infrastructure view**.
3. If time permits, wait until the status of the Azure VM changes to **Protected**. This might take additional 15-20 minutes. At that point, examine the values **Crash-consistent** and **App-consistent** recovery points. In order to view **RPO**, you should perform a test failover.

Task 3: Disable replication of an Azure VM and delete the Azure Recovery Services vault

1. In the Azure portal, disable replication of the Azure VM **az3000601-vm**.
2. Wait until the replication is disabled.
3. From the Azure portal, delete the Recovery Services vault.

Note: You must ensure that the replicated item is removed first before you can delete the vault.

Result: After you completed this exercise, you have implemented automatic replication of an Azure VM.

Review Questions

Module 1 Review Questions

Migration Goals

You are hired by an organization to evaluate IT department regarding needs and department spending.

The organization uses a pre-purchase model. Resources have a three to five year life cycle. All hardware and software is managed and maintained on-premises or in shared datacenters.

You need to evaluate whether to migrate some or all resources to Azure

What should you consider? What are the benefits? Which tool can help you plan and assess costs and cost-savings?

Suggested Answer
When migrating any workload to a new environment, whether it be another datacenter or to a public cloud, you should have a clear set of goals for migration in mind. Note that there are both technology-focused and business-focused goals that motivate potential migrations. All migration efforts should result in direct benefits to the organization's business.

Azure Site Recovery

You are hired to recommend a disaster recovery solution for an organization. The organization has a mix of Hyper-V virtual machines (VMs), VMware VMs, and physical servers.

You are considering Azure Site Recovery.

What must be taken into consideration for each type of resource? Why is it important that Azure Site Recovery includes Orchestration? What are some benefits to consider for Azure Site Recovery and Orchestration?

Suggested Answer
You can use Azure Site Recovery to replicate on-premises physical or virtual machines that run Windows or Linux. Azure Site Recovery includes support for Hyper-V and VMware virtual machines. You can replicate data from your on-premises datacenter to Azure or to a secondary site.
You can use Azure Site Recovery to failover to the replicated resource in either Azure or your secondary site. Here are some reasons to use Azure Site Recovery.
• Eliminate the need for disaster recovery sites. Your environment can be protected by automating the replication of the virtual machines based on policies that you set and control. Site Recovery is heterogeneous and can protect Hyper-V, VMware, and physical servers.

• Reduce infrastructure costs. Lower your on-premises infrastructure costs by using Azure as a secondary site for conducting business during outages. Or, eliminate datacenter costs altogether by moving to Azure and setting up disaster recovery between Azure regions. You can pre-assess network, storage, and compute resources needed to replicate applications from on-premises to Azure—and pay only for compute and storage resources needed to run apps in Azure during outages.

• Automatically replicate to Azure. Automate the orderly recovery of services in the event of a site outage at the primary datacenter. Automate the orderly recovery of services in the event of a site outage at the primary datacenter.

• Safeguard against outages of complex workloads. Protect applications in SQL Server, SharePoint, SAP, and Oracle.

• Extend or boost capacity. Applications can be Migrated to Azure with just a few clicks or burst to Azure temporarily when you encounter a surge in demand.

• Monitor resource health. Site Recovery monitors the state of your protected instances continuously and remotely from Azure. When replicating between two sites you control, your virtual machines' data and replication remains on your networks. All communication with Azure is encrypted.

Planned and Unplanned Failovers

An organization plans to replicate all on-premises servers and systems to Azure as a failover location in the event that the on-premises datacenter becomes unavailable.

How do you initiate a failover? What types of failover scenarios should you consider? How can you ensure data resiliency?

Suggested Answer
Failover isn't automatic. You can initiate failovers in the portal or with PowerShell, but it is a deliberate act. There are two types of failover: planned and unplanned. An example of a planned failover is when your datacenter has scheduled downtime. An example of an unplanned failover is when your datacenter has a power outage.
LRS or GRS storage is recommended, so the data is resilient if a regional outage occurs, or if the primary region cannot be recovered.

Module 2 Implementing and Managing Application Services

Deploying Web Apps

Web Apps Features

In App Service, a web app is the compute resources that Azure provides for hosting a website or web application.

The compute resources may be on shared or dedicated virtual machines (VMs), depending on the pricing tier that you choose. Your application code runs in a managed VM that is isolated from other customers.

Here are some key features and capabilities of App Service:

- **Multiple languages and frameworks** - App Service has first-class support for ASP.NET, Node.js, Java, PHP, and Python. You can also run Windows PowerShell and other scripts or executables on App Service VMs.
- **DevOps optimization** - Set up continuous integration and deployment with Visual Studio Team Services, GitHub, or BitBucket. Promote updates through test and staging environments. Perform A/B testing. Manage your apps in App Service by using Azure PowerShell or the cross-platform command-line interface (CLI).
- **Global scale with high availability** - Scale up or out manually or automatically. Host your apps anywhere in Microsoft's global datacenter infrastructure, and the App Service SLA promises high availability.
- **Connections to SaaS platforms and on-premises data** - Choose from more than 50 connectors for enterprise systems (such as SAP, Siebel, and Oracle), SaaS services (such as Salesforce and Office 365), and internet services (such as Facebook and Twitter). Access on-premises data using Hybrid Connections and Azure Virtual Networks.
- **Security and compliance** - App Service is ISO, SOC, and PCI compliant.
- **Application templates** - Choose from an extensive list of templates in the Azure Marketplace that let you use a wizard to install popular open-source software such as WordPress, Joomla, and Drupal.

- **Visual Studio integration** - Dedicated tools in Visual Studio streamline the work of creating, deploying, and debugging.
- **API and mobile features** - Turn-key CORS support for RESTful API scenarios, authentication for mobile app scenarios, and offline data sync, and push notifications.
- **Serverless code** - Run a code snippet or script on-demand without having to explicitly provision or manage infrastructure, paying only for the compute time that the code uses.

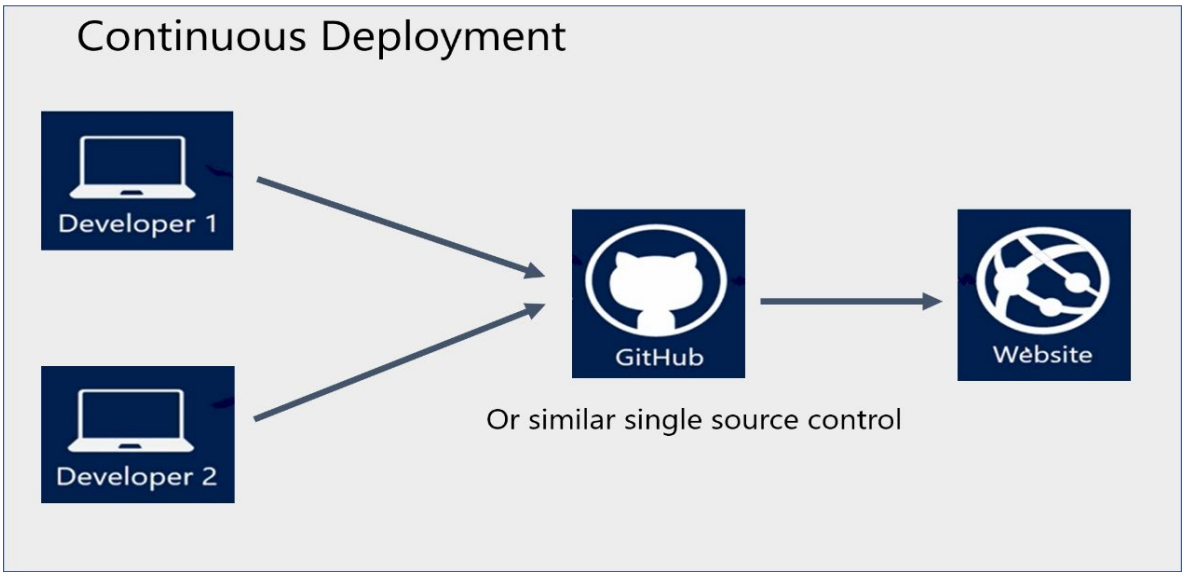
✓ Do you have any web app projects in mind for your organization?

For more information, you can see:

Web apps overview - **https://docs.microsoft.com/en-us/azure/app-service/app-service-web-overview**

What is Continuous Deployment

Multiple developers want to be able to work in a single source control. Whenever code updates are pushed to the source control, then the website or web app will automatically pick up the updates. A continuous deployment workflow publishes the most recent updates from a project.



The Azure portal makes it easy to set up continuous deployment from GitHub, Bitbucket, or Visual Studio Team Services. You can also set up continuous deployment from a git host that the portal doesn't directly support, like GitLab.

✓ Continuous deployment is a great option for projects where multiple and frequent contributions are being integrated.

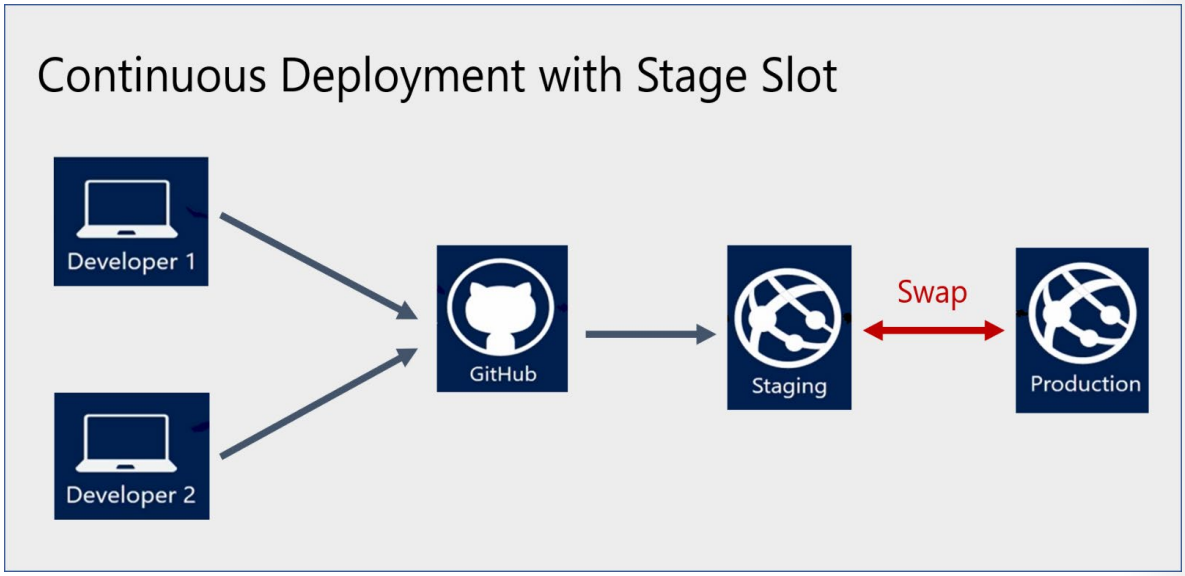
For more information , you can see:

Continuous deployment - **https://github.com/projectkudu/kudu/wiki/Continuous-deployment#setting-up-continuous-deployment-using-manual-steps**[1]

1 https://github.com/projectkudu/kudu/wiki/Continuous-deployment

Staging Environments in App Service

When you deploy your web app, mobile back end, and API app to App Service, you can deploy to a separate deployment slot instead of the default production slot when running in the **Standard** or **Premium** App Service plan mode.



Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot. Using separate staging and production slots has several advantages.

- You can validate app changes in a staging deployment slot before swapping it with the production slot.
- Deploying an app to a slot first and swapping it into production ensures that all instances of the slot are warmed up before being swapped into production. This eliminates downtime when you deploy your app. The traffic redirection is seamless, and no requests are dropped because of swap operations. This entire workflow can be automated by configuring Auto Swap when pre-swap validation is not needed.
- After a swap, the slot with previously staged app now has the previous production app. If the changes swapped into the production slot are not as you expected, you can perform the same swap immediately to get your "last known good site" back.

✓ Each App Service plan mode supports a different number of deployment slots. To find out the number of slots your app's mode supports, see **App Service Limits**[2].

For more information, you can see:

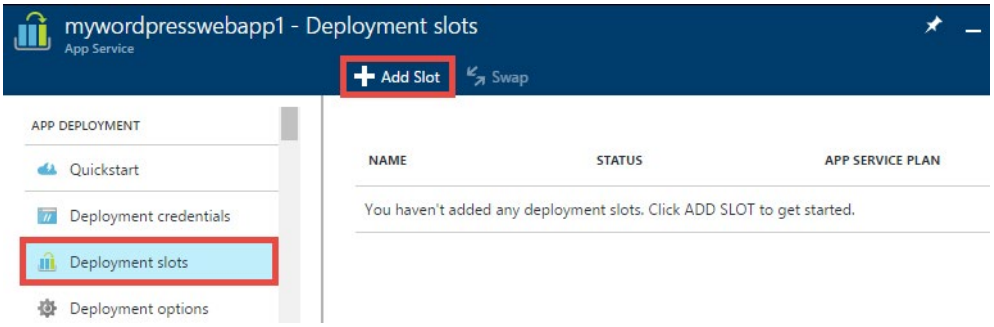
Set up staging environments - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing?toc=%2Fazure%2Fapp-service%2Ftoc.json#add-a-deployment-slot**[3]

App Service Web App – block web access to non-production deployment slots - **http://ruslany.net/2014/04/azure-web-sites-block-web-access-to-non-production-deployment-slots/**

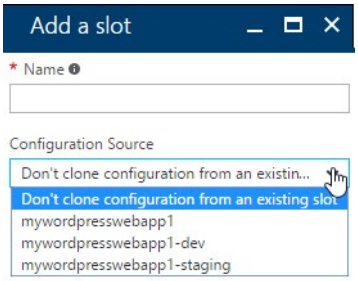
2 https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits
3 https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing?toc=%2Fazure%2Fapp-service%2Ftoc.json

Add a Deployment Slot

Your app must be running in the **Standard** or **Premium** tier for you to enable multiple deployment slots. If the app is not already in the Standard or Premium tier, you will receive a message indicating the supported tiers for enabling staged publishing. At this point, you have the option to select Upgrade and navigate to the Scale tab of your app before continuing.



The first time you add a slot, you only have two choices: clone configuration from the default slot in production or not at all. After you have created several slots, you will be able to clone a configuration from a slot other than the one in production.



✓ There is no content after deployment slot creation. You can deploy to the slot from a different repository branch, or an altogether different repository. You can also change the slot's configuration. Use the publish profile or deployment credentials associated with the deployment slot for content updates.

For more information, you can see:

Add a deployment slot - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing?toc=%2Fazure%2Fapp-service%2Ftoc.json#add-a-deployment-slot**[4]

Swap Deployment Slots

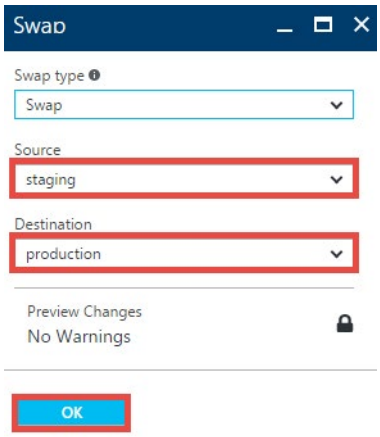
When you clone configuration from another deployment slot, the cloned configuration is editable. Furthermore, some configuration elements will follow the content across a swap (not slot specific) while other configuration elements will stay in the same slot after a swap (slot specific).

- Settings that **are** swapped: general settings, handler mappings, monitoring, diagnostics, and WebJobs.
- Settings that **are not** swapped: publishing endpoints, custom domain names, SSL certificates and bindings, scale settings, and WebJob schedulers.

4 https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing?toc=%2Fazure%2Fapp-service%2Ftoc.json

Before you swap an app from a deployment slot into production, make sure that all non-slot specific settings are configured exactly as you want to have it in the swap target. To swap deployment slots, click the Swap button in the command bar of the app or in the command bar of a deployment slot.

Make sure that the swap source and swap target are set properly. Usually, the swap target is the production slot.



✓ You can configure app settings and connections to stick to a slot and not be swapped. This done in the App Settings blade. A developer can create new settings for the web app. The last video in this lesson reviews this concept.

Optional Practice- Deployment Slots

Take a few minutes to complete the **Add a deployment slot**[5] practice and the **Swap deployment slots**[6] practice. As you have time continue through the other tutorials. In this tutorial, you will learn how to:

- Add a deployment slot.
- Swap deployment slots.
- Configure auto swap.
- Monitor swap progress.
- Delete a deployment slot.

For more information, you can see:

Set up staging environments for web apps - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing**

5 https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing
6 https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing

Web App Templates

Azure Resource Manager has many templates for the Web Apps feature of Azure App Service. The templates can generally be divided into: Deploying a Web App, Configuring a Web App, Linux Web App, Web App with Connected Resources, and App Service Environment for PowerApps.

- **Deploying a Web App**. For example, deploy an Azure web app that pulls code from GitHub, and a Web app with custom deployment slots.
- **Configuring a Web App**. For example, deploy a web app with a custom domain name.
- **Linux Web App**. For example, deploy an Azure web app on Linux with Azure Database for PostgreSQL or Azure Database with MySQL.
- **Web Apps with Connected Resources**. For example, deploy an Azure web app with an Azure Blob storage connection string, and deploy an Azure web app and a SQL database at the Basic service level.
- **App Service Environment for PowerApps**. For example, create an App Service environment v2 in your virtual network.

✓ Defining dependencies for web apps requires an understanding of how the resources within a web app interact. If you specify dependencies in an incorrect order, you might cause deployment errors or create a race condition that stalls the deployment. Read more about this in the reference link.

For more information, you can see:

Azure Resource Manager templates for Web Apps - **https://docs.microsoft.com/en-us/azure/app-service/app-service-rm-template-samples**

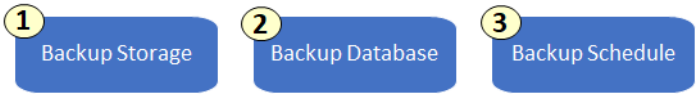
Guidance on deploying web apps with Azure Resource Manager templates - **Guidance on deploying web apps with Azure Resource Manager templates**[7]

7 https://docs.microsoft.com/en-us/azure/app-service/web-sites-rm-template-guidance

Managing Web Apps

Backup Your App

The Azure App Service backup feature lets you easily create app backups manually or on a schedule. When configuring your backups consider three things: backup storage, backup database, and backup schedule.



1. **Backup storage**. Choose your backup destination by selecting a Storage Account and Container. The storage account must belong to the same subscription as the app you want to backup. It is probably a good idea to create a new storage account or a new container just for backups.
2. **Backup database**. For a database to appear in the backup list, its connection string must exist in the **Connectionstrings** section of the Application settings page for your app. The backup feature supports the following database solutions:

- **SQL Database**[8]
- **Azure Database for MySQL**[9]
- **Azure Database for PostgreSQL**[10]
- **MySQL in-app**[11]

3. **Backup schedule**. Creating a backup schedule is an easy way to automate the backup process. You can configure how often to backup (hours/days), when to backup (calendar with times), and how long to keep the backup (retention days).

By default, your app configuration, file content, and database content is backed up. Each backup is a complete offline copy of your app, not an incremental update. See the reference link on how to configure a partial backup.

✓ Take a few minutes to use the reference link and create a backup of your app.

For more information, you can see:

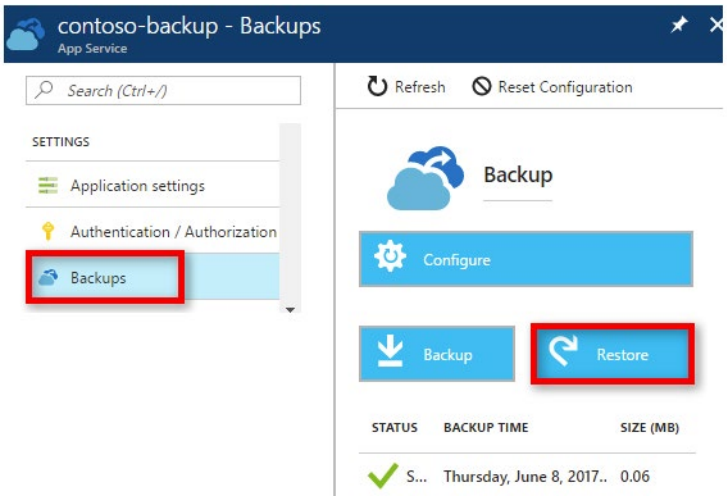
Back up your App in Azure - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup**

Configure partial backups - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup**

Restore a Backup

After you have backed up your app you can restore the app, with its linked databases, to a previous state, or create a new app using the backup. Notice in the next image, the Restore button and the Backup button discussed in the previous topic.

8 https://azure.microsoft.com/services/sql-database/
9 https://azure.microsoft.com/services/mysql
10 https://azure.microsoft.com/en-us/services/postgresql/
11 https://blogs.msdn.microsoft.com/appserviceteam/2017/03/06/announcing-general-availability-for-mysql-in-app



When configuring a restore there are two things to consider: The **Restore source** and the **Restore destination**.

- **Restore source**. You can select **App Backup** to select any previous existing backup of the current app. You can also select **Storage** and select any backup ZIP file from any existing Azure Storage account and container in your subscription.
- **Restore destination**. You can select **Existing App** to restore the app backup to another app in the same resource group. Before you use this option, you should have already created another app in your resource group with mirroring database configuration to the one defined in the app backup. You can also **Create a New app** to restore your content to.

✓ Restoring from backups is available to apps running in the **Standard** and **Premium** tiers. The **Premium** tier allows a greater number of daily backups to be performed than the **Standard** tier. Take a few minutes to explore and restore an app.

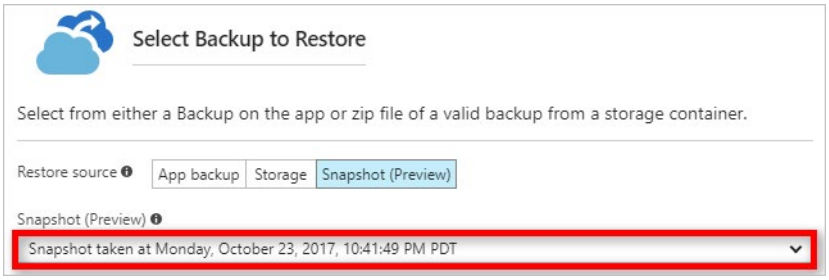
For more information, you can see:

Restore an app in Azure - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-restore**

Restore a Snapshot

If your app is running in the **Premium** tier or higher, the platform automatically saves snapshots for data recovery purposes. Snapshots are incremental shadow copies that have several advantages over backups:

- No file copy errors due to file locks.
- No storage size limitation.
- No configuration required.



At the time of this writing, the snapshot feature is in preview. Also, here are a few other things to know:

- You can only restore to the same app or to a slot belonging to that app.
- App Service stops the target app or target slot while doing the restore.
- App Service keeps three months' worth of snapshots for platform data recovery purposes.
- You can only restore snapshots for the last 30 days.

✓ The Restore destination can either be: **Overwrite** or **New or Existing App**. If you choose **Overwrite**, all existing data in your app's current file system is erased and overwritten. Before you click **OK**, make sure that it is what you want to do.

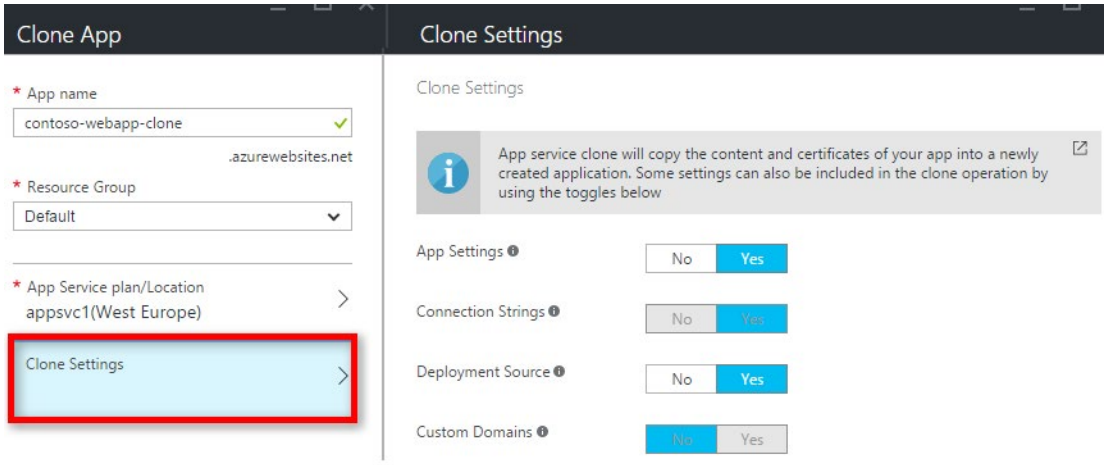
For more information, you can see:

Restore an app in Azure from a snapshot - **https://docs.microsoft.com/en-us/azure/app-service/app-service-web-restore-snapshots**

Cloning an App

The cloning feature in Azure App Service Web Apps lets you easily clone existing web apps to a newly created app in a different region or in the same region. This feature lets you to deploy apps across different regions quickly and easily. App cloning is currently only supported for Premium tier app service plans.

You can clone an app in the Azure Portal or with Azure PowerShell. When you use the portal, you can decide which settings are cloned. For example, you can choose to include App Settings, Connection Strings, Deployment Source, and Custom Domains.



Current Restrictions

App cloning is supported for Standard, Premium, Premium V2, and Isolated app service plans. The new feature uses the same limitations as App Service Backup feature. There are some restrictions in the current version of app cloning. Here is a list of what is not currently cloned as well as any impacts of app cloning:

- Auto scale settings
- Backup schedule settings
- VNET settings
- Easy Auth settings
- Kudu Extensions
- TiP rules
- Database content
- App Insights are not automatically set up on the destination web app.
- Outbound IP Addresses change if cloning to a different scale unit.

✓ Can you see a need for app cloning in your organization?

For more information , you can see:

Web App Cloning - **https://azure.microsoft.com/en-us/updates/azure-app-service-cloning-available-between-regions/**

Optional Practice- Azure Backup and Restore

The Backup and Restore feature in Azure App Service lets you easily create app backups manually or on a schedule. You can restore the app to a snapshot of a previous state by overwriting the existing app or restoring to another app.

Either create a web app or use an existing one, and take some time to work with the **backup and restore**[12] functionality in the Azure portal.

✓ Be sure to read through the **requirements and restrictions**[13] for backup and restore in the documentation.

In this exercise, you will:

- Create a manual backup of an app.
- Configure an automated backup
- Configure a partial backup

12 https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup
13 https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup

Restoring from backups is available to apps running in **Standard** and **Premium** tier. To work with restore, go to **Restore an app in Azure**[14] and try the following:

- Restore an app from an existing backup
- Download or delete a backup from a storage account
- Monitor a restore operation

You can also try the same tasks using sample scripts, either **PowerShell**[15] or the **Azure CLI**[16].

For more information, you can see:

Back up your App in Azure - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup**

Configure partial backups - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-backup**

Restore an app in Azure - **https://docs.microsoft.com/en-us/azure/app-service/web-sites-restore**

14 https://docs.microsoft.com/en-us/azure/app-service/web-sites-restore

15 https://docs.microsoft.com/en-us/azure/app-service/scripts/app-service-powershell-backup-onetime?toc=%2fpowershell%2fmodule%2ftoc.json

16 https://docs.microsoft.com/en-us/azure/app-service/scripts/app-service-cli-backup-onetime?toc=%2fcli%2fazure%2ftoc.json

App Service Security

App Service Security Levels

The Azure App Service has two security levels.

- **Infrastructure and platform security**. You trust Azure to provide an infrastructure and platform to securely run your services.
- **Application security**. You design an app with security features. This includes how you integrate with Azure Active Directory, how you manage certificates, and how you make sure that you can securely communicate with different services.

Infrastructure and platform security

The App Service maintains Azure VMs, storage, network connections, web frameworks, management, and integration features, and much more. The App Service is actively secured and hardened and goes through vigorous compliance checks on a continuous basis. These security checks ensure:

- Your App Service apps are isolated from both the Internet and from the other customers' Azure resources.
- Communication of secrets (e.g. connection strings) between your App Service app and other Azure resources (e.g. SQL Database) in a resource group stays within Azure and doesn't cross any network boundaries. Secrets are always encrypted.
- All communication between your App Service app and external resources, such as PowerShell management, command-line interface, Azure SDKs, REST APIs, and hybrid connections, are properly encrypted.
- 24-hour threat management protects App Service resources from malware, distributed denial-of-service (DDoS), man-in-the-middle (MITM), and other threats.

Application security

While Azure is responsible for securing the infrastructure and platform that your application runs on, it is your responsibility to secure your application itself. In other words, you need to develop, deploy, and manage your application code and content in a secure way. Without this, your application code or content can still be vulnerable to threats such as:

- **SQL Injection**. SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.
- **Session hijacking**. There are two types of session hijacking depending on how they are done. If the attacker directly gets involved with the target, it is called active hijacking, and if an attacker just passively monitors the traffic, it is passive hijacking.

- **Cross-site-scripting**. Cross site scripting attacks work by embedding script tags in URLs and enticing users to click them, ensuring that the malicious script gets executed on the user's computer. These attacks leverage the trust between the user and the server and the fact that there is no input/output validation on the server to reject script language characters. Most browsers are installed with the capability to run scripts enabled by default.
- **Application level Man-In-the-Middle (MITM)**. A MITM attack occurs when an attacker reroutes communication between two users through the attacker's computer without the knowledge of the two communicating users. The attacker can monitor and read the traffic before sending it on to the intended recipient.

For more information , you can see:

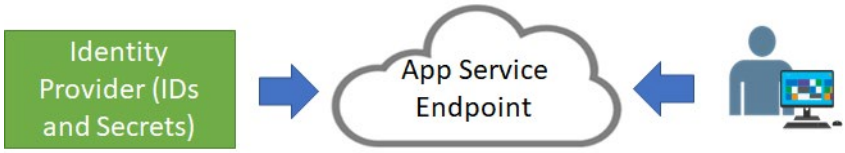
Azure Security Center - **https://azure.microsoft.com/en-us/services/security-center/**

SQL Injection - **https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-injection?view=sql-server-2017**

Session Hijacking - **https://www.greycampus.com/opencampus/ethical-hacking/session-hijacking-and-its-types**

App Service Authentication

How App Service *authentication* works



To authenticate by using one of the identity providers, you first need to configure the identity provider to know about your application. The identity provider will then provide IDs and secrets that you provide to App Service. This completes the trust relationship so that App Service can validate user assertions, such as authentication tokens, from the identity provider.

To sign in a user by using one of these providers, the user must be redirected to an endpoint that signs in users for that provider. If customers are using a web browser, you can have App Service automatically direct all unauthenticated users to the endpoint that signs in users. Otherwise, you will need to direct your customers to *{your App Service base URL}/.auth/login/<provider>*, where <provider> is one of the following values: AAD, Facebook, Google, Microsoft, or Twitter.

Users who interact with your application through a web browser will have a cookie set so that they can remain authenticated as they browse your application. For other client types, such as mobile, a JSON web token (JWT), which should be presented in the X-ZUMO-AUTH header, will be issued to the client. The Mobile Apps client SDKs will handle this for you. Alternatively, an Azure Active Directory identity token or access token may be directly included in the Authorization header as a bearer token.

✓ You're not required to use App Service for authentication and authorization. Many web frameworks are bundled with security features, and you can use them if you like. If you need more flexibility than App Service provides, you can also write your own utilities

For more information, you can see:

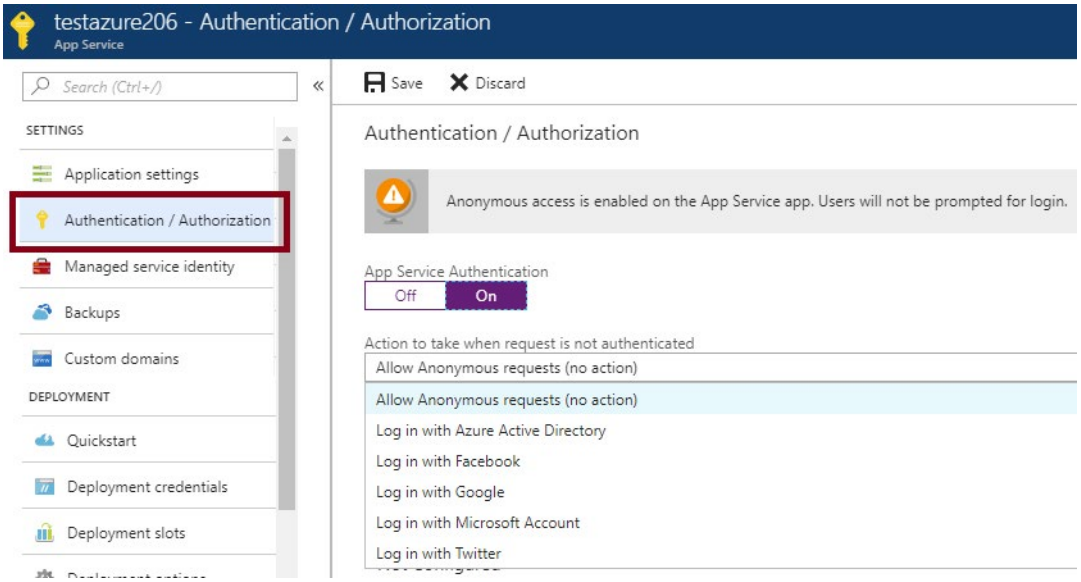
Authentication and authorization in Azure App Service - **https://docs.microsoft.com/en-us/azure/app-service/app-service-authentication-overview**

Authentication Providers

The App Service Authentication / Authorization feature provides a way for your application to sign in users so that you don't have to change code on the app backend. The App Service uses federated identity, in which a third-party identity provider stores accounts and authenticates users. The application relies on the provider's identity information so that the app doesn't have to store that information itself.

The App Service supports five identity providers out of the box: Azure Active Directory, Facebook, Google, Microsoft Account, and Twitter. Your app can use any number of these identity providers to provide your users with options for how they sign in. To expand the built-in support, you can integrate another identity provider or your own custom identity solution.

By default, anonymous access is allowed on the App Service app. To make your App Service more secure you can enable App Service Authentication in the Settings panel.



When App Service authentication is enabled there are several authentication options.

- **Authenticate with Azure Active Directory**[17]. Express mode will use your default AAD and create an AAD application for you. There is also a custom mode if you would like more control over the configuration.
- **Authenticate with Facebook**[18]. You will need your App ID and App Secret from the **Facebook Developer's website**[19].
- **Authenticate with Google**[20]. You will need the client ID and client secret from the **Google APIs**[21] website.
- **Authenticate with Microsoft Account**[22]. You will need the Application ID and Password values from the **My Applications page**[23] in the Microsoft Account Developer Center.

17 https://docs.microsoft.com/en-us/azure/app-service/app-service-mobile-how-to-configure-active-directory-authentication
18 https://docs.microsoft.com/en-us/azure/app-service/app-service-mobile-how-to-configure-facebook-authentication
19 http://go.microsoft.com/fwlink/p/?LinkId=268286
20 https://docs.microsoft.com/en-us/azure/app-service/app-service-mobile-how-to-configure-google-authentication
21 http://go.microsoft.com/fwlink/p/?LinkId=268303
22 https://docs.microsoft.com/en-us/azure/app-service/app-service-mobile-how-to-configure-microsoft-authentication
23 http://go.microsoft.com/fwlink/p/?LinkId=262039

- **Authenticate with Twitter**[24]. You must have a Twitter account that has a verified email address and phone number. To create a new Twitter account, go to **twitter.com**[25].

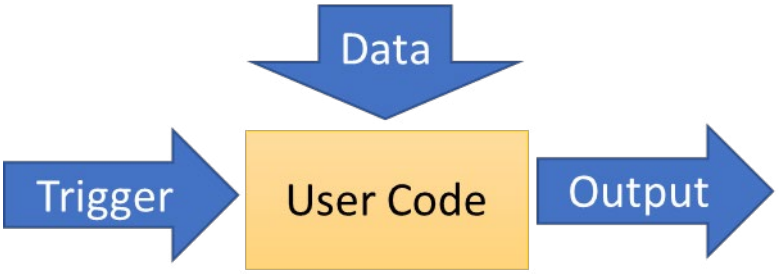
✓ Take a minute to create an App Service and view the Authentication and Authorization Settings. Try each of the drop-down options to see what additional information is required. Which option are you most interested in?

24 https://docs.microsoft.com/en-us/azure/app-service/app-service-mobile-how-to-configure-twitter-authentication
25 http://go.microsoft.com/fwlink/p/?LinkID=268287

Serverless Computing Concepts

Serverless Computing

Developers focus most of their time building and deploying apps, but must often spend time also managing the servers those apps will run on. Having to consider the infrastructure is critical but consumes time that could be spent on app development. Serverless computing provides a real solution to this challenge. Serverless computing is the abstraction of servers, infrastructure, and operating systems. When building serverless apps, developers don't need to provision and manage any servers, and can take their minds off infrastructure concerns.



Infrastructure spun-up, scaled, and spun-down when no longer needed

Serverless computing is driven by the reaction to events and triggers happening in near-real-time—in the cloud. As a fully managed service, server management and capacity planning are invisible to the developer and billing is based just on resources consumed or the actual time your code is running.

Serverless computing has many advantages. Here are a few:

- **Benefit from a fully managed service**. Organizations can relieve their teams from the burden of managing servers. By utilizing fully managed services, developers focus on application business logic and avoid administrative tasks. With serverless architecture developers simply deploy their code, and it runs with high availability.
- **Scale flexibly**. Serverless compute scales from nothing to handling tens of thousands of concurrent functions almost instantly (within seconds), to match any workload, and without requiring scale configuration.
- **Only pay for the resources used**. With serverless architecture, your organization only pays for the time the application code is running. Serverless computing is event-driven, and resources are allocated as soon as they're triggered by an event. You're only charged for the time and resources it takes to execute the application code—through sub-second billing.

For more information, you can see:

Serverless computing - **https://azure.microsoft.com/en-us/overview/serverless-computing/**

Serverless Applications

Serverless computing covers a wide area and has many applications. In this course we will cover four of the main applications in the areas of compute, cloud messaging, and workflow orchestration.

Compute

- **Azure Functions** is an event-driven compute experience that allows an app developer to execute code, written in the programming language of their choice, without worrying about servers. An organization benefits from scale on demand without incurring charges for idle capacity.

Cloud Messaging

- **Event Grid** is a fully managed event routing service that enables rich application scenarios by connecting serverless logic to events coming from multiple Azure services or from a developer or organization's custom apps.
- **Service Bus** is a fully managed messaging infrastructure that enables an organization to build distributed and scalable cloud solutions with connections across private and public cloud environments.

Workflow Orchestration

- **Logic Apps** provide serverless workflows that allow developers to easily integrate data with their apps instead of writing complex glue code between disparate systems. Logic Apps also allow the orchestration and connecting of the serverless functions and APIs in an application.

✓ Processing background jobs, **WebJobs**, will also be covered in this module.

For more information, you can see:

Azure Serverless Computing Cookbook - **https://azure.microsoft.com/en-us/resources/azure-serverless-computing-cookbook/**

Comparing Serverless Options

After learning about the different serverless computing options in this module you may be wondering which to choose for your application. Here is a quick summary of what is to come.

Azure Functions vs Logic Apps

Functions and Logic Apps are Azure services that enable serverless workloads. Azure Functions is a serverless compute service, while Azure Logic Apps provides serverless workflows. The following table describes different aspects of Azure Functions and Logic Apps

	Durable Functions	Logic Apps
Development	Code-first (imperative)	Designer-first (declarative)

	Durable Functions	Logic Apps
Connectivity	**About a dozen built-in binding types** *(https://docs.microsoft.com/en-us/azure/azure-functions/functions-triggers-bindings)*, write code for custom bindings	**Large collection of connectors** *(https://docs.microsoft.com/en-us/azure/connectors/apis-list)*, **Enterprise Integration Pack for B2B scenarios** *(https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-enterprise-integration-overview)*, **build custom connectors** *(https://docs.microsoft.com/en-us/azure/logic-apps/custom-connector-overview)*
Actions	Each activity is an Azure function; write code for activity functions	**Large collection of ready-made actions** *(https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-workflow-actions-triggers)*
Monitoring	**Azure Application Insights** *(https://docs.microsoft.com/en-us/azure/application-insights/app-insights-overview)*	**Azure portal** *(https://docs.microsoft.com/en-us/azure/logic-apps/quickstart-create-first-logic-app-workflow)*, **Operations Management Suite** *(https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-monitor-your-logic-apps-oms)*, **Log Analytics** *(https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-monitor-your-logic-apps)*
Management	**REST API** *(https://docs.microsoft.com/en-us/azure/azure-functions/durable-functions-http-api)*, **Visual Studio** *(https://docs.microsoft.com/azure/vs-azure-tools-resources-managing-with-cloud-explorer)*	**Azure portal** *(https://docs.microsoft.com/en-us/azure/logic-apps/quickstart-create-first-logic-app-workflow)*, **REST API** *(https://docs.microsoft.com/rest/api/logic/)*, **PowerShell** *(https://docs.microsoft.com/en-us/powershell/module/az.logicapp/?view=azps-3.3.0)*, **Visual Studio** *(https://docs.microsoft.com/azure/logic-apps/manage-logic-apps-with-visual-studio)*
Execution context	Can run **locally** *(https://docs.microsoft.com/en-us/azure/azure-functions/functions-runtime-overview)* or in the cloud.	Runs only in the cloud.

Functions and WebJobs

The WebJobs feature of App Service enables you to run a script or code in the context of an App Service web app. Azure Functions is built on the WebJobs SDK, so it shares many of the same event triggers and connections to other Azure services.

	Functions	WebJobs with WebJobs SDK
Serverless app model *(https://azure.microsoft.com/overview/serverless-computing/)* with **automatic scaling** *(https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale)*	Yes	No
Develop and test in browser *(https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-first-azure-function)*	Yes	No
Pay-per-use pricing *(https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale)*	Yes	No
Integration with Logic Apps *(https://docs.microsoft.com/en-us/azure/azure-functions/functions-twitter-email)*	Yes	No

✓ You may want to bookmark this page and return when you've learned a bit more.

For more information, you can see:

Compare Azure Functions and Azure Logic Apps - **https://docs.microsoft.com/en-us/azure/azure-functions/functions-compare-logic-apps-ms-flow-webjobs#compare-azure-functions-and-azure-logic-apps**[26]

Compare Functions and WebJobs - **https://docs.microsoft.com/en-us/azure/azure-functions/functions-compare-logic-apps-ms-flow-webjobs#compare-functions-and-webjobs**[27]

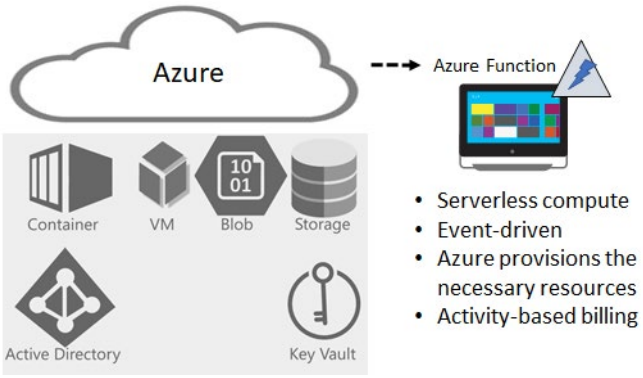
26 https://docs.microsoft.com/en-us/azure/azure-functions/functions-compare-logic-apps-ms-flow-webjobs
27 https://docs.microsoft.com/en-us/azure/azure-functions/functions-compare-logic-apps-ms-flow-webjobs

Managing Azure Functions

Overview of Azure Functions

Azure Functions is a serverless compute service that enables you to run code on-demand without having to explicitly provision or manage infrastructure. Serverless relieves the developer from the operational complexity of running applications. He or she no longer must worry about servers, virtual machines, patching, and scaling. This differs slightly from PaaS, because with PaaS, you still need to choose your operating system and the VM size, which means you need to be able to forecast your demand and then pay for that capacity, even if it's not fully utilized.

With serverless, Azure has compute resources ready to be allocated. Their usage is triggered by an event. The developer provides the code and when an event occurs, such as an Azure alert or when a message is received, Azure provisions the necessary compute resources. This is activity-based billing, so a developer, or the organization, only incurs charges when using the resources.



For more information you can see:

Build apps faster with Azure Serverless - **https://azure.microsoft.com/en-us/blog/build-apps-faster-with-azure-serverless/**

Features of Azure Functions

Azure Functions is a solution for easily running small pieces of code, or "functions," in the cloud. The developer simply writes the code needed for the problem at hand, without worrying about an entire application or the infrastructure to run it.

Features

Here are some key features of Azure Functions that it make it an ideal solution for web app developers:

- **Choice of language**. Write functions using C#, F#, Node.js, Python, PHP, batch, bash, or any executable.
- **Pay-per-use pricing model**. Pay only for the time spent running application code.
- **Bring your own dependencies**. Functions supports NuGet and NPM, allowing use of preferred libraries.
- **Integrated security**. Protect HTTP-triggered functions with OAuth providers such as Azure Active Directory, Facebook, Google, Twitter, and Microsoft Account.
- **Simplified integration**. Easily leverage Azure services and software-as-a-service (SaaS) offerings.

- **Flexible development**. Developers can code their functions directly in the portal or set up continuous integration to deploy their code through GitHub, Visual Studio Team Services, and other supported development tools.
- **Open-source**. The Functions runtime is open-source and available on GitHub.
- **Reuse**. Developers can reuse their functions in multiple applications.

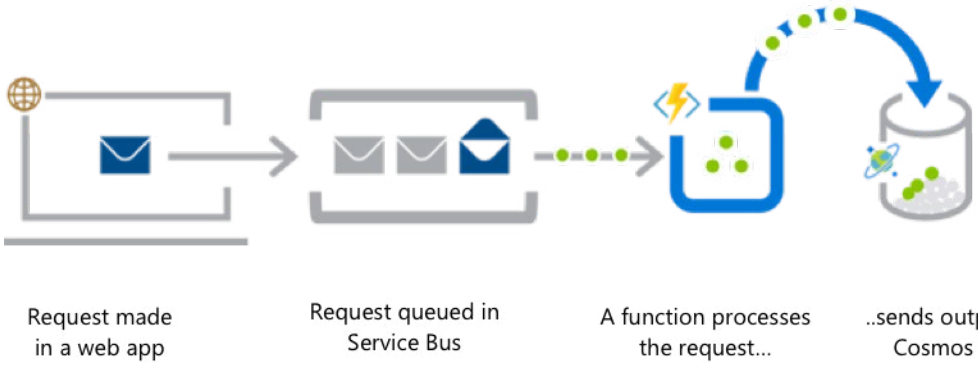
For more information, you can see:

Azure Functions Documentation - **https://docs.microsoft.com/en-us/azure/azure-functions/**

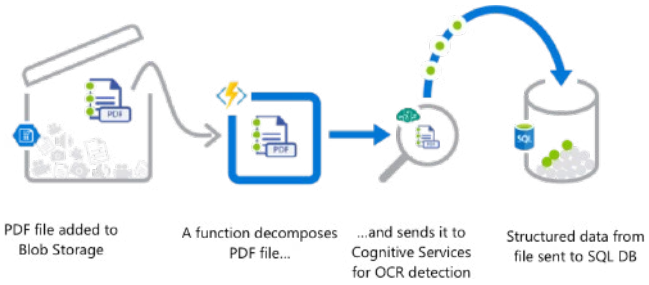
Azure Functions (Examples)

Azure Functions is a great solution for processing data, integrating systems, working with the internet-of-things (IoT), and building simple APIs and microservices. Functions should be considered for tasks like image or order processing, file maintenance, long-running tasks that need to run in a background thread, or for any tasks that run on a schedule. Here are three examples of how you can use Functions.

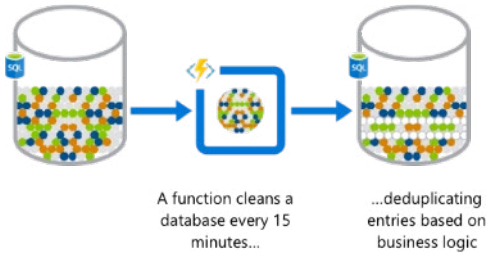
Web application backends. Online orders are picked up from a queue, processed, with the resulting data stored in a database.



Real-time file processing. Patient records are securely uploaded as PDF files. That data is then decomposed, processed using Optical Character Recognition (OCR) detection, and added to a database for customers who can search the information.



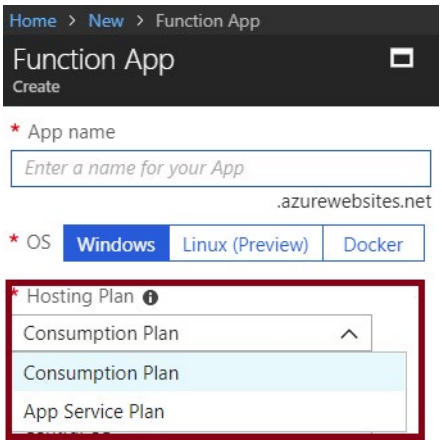
Automation of scheduled tasks. A customer database is analyzed for duplicate entries every 15 minutes. The removal of duplicates ensures multiple communications are not being sent out to same customers.



✓ Can you think of any apps that could benefit from functions?

Function Service Plans

When you create a function app, you must decide on a name, OS, and hosting plan. There are two hosting plans: **Consumption Plan** and **App Service Plan**. Choose the one that best fits your needs.



App Service plan

A developer can run their functions just like any web, mobile, and API apps. While already using App Service for your other applications, the developer can run those functions on the same plan at no additional cost. Currently, Linux hosting is currently only available on an App Service plan.

Consumption plan

When a function runs, Azure provides all the necessary compute resources. The developer or the organization doesn't need to worry about resource management, and only pays for the time that the code runs.

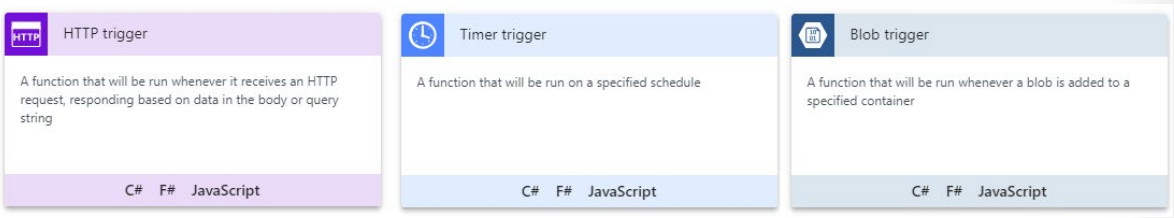
The Consumption plan automatically scales CPU and memory resources by adding additional processing instances based on the runtime needs of the functions in the Function App. The Consumption plan is the default hosting plan and offers the following benefits:

- Pay only when functions are running. Billing is based on number of executions, execution time, and memory used.
- Scale out automatically, even during periods of high load.

✓ Can you see why the Consumption plan is the default?

Function Templates

After creating a function and selecting the service plan, a developer can use a template for many different key scenarios. The template will create a function triggered to different events. The trigger will start the execution of the code. Here are some example templates.



HTTP Trigger. A function that will run whenever it receives an HTTP request. The function responds based on data in the body or query string.

Timer Trigger. A function that runs on a specified schedule. For example, cleanup or batch tasks.

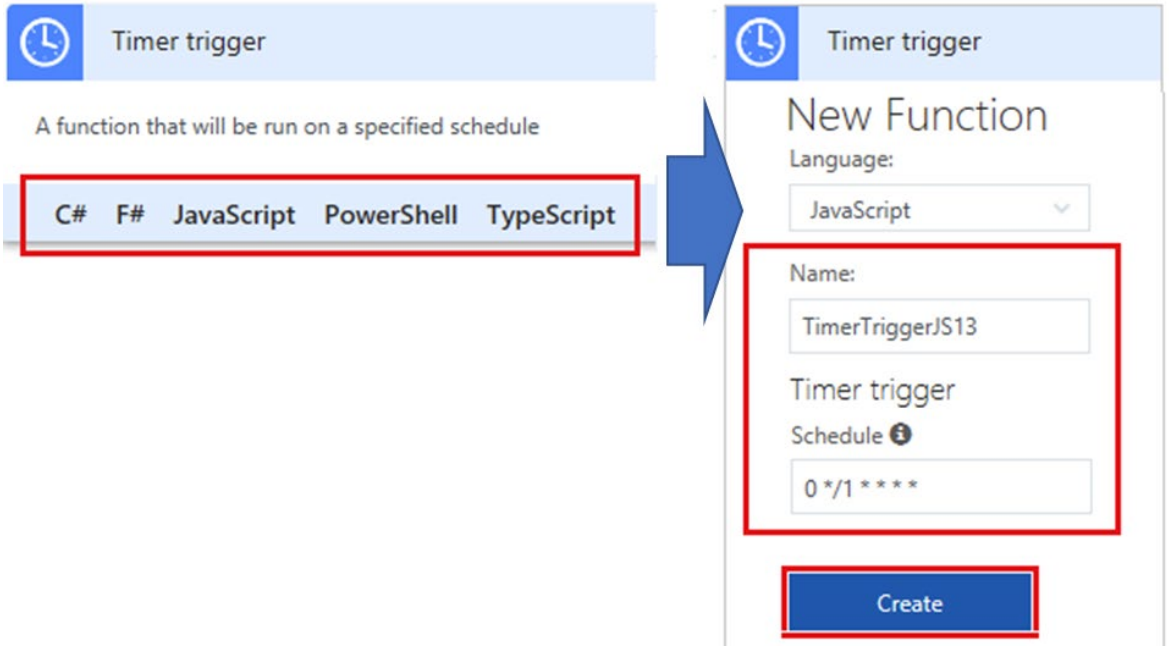
Blob Trigger. A function that will run whenever a blob is added to a specified container. This function might be used for resizing images that will be added to web pages.

There are other triggers that respond to Event Hub, GitHub, webhook, and queue events. By default, a function will timeout after 5 minutes, and a function can run for a maximum of 10 minutes.

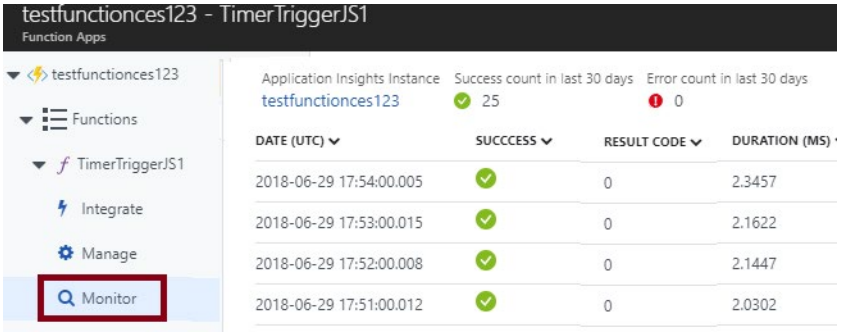
✓ Use the reference link to learn more about triggers.

Implementing Functions

Once of the easiest functions to understand is the Timer. After choosing the language, the Timer template only requires the timer name and the schedule. Azure Functions uses the NCronTab library to interpret NCRONTAB expressions. An NCRONTAB expression is similar to a CRON expression except that it includes an additional sixth field at the beginning to use for time precision in seconds. For NCRONTAB expressions, see: **https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-timer?tabs=csharp**



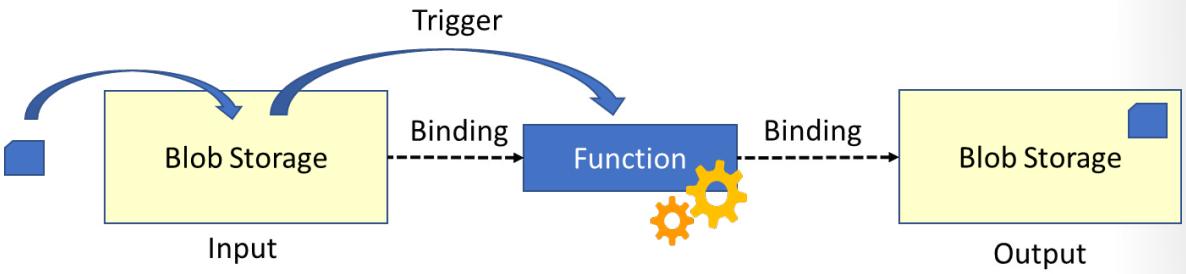
Once your function is running you can monitor its progress.



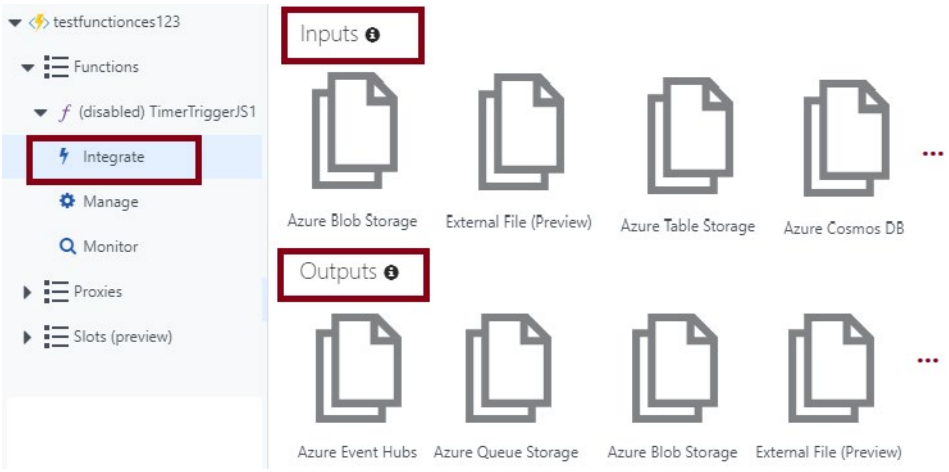
✓ Use the Manage link to disable or delete your function. Click the name of the function to see the code behind the function. Creating a timer function is one of the practices for this lesson.

Bindings

So far you have learned that a trigger defines how a function is invoked. Bindings are a way to provide input and output to the function. For example, if the function is resizing an image then it could be bound to the incoming Blob storage. When an image arrives in that storage, a trigger would start the resizing function. The processed image could then be stored in the same or different Blob storage. A function can have multiple input and output bindings. Bindings are always optional.



To see what bindings are available to your function use the **Integrate** link.



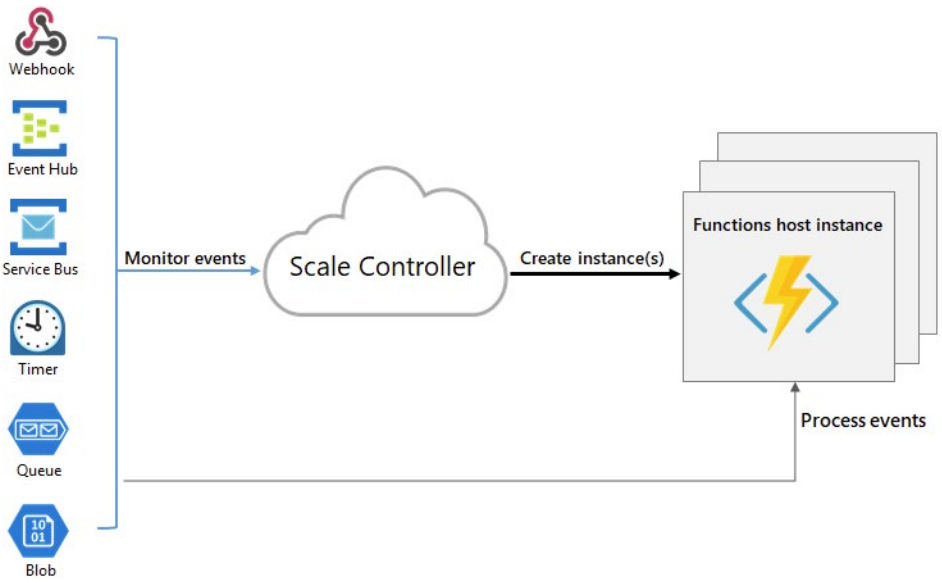
Each input or output binding will require different configuration parameters. For example, if you select Blob storage you would be prompted for the storage account name and the blob storage path.

✓ There are a variety of bindings to choose from and each function will have different bindings that are available. Use the reference link to learn more. Do you have an idea of a function that might need bindings?

Function Scaling

Azure Functions can scale to meet your needs. Azure Functions uses a component called the *scale controller* to monitor the rate of events and determine whether to scale out (add host instances) or scale in (remove host instances).

The scale controller uses heuristics for each trigger type. For example, when you're using an Azure Queue storage trigger, it scales based on the queue length and the age of the oldest queue message.



The unit of scale is the function app. When the function app is scaled out, additional resources are allocated to run multiple instances of the Azure Functions host. Conversely, as compute demand is reduced, the scale controller removes function host instances. The number of instances is eventually scaled down to zero when no functions are running within a function app.

✓ A single function app will only scale to a maximum of 200 instances. A single instance may process more than one message or request at a time though, so there isn't a set limit on number of concurrent executions. New instances will only be allocated at most once every 10 seconds.

For more information, you can see:

Runtime scaling - **https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale#runtime-scaling**[28]

Scalability best practices - **https://docs.microsoft.com/en-us/azure/azure-functions/functions-best-practices#scalability-best-practices**[29]

Optional Practice- Blob Storage Function

Take a few minutes to **Create a function triggered by Azure Blob storage**[30]. In this exercise you will earn how to create a function triggered when files are uploaded to or updated in Azure Blob storage. In this practice you will learn how to:

- Create an Azure Function app.
- Create a Blob storage triggered function.
- Create the container.

28 https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale
29 https://docs.microsoft.com/en-us/azure/azure-functions/functions-best-practices
30 https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-storage-blob-triggered-function

- Test the function.
- Clean up resources.

For more information, you can see:

Azure Functions Blob storage bindings - **https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-storage-blob**

Optional Practice- Timer Function

Take a few minutes to **Create a function in Azure that is triggered by a timer**[31]. In this exercise you will earn how to create a function that runs based a schedule that you define. In this practice you will learn how to:

- Create an Azure Function app.
- Create a timer triggered function.
- Update the timer schedule.

✓ The Azure documentation has other function examples. As you have time, try the queue storage example at the reference link.

For more information, you can see:

Create a function triggered by Azure Queue storage - **https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-storage-queue-triggered-function**

31 https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-scheduled-function

Managing Event Grid

Overview of Event Grid

Simplify event-based apps with Event Grid, a single service for managing routing of all events from any source to any destination. Designed for high availability, consistent performance, and dynamic scale, Event Grid lets a developer focus on the app logic rather than infrastructure. Here are a few advantages:

Simplify event delivery

Eliminate polling—and the associated cost and latency. With Event Grid, event publishers are decoupled from event subscribers using a pub/sub model and simple HTTP-based event delivery, allowing developers to build scalable serverless applications, microservices, and distributed systems.

Build reliable cloud applications

Gain massive scale, dynamically, while getting near-real-time notifications for changes that the developer or organization is interested in. Build better, more reliable applications through reactive programming, capitalizing on guaranteed event delivery and the high availability of the cloud.

Focus on product innovation

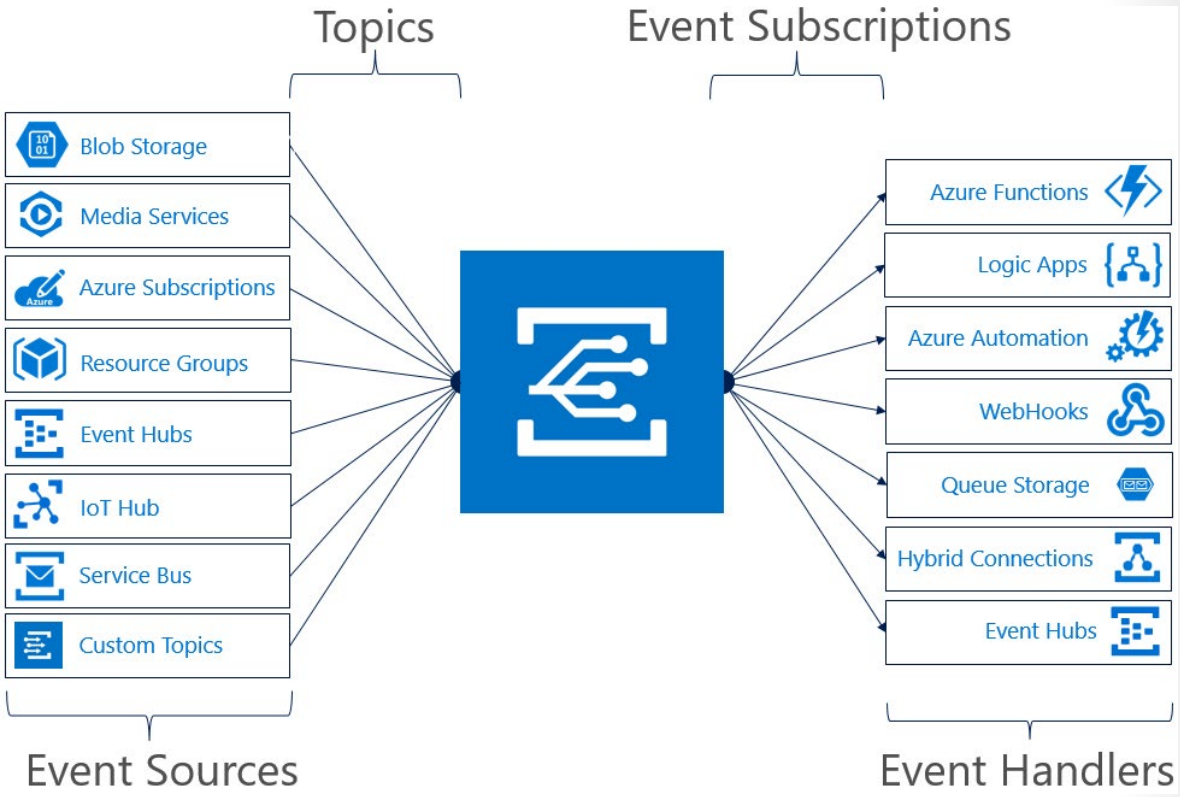
Develop richer application scenarios by connecting multiple possible sources and destinations of events. Your business logic can be triggered by virtually all Azure services, as well as custom sources. Fully managed event delivery, intelligent filtering, and the ability to send events to multiple recipients at once allowing the developer to focus on solving business problems rather than infrastructure.

For more information, you can see:

Event Grid - **https://azure.microsoft.com/en-us/services/event-grid/**

Event Grid Concepts

This diagram shows the four basic concepts in Event Grid: Event Source, Topics, Event Subscriptions, and Event Handlers.



Event Source. An event source is where the event happens. Several Azure services are automatically configured to send events. For example, Azure Storage is the event source for blob created events. Developers can also create custom applications that send events. Custom applications do not need to be hosted in Azure to use Event Grid for event distribution.

Topic. The event grid topic provides an endpoint where the source sends events. A topic is used for a collection of related events.

Event Subscription. A subscription tells Event Grid which events on a topic you are interested in receiving. When creating the subscription, you provide an endpoint for handling the event. You can filter the events that are sent to the endpoint.

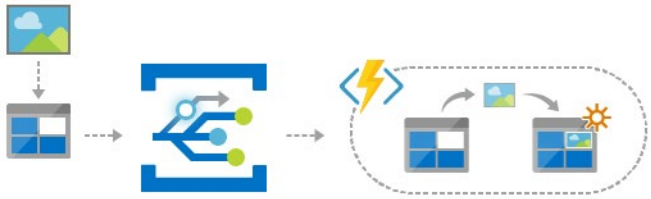
Event Handler. An event handler is the place where the event is sent. The handler takes some further action to process the event. Event Grid supports multiple handler types. For example, Azure Automation, Queue Storage, and Logic Apps.

For more information, you can see:

Event Grid Concepts - **https://docs.microsoft.com/en-us/azure/event-grid/concepts**

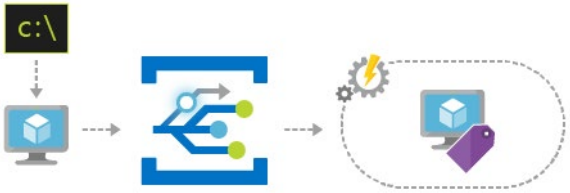
Event Grid Examples

Serverless application architectures



Use Event Grid to instantly trigger a serverless function to run image analysis each time a new photo is added to a blob storage container.

Ops automation



Notify Azure Automation when a virtual machine is created, or a SQL Database is spun up. These events can be used to automatically check that service configurations are compliant, put metadata into operations tools, tag virtual machines, or file work items.

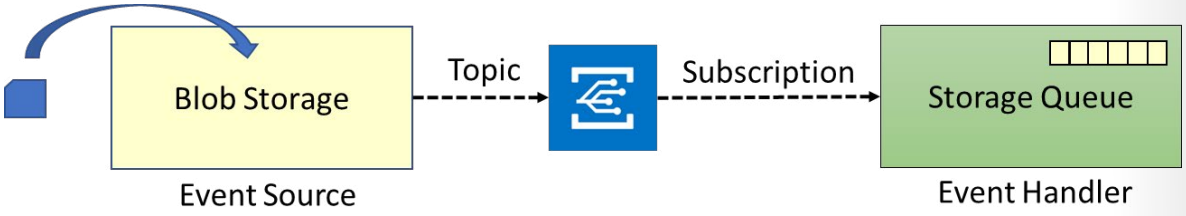
Application integration

Use Event Grid with serverless computing to process data anywhere, without writing code.

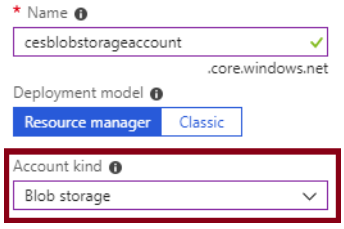
✓ Can you think of any other applications where you can use Event Grid?

Implementing Event Grid (Part 1)

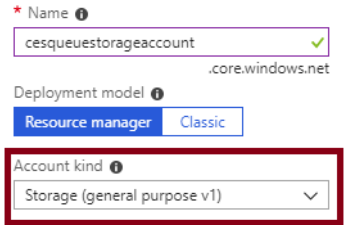
To demonstrate Event Grid let's pick an Event Source (Azure Blob Storage) and an Event Handler (Azure Queue Storage). Let's step through writing a message to a queue when a blob is uploaded.



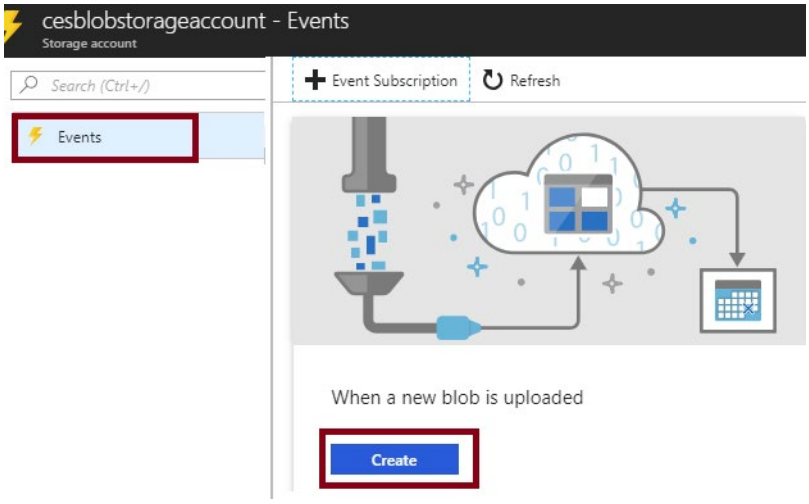
1. Create an Azure Storage account. Ensure the Account Kind is Blob Storage. This is the event source.



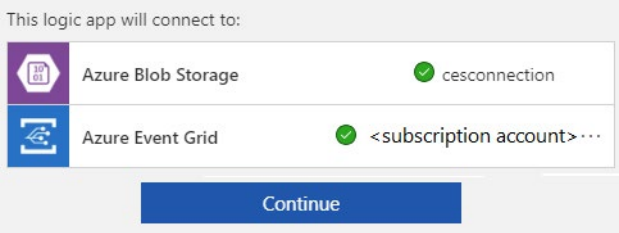
2. Create an Azure Storage Account. Ensure the Account Kind is Standard (general purpose v1). This will be the event handler.



3. Create a queue in the Standard storage account. This will receive the message traffic when a blob is uploaded.
4. Using the Blob storage account and the Events blade, create the When a new blob is updated template. Notice the other templates that are available.



5. When prompted give your Blob storage account a connection name. Also, connect to the Event Grid by providing your subscription information. This will be used to connect to the queue storage.

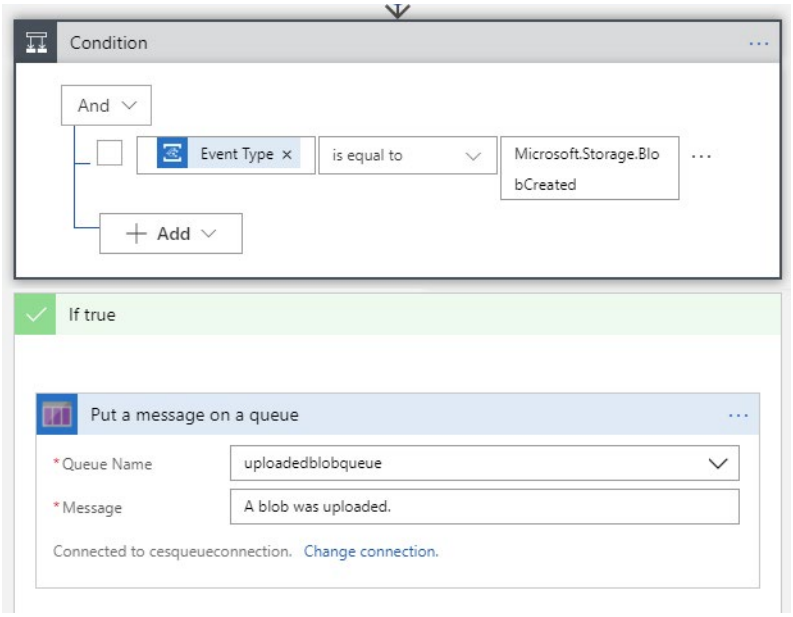


✓ This topic continues on the next page.

Implementing Event Grid (Part 2)

✓ This topic is a continuation of the previous.

6. Edit the Logic App so that it has one condition and one action. The condition is true whenever a blob is created. The action is to put a message in the queue. The original template has several actions that you need to remove. Delete them from the bottom up to avoid dependency problems. Your finished workflow should look like this. For this simple example, the if false action is not specified.



7. Save your changes and run your logic app.
8. Return to the Blob storage account, create a container, and upload a blob.
9. View your Queue storage account and ensure messages have been added to the queue.

ID	MESSAGE TEXT	INSERTION TIME	EXPIRATION TIME	DEQUEUE COUNT
5d9fe07a-efaa-47f1-a587...	A blob was uploaded.	Thu, 05 Jul 2018 23:55:36 GMT	Thu, 12 Jul 2018 23:55:36 GMT	0
8baedddd-44b2-4dc2-a1...	A blob was uploaded.	Thu, 05 Jul 2018 23:55:54 GMT	Thu, 12 Jul 2018 23:55:54 GMT	0

10. To avoid billing charges, remove your storage accounts and logic app.

✓ Can you see the benefits of Event Grid in providing you a way to connect two services or applications without any coding?

Optional Practice- Event Grid

The documentation has many Event Grid Quickstarts and tutorials for the portal, PowerShell, and the CLI. Here are just a few.

- **Create and route Blob storage events with the Azure portal and Event Grid**[32].
- **Route Blob storage events to a custom web endpoint with PowerShell**[33].
- **Monitor virtual machine changes with Azure Event Grid and Logic Apps**[34].

✓ If you don't see something you would like to work on search the documentation for other examples. Perhaps you would like to try one of the Resource Manager templates instead? The reference link will take you there.

For more information, you can see:

Azure Resource Manager templates for Event Grid - **https://docs.microsoft.com/en-us/azure/event-grid/template-samples**

32 https://docs.microsoft.com/en-us/azure/event-grid/blob-event-quickstart-portal
33 https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-event-quickstart-powershell?toc=%2fazure%2fevent-grid%2ftoc.json
34 https://docs.microsoft.com/en-us/azure/event-grid/monitor-virtual-machine-changes-event-grid-logic-app

Managing Service Bus

Queues

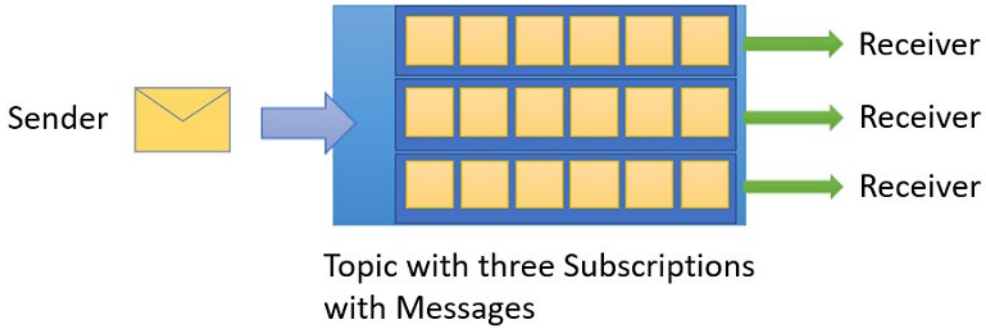
Azure Service Bus is a multi-tenant cloud messaging service that sends information between applications and services. The information is stored in a message queue. The asynchronous operations give you flexible, brokered messaging, along with structured processing, and publish/subscribe capabilities.

Queues offer *First In, First Out* (FIFO) message delivery to one or more competing consumers. That is, receivers typically receive and process messages in the order in which they were added to the queue, and only one message consumer receives and processes each message.

A key benefit of using queues is to achieve "temporal decoupling" of application components. In other words, the producers (senders) and consumers (receivers) do not have to be sending and receiving messages at the same time, because messages are stored durably in the queue. Furthermore, the producer does not have to wait for a reply from the consumer to continue to process and send messages. And, the consumer doesn't have to be online.

Topics and Subscriptions

In contrast to queues, in which each message is processed by a single consumer, topics and subscriptions provide a one-to-many form of communication, in a publish/subscribe pattern. Useful for scaling to large numbers of recipients, each published message is made available to each subscription registered with the topic.



Messages are sent to a topic and delivered to one or more associated subscriptions, depending on filter rules that can be set on a per-subscription basis. The subscriptions can use additional filters to restrict the messages that they want to receive. For example, if you were processing delivery orders, rules could be used to identify the nearest subscriber to make the delivery.

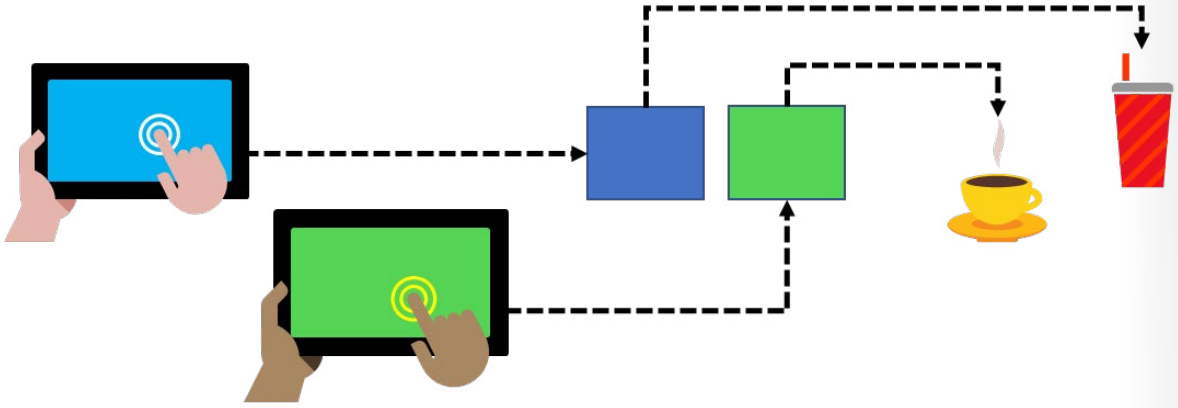
Messages are sent to a topic in the same way they are sent to a queue, but messages are not received from the topic directly. Instead, they are received from subscriptions. A topic subscription resembles a

virtual queue that receives copies of the messages that are sent to the topic. Messages are received from a subscription identically to the way they are received from a queue.

✓ You can use rules and filters to define conditions that trigger optional **actions**[35], filter specified messages, and set or modify message properties. Do you see the difference between queues and topics?

Service Bus Features

Let's look at the benefits of Service Bus by examining a scenario. In this scenario, you have a web application that takes online orders and several workers ready to fulfill those orders.



Here are several benefits of using a message queueing system in this situation.

Load Leveling. During the day certain times will generate more orders than at other times. By using a queue, the orders can be stored awaiting fulfillment. The queue automatically increases and decreases in length. This ultimately saves you money because you don't have to pay for a system that is underutilized part of the time. Also, customers do not have to wait to place their order.

Loose Coupling. Your message queues are durable and will reach the worker even if they are busy with another order. This provides a lot of resilience for your ordering system. Consider a scenario where someone else is handling the orders and their system is down. When the system comes back up the orders will still be there.

Load Balancing. When you have more than one fulfillment worker they may work at different speeds. You don't have to programmatically design some way to balance the load, that will naturally occur. You can bring on more workers as the queue increases.

✓ Service bus has many advanced queueing features such as auto-forwarding, batching, scheduled delivery, and message deferral. Read more at the reference link. Can you see how this scenario could be expanded to the topic and subscriber situation?

For more information, you can see:

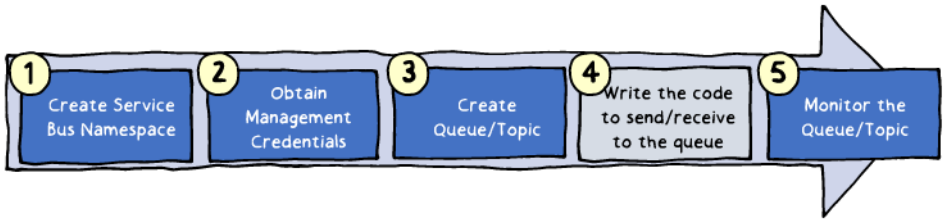
What is Azure Service Bus - **https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview**

Implementing Service Bus

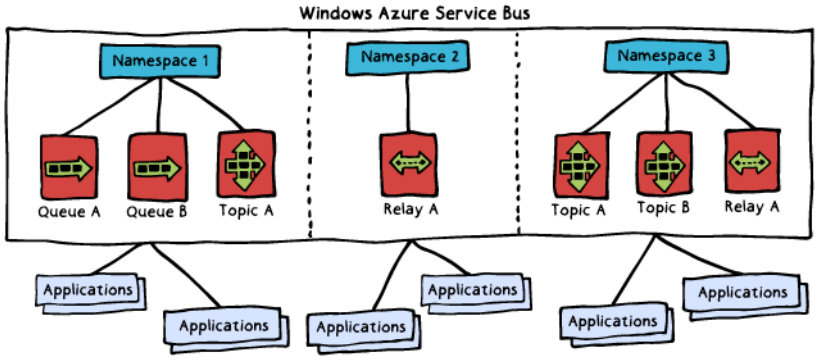
As a Solutions Architect you will not be responsible for understanding the code to produce or retrieve the messages. You will be responsible for interpreting the Service Bus namespace, obtaining management

35 https://docs.microsoft.com/en-us/azure/service-bus-messaging/topic-filters

credentials, creating the queue/topic, and then managing and monitoring the queues/topics. These steps can be done programmatically but let's look at how to do it in the portal.



First, Service Bus services are typically partitioned into namespaces. Each namespace provides both a service and security boundary. A namespace is a scoping container for all messaging components. Multiple entities can reside within a single namespace, and namespaces often serve as application container.



In the diagram, a Service Bus relay is shown. The Azure Relay service facilitates your hybrid applications by helping you more securely expose services that reside within a corporate enterprise network to the public cloud. You can expose the services without opening a firewall connection, and without requiring intrusive changes to a corporate network infrastructure.

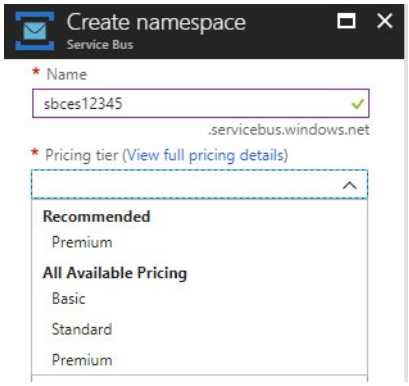
✓ Can you see why you would use multiple namespaces. Will you need to use more than one name-space?

Creating the Namespace

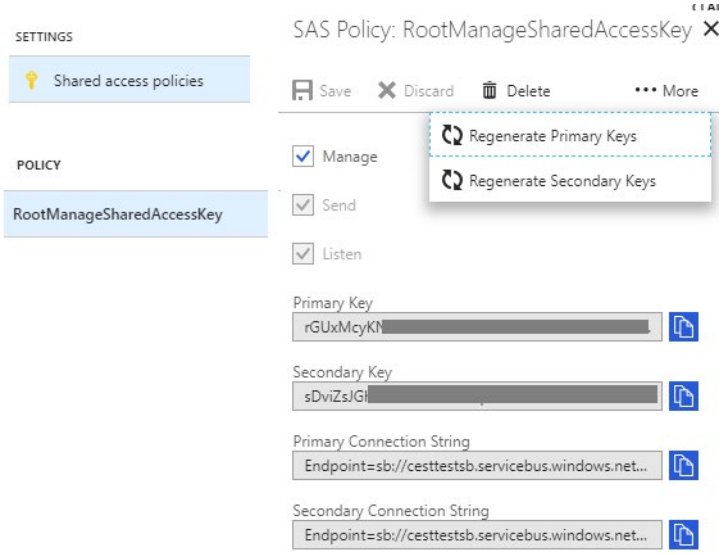
Creating the namespace is easy. The name provides a unique identifier for the object. For example, sbces12345.servicebus.windows.net. Applications can provide this name to Service Bus, then use any entity in the namespace.

Azure Service Bus is offered in Basic, Standard, and **Premium**[36] pricing tiers. You can choose a service tier for each Service Bus service namespace that you create, and this tier selection applies across all entities created within that namespace. Queues are available in all pricing tiers. Topics require a Standard or Premium pricing tier.

36 https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-premium-messaging



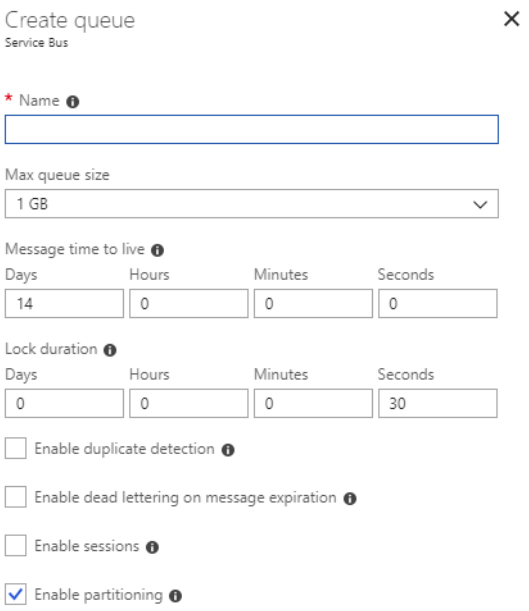
Creating a new namespace automatically generates an initial Shared Access Signature (SAS) rule with an associated pair of primary and secondary keys that each grant full control over all aspects of the namespace. Your developer will need the namespace and the connection string.



✓ Be sure to read about the different pricing tiers. Which one do you think you will need? Have you thought about how often you will rotate the SAS keys?

Create a Queue

When you create a queue, you must provide a Name and Max queue size. Additionally, there are some parameters that will affect how the queue performs.



Message time to live. Determines how long a message will stay in the queue before it expires and is removed or dead lettered. This default will be used for all messages in the queue which do not specify a time to live for themselves.

Lock duration. Sets the amount of time a message is locked from other receivers. After its lock expires, a message is pulled by one receiver before being available to be pulled by other receivers. The default is 30 seconds, with a maximum of 5 minutes.

Enable duplicate detection. Configures your queue to keep a history of all messages sent to the queue during a configurable amount of time. During that interval, your queue will not accept any duplicate messages.

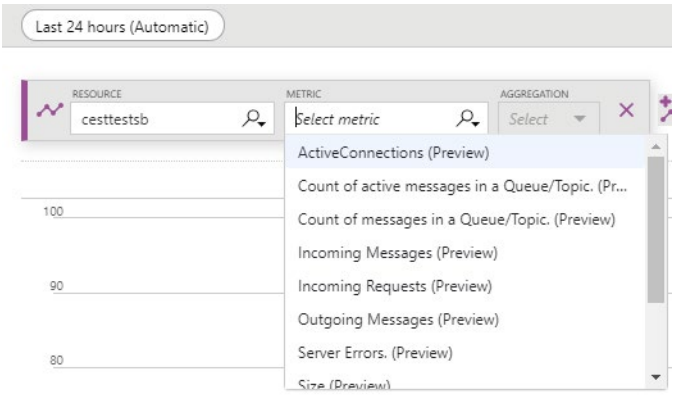
Enable dead lettering. Enables holding messages that cannot be successfully delivered to any receiver. The messages are held in a separate queue after they expire. You can inspect this queue.

Enable sessions. Allows ordered handling of unbound sequences of related messages. This guarantees first-in-first-out delivery of messages.

Enable partitioning. Partitions a queue across multiple message brokers and message stores. Partitioning means that the overall throughput of a partitioned entity is no longer limited by the performance of a single message broker or messaging store. In addition, a temporary outage of a messaging store does not render a partitioned queue or topic unavailable.

Monitoring Service Bus

Service Bus metrics gives you the state of resources in your subscription. With a rich set of metrics data, you can assess the overall health of your Service Bus resources, not only at the namespace level, but also at the queue/topic/message level. These statistics can be important as they help you to monitor the state of Service Bus and help you troubleshoot root-cause issues.



Diagnostic logs

You can configure diagnostic logs for richer information about everything that happens within a job. Diagnostic logs cover activities from the time the job is created until the job is deleted, including updates and activities that occur while the job is running.

Comparing Service Bus and Storage Queues

Azure supports two types of queue mechanisms: Storage queues and Service Bus queues. Now that you have learned about Service Bus queues you may be wondering how they are different from Storage queues. This table provides a summary.

Comparison Criteria	Storage Queues	Service Bus Queues
Ordering guarantee	No	Yes – FIFO
Delivery guarantee	At-Least-Once	At-Least-Once At-Most-Once
Lease/lock level	Message level	Queue level
Batch receive	Yes	Yes
Batch send	No	Yes
Scheduled delivery	Yes	Yes
Automatic dead lettering	No	Yes
Message auto-forwarding	No	Yes
Message groups	No	Yes
Duplicate detection	No	Yes

This is a very short table. The reference link provides other information such as queue sizes, message sizes, and authentication options. Notice if your queue size will exceed 80 GB, then you must use storage queues.

✓ By gaining a deeper understanding of the two technologies, you will be able to make a more informed decision on which queue technology to use, and when. Your decision will depend heavily on the individual needs of your application and its architecture. Which option do you think you will use?

For more information, you can see:

Storage queues and Service Bus queues - compared and contrasted - **https://azure.microsoft.com/en-us/documentation/articles/service-bus-azure-and-service-bus-queues-compared-contrasted/**

Optional Practice- Service Bus Message Queues

Take a few minutes to try the **Quickstart: Send and receive messages using the Azure portal and .NET**[37]. In this practice you will earn how:

- Create a Service Bus namespace.
- Obtain management credentials.
- Create a queue.
- Send and receive messages.

✓ Rather than complete the coding part of the practice try to see if you can identify where your connection string and queue information will be used. Also, read the reference link scenario to see how topics can be used in multiple subscription and multiple receiver scenarios.

For more information, you can see:

Tutorial: Update inventory using Azure portal and topics/subscriptions - **https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-tutorial-topics-subscriptions-portal**

Optional Practice- Service Bus Templates

There are several Azure Resource Manager templates you can use to create namespaces, queues, and topics.

- **Create a namespace**[38]
- **Create a Service Bus namespace with queue**[39]
- **Create a Service Bus namespace with topic and subscription**[40]

✓ To check for the latest templates, visit the **Azure Quickstart Templates**[41] gallery and search for Service Bus.

For more information, you can see:

Azure Quickstart templates - **https://github.com/Azure/azure-quickstart-templates**

37 https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-quickstart-portal
38 https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-resource-manager-namespace
39 https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-resource-manager-namespace-queue
40 https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-resource-manager-namespace-topic
41 https://azure.microsoft.com/documentation/templates/?term=service+bus

Managing Logic App

Logic Apps

Logic Apps provide a way to simplify and implement scalable integrations and workflows in the cloud. It provides a visual designer to model and automate your process as a series of steps known as a workflow. There are many connectors across the cloud and on-premises to quickly integrate across services and protocols. A logic app begins with a trigger, like 'When an account is added to Dynamics CRM', and after firing, can begin many combinations actions, conversions, and conditional logic.

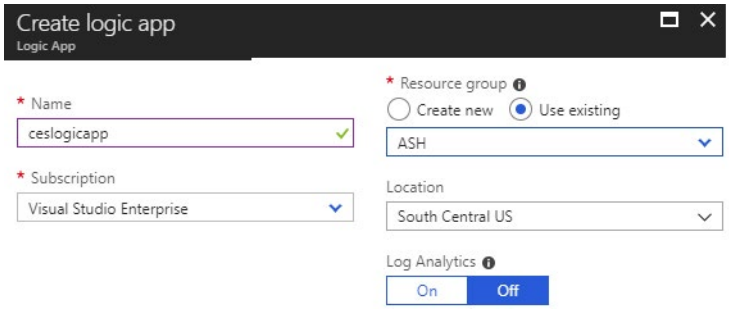
The advantages of using Logic Apps include the following:

- Getting started quickly from templates.
- Saving time by designing complex processes using easy to understand design tools.
- Implementing patterns and workflows seamlessly, that would otherwise be difficult to implement in code.
- Customizing your logic app with your own custom APIs, code, and actions.
- Connecting and synchronizing disparate systems across on-premises and the cloud.

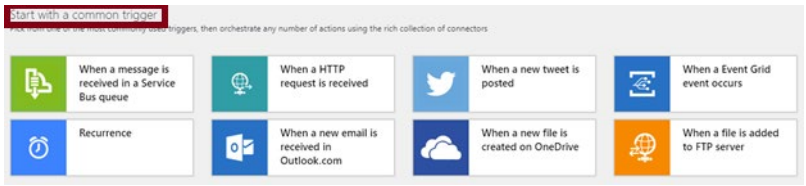
Logic Apps is a fully managed iPaaS (integration Platform as a Service) freeing users from worry about building hosting, scalability, availability, and management. Logic Apps will scale up automatically to meet demand.

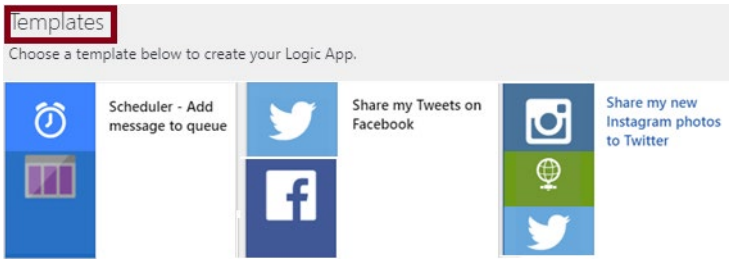
Implementing Logic Apps

To begin using Logic Apps simply create a logic app with Name, Subscription, Resource Group, Location, and Log Analytics (optional).



After Azure deploys your app, the Logic Apps Designer opens and shows a page with commonly used triggers and templates. Logic Apps can be designed end-to-end in the browser. Start with a trigger, including things like a simple schedule, or whenever a tweet appears about your company. Then orchestrate any number of actions using the rich gallery of connectors.





✓ Take a minute to create a Logic App in the portal and browse the triggers and templates that are available. Does anything seem of interest to you?

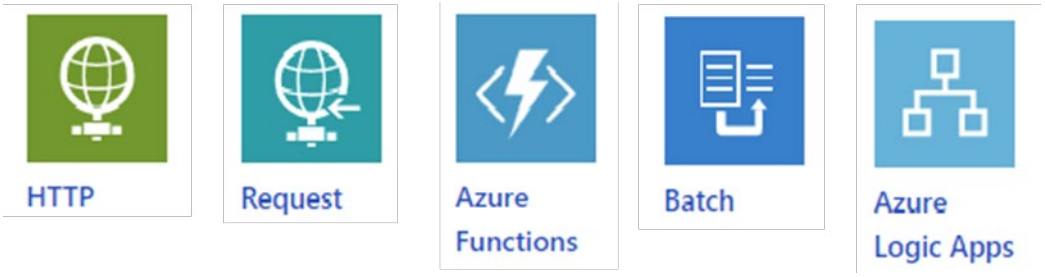
For more information, you can see:

Logic Apps documentation - **https://docs.microsoft.com/en-us/azure/logic-apps/**

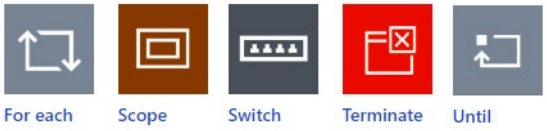
Built-In Triggers and Actions

Logic Apps provides built-in triggers and actions, so you can create schedule-based workflows, help your logic apps communicate with other apps and services, control the workflow through your logic apps, and manage or manipulate data.

In the previous example we used the Schedule built-in. With the Recurrence trigger, you can set a date and time for starting the recurrence and a recurrence schedule for performing tasks. Other built-in triggers include: HTTP, Request, Azure Functions, Batch, and other Azure Logic apps.



There are also built-in actions for structuring and controlling the actions in your logic app's workflow. For example, you could insert a Condition to evaluate a condition and run different actions based on whether the condition is true or false. Other built-in actions are: For each, Scope, Switch, Terminate, and Until.



The Logic App designer will automatically apply the built-ins when creating your workflow, but you can customize the workflow at any time.

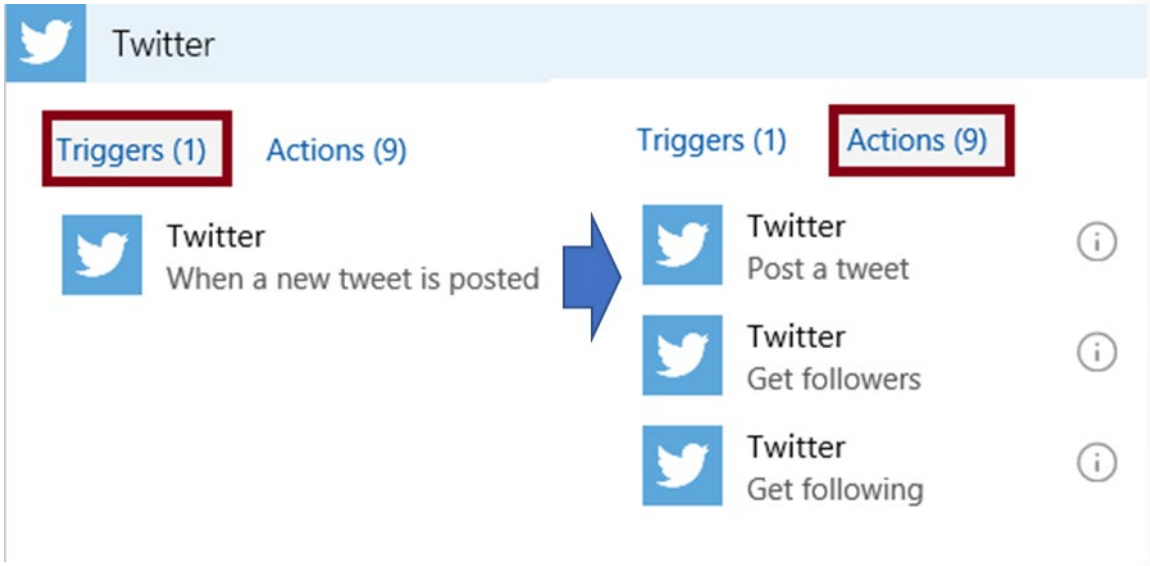
Managed Connectors

Managed connectors play an integral part when you create automated workflows with Azure Logic Apps. By using connectors in your logic apps, you expand the capabilities for your on-premises and cloud apps to perform tasks with the data that you create and already have.

Logic Apps offers ~200+ connectors, including:

- **Managed API connectors**[42]. This includes Azure Blob Storage, Office 365, Dynamics, Power BI, OneDrive, Salesforce, and SharePoint Online.
- **On-premises connectors**[43]. This includes SQL Server, SharePoint Server, Oracle DB, Twitter, Salesforce, Facebook, and file shares.
- **Integration account connectors**[44]. Available when you create and pay for an integration account, these connectors transform and validate XML, encode, and decode flat files, and process business-to-business (B2B) messages with AS2, EDIFACT, and X12 protocols.
- **Enterprise connectors**[45]. Provide access to enterprise systems such as SAP and IBM MQ for an additional cost.

Whenever you select to include a managed connector, Logic Apps has already configured triggers and actions for that product. For example, with Twitter whenever a new tweet is posted you can get those who are following the tweet.

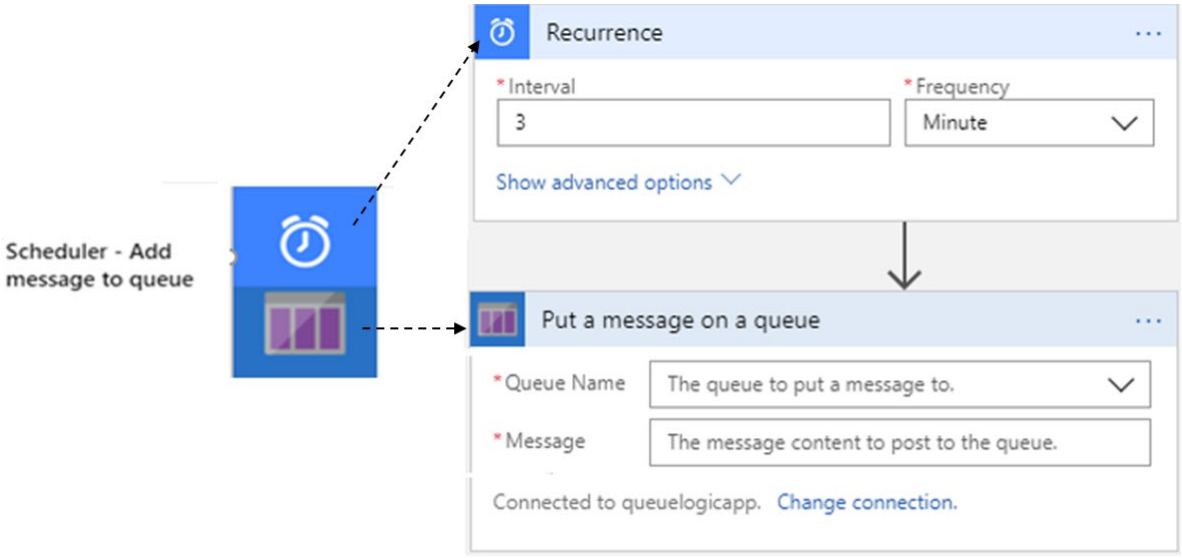


✓ Are you planning to use any of these connectors?

Logic App Example

One of the easiest Logic App templates to understand is the Scheduler – Add message to queue. Let's take a closer look at this template. The template has two parts: Recurrence and Put a message on a queue. Recurrence is where you configure the schedule for putting messages on the queue. Putting a message on the queue is where you select the Azure queue you want to use. This template also has error handling (not shown) where you can configure a second queue for messages related to that.

42 https://docs.microsoft.com/en-us/azure/connectors/apis-list
43 https://docs.microsoft.com/en-us/azure/connectors/apis-list
44 https://docs.microsoft.com/en-us/azure/connectors/apis-list
45 https://docs.microsoft.com/en-us/azure/connectors/apis-list

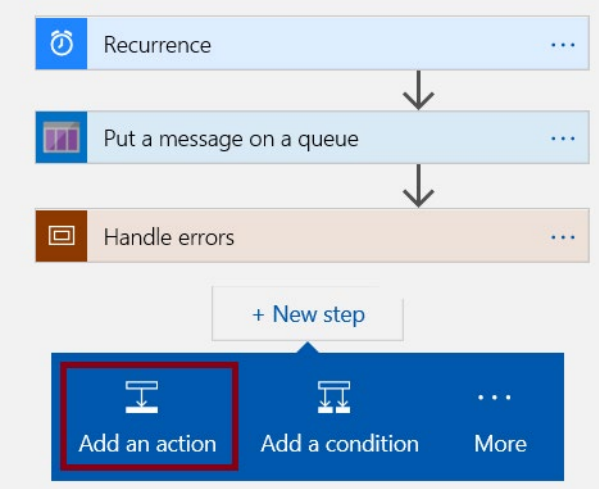


The Logic App designer provides these steps in an easy to use format. The designer steps you through the process of building a workflow. No coding is required. When everything has been validated you can save and run the workflow.

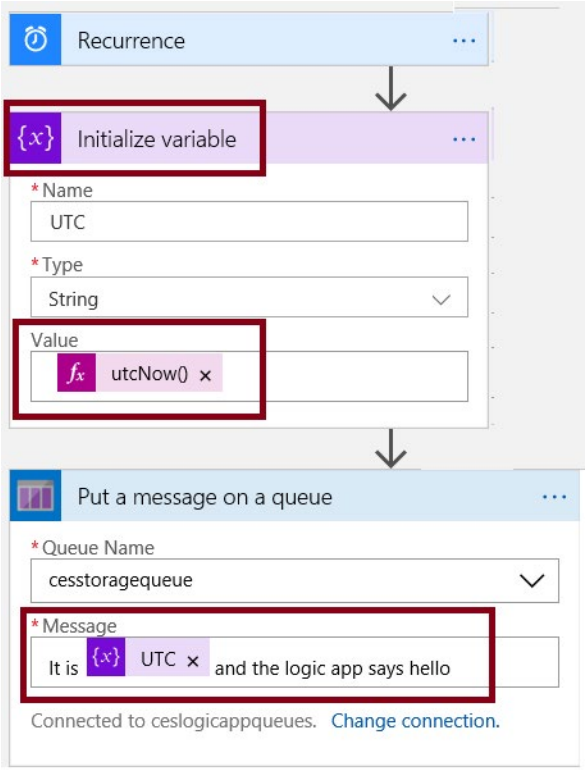
✓ Take a few minutes to create an Azure queue and then use this template to populate the queue. Check to ensure queue messages are arriving on the schedule you configure.

Logic App Example (cont.)

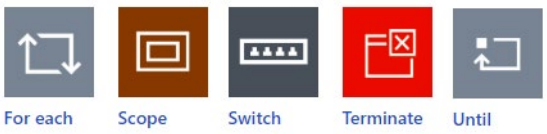
Let's continue with our previous example and customize the workflow. Here is what you should have so far. Click New Step and then Add an action. Scroll through all the different connectors and actions that are available.



In the Actions area select Variable (Initialize Variable). Give your variable a name, String type, and then search the Expressions for UtcNow( ). That will set the value of the variable to the current timestamp. After creating Initialize Variable move it up in the workflow, between Recurrence and Put message on queue. Lastly, add the variable to your message.



✓ Take a few minutes to try this and experiment with actions and using the designer. Be sure to check the Azure queue and make sure the message is working.



Optional Practice- Logic App Workflow (Advanced)

If you are up for a challenge try the **Check traffic with a scheduler-based logic app**[46]. In this practice you will learn how to:

- Create a logic app.
- Add a scheduler trigger.
- Get the travel time for a route.
- Create a variable to store the travel time.
- Add a condition to compare the travel time with the limit.
- Send email when the travel time is exceeded.
- Run and monitor your logic app.

✓ If this practice does not appeal to you, there are other choices in the reference links.

For more information, you can see:

Manage mailing list requests with a logic app - **https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-process-mailing-list-subscriptions-workflow**

Process emails and attachments with a logic app - **https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-process-email-attachments-workflow**

46 https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-build-schedule-recurring-logic-app-workflow

Review Questions

Module 2 Review Questions

Web Apps Features

Your organization plans to host a corporate website in Azure. Traffic to the website is expected to vary at different times of the year.

The website must scale based on demand.

What benefits can you realize by hosting the web as a Web App in Azure?

Suggested Answer
A web app is the compute resources that Azure provides for hosting a website or web application.
The compute resources may be on shared or dedicated virtual machines (VMs), depending on the pricing tier that you choose. Your application code runs in a managed VM that is isolated from other customers.

Web Apps Features (Deployment)

Your organization plans to host a corporate website in Azure. The website includes an e-commerce solution which must be available to customers at all time.

Developers continuously create new solutions to improve customer experiences.

You need to ensure that you can deploy code without affecting user access or any orders in progress.

What should you use? What benefits you will realize?

Suggested Answer
When you deploy your web app, mobile back end, and API app to App Service, you can deploy to a separate deployment slot instead of the default production slot when running in the Standard or Premium App Service plan mode.
Deployment slots are live apps with their own hostnames. App content and configuration elements can be swapped between two deployment slots.

Event Grid

Your organization develops an Azure-based photo management and editing app. You are designing a solution that implements Event Grid to run image analysis code each time a new photo is uploaded.

What are the benefits and limitations of Event Grid?

Suggested Answer
Serverless computing is driven by the reaction to events and triggers happening in near-real-time—in the cloud. As a fully managed service, server management and capacity planning are invisible to the developer and billing is based just on resources consumed or the actual time your code is running.
Serverless computing has many advantages. Here are a few:
• Benefit from a fully managed service. Organizations can relieve their teams from the burden of managing servers. By using fully managed services, developers focus on application business logic and avoid administrative tasks. With serverless architecture developers simply deploy their code, and it runs with high availability.

• Scale flexibly. Serverless compute scales from nothing to handling tens of thousands of concurrent functions almost instantly (within seconds), to match any workload, and without requiring scale configuration.

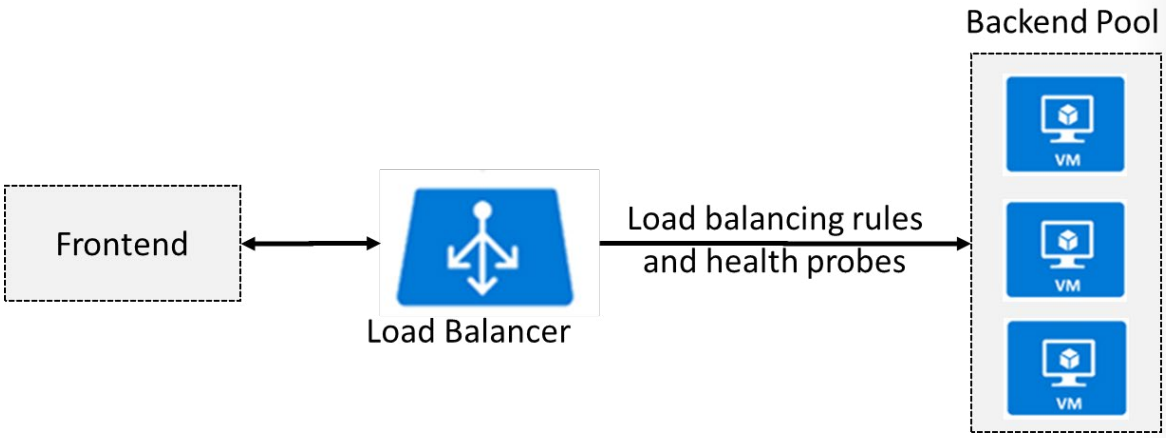
• Only pay for the resources used. With serverless architecture, your organization only pays for the time the application code is running. Serverless computing is event-driven, and resources are allocated as soon as they are triggered by an event. You are only charged for the time and resources it takes to execute the application code—through sub-second billing.

Module 3 Implementing Advanced Virtual Networking

Azure Load Balancer

Azure Load Balancer

The Azure Load Balancer delivers high availability and network performance to your applications. It is an OSI Layer 4 (TCP and UDP) load balancer that distributes inbound traffic to backend resources using load balancing rules and health probes. Load balancing rules determine how traffic is distributed to the backend. Health probes ensure the resources in the backend are healthy.



The Load Balancer can be used for inbound as well as outbound scenarios and scales up to millions of flows for all TCP and UDP applications.

✓ Keep this diagram in mind since it covers the four components that must be configured for your load balancer: Frontend IP configuration, Backend pools, Health probes, and Load balancing rules.

For more information, you can see:

Load Balancer - **https://azure.microsoft.com/en-us/services/load-balancer/**

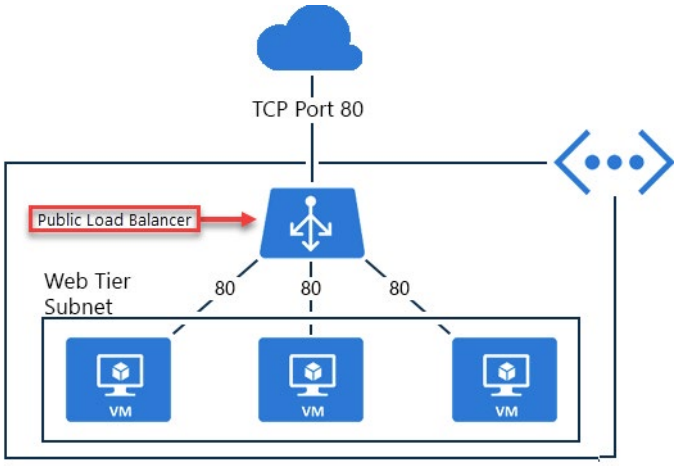
Load Balancer documentation - **https://docs.microsoft.com/en-us/azure/load-balancer/**

Public load balancer

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

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

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



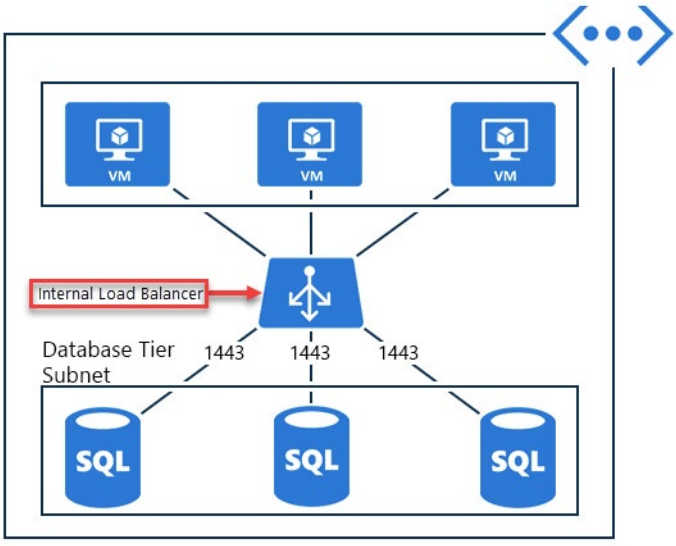
For more information, you can see:

Public load balancer - **https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview#a-name–publicloadbalancerapublic-load-balancer**[1]

Internal load balancer

An internal load balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure. Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint. Internal line-of-business applications run in Azure and are accessed from within Azure or from on-premises resources. For example, an internal load balancer could receive database requests that need to be distributed to backend SQL servers.

1 https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview



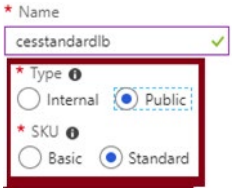
An internal load balancer enables the following types of load balancing:

- **Within a virtual network**. Load balancing from VMs in the virtual network to a set of VMs that reside within the same virtual network.
- **For a cross-premises virtual network**. Load balancing from on-premises computers to a set of VMs that reside within the same virtual network.
- **For multi-tier applications**. Load balancing for internet-facing multi-tier applications where the backend tiers are not internet-facing. The backend tiers require traffic load-balancing from the internet-facing tier.
- **For line-of-business applications**. Load balancing for line-of-business applications that are hosted in Azure without additional load balancer hardware or software. This scenario includes on-premises servers that are in the set of computers whose traffic is load-balanced.

✓ Can you see how a public load balancer could be placed in front of the internal load balancer to create a multi-tier application.

Load Balancer SKUs

When you create an Azure Load Balancer you will select for the type (Internal or Public) of load balancer. You will also select the SKU. The load balancer supports both Basic and Standard SKUs, each differing in scenario scale, features, and pricing. The Standard Load Balancer is the newer Load Balancer product with an expanded and more granular feature set over Basic Load Balancer. It is a superset of Basic Load Balancer.



Here is some general information about the SKUs.

- SKUs are not mutable. You may not change the SKU of an existing resource.

- A standalone virtual machine resource, availability set resource, or virtual machine scale set resource can reference one SKU, never both.
- A Load Balancer rule cannot span two virtual networks. Frontends and their related backend instances must be in the same virtual network.
- There is no charge for the Basic load balancer. The Standard load balancer is charged based on number of rules and data processed. Read more at the reference link.
- Load Balancer frontends are not accessible across global virtual network peering.

✓ New designs and architectures should consider using Standard Load Balancer.

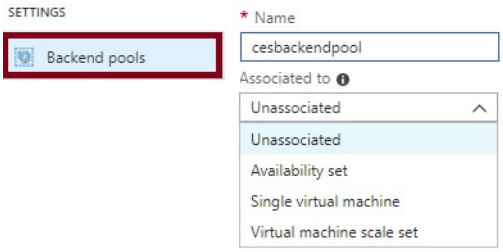
Backend Pool

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

How you configure the backend pool depends on whether you are using the Standard or Basic SKU.

-	Standard SKU	Basic SKU
Backend pool endpoints	Any VM in a single virtual network, including a blend of VMs, availability sets, and VM scale sets.	VMs in a single availability set or VM scale set.

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

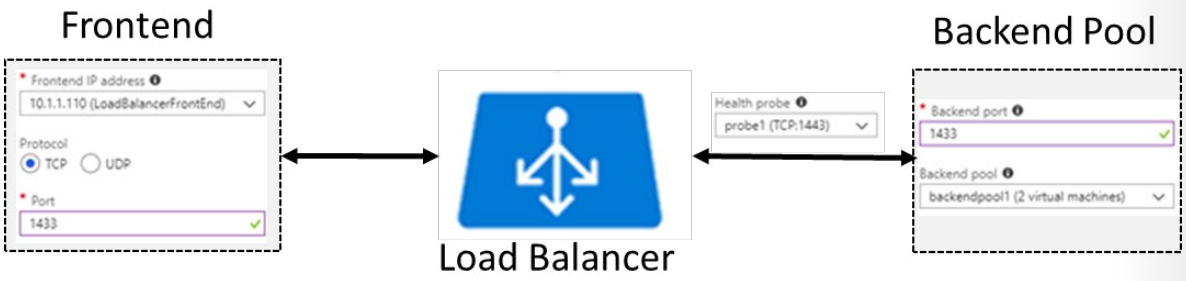


✓ In the Standard SKU you can have up to 1000 instances in the backend pool. In the Basic SKU you can have up to 100 instances.

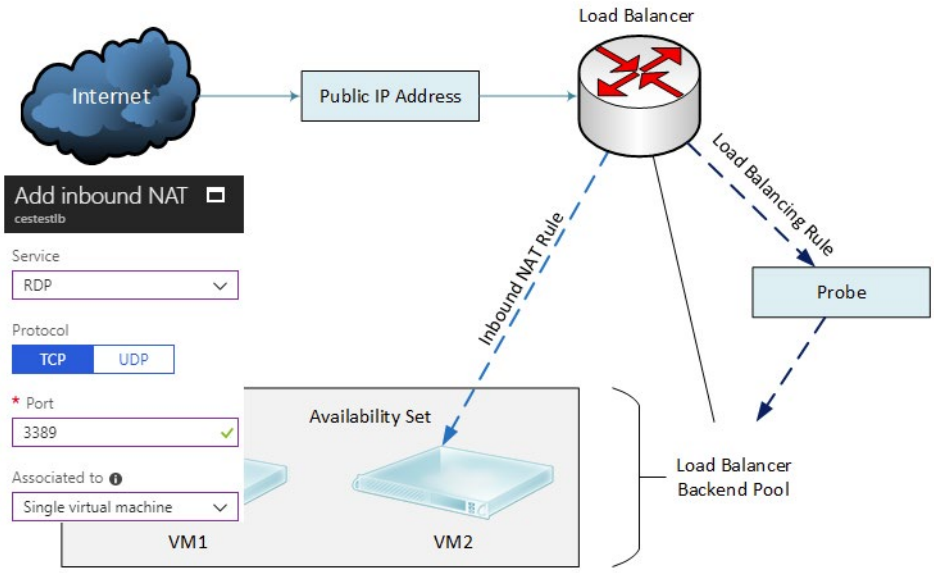
Load Balancer Rules

A load balancer rule is used to define how traffic is distributed to the backend pool. The rule maps a given frontend IP and port combination to a set of backend IP addresses and port combination. To create the rule the frontend, backend, and health probe information should already be configured. Here is a rule

that passes frontend TCP connections to a set of backend SQL (port 1433) servers. The rule uses a health probe that checks on TCP 1443.



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



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

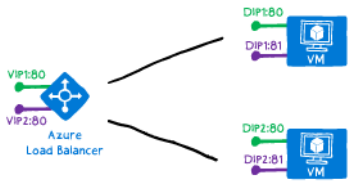
Multiple Frontends

Azure Load Balancer allows you to load balance services on multiple ports, multiple IP addresses, or both. You can use public and internal load balancer definitions to load balance flows across a set of VMs. Adding multiple frontends is incremental to a single frontend configuration.

When you define an Azure Load Balancer, frontend and backend pool configurations are connected with rules. There are two types of rules:

1. The default rule with no backend port reuse
2. The Floating IP rule where backend ports are reused

Rule type 1: No backend port reuse



In this scenario, the default rule, the frontends are configured with values for IP address, protocol, and port. The DIP is the destination of the inbound flow. In the backend pool, each VM exposes the desired service on a unique port on a DIP. This service is associated with the frontend through a rule definition.

Each rule must produce a flow with a unique combination of destination IP address and destination port. By changing the destination port of the flow, multiple rules can distribute flows to the same DIP on different ports.

✓ This topic continues on the next page.

Multiple Frontends (Rule 2)

Multiple Frontends

Rule type #2: backend port reuse by using Floating IP

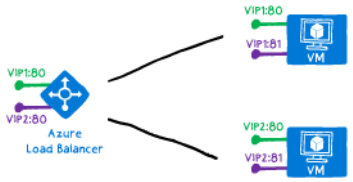
If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition. Floating IP refers to the portion of what is known as Direct Server Return (DSR). DSR consists of two parts:

- A flow topology
- IP address mapping scheme.

At a platform level, Azure Load Balancer always operates in a DSR flow topology regardless of whether Floating IP is enabled or not. This means that the outbound part of a flow is always correctly rewritten to flow directly back to the origin.

As opposed to the traditional load balancing mapping scheme used by the default rule, enabling Floating IP changes the IP address mapping scheme to allow for additional flexibility as explained below.

The following diagram illustrates this configuration:



For this scenario, every VM in the backend pool has three network interfaces:

- **DIP**. A Virtual NIC associated with the VM (IP configuration of Azure's NIC resource)
- **Frontend 1**. A loopback interface within guest OS that is configured with IP address of Frontend 1
- **Frontend 2**. A loopback interface within guest OS that is configured with IP address of Frontend 2

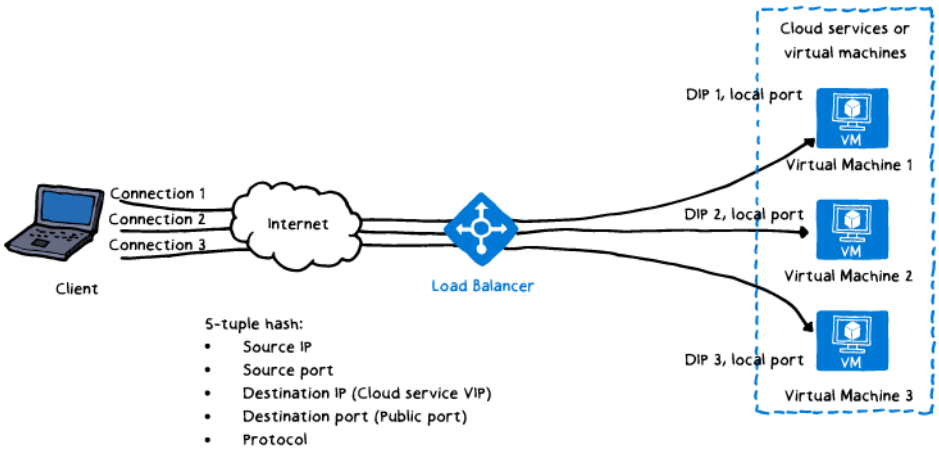
If we define rules mapping the frontend to the backend pool, the mapping in the load balancer would include frontend IP address, protocol, destination and ports. The destination of the inbound flow is the frontend IP address on the loopback interface in the VM. By changing the destination IP address, you can enable port reuse on the same VM.

✓ Make sure to take into account **limitations to using load balancers with multiple frontends**[2].

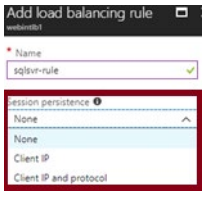
✓ Can you think of ways in which extending your load balancer to multiple ports and IP addresses would benefit your network configuration?

Session Persistence

By default, Azure Load Balancer distributes network traffic equally among multiple VM instances. The load balancer uses a 5-tuple (source IP, source port, destination IP, destination port, and protocol type) hash to map traffic to available servers. It provides stickiness only within a transport session.



Session persistence specifies how traffic from a client should be handled. The default behavior (None) is that successive requests from a client may be handled by any virtual machine. You can change this behavior.



- **Client IP** specifies that successive requests from the same client IP address will be handled by the same virtual machine.
- **Client IP and protocol** specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.

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

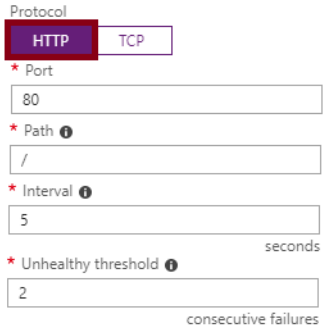
2 https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview

Health Probes

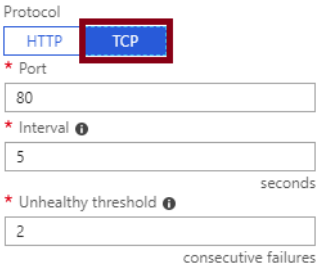
A health probe allows the load balancer to monitor the status of your app. The health probe dynamically adds or removes VMs from the load balancer rotation based on their response to health checks. When a probe fails to respond, the load balancer stops sending new connections to the unhealthy instances.

There are two main ways to configure health probes: **HTTP** and **TCP**.

HTTP custom probe. The load balancer regularly probes your endpoint (every 15 seconds, by default). The instance is healthy if it responds with an HTTP 200 within the timeout period (default of 31 seconds). Any status other than HTTP 200 causes this probe to fail. You can specify the port (Port), the URI for requesting the health status from the backend (URI), amount of time between probe attempts (Interval), and the number of failures that must occur for the instance to be considered unhealthy (Unhealthy threshold).



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



✓ There is also a guest agent probe. This probe uses the guest agent inside the VM. It is not recommended when HTTP or TCP custom probe configurations are possible.

Optional Practice- Standard Load Balancer

Take a few minutes to try the **QuickStart: Create a Standard Load Balancer to load balance VMs using the Azure portal**[3]. This QuickStart shows you how to load balance VMs using a Standard Load Balancer. Specifically, you will learn how to:

- Create a public load balancer.
- Create backend servers (virtual network, virtual machines, NSG rules, .
- Create load balancer resources (backend address pool, health probe, load balancer rules).
- Test the load balancer.

Also, be sure to try the **QuickStart: Create a Standard Load Balancer using Azure PowerShell**[4]. This QuickStart shows you how to configure the load balancer with PowerShell.

✓ If you prefer, use the reference link to try the CLI version of this QuickStart.

For more information, you can see:

QuickStart: Create a Standard Load Balancer to load balance VMS using Azure CLI 2.0 - **https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-cli**

Optional Practice- Load Balancer ARM Deployments

Take a few minutes to try at least one of the QuickStart templates to deploy a load balancer. For example, **2 VMs in a Load Balancer and load balancing rules**[5]. This template allows you to create 2 Virtual Machines under a Load balancer and configure a load balancing rule on Port 80. This template also deploys a Storage Account, Virtual Network, Public IP address, Availability Set and Network Interfaces. Another example is **2 VMs in VNET - Internal Load Balancer and LB rules**[6].

For more information, you can see:

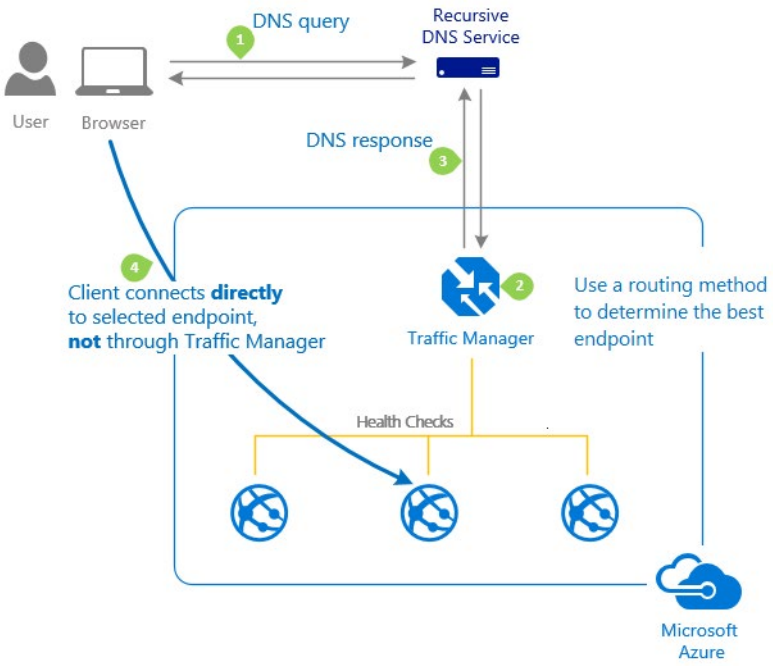
Azure QuickStart Templates - **https://azure.microsoft.com/en-us/resources/templates/**

3 https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal
4 https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-create-standard-load-balancer-powershell
5 https://azure.microsoft.com/en-us/resources/templates/201-2-vms-loadbalancer-lbrules/
6 https://azure.microsoft.com/en-us/resources/templates/201-2-vms-internal-load-balancer/

Application Load Balancing

Azure Traffic Manager

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



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

Traffic Manager Features

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

Here are some specific ways you can use Traffic Manager.

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

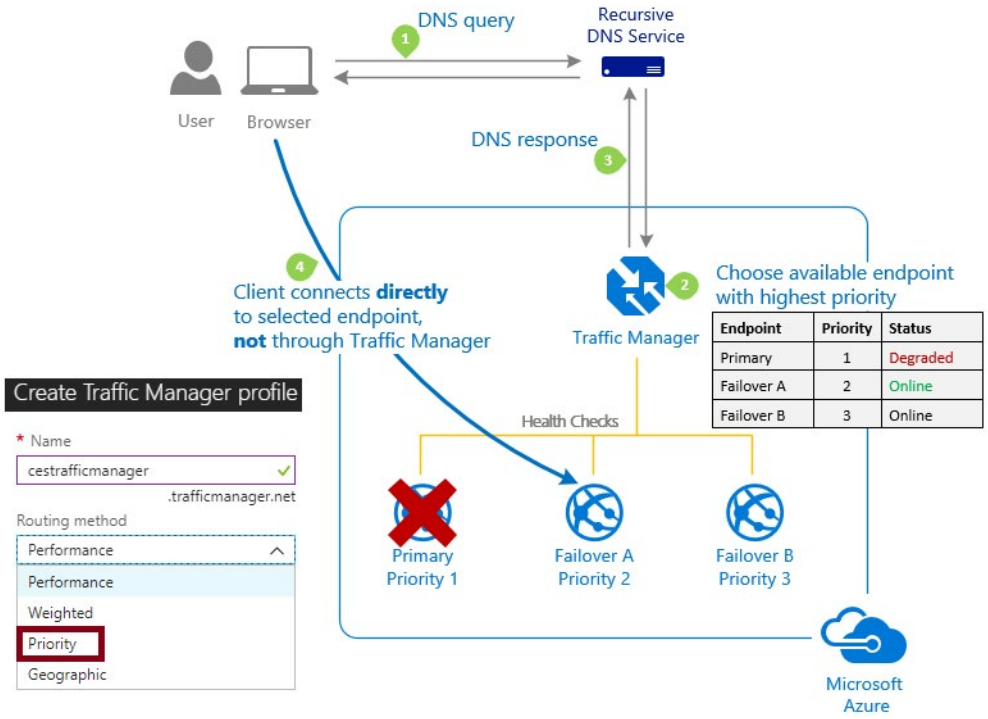
- **Improve responsiveness for high performance applications**. Azure allows you to run cloud services or websites in datacenters located around the world. Traffic Manager provides faster page loads and better end-user experience by serving users with the hosted service that is "closest" to them.
- **Upgrade and perform service maintenance without downtime**. You can seamlessly carry out upgrade and other planned maintenance operations on your applications without downtime for end users by using Traffic Manager to direct traffic to alternative endpoints when maintenance is in progress.
- **Combine on-premises and Cloud-based applications**. Traffic Manager supports external, non-Azure endpoints enabling it to be used with hybrid cloud and on-premises deployments.
- **Distribute traffic for large, complex deployments**. Traffic-routing methods can be combined using nested Traffic Manager profiles to create sophisticated and flexible traffic-routing configurations to meet the needs of larger, more complex deployments.

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

Priority Routing

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

In this case the Traffic Manager profile contains a prioritized list of service endpoints. Traffic Manager sends all traffic to the primary (highest-priority) endpoint first. If the primary endpoint is not available, Traffic Manager routes the traffic to the second endpoint, and so on. Availability of the endpoint is based on the configured status (enabled or disabled) and the ongoing endpoint monitoring.

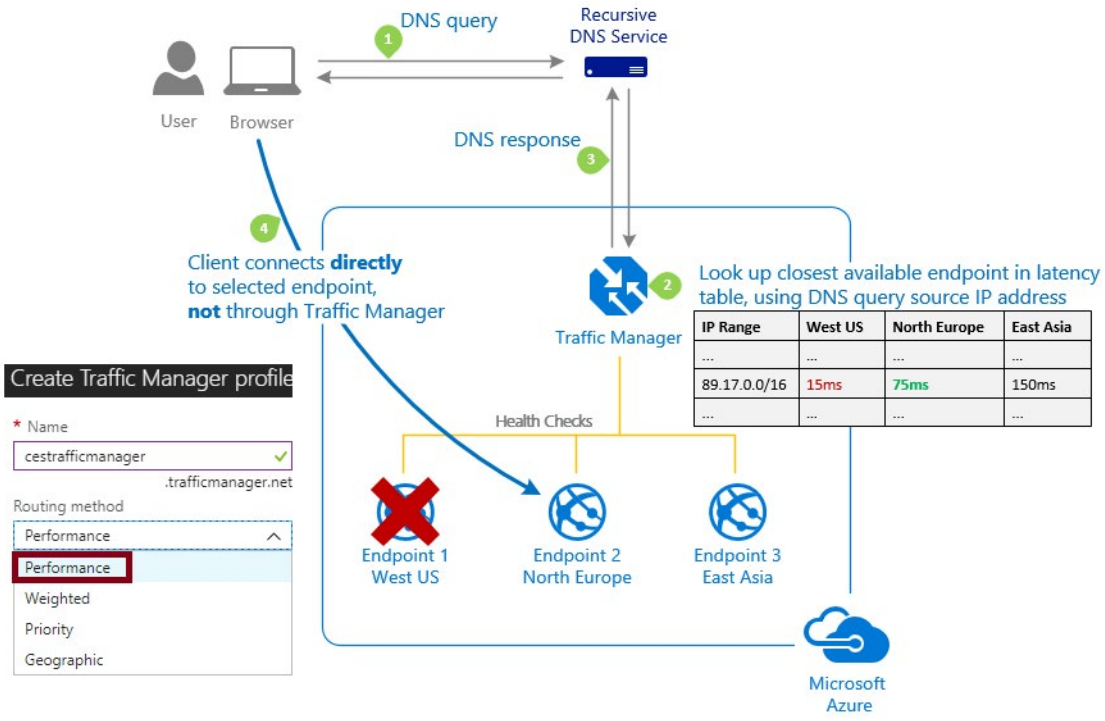


The Priority traffic routing method allows you to easily implement a failover pattern. You configure the endpoint priority explicitly or use the default priority based on the endpoint order.

Performance Routing

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

The Performance routing method is designed to improve the responsiveness by routing traffic to the location that is closest to the user. The closest endpoint is not necessarily measured by geographic distance. Instead Traffic Manager determines closeness by measuring network latency. Traffic Manager maintains an Internet Latency Table to track the round-trip time between IP address ranges and each Azure datacenter.



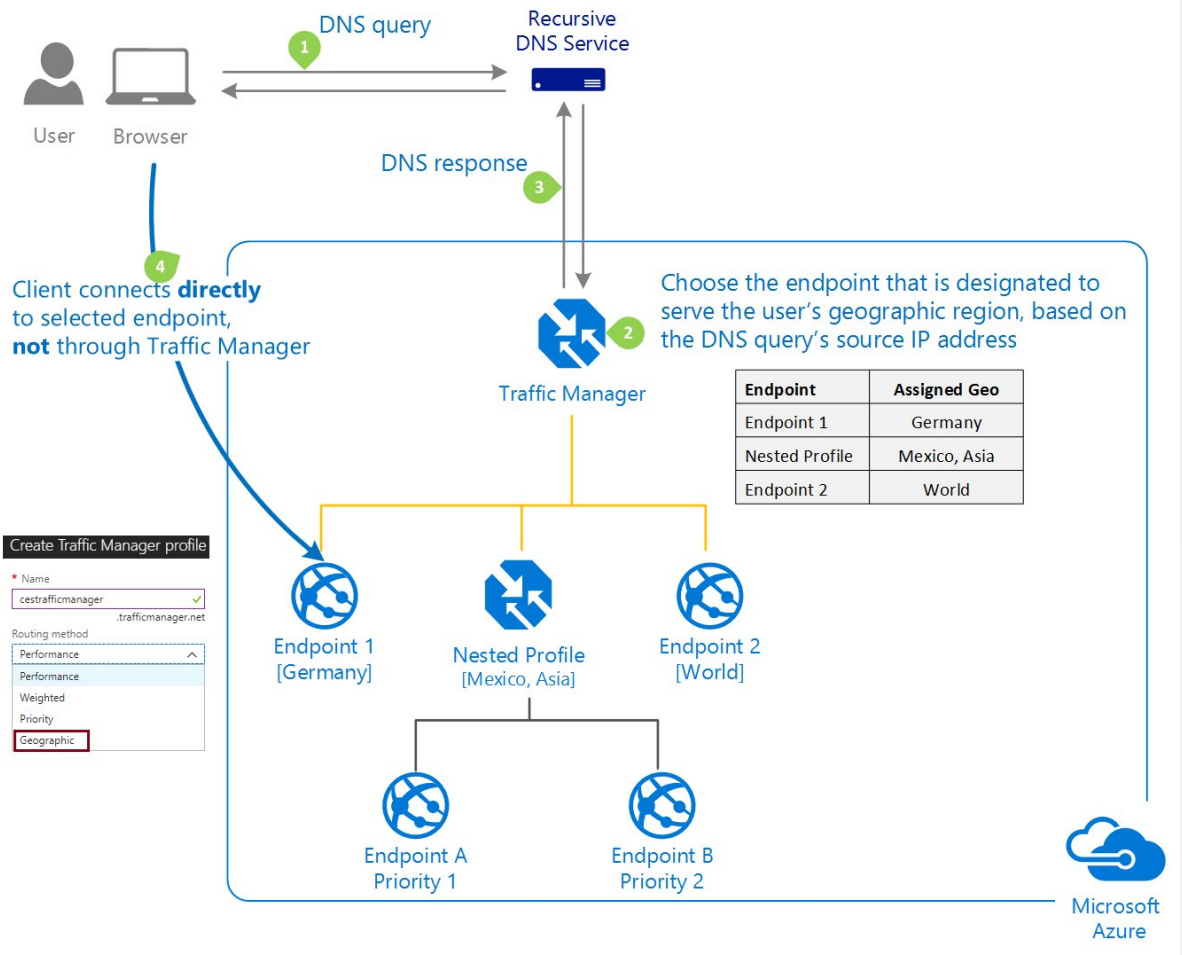
With this method Traffic Manager looks up the source IP address of the incoming DNS request in the Internet Latency Table. Traffic Manager chooses an available endpoint in the Azure datacenter that has the lowest latency for that IP address range, then returns that endpoint in the DNS response.

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

Geographic Routing

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

When a Traffic Manager profile is configured for Geographic routing, each endpoint associated with that profile needs will have a set of geographic locations assigned to it. Any requests from those regions gets routed only to that endpoint.



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

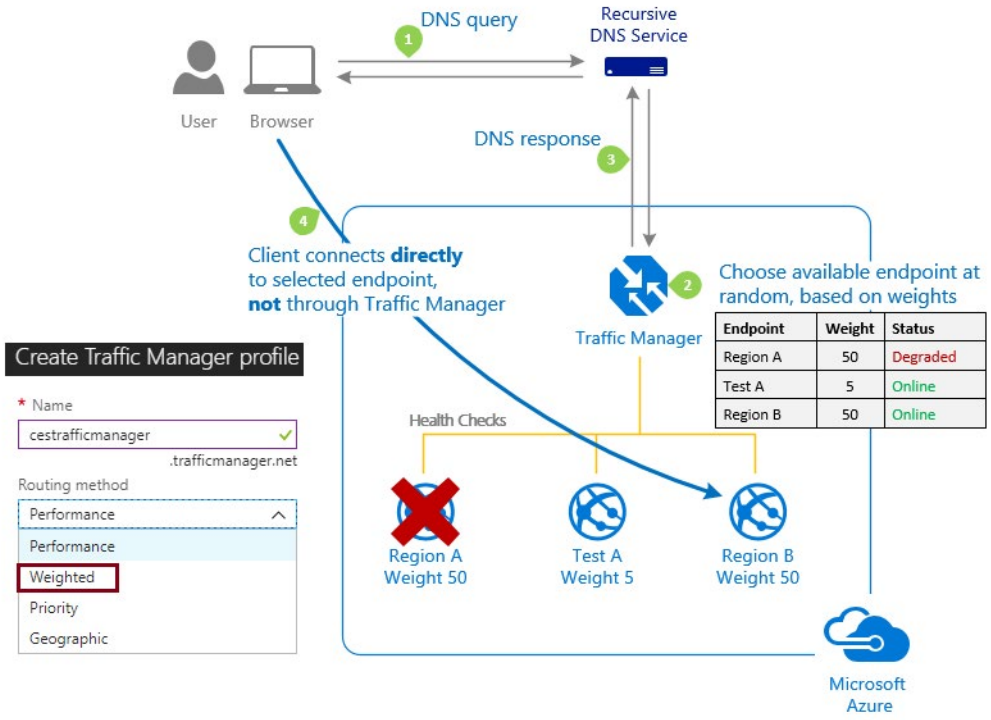
- **Regional Grouping**. For example, All (World), Europe, Middle East, or Asia.
- **Country/Region**. For example, Europe Denmark and Middle East Turkey.
- **State/Province** (only available in Australia, Canada, UK, and USA). For example, North America / Central America / Caribbean United States Maryland or North America / Central America / Caribbean Canada Ontario.

✓ Similar to Performance routing Traffic Manager uses the source IP address of the DNS query to determine the region from which a user is querying from. Usually, this is the IP address of the local DNS resolver doing the query on behalf of the user.

Weighted Routing

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

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



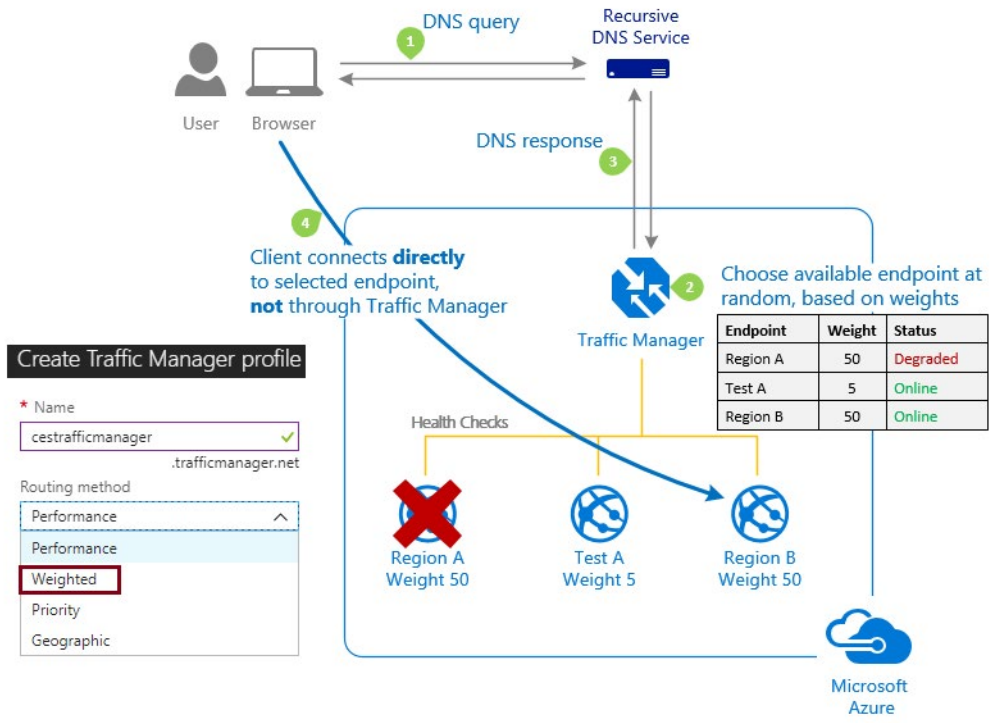
In the Weighted traffic-routing method, you assign a weight to each endpoint in the Traffic Manager profile configuration. The weight is an integer from 1 to 1000. This parameter is optional. If omitted, Traffic Manager uses a default weight of '1'. The higher weight, the higher the priority.

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

Implementing Traffic Manager Profiles

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

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



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

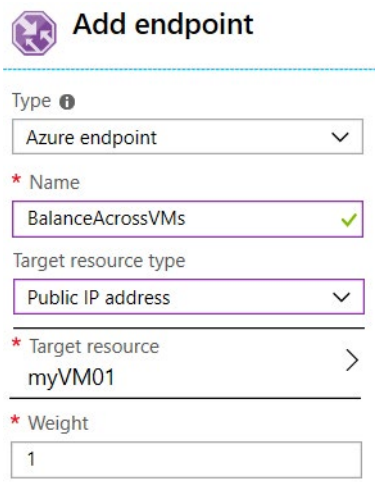
✓ Using the same weight across all endpoints results in an even traffic distribution. Using higher or lower weights on specific endpoints causes those endpoints to be returned more or less frequently in the DNS responses.

Implementing Traffic Manager Endpoints

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

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

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



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

Azure Front Door Service Overview

Azure Front Door Service

Azure Front Door Service enables you to define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability. With Front Door, you can transform your global (multi-region) consumer and enterprise applications into robust, high-performance personalized modern applications, APIs, and content that reach a global audience with Azure.

Front Door works at Layer 7 or HTTP/HTTPS layer and uses anycast protocol with split TCP and Microsoft's global network for improving global connectivity. So, per your routing method selection in the configuration, you can ensure that Front Door is routing your client requests to the fastest and most available application backend. An application backend is any Internet-facing service hosted inside or outside of Azure. Front Door provides a range of traffic-routing methods and backend health monitoring options to suit different application needs and automatic failover models. Similar to Traffic Manager, Front Door is resilient to failures, including the failure of an entire Azure region.

The following features are included with Front Door:

Accelerate application performance

Using split TCP-based anycast protocol, Front Door ensures that your end users promptly connect to the nearest Front Door POP (Point of Presence). Using Microsoft's global network for connecting to your application backends from Front Door POPs, ensure higher availability and reliability while maintaining performance. This connectivity to your backend is also based on least network latency. Learn more about Front Door routing techniques like Split TCP and Anycast protocol.

Increase application availability with smart health probes

Front Door delivers high availability for your critical applications using its smart health probes, monitoring your backends for both latency and availability and providing instant automatic failover when a backend goes down. So, you can run planned maintenance operations on your applications without downtime. Front Door directs traffic to alternative backends while the maintenance is in progress.

URL-based routing

URL Path Based Routing allows you to route traffic to backend pools based on URL paths of the request. One of the scenarios is to route requests for different content types to different backend pools.

For example, requests for `http://www.contoso.com/users/*` are routed to `UserProfilePool`, and `http://www.contoso.com/products/*` are routed to `ProductInventoryPool`. Front Door allows even more complex route matching scenarios using best match algorithm and so if none of the path patterns match then your default routing rule for `http://www.contoso.com/*` is selected and the traffic is directed to default catch-all routing rule.

Multiple-site hosting

Multiple-site hosting enables you to configure more than one web site on the same Front Door configuration. This feature allows you to configure a more efficient topology for your deployments by adding different web sites to a single Front Door configuration. Based on your application's architecture, you can configure Azure Front Door Service to either direct each web site to its own backend pool or have various web sites directed to the same backend pool. For example, Front Door can serve traffic for `images.contoso.com` and `videos.contoso.com` from two backend pools called `ImagePool` and `VideoPool`. Alternatively you can configure both the front-end hosts to direct traffic to a single backend pool called `MediaPool`.

Similarly, you can have two different domains `www.contoso.com` and `www.fabrikam.com` configured on the same Front Door.

Session affinity

The cookie-based session affinity feature is useful when you want to keep a user session on the same application backend. By using Front Door managed cookies, subsequent traffic from a user session gets directed to the same application backend for processing. This feature is important in cases where session state is saved locally on the backend for a user session.

Secure Sockets Layer (SSL) termination

Front Door supports SSL termination at the edge that is, individual users can set up SSL connection with Front Door environments instead of establishing it over long haul connections with the application backend. Additionally, Front Door supports both HTTP as well as HTTPS connectivity between Front Door environments and your backends. So, you can also set up end-to-end SSL encryption. For example, if Front Door for your application workload receives over 5000 requests in a minute, due to warm connection reuse, for active services, it will only establish say about 500 connections with your application backend, thereby reducing significant load from your backends.

Custom domains and certificate management

When you use Front Door to deliver content, a custom domain is necessary if you would like your own domain name to be visible in your Front Door URL. Having a visible domain name can be convenient for your customers and useful for branding purposes. Front Door also supports HTTPS for custom domain names. Use this feature by either choosing Front Door managed certificates for your traffic or uploading your own custom SSL certificate.

Application layer security

Azure Front Door allows you to author custom Web Application Firewall (WAF) rules for access control to protect your HTTP/HTTPS workload from exploitation based on client IP addresses, country code, and http parameters. Additionally, Front Door also enables you to create rate limiting rules to battle malicious bot traffic.

Front Door platform itself is protected by Azure DDoS Protection Basic. For further protection, Azure DDoS Protection Standard may be enabled at your VNETs and safeguard resources from network layer (TCP/UDP) attacks via auto tuning and mitigation. Front Door is a layer 7 reverse proxy, it only allows web traffic to pass through to backends and block other types of traffic by default.

URL redirection

With the strong industry push on supporting only secure communication, web applications are expected to automatically redirect any HTTP traffic to HTTPS. This ensures that all communication between the users and the application occurs over an encrypted path.

Traditionally, application owners have dealt with this requirement by creating a dedicated service, whose sole purpose was to redirect requests it receives on HTTP to HTTPS. Azure Front Door Service supports the ability to redirect traffic from HTTP to HTTPS. This simplifies application configuration, optimizes the resource usage, and supports new redirection scenarios, including global and path-based redirection. URL redirection from Azure Front Door Service is not limited to HTTP to HTTPS redirection alone, but also to redirect to a different hostname, redirecting to a different path, or even redirecting to a new query string in the URL.

URL rewrite

Front Door supports URL rewrite by allowing you to configure an optional Custom Forwarding Path to use when constructing the request to forward to the backend. Front Door further allows you to configure Host header to be sent when forwarding the request to your backend.

Protocol support - IPv6 and HTTP/2 traffic

Azure Front Door natively supports end-to-end IPv6 connectivity and also HTTP/2 protocol.

The HTTP/2 protocol enables full-duplex communication between application backends and a client over a long-running TCP connection. HTTP/2 allows for a more interactive communication between the backend and the client, which can be bidirectional without the need for polling as required in HTTP-based implementations. HTTP/2 protocol has low overhead, unlike HTTP, and can reuse the same TCP connection for multiple request or responses resulting in a more efficient utilization of resources.

Optional Practice- Create a Front Door Profile

This practice exercise explains how to create a Front Door profile that delivers high availability and high performance for a global web application.

The scenario described in this exercise includes two instances of a web application running in different Azure regions. A Front Door configuration based on equal weighted and same priority backends is created that helps direct user traffic to the nearest set of site backends running the application. Front Door continuously monitors the web application and provides automatic failover to the next available backend when the nearest site is unavailable.

Sign in to Azure

Sign in to the Azure portal at **https://portal.azure.com**.

Prerequisites

This exercise requires that you have deployed two instances of a web application running in different Azure regions (East US and West Europe). Both the web application instances run in Active/Active mode, that is, either of them can take traffic at any time unlike a Active/Stand-By configuration where one acts as a failover.

1. On the top left-hand side of the screen, select Create a resource > Web > Web App > Create.
2. In Web App, enter or select the following information and enter default settings where none are specified:

Setting	Value
Name	Enter a unique name for your web app
Resource group	Select New, and then type myResourceGroupFD1

Setting	Value
App Service plan/Location	Select New. In the App Service plan, enter myAppServicePlanEastUS, and then select OK.
Location	East US

3. Select Create.
4. A default website is created when the Web App is successfully deployed.
5. Repeat steps 1-3 to create a second website in a different Azure region with the following settings:

Setting	Value
Name	Enter a unique name for your web app
Resource group	Select New, and then type myResourceGroupFD1
App Service plan/Location	Select New. In the App Service plan, enter myAppServicePlanEastUS, and then select OK.
Location	East US

Create a Front Door for your application

A. Add a frontend host for Front Door

Create a Front Door configuration that directs user traffic based on lowest latency between the two backends.

1. On the top left-hand side of the screen, select Create a resource > Networking > Front Door > Create.
2. In the Create a Front Door, you start with adding the basic info and provide a subscription where you want the Front Door to be configured. Similarly, like any other Azure resource you also need to provide a ResourceGroup and a Resource Group region if you are creating a new one. Lastly, you need to provide a name for your Front Door.
3. Once the basic info is filled in, the first step you need to define is the frontend host for the configuration. The result should be a valid domain name like myappfrontend.azurefd.net. This hostname needs to be globally unique but Front Door will take care of that validation.

B. Add application backend and backend pools

Next, you need to configure your application backend(s) in a backend pool for Front Door to know where your application resides.

1. Click the '+' icon to add a backend pool and then specify a name for your backend pool, say myBackendPool.
2. Next, click on Add Backends to add your websites created earlier.
3. Select Target host type as 'App Service', select the subscription in which you created the web site and then choose the first web site from the Target host name, that is, myAppServicePlanEastUS.azurewebsites.net.
4. Leave the remaining fields as is for now and click Add'.
5. Repeat steps 2 to 4 to add the other website, that is, myAppServicePlanWestEurope.azurewebsites.net
6. You can optionally choose to update the Health Probes and Load Balancing settings for the backend pool, but the default values should also work. Click Add.

C. Add a routing rule

Lastly, click the '+' icon on Routing rules to configure a routing rule. This is needed to map your frontend host to the backend pool, which basically is configuring that if a request comes to myappfrontend.

azurefd.net, then forward it to the backend pool myBackendPool. Click Add to add the routing rule for your Front Door. You should now be good to creating the Front Door and so click on Review and Create.

Warning

You must ensure that each of the frontend hosts in your Front Door has a routing rule with a default path ('/') *associated with it. That is, across all your routing rules there must be at least one routing rule for each of your frontend hosts defined at the default path ('/'*). Failing to do so, may result in your end-user traffic not getting routed correctly.

View Front Door in action

Once you create a Front Door, it will take a few minutes for the configuration to be deployed globally everywhere. Once complete, access the frontend host you created, that is, go to a web browser and hit the URL myappfrontend.azurefd.net. Your request will automatically get routed to the nearest backend to you from the specified backends in the backend pool.

View Front Door handle application failover

If you want to test Front Door's instant global failover in action, you can go to one of the web sites you created and stop it. Based on the Health Probe setting defined for the backend pool, we will instantly fail over the traffic to the other web site deployment. You can also test behavior, by disabling the backend in the backend pool configuration for your Front Door.

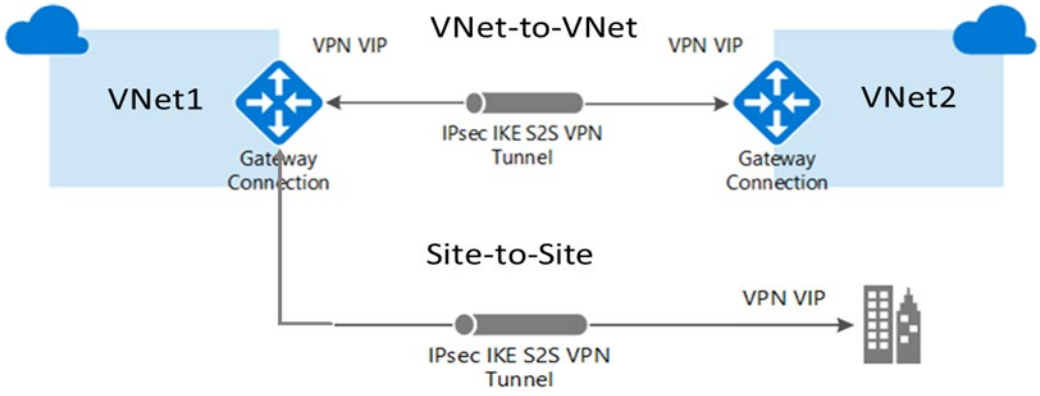
Clean up resources

When no longer needed, delete the resource groups, web applications, and all related resources.

VNet-to-VNet Connections

VNet-to-VNet Connections

You can connect your VNets with a VNet-to-VNet VPN connection. Using this connection method, you create a VPN gateway in each virtual network. A secure tunnel using **IPsec/IKE**[7] provides the communication between the networks.



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

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

Benefits

Cross region geo-redundancy and geo-presence

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

Regional multi-tier applications with isolation or administrative boundary

- Within the same region, you can set up multi-tier applications with multiple virtual networks connected together due to isolation or administrative requirements.
- VNet-to-VNet communication can be combined with multi-site configurations. This lets you establish network topologies that combine cross-premises connectivity with inter-virtual network connectivity.

✓ You will use VNet-to-VNet connections when you cannot use VNet peering.

✓ Connections to on-premises viirtual networks are called Site-to-Site (S2S) connections.

For more information, you can see:

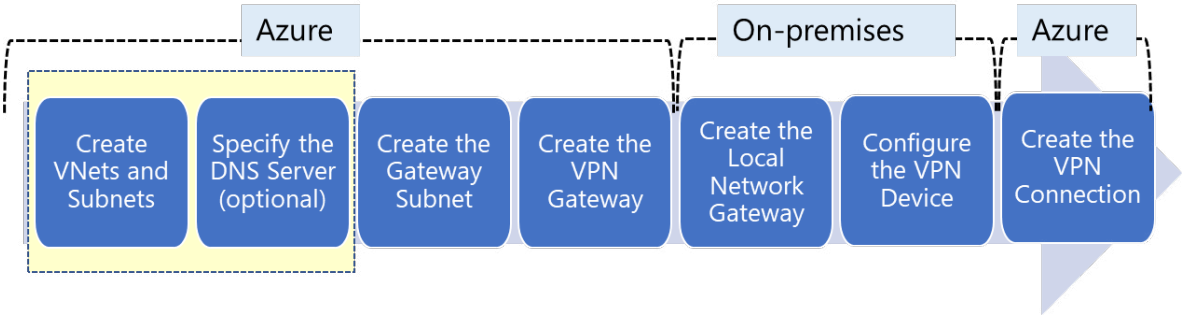
VNet-to-VNet Connectivity - **https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal#vnet-to-vnet**

7 https://docs.microsoft.com/en-us/windows/desktop/FWP/ipsec-configuration

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

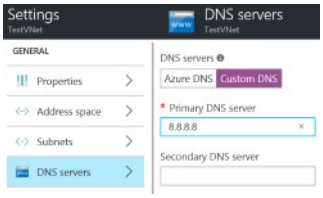
Implement VNet-to-VNet Connections

Here are the steps to creating a VNet-to-VNet connections. The on-premises part is necessary only if you are configuring Site-to-Site. We will look in detail at each step.



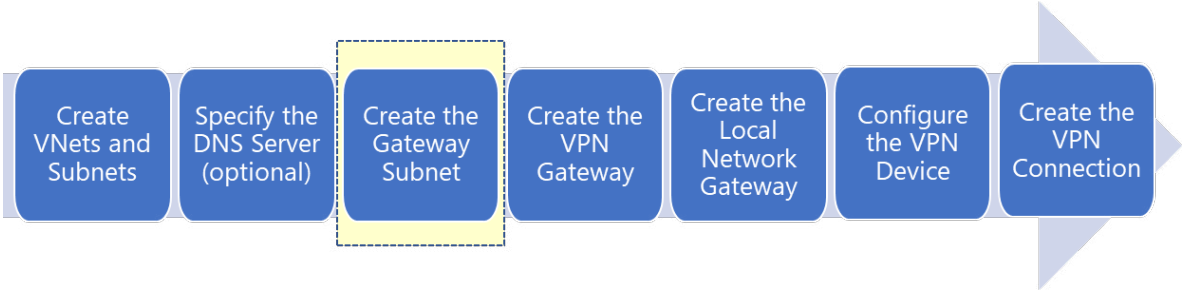
Create VNets and subnets. By now you should be familiar with creating virtual networks and subnets. Remember for this VNet to connect to an on-premises location. You need to coordinate with your on-premises network administrator to reserve an IP address range that you can use specifically for this virtual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

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



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

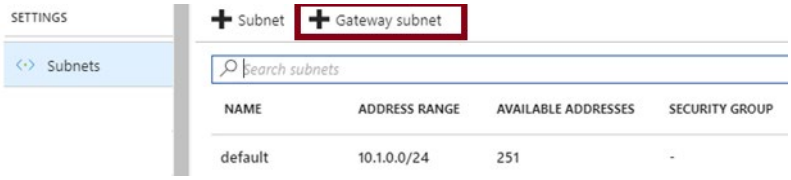
Create the Gateway Subnet



Before creating a virtual network gateway for your virtual network, you first need to create the gateway subnet. The gateway subnet contains the IP addresses that are used by the virtual network gateway. If possible, it's best to create a gateway subnet by using a CIDR block of /28 or /27 to provide enough IP addresses to accommodate future additional configuration requirements.

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

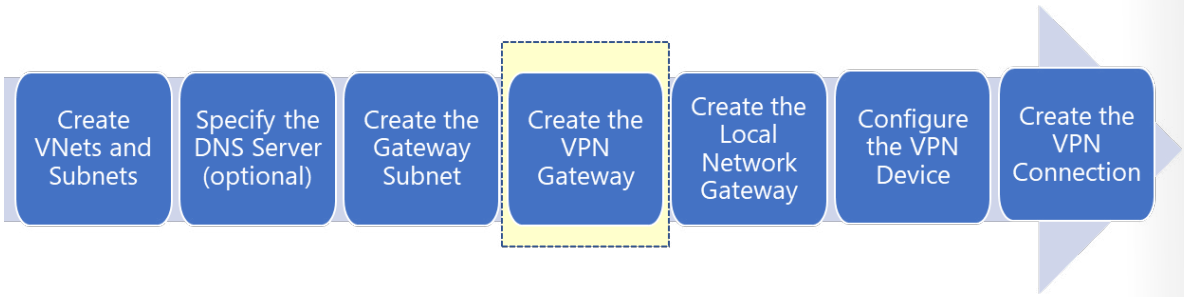
To deploy a gateway in your virtual network simply add a gateway subnet.



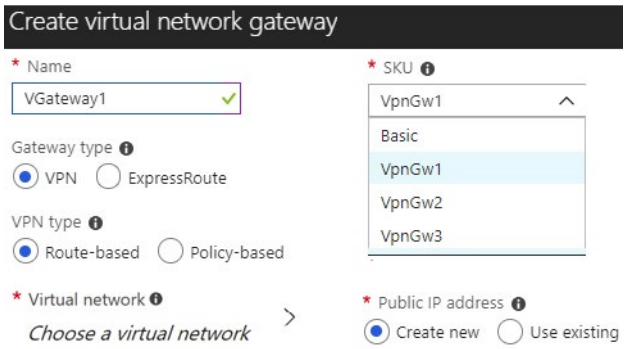
✓ When working with gateway subnets, avoid associating a network security group (NSG) to the gateway subnet. Associating a network security group to this subnet may cause your VPN gateway to stop functioning as expected.

✓ This is the same step in configuring VNet Peering.

Create the VPN Gateway



A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway. When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.



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

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

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

It can take up to 45 minutes to provision the VPN gateway.

✓ After the gateway is created, view the IP address that has been assigned to it by looking at the virtual network in the portal. The gateway should appear as a connected device. In this last step you will create a connection for the device.

VPN Types

When you create the virtual network gateway for a VPN gateway configuration, you must specify a VPN type. The VPN type that you choose depends on the connection topology that you want to create. For example, a Point-to-Site (P2S) connection requires a Route-based VPN type. A VPN type can also depend on the hardware that you are using. Site-to-Site (S2S) configurations require a VPN device. Some VPN devices only support a certain VPN type.

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

There are two VPN types:

- **Policy-based VPNs**. Policy-based VPNs encrypt and direct packets through IPsec tunnels based on the IPsec policies configured with the combinations of address prefixes between your on-premises network and the Azure VNet. The policy (or traffic selector) is usually defined as an access list in the VPN device configuration. When using a Policy-based VPN, keep in mind the following limitations:
  - Policy-Based VPNs can only be used on the Basic gateway SKU and is not compatible with other gateway SKUs.
  - You can have only 1 tunnel when using a Policy-based VPN.
  - You can only use Policy-based VPNs for S2S connections, and only for certain configurations. Most VPN Gateway configurations require a Route-based VPN.
- **Route-based VPNs**. Route-based VPNs use *routes* in the IP forwarding or routing table to direct packets into their corresponding tunnel interfaces. The tunnel interfaces then encrypt or decrypt the packets in and out of the tunnels. The policy (or traffic selector) for Route-based VPNs are configured as any-to-any (or wild cards).

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

Gateway SKUs

When you create a virtual network gateway, you need to specify the gateway SKU that you want to use. Select the SKU that satisfies your requirements based on the types of workloads, throughputs, features, and SLAs.

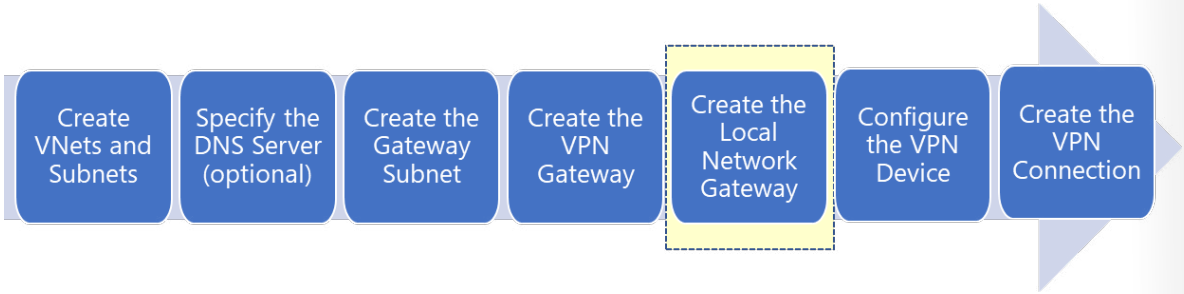
SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2 Connections	Aggregate Throughput Benchmark
Basic	Max. 10	Max. 128	Not Supported	100 Mbps
VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps
VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps
VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps

Aggregate Throughput Benchmark is based on measurements of multiple tunnels aggregated through a single gateway. The Aggregate Throughput Benchmark for a VPN Gateway is S2S + P2S combined. The Aggregate Throughput Benchmark is not a guaranteed throughput due to Internet traffic conditions and your application behaviors.

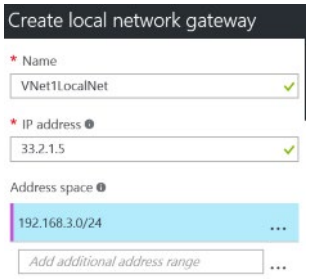
These connection limits are separate. For example, you can have 128 SSTP connections and also 250 IKEv2 connections on a VpnGw1 SKU.

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

Create the Local Network Gateway



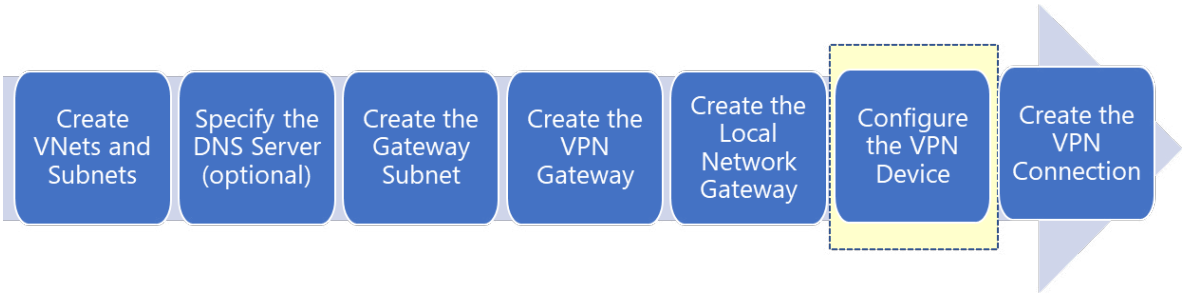
The local network gateway typically refers to the on-premises location. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device for the connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN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



IP Address. The public IP address of the local gateway.

Address Space. One or more IP address ranges (in CIDR notation) that define your local network's address space. For example: 192.168.0.0/16. If you plan to use this local network gateway in a BGP-enabled connection, then the minimum prefix you need to declare is the host address of your BGP Peer IP address on your VPN device.

Configure the On-Premises VPN Device



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

To configure your VPN device, you need the following:

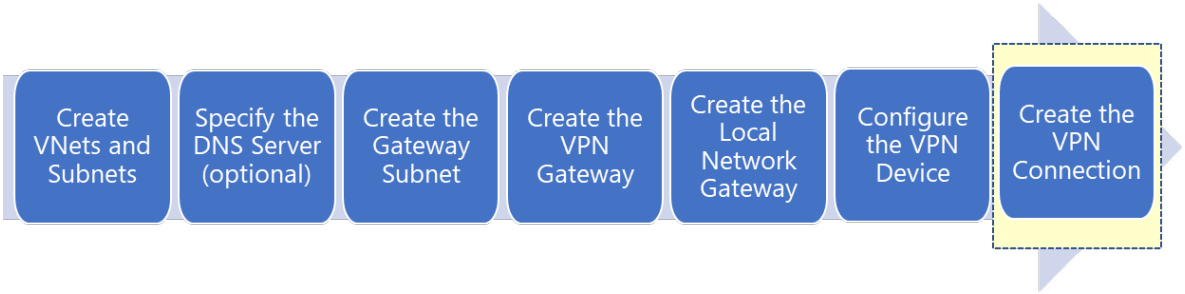
- **A shared key**. This is the same shared key that you will specify when creating the VPN connection (next step).
- **The public IP address of your VPN gateway**. When you created the VPN gateway you may have configured a new public IP address or used an existing IP address.

✓ Depending on the VPN device that you have, you may be able to **download a VPN device configuration script**[8].

For more information, you can see:

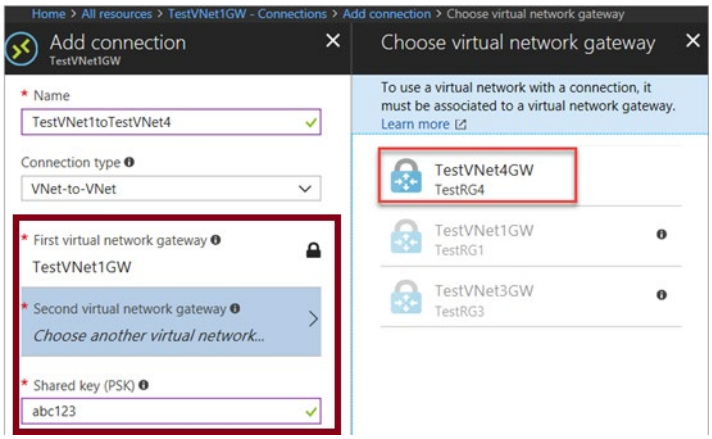
Validated VPN devices list - **https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#devicetable**[9]

Create the VPN Connection



8 https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-download-vpndevicescript
9 https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices

Once your VPN gateways are created, you can create the connection between them. If your VNets are in the same subscription, you can use the portal.



- **Name**. Enter a name for your connection.
- **Connection type**. Select VNet-to-VNet from the drop-down.
- **First virtual network gateway**. This field value is automatically filled in because you're creating this connection from the specified virtual network gateway.
- **Second virtual network gateway**. This field is the virtual network gateway of the VNet that you want to create a connection to.
- **Shared key (PSK)**. In this field, enter a shared key for your connection. You can generate or create this key yourself. In a site-to-site connection, the key you use is the same for your on-premises device and your virtual network gateway connection. The concept is similar here, except that rather than connecting to a VPN device, you're connecting to another virtual network gateway.

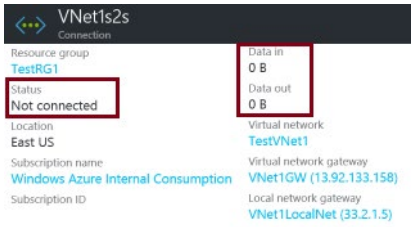
✓ If your VNets are in different subscriptions, you must use PowerShell to make the connection. You can use the New-AzVirtualNetworkGatewayConnection.

Verify the VPN Connection

After you have configured all the Site-to-Site components it is time to verify that everything is working. You can verify the connections either in the portal, or by using PowerShell.

Portal

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



PowerShell

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

```
    Get-AzVirtualNetworkGatewayConnection -Name MyGWConnection -Resource-
GroupName MyRG
```

After the cmdlet has finished, view the values. The connection status should show 'Connected' and you can see ingress and egress bytes.

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

Demonstration - VNet to VNet Connections

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

Explore the Gateway subnet blade

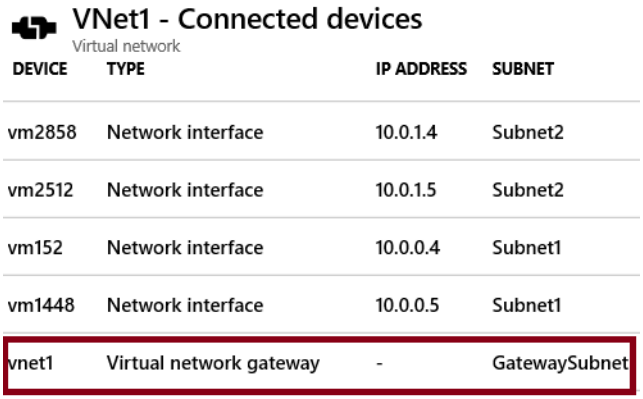
1. For one of your virtual network, select the **Subnets** blade.
2. Select **+ Gateway subnet**.

   Notice the name of the subnet cannot be changed.

   Notice the **address range** of the gateway subnet. The address must be contained by the address space of the virtual network.
3. Remember each virtual network needs a gateway subnet.
4. Close the Add gateway subnet page. You do not need to save your changes.

Explore the Connected Devices blade

1. For the virtual network, select the **Connected Devices** blade.
2. After a gateway subnet is deployed it will appear on the list of connected devices.



Explore adding a virtual network gateway

1. Search for **Virtual network gateways**.
2. Click **+ Add**.
3. Review each setting for the virtual netowrk gateway.
4. Use the Information icons to learn more about the settings.
5. Notice the **Gateway type**, **VPN type**, and **SKU**.

6. Notice the need for a **Public IP address**.
7. Remember each virtual network will need a virtual network gateway.
8. Close the Add virtual network gateway. You do not need to save your changes.

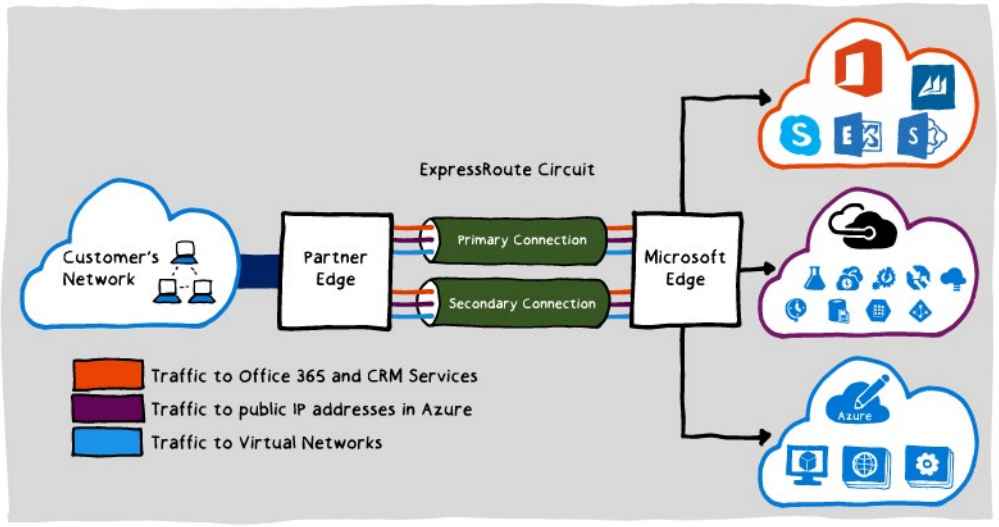
Explore adding a connection between the virtual networks

1. Search for **Connections**.
2. Click **+ Add**.
3. Notice the **Connection type** can be VNet-to-VNet, Site-to-Site (IPsec), or ExpressRoute.
4. Provide enough information, so you can click the **Ok** button.
5. On the **Settings** page, notice that you will need select the two different virtual networks.
6. Read the Help information on the **Establilsh bidirectional connnectivity** checkbox.
7. Notice the **Shared key (PSK)** information.
8. Close the Add connection page. You do not need to save your changes.

ExpressRoute Connections

ExpressRoute

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



Make your connections fast, reliable, and private

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections. In some cases, using ExpressRoute connections to transfer data between on-premises systems and Azure can give you significant cost benefits.

With ExpressRoute, establish connections to Azure at an ExpressRoute location, such as an Exchange provider facility, or directly connect to Azure from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider.

Use a virtual private cloud for storage, backup, and recovery

ExpressRoute gives you a fast and reliable connection to Azure with bandwidths up to 100 Gbps, which makes it excellent for scenarios like periodic data migration, replication for business continuity, disaster recovery, and other high-availability strategies. It can be a cost-effective option for transferring large amounts of data, such as datasets for high-performance computing applications, or moving large virtual machines between your dev-test environment in an Azure virtual private cloud and your on-premises production environments.

Extend and connect your datacenters

Use ExpressRoute to both connect and add compute and storage capacity to your existing datacenters. With high throughput and fast latencies, Azure will feel like a natural extension to or between your datacenters, so you enjoy the scale and economics of the public cloud without having to compromise on network performance.

Build hybrid applications

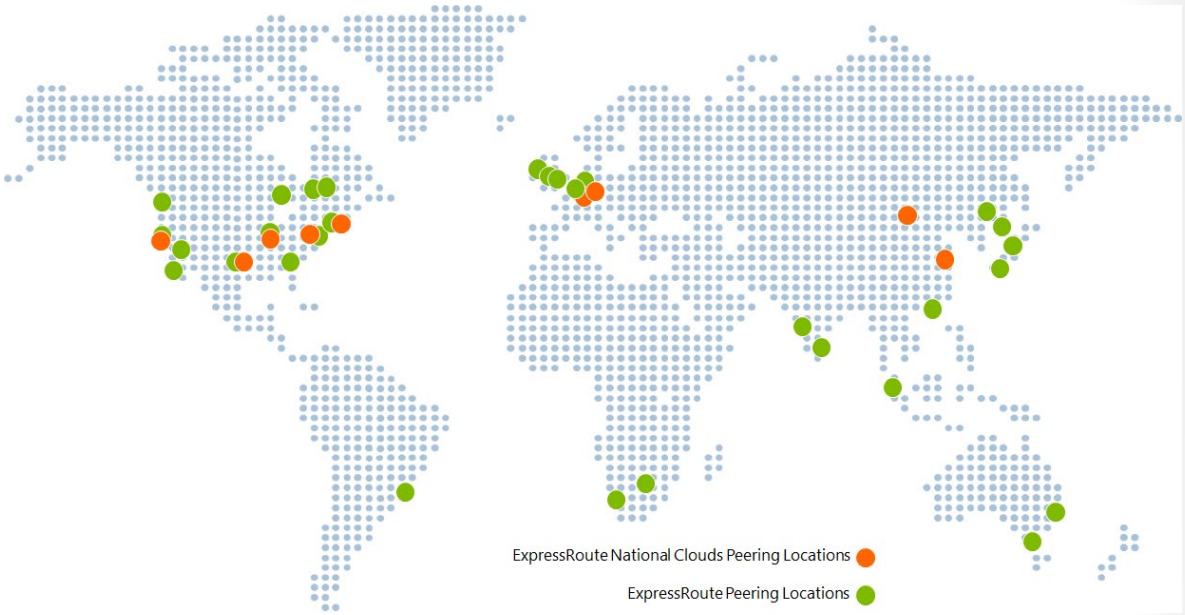
With predictable, reliable, and high-throughput connections offered by ExpressRoute, build applications that span on-premises infrastructure and Azure without compromising privacy or performance. For example, run a corporate intranet application in Azure that authenticates your customers with an on-premises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

For more information, you can see:

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

ExpressRoute Capabilities

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



There are many benefits to using ExpressRoute.

Layer 3 connectivity

Microsoft uses BGP, an industry standard dynamic routing protocol, to exchange routes between your on-premises network, your instances in Azure, and Microsoft public addresses. We establish multiple BGP sessions with your network for different traffic profiles.

Redundancy

Each ExpressRoute circuit consists of two connections to two Microsoft Enterprise edge routers (MSEEs) from the connectivity provider/your network edge. Microsoft requires dual BGP connection from the connectivity provider/your network edge – one to each MSEE. The graphic on the previous topics shows the primary and secondary connection.

Connectivity to Microsoft cloud services

ExpressRoute connections enable access to the following services: Microsoft Azure services, Microsoft Office 365 services, and Microsoft Dynamics 365. Office 365 was created to be accessed securely and reliably via the Internet, so ExpressRoute requires **Microsoft authorization**[10].

Connectivity to all regions within a geopolitical region

You can connect to Microsoft in one of our peering locations and access regions within the geopolitical region. For example, if you connect to Microsoft in Amsterdam through ExpressRoute, you'll have access to all Microsoft cloud services hosted in Northern and Western Europe.

Global connectivity with ExpressRoute premium add-on

You can enable the ExpressRoute premium add-on feature to extend connectivity across geopolitical boundaries. For example, if you connect to Microsoft in Amsterdam through ExpressRoute, you will have access to all Microsoft cloud services hosted in all regions across the world (national clouds are excluded).

Across on-premises connectivity with ExpressRoute Global Reach

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, if you have a private data center in California connected to ExpressRoute in Silicon Valley, and another private data center in Texas connected to ExpressRoute in Dallas, with ExpressRoute Global Reach, you can connect your private data centers together through two ExpressRoute circuits. Your cross-data-center traffic will traverse through Microsoft's network.

Bandwidth options

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

Flexible billing models

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

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

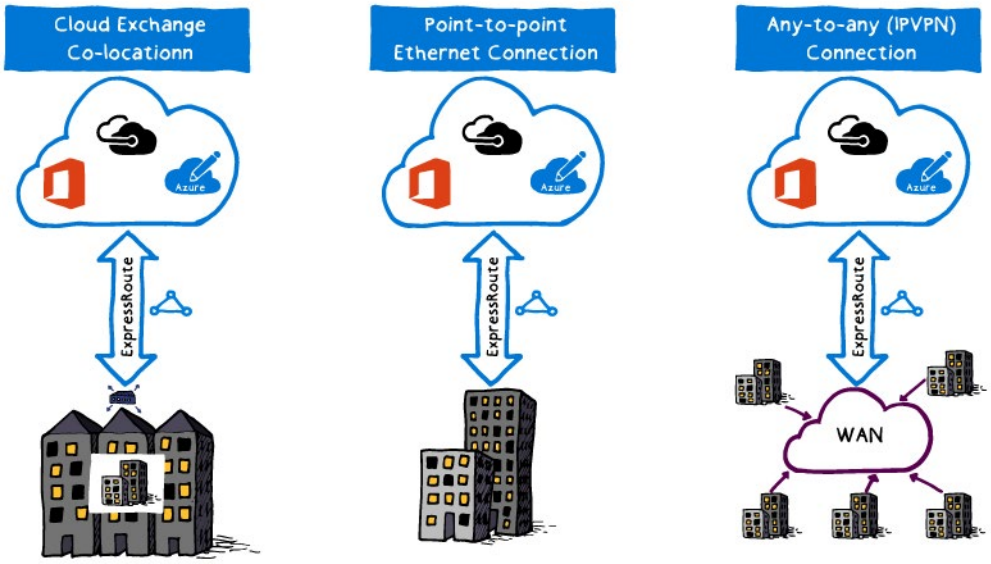
For more information, you can see:

FAQ - Azure ExpressRoute - **https://docs.microsoft.com/en-us/azure/expressroute/expressroute-faqs**

ExpressRoute Connection Options

You can create a connection between your on-premises network and the Microsoft cloud in three different ways, **CloudExchange Co-location**[11], **Point-to-point Ethernet Connection**[12], and **Any-to-any (IPVPN) Connection**[13]. Connectivity providers can offer one or more connectivity models. You can work with your connectivity provider to pick the model that works best for you.

10 https://docs.microsoft.com/en-us/office365/enterprise/azure-expressroute
11 https://docs.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models
12 https://docs.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models
13 https://docs.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models



CloudExchange Co-location

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

Point-to-point Ethernet connections

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

Any-to-any (IPVPN) networks

You can integrate your WAN with the Microsoft cloud. IPVPN providers, typically Multiprotocol Label Switching (MPLS) VPN, offer any-to-any connectivity between your branch offices and datacenters. The Microsoft cloud can be interconnected to your WAN to make it look just like any other branch office. WAN providers typically offer managed Layer 3 connectivity.

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

For more information, you can see:

ExpressRoute connectivity models - **https://docs.microsoft.com/en-us/azure/expressroute/express-route-connectivity-models**

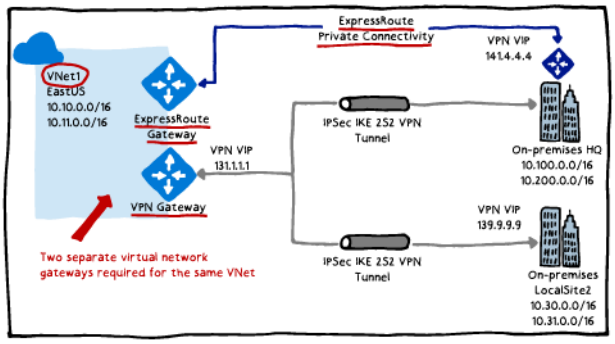
Site-to-Site and ExpressRoute Coexisting Connections

ExpressRoute is a direct, private connection from your WAN (not over the public Internet) to Microsoft Services, including Azure. Site-to-Site VPN traffic travels encrypted over the public Internet. Being able to configure Site-to-Site VPN and ExpressRoute connections for the same virtual network has several advantages.

You can configure a Site-to-Site VPN as a secure failover path for ExpressRoute or use Site-to-Site VPNs to connect to sites that are not part of your network, but that are connected through ExpressRoute.

Notice that this configuration requires two virtual network gateways for the same virtual network, one using the gateway type 'VPN', and the other using the gateway type 'ExpressRoute'.

ExpressRoute and VPN Gateway coexisting connections example



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

For more information, see:

Site-to-Site and ExpressRoute coexisting connections – **https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#coexisting**[14]

14 https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

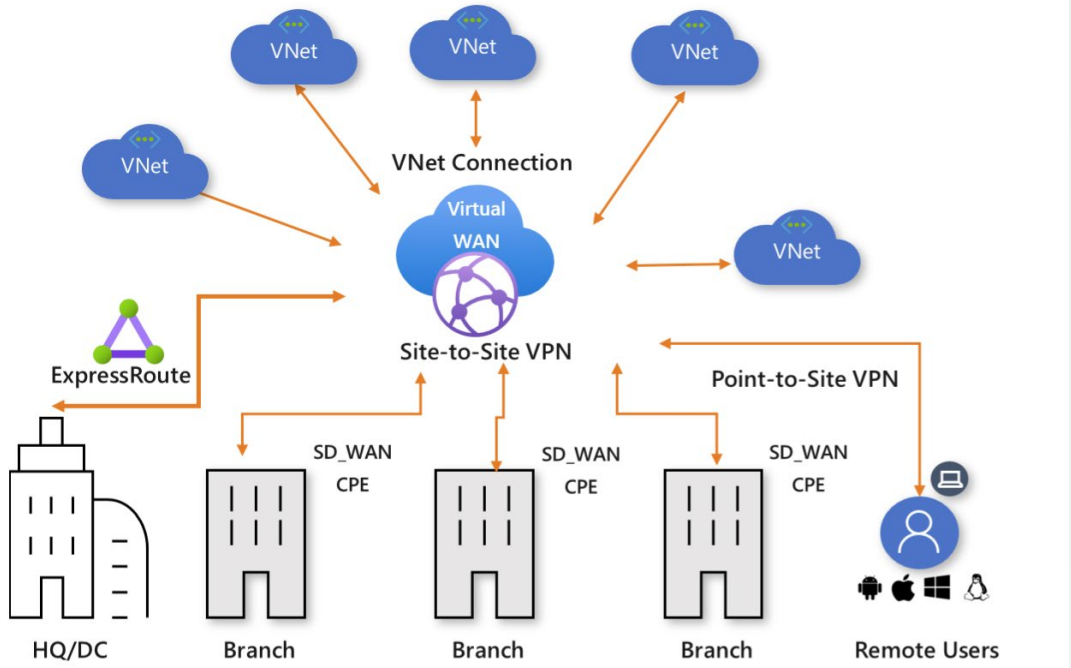
Azure Virtual WAN

Azure Virtual WAN Overview

About Azure Virtual WAN

Azure Virtual WAN is a networking service that provides optimized and automated branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to. You can leverage the Azure backbone to also connect branches and enjoy branch-to-VNet connectivity.

Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, User VPN (point-to-site), and ExpressRoute into a single operational interface. Connectivity to Azure VNets is established by using virtual network connections. It enables global transit network architecture based on a classic hub-and-spoke connectivity model where the cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.



This article provides a quick view into the network connectivity in Azure Virtual WAN. Virtual WAN offers the following advantages:

- Integrated connectivity solutions in hub and spoke: Automate site-to-site configuration and connectivity between on-premises sites and an Azure hub.
- Automated spoke setup and configuration: Connect your virtual networks and workloads to the Azure hub seamlessly.
- Intuitive troubleshooting: You can see the end-to-end flow within Azure, and then use this information to take required actions.

Basic and Standard virtual WANs

There are two types of virtual WANs: Basic and Standard. The following table shows the available configurations for each type.

Setting	Value
Name	Enter a unique name for your web app
Resource group	Select New, and then type myResourceGroupFD1
App Service plan/Location	Select New. In the App Service plan, enter myAppServicePlanEastUS, and then select OK.
Location	East US

Note: You can upgrade from Basic to Standard, but cannot revert from Standard back to Basic.

Virtual WAN resources

To configure an end-to-end virtual WAN, you create the following resources:

- virtualWAN: The virtualWAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. It contains links to all your virtual hubs that you would like to have within the virtual WAN. Virtual WAN resources are isolated from each other and cannot contain a common hub. Virtual hubs across Virtual WAN do not communicate with each other.
- Hub: A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity. From your on-premises network (vpnsite), you can connect to a VPN Gateway inside the virtual hub, connect ExpressRoute circuits to a virtual hub, or even connect mobile users to a Point-to-site gateway in the virtual hub. The hub is the core of your network in a region. There can only be one hub per Azure region.

A hub gateway is not the same as a virtual network gateway that you use for ExpressRoute and VPN Gateway. For example, when using Virtual WAN, you don't create a site-to-site connection from your on-premises site directly to your VNet. Instead, you create a site-to-site connection to the hub. The traffic always goes through the hub gateway. This means that your VNets do not need their own virtual network gateway. Virtual WAN lets your VNets take advantage of scaling easily through the virtual hub and the virtual hub gateway.

- Hub virtual network connection: The Hub virtual network connection resource is used to connect the hub seamlessly to your virtual network.
- (Preview) Hub-to-Hub connection - Hubs are all connected to each other in a virtual WAN. This implies that a branch, user, or VNet connected to a local hub can communicate with another branch or VNet using the full mesh architecture of the connected hubs. You can also connect VNets within a hub transiting through the virtual hub, as well as VNets across hub, using the hub-to-hub connected framework.
- Hub route table: You can create a virtual hub route and apply the route to the virtual hub route table. You can apply multiple routes to the virtual hub route table.

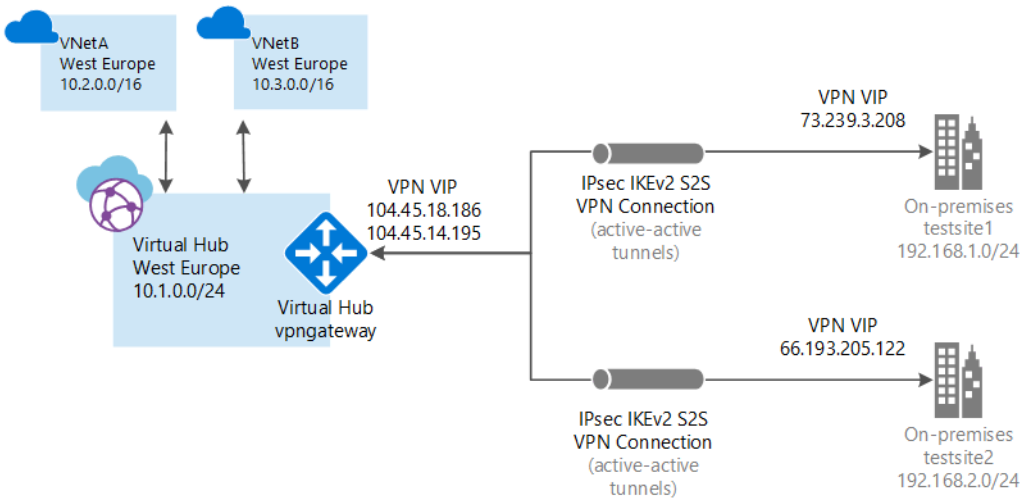
Additional Virtual WAN resources

- Site: This resource is used for site-to-site connections only. The site resource is vpnsite. It represents your on-premises VPN device and its settings. By working with a Virtual WAN partner, you have a built-in solution to automatically export this information to Azure.

Connectivity

Virtual WAN allows the following types of connectivity: Site-to-Site VPN, User VPN (Point-to-Site), and ExpressRoute.

Site-to-site VPN connections



When you create a virtual WAN site-to-site connection, you can work with an available partner. If you don't want to use a partner, you can configure the connection manually.

Virtual WAN partner workflow

When you work with a Virtual WAN partner, the workflow is:

1. The branch device (VPN/SDWAN) controller is authenticated to export site-centric information into Azure by using an Azure Service Principal.
2. The branch device (VPN/SDWAN) controller obtains the Azure connectivity configuration and updates the local device. This automates the configuration download, editing, and updating of the on-premises VPN device.
3. Once the device has the right Azure configuration, a site-to-site connection (two active tunnels) is established to the Azure WAN. Azure supports both IKEv1 and IKEv2. BGP is optional.

User VPN (point-to-site) connections

You can connect to your resources in Azure over an IPsec/IKE (IKEv2) or OpenVPN connection. This type of connection requires a VPN client to be configured on the client computer.

ExpressRoute connections

ExpressRoute lets you connect on-premises network to Azure over a private connection.

Online Lab - Configuring VNet Peering and Service Chaining

Lab Steps

Online Lab: Configuring VNet Peering and Service Chaining

NOTE: For the most recent version of this online lab, see: **https://github.com/MicrosoftLearning/AZ-300-MicrosoftAzureArchitectTechnologies**

Scenario

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

Objectives

After completing this lab, you will be able to:

- Deploy Azure VMs by using Azure Resource Manager templates.
- Configure VNet peering.
- Implement routing
- Validate service chaining

Lab Setup

Estimated Time: 45 minutes

User Name: **Student**

Password: **Pa55w.rd**

Exercise 1: Creating an Azure lab environment by using deployment templates

The main tasks for this exercise are as follows:

1. Create the first Azure virtual network environment by using an Azure Resource Manager template
2. Create the second Azure virtual network environment by using an Azure Resource Manager template

Task 1: Create the first Azure virtual network environment by using an Azure Resource Manager template

1. From the lab virtual machine, start Microsoft Edge and browse to the Azure portal at **http://portal.azure.com** and sign in by using the Microsoft account that has the Owner role in the target Azure subscription.
2. In the Azure portal, in the Microsoft Edge window, start a **Bash** session within the **Cloud Shell**.
3. If you are presented with the **You have no storage mounted** message, configure storage using the following settings:
   - Subsciption: the name of the target Azure subscription
   - Cloud Shell region: the name of the Azure region that is available in your subscription and which is closest to the lab location
   - Resource group: the name of a new resource group **az3000400-LabRG**
   - Storage account: a name of a new storage account
   - File share: a name of a new file share
4. From the Cloud Shell pane, create two resource groups by running (replace the `<Azure region>` placeholder with the name of the Azure region that is available in your subscription and which is closest to the lab location)

   ```
   az group create --resource-group az3000401-LabRG --location <Azure region>
   az group create --resource-group az3000402-LabRG --location <Azure region>
   ```

5. From the Cloud Shell pane, upload the first Azure Resource Manager template **\allfiles\AZ-300T02\Module_03\azuredeploy0401.json** into the home directory.
6. From the Cloud Shell pane, upload the parameter file **\allfiles\AZ-300T02\Module_03\azuredeploy04.parameters.json** into the home directory.
7. From the Cloud Shell pane, deploy the two Azure VMs hosting Windows Server 2016 Datacenter into the first virtual network by running:

   ```
   az group deployment create --resource-group az3000401-LabRG --template-file
   azuredeploy0401.json --parameters @azuredeploy04.parameters.json
   ```

   Note: Do not wait for the deployment to complete but proceed to the next task.

Task 2: Create the second Azure virtual network environment by using an Azure Resource Manager template

1. From the Cloud Shell pane, upload the second Azure Resource Manager template **\allfiles\AZ-300T02\Module_03\azuredeploy0402.json** into the home directory.

2. From the Cloud Shell pane, deploy an Azure VM hosting Windows Server 2016 Datacenter into the second virtual network by running:

```
az group deployment create --resource-group az3000402-LabRG --template-file
azuredeploy0402.json --parameters @azuredeploy04.parameters.json
```

Note: The second template uses the same parameter file.

Note: Do not wait for the deployment to complete but proceed to the next exercise.

Result: After completing this exercise, you should have created two Azure virtual networks hosting Azure VMs running Windows Server 2016 Datacenter.

Exercise 2: Configuring VNet peering

The main tasks for this exercise are as follows:

1. Configure VNet peering for the first virtual network
2. Configure VNet peering for the second virtual network

Task 1: Configure VNet peering for the first virtual network

1. In the Microsoft Edge window displaying the Azure portal, navigate to the **az3000401-vnet** virtual network blade.
2. From the **az3000401-vnet** blade, create a VNet peering with the following settings:
   - Name: **az3000401-vnet-to-az3000402-vnet**
   - Virtual network deployment model: **Resource manager**
   - Subscription: the name of the Azure subscription you are using for this lab
   - Virtual network: **az3000402-vnet**
   - Allow virtual network access: **Enabled**
   - Allow forwarded traffic: disabled
   - Allow gateway transit: disabled
   - Use remote gateways: disabled

Task 2: Configure VNet peering for the second virtual network

1. In Microsoft Edge, navigate to the **az3000402-vnet** virtual network blade.

2. From the **az3000402-vnet** blade, create a VNet peering with the following settings:
   - Name: **az3000402-vnet-to-az3000401-vnet**
   - Virtual network deployment model: **Resource manager**
   - Subscription: the name of the Azure subscription you are using for this lab
   - Virtual network: **az3000401-vnet**
   - Allow virtual network access: **Enabled**
   - Allow forwarded traffic: disabled
   - Allow gateway transit: disabled
   - Use remote gateways: disabled

   Result: After completing this exercise, you should have configured VNet peering between two virtual networks.

Exercise 3: Implementing routing

The main tasks for this exercise are as follows:

1. Enable IP forwarding
2. Configure user defined routing
3. Configure routing on an Azure VM running Windows Server 2016

Task 1: Enable IP forwarding

1. In Microsoft Edge, navigate to the **az3000401-nic2** blade (the NIC of **az3000401-vm2**)
2. On the **az3000401-nic2** blade, modify the **IP configurations** by setting **IP forwarding** to **Enabled**.

Task 2: Configure user defined routing

1. In the Azure portal, create a new route table with the following settings:
   - Name: **az3000402-rt1**
   - Subscription: the name of the Azure subscription you use for this lab
   - Resource group: **az3000402-LabRG**
   - Location: the same Azure region in which you created the virtual networks
   - BGP route propagation: **Disabled**
2. In the Azure portal, add to the route table a route with the following settings:
   - Route name: **custom-route-to-az3000401-vnet**

- Address prefix: **10.0.0.0/22**
- Next hop type: **Virtual appliance**
- Next hop address: **10.0.1.4**

3. In the Azure portal, associate the route table with the **subnet-1** of the **az3000402-vnet**.

Task 3: Configure routing on an Azure VM running Windows Server 2016

1. On MIA-CL1, from the Azure portal, start a Remote Desktop session to **az3000401-vm2** Azure VM.
2. When prompted to authenticate, specify the following credentials:
   - User name: **Student**
   - Password: **Pa55w.rd1234**
3. Once you are connected to az3000401-vm2 via the Remote Desktop session, from **Server Manager**, install the **Remote Access** server role with the **Routing** role service and all required features.
4. In the Remote Desktop session to az3000401-vm2, start the **Routing and Remote Access** console.
5. In the **Routing and Remote Access** console, run **Routing and Remote Access Server Setup Wizard** and enable **LAN routing**.
6. Start **Routing and Remote Access** service.
7. In the Remote Desktop session to az3000401-vm2, start the **Windows Firewall with Advanced Security** console and enable **File and Printer Sharing (Echo Request - ICMPv4-In)** inbound rule for all profiles.

   Result: After completing this exercise, you should have configured custom routing within the second virtual network.

Exercise 4: Validating service chaining

The main tasks for this exercise are as follows:

1. Configure Windows Firewall with Advanced Security on an Azure VM
2. Test service chaining between peered virtual networks

Task 1: Configure Windows Firewall with Advanced Security on the target Azure VM

1. On MIA-CL1, from the Azure portal, start a Remote Desktop session to **az3000401-vm1** Azure VM.

2. When prompted to authenticate, specify the following credentials:
   - User name: **Student**
   - Password: **Pa55w.rd1234**
3. In the Remote Desktop session to az3000401-vm1, start the **Windows Firewall with Advanced Security** console and enable **File and Printer Sharing (Echo Request - ICMPv4-In)** inbound rule for all profiles.

Task 2: Test service chaining between peered virtual networks

1. On MIA-CL1, from the Azure portal, start a Remote Desktop session to **az3000402-vm1** Azure VM.
2. When prompted to authenticate, specify the following credentials:
   - User name: **Student**
   - Password: **Pa55w.rd1234**
3. Once you are connected to az3000402-vm1 via the Remote Desktop session, start **Windows PowerShell**.
4. In the **Windows PowerShell** window, run the following:

   ```
   Test-NetConnection -ComputerName 10.0.0.4 -TraceRoute
   ```

5. Verify that test is successful and note that the connection was routed over 10.0.1.4

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

Review Questions

Module 3 Review Questions

Load Balancer SKUs

You manage an application which uses SQL Server for data storage. Instances of the application that connect to SQL Server vary with respect to their compute needs.

You need ensure the SQL Server instance is load-balanced to optimize performance.

What load balancing options are available? What should you consider before you implement load balancing?

Suggested Answer
When you create an Azure Load Balancer you will select for the type (Internal or Public) of load balancer. You will also select the SKU. The load balancer supports both Basic and Standard SKUs, each differing in scenario scale, features, and pricing. The Standard Load Balancer is the newer Load Balancer product with an expanded and more granular feature set over Basic Load Balancer. It is a superset of Basic Load Balancer.

Load Balancer SKUs

You manage an online training platform that provides consumers with online videos and text-based content. Videos files are often very large.

You must place video content geographically close to customers.

You need to recommend a load-balancing solution that redirects user video requests to the closest CDN.

Which should you recommend and why?

Suggested Answer
Implement a solution that uses Azure Traffic Manager: It provides DNS-based routing to redirect end user traffic to globally distributed end points.

On Demand Capacity

A company is expanding rapidly to new geographical locations. You need to ensure that the company can quickly provide infrastructure and services for new remote offices.

How can you provide access to on-premises services from Azure? What other scenarios should you consider?

Suggested Answer
There are many scenarios where Site-to-Site connections can be useful. Here are a few.

- **Capacity On-Demand**

Azure provides capacity on demand. By creating a connection to Azure, more storage or compute resources can easily be brought online.

- **Strategic Migration**

There are many strategic reasons for moving to Azure. Organizations whose core purpose is not related to managing complex datacenter deployments, may want to shed competing interests and focus on improving their core business. They may also want to reduce costs by moving to a pay as you go model.

- **Disaster Recovery**

The cloud offers an efficient, cost effective choice for data backup and recovery. Most cloud platforms let you run third-party software for backup and disaster recovery, but with Microsoft these services are fully integrated and easy to turn on, which means you do not have to install and manage a separate product in the cloud.

Module 4 Determining Azure Workload Requirements

Overview of Customer Case Study

Customer Situation

Contoso is a US-based financial company based in Boston. There are three additional local branches across the United States. The main datacenter is connected to the internet with a fiber metro Ethernet connection (500 Mbps). Each branch is connected locally to the Internet using business class connections using IPSec VPN tunnels back to the main datacenter. This allows the entire network to be permanently connected and optimizes internet connectivity.

Contoso has one main datacenter in its primary location. The main datacenter is fully virtualized with VMware. Contoso has 100 ESXi 6.5 virtualization hosts, managed by vCenter Server 6.5.

Contoso uses Active Directory for identity management, and DNS servers on the internal network. The domain controllers in the datacenter run on VMware VMs. The domain controllers at local branches run on physical servers.

Contoso plans to migrate majority of its workloads to Azure. Contoso's IT leadership team has worked closely with the company's business partners to understand what the business wants to achieve with this migration:

- **Address business growth:** Contoso is growing. As a result, pressure has increased on the company's on-premises systems and infrastructure.
- **Increase efficiency:** Contoso needs to remove unnecessary procedures and streamline processes for its developers and users. The business needs IT to be fast and to not waste time or money, so the company can deliver faster on customer requirements.
- **Increase agility:** Contoso IT needs to be more responsive to the needs of the business. It must be able to react faster than the changes that occur in the marketplace for the company to be successful in a global economy. IT at Contoso must not get in the way or become a business blocker.
- **Scale:** As the company's business grows successfully, Contoso IT must provide systems that can grow at the same pace.

As Contoso considers migrating to Azure, the company wants to run a technical and financial assessment to determine whether its on-premises workloads are suitable for migration to the cloud. In particular, the Contoso team wants to assess machine and database compatibility for migration. It wants to estimate capacity and costs for running Contoso's resources in Azure. Contoso team is also interested in leveraging the company's Software Assurance contract in order to minimize costs when running migrated workloads in Azure.

The company will assess migration scenarios that rehost and refactor the apps.

To get started and to better understand the technologies involved, Contoso plans to assess two of its on-premises apps, summarized in the following table.

App name	Platform	App tiers
SmartHotel360 (manages Contoso travel requirements)	Windows Server 2008 R2 with a SQL Server 2008 R2 database	Two-tiered app. The front-end ASP.NET website runs on one VM (WEBVM) and the SQL Server runs on another VM (SQLVM).
osTicket (Contoso service desk app, tracking issues for internal employees and external customers)	Linux Ubuntu 16.04 LTS, Apache 2, and MySQL 5.7 with MySQL PHP 7.0 (LAMP)	Two-tiered app. A front-end PHP website runs on one VM (OSTICKETWEB) and the MySQL database runs on another VM (OSTICKETMYSQL).

Assessment Goals

1. After migration, apps in Azure should have the same performance capabilities that they have today in Contoso's on-premises VMWare environment. Moving to the cloud does not mean that app performance is less critical.
2. Contoso needs to understand the compatibility of its applications and databases with Azure requirements. Contoso also needs to understand its hosting options in Azure.
3. Contoso's database administration should be minimized after apps move to the cloud. At the same time, Contoso would like to minimize impact of any potential compatibility issues of its SQL Server-based workloads.
4. Contoso wants to understand not only its migration options, but also the costs associated with the infrastructure after it moves to the cloud.

Assessment Tools

Contoso will use Microsoft tools for its migration assessment. The tools align with the company's goals and should provide Contoso with all the information it needs.

Technology	Description	Cost
Data Migration Assistant	Contoso will use Data Migration Assistant to assess and detect compatibility issues that might affect its database functionality in Azure. Data Migration Assistant assesses feature parity between SQL sources and targets. It recommends performance and reliability improvements.	Data Migration Assistant is a free, downloadable tool.
Azure Migrate	Contoso will use the Azure Migrate service to assess its VMware VMs. Azure Migrate assesses the migration suitability of the machines. It provides sizing and cost estimates for running in Azure.	As of May 2018, Azure Migrate is a free service.
Service Map	Azure Migrate will use Service Map to show dependencies between machines that the company wants to migrate.	Service Map is part of Azure Log Analytics. Currently, Contoso can use Service Map for 180 days without incurring charges.

Assessment Architecture

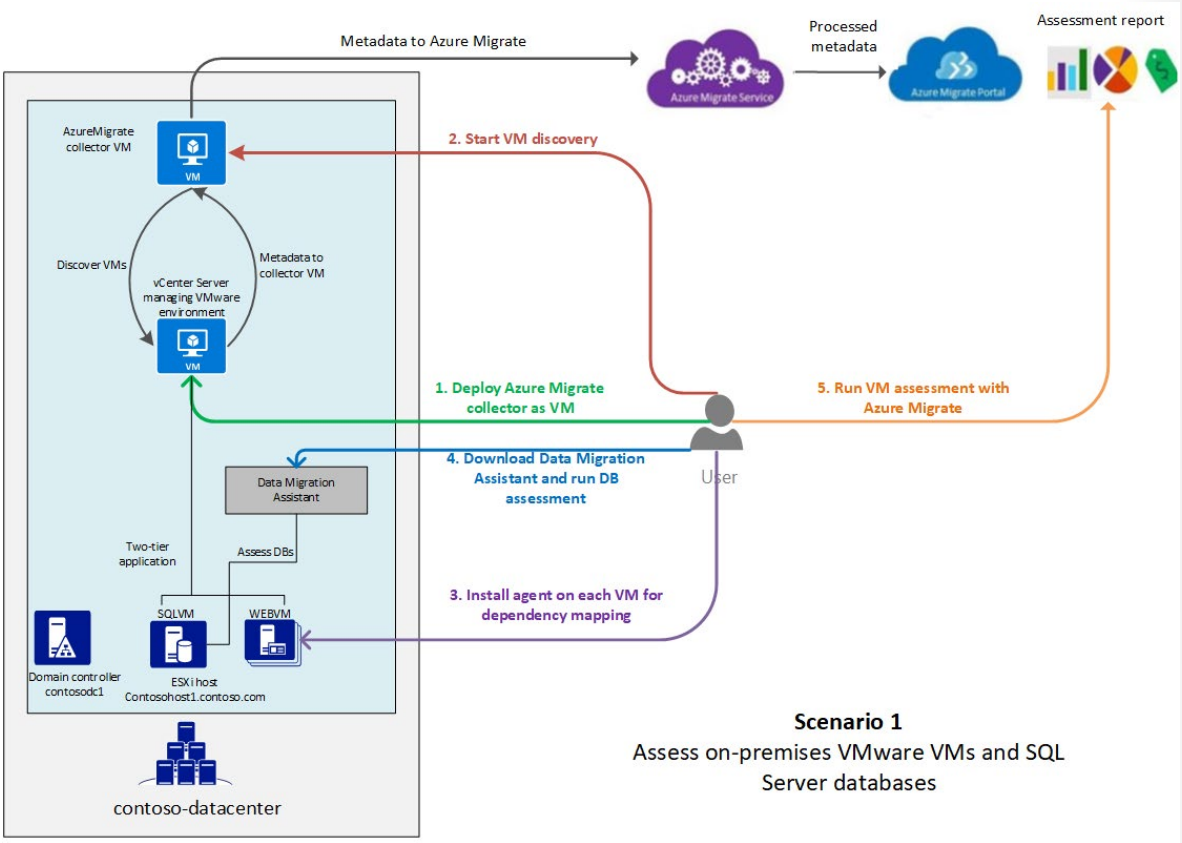
Contoso has an on-premises datacenter (contoso-datacenter) and on-premises domain controllers (CONTOSODC1, CONTOSODC2). VMware ESXi 6.5 hosts include contosohost1 and contosohost2. The VMware environment is managed by vCenter Server 6.5, running on the vcenter.contoso.com VM.

The SmartHotel360 travel app has these characteristics:

- The app is tiered across two VMware VMs (WEBVM and SQLVM).
- The VMs are located on VMware ESXi host contosohost1.contoso.com.
- The VMs are running Windows Server 2008 R2 Datacenter with SP1.

The osTicket service desk app has the following characteristics:

- The app is tiered across two VMs (OSTICKETWEB and OSTICKETMYSQL).
- The VMs are running Ubuntu Linux Server 16.04-LTS.
- OSTICKETWEB is running Apache 2 and PHP 7.0.
- OSTICKETMYSQL is running MySQL 5.7.22.



Prerequisites

Contoso must ensure that the following requirements are in place in order to perform an assessment:

- An Azure subscription and either a Microsoft account (MSA) or "Work or School" account with the Owner or Contributor role in the subscription.
- An on-premises vCenter Server instance running version 6.5, 6.0, or 5.5.
- A read-only account in vCenter Server, or permissions to create one.
- Permissions to create a VM on the vCenter Server instance by using an .ova template.
- At least one ESXi host running version 5.0 or later.
- At least two on-premises VMware VMs, one running a SQL Server database.
- Permissions to install Azure Migrate agents on each ESXi VM.
- Direct connectivity from ESXi VMs to internet. If ESXi VMs do not have direct internet connectivity, Contoso will need to deploy Azure Log Analytics Gateway and redirect agent traffic through it.
- Connectivity to the SQL Server instance running on the ESXi VM, for database assessment.

Assessment Overview

The assessment consists of the following steps:

- Downloading and installing Data Migration Assistant: a Contoso IT technician prepares Data Migration Assistant for assessment of the on-premises SQL Server database.
- Generating the database assessment by using Data Migration Assistant: the Contoso IT technician runs the database assessment.
- Reviewing the database assessment by using Data Migration Assistant: the Contoso IT technician reviews the database assessment.
- Preparing for VM assessment by using Azure Migrate: the Contoso IT technician sets up on-premises accounts and adjusts VMware settings.
- Discovering on-premises VMs by using Azure Migrate: the Contoso IT technician creates an Azure Migrate collector VM. Then, the Contoso IT technician runs the collector to discover VMs for assessment.
- Preparing for dependency analysis by using Azure Migrate: the Contoso IT technician installs Azure Migrate agents on the VMs, so the company can see dependency mapping between VMs.
- Reviewing the VM assessment by using Azure Migrate: the Contoso IT technician checks dependencies, groups the VMs, and runs the assessment. When the assessment is ready, the Contoso IT technician analyzes the assessment in preparation for migration.

Primary References

Migration Strategies

Strategies for migration to the cloud fall into four broad categories: rehost, refactor, rearchitect, or rebuild. The strategy you adopt depends upon your business drivers, and migration goals. You might

adopt multiple strategies. For example, you could choose to rehost (lift-and-shift) simple apps, or apps that are not critical to your business, but rearchitect those that are more complex and business-critical.

Strategy	Definition	When to use
Rehost	Often referred to as a "lift-and-shift" migration. This option doesn't require code changes, and lets you migrate your existing apps to Azure quickly. Each app is migrated as is, to reap the benefits of the cloud, without the risk and cost associated with code changes.	When you need to move apps quickly to the cloud. When you want to move an app without modifying it. When your apps are architected so that they can leverage Azure IaaS scalability after migration. When apps are important to your business, but you don't need immediate changes to app capabilities.
Refactor	Often referred to as "repackaging," refactoring requires minimal changes to apps, so that they can connect to Azure PaaS, and use cloud offerings. For example, you could migrate existing apps to Azure App Service or Azure Kubernetes Service (AKS). Or, you could refactor relational and non-relational databases into options such as Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB.	If your app can easily be repackaged to work in Azure. If you want to apply innovative DevOps practices provided by Azure, or you are thinking about DevOps using a container strategy for workloads. For refactoring, you need to think about the portability of your existing code base, and available development skills.
Rearchitect	Rearchitecting for migration focuses on modifying and extending app functionality and the code base to optimize the app architecture for cloud scalability. For example, you could break down a monolithic application into a group of microservices that work together and scale easily. Or, you could rearchitect relational and non-relational databases to a fully managed DBaaS solutions, such as Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB.	When your apps need major revisions to incorporate new capabilities, or to work effectively on a cloud platform. When you want to use existing application investments, meet scalability requirements, apply innovative Azure DevOps practices, and minimize use of virtual machines.
Rebuild	Rebuild takes things a step further by rebuilding an app from scratch using Azure cloud technologies. For example, you could build green field apps with cloud-native technologies like Azure Functions, Azure AI, Azure SQL Database Managed Instance, and Azure Cosmos DB.	When you want rapid development, and existing apps have limited functionality and lifespan. When you're ready to expedite business innovation (including DevOps practices provided by Azure), build new applications using cloud-native technologies, and take advantage of advancements in AI, Blockchain, and IoT.

Step-by-Step: Determining Azure Workload Requirements

Step 1: Downloading and Installing Data Migration Assistant

- The Contoso IT technician downloads Data Migration Assistant from the Microsoft Download Center. Data Migration Assistant can be installed on any machine with direct connectivity to the SQL Server instance. Contoso Data Migration Assistant should not be run on the SQL Server host machine.
- The Contoso IT technician runs the downloaded setup file (DownloadMigrationAssistant.msi) to begin the installation.
- On the Finish** page, the Contoso IT technician selects Launch Microsoft Data Migration Assistant** before finishing the wizard.

Get Data Migration Assistant[1]

To install DMA, download the latest version of the tool from the **Microsoft Download Center**[2], and then run the **DataMigrationAssistant.msi** file.

Capabilities[3]

- Assess on-premises SQL Server instance(s) migrating to Azure SQL database(s). The assessment workflow helps you to detect the following issues that can affect Azure SQL database migration and provides detailed guidance on how to resolve them.
  - Migration blocking issues: Discovers the compatibility issues that block migrating on-premises SQL Server database(s) to Azure SQL Database(s). DMA provides recommendations to help you address those issues.
  - Partially supported or unsupported features: Detects partially supported or unsupported features that are currently in use on the source SQL Server instance. DMA provides a comprehensive set of recommendations, alternative approaches available in Azure, and mitigating steps so that you can incorporate them into your migration projects.
- Discover issues that can affect an upgrade to an on-premises SQL Server. These are described as compatibility issues and are organized in the following categories:
  - Breaking changes
  - Behavior changes
  - Deprecated features
- Discover new features in the target SQL Server platform that the database can benefit from after an upgrade. These are described as feature recommendations and are organized in the following categories:
  - Performance
  - Security

1 https://docs.microsoft.com/en-us/sql/dma/dma-overview?view=sql-server-2017#get-data-migration-assistant
2 https://www.microsoft.com/download/details.aspx?id=53595
3 https://docs.microsoft.com/en-us/sql/dma/dma-overview?view=sql-server-2017#capabilities

    - Storage
- Migrate an on-premises SQL Server instance to a modern SQL Server instance hosted on-premises or on an Azure virtual machine (VM) that is accessible from your on-premises network. The Azure VM can be accessed using VPN or other technologies. The migration workflow helps you to migrate the following components:
    - Schema of databases
    - Data and users
    - Server roles
    - SQL Server and Windows logins
- After a successful migration, applications can connect to the target SQL Server databases seamlessly.

Prerequisites[4]

To run an assessment, you have to be a member of the SQL Server **sysadmin** role.

Supported source and target versions[5]

DMA replaces all previous versions of SQL Server Upgrade Advisor and should be used for upgrades for most SQL Server versions. Supported source and target versions are:

Sources

- SQL Server 2005
- SQL Server 2008
- SQL Server 2008 R2
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017 on Windows

Targets

- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017 on Windows and Linux
- Azure SQL Database
- Azure SQL Database Managed Instance

4 https://docs.microsoft.com/en-us/sql/dma/dma-overview?view=sql-server-2017#prerequisites
5 https://docs.microsoft.com/en-us/sql/dma/dma-overview?view=sql-server-2017#supported-source-and-target-versions

Step 2: Generating the Database Assessment for SmartHotel360

The Contoso IT technician must run assessment of the on-premises SQL Server database for the SmartHotel360 app.

In Data Migration Assistant, the Contoso IT technician selects New > Assessment, and then gives the assessment a project name.

- For Source server type, the Contoso IT technician selects SQL Server on Azure Virtual Machines.

Note: Currently, Data Migration Assistant does not support assessment for migrating to an Azure SQL Database Managed Instance. As a workaround, the Contoso IT technician uses SQL Server on an Azure VM as the supposed target for the assessment.

By selecting Azure SQL Database Managed Instance as target for migrating its on-premises SQL Server database, Contoso considerably minimizes potential for any compatibility issues during migration. Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, Managed Instance preserves all PaaS capabilities, such as automatic patching and version updates, automated backups, and high-availability, effectively drastically reducing management overhead and TCO.

- In Select Target Version, the Contoso IT technician selects SQL Server 2017 as the target version. The Contoso IT technician needs to select this version because this is the version used by SQL Database Managed Instance.
- The Contoso IT technician selects reports to help discover information about compatibility and new features:

Compatibility Issues note changes that might break migration or that require a minor adjustment before migration. This report keeps the Contoso IT technician informed about any features currently in use that are deprecated. Issues are organized by compatibility level.

New features' recommendation notes new features in the target SQL Server platform that can be used for the database after migration. New feature recommendations are organized under the headings Performance, Security, and Storage.

- In Connect to a server, the Contoso IT technician enters the name of the VM running the database and credentials to access it. The Contoso IT technician selects Trust server certificate to make sure the VM can access SQL Server. Then, the Contoso IT technician selects Connect.
- In Add source, the Contoso IT technician adds the database it wants to assess, and then selects Next to start the assessment.
- The assessment is created.

Step 3: Reviewing the Database Assessment for SmartHotel360

The Contoso IT technician must review the assessment to determine the viability of migrating its on-premises SQL Server database for the SmartHotel360 app.

In **Review Results**, the Contoso IT technician views the assessment results.

Results are displayed as soon as they are available. If any discovered issues are resolved, the Contoso IT technician must select **Restart Assessment** to rerun the assessment.

In the **Compatibility issues** report, the Contoso IT technician checks for any issues at each compatibility level. Compatibility levels map to SQL Server versions as follows:

- 100: SQL Server 2008/Azure SQL Database
- 110: SQL Server 2012/Azure SQL Database
- 120: SQL Server 2014/Azure SQL Database
- 130: SQL Server 2016/Azure SQL Database
- 140: SQL Server 2017/Azure SQL Database

In the **Feature recommendations** report, the Contoso IT technician views performance, security, and storage features that the assessment recommends after migration. A variety of features are recommended, including In-Memory OLTP, columnstore indexes, Stretch Database, Always Encrypted, dynamic data masking, and transparent data encryption.

- Note: The Contoso IT technician should enable transparent data encryption for all SQL Server databases. This is even more critical when a database is in the cloud than when it is hosted on-premises. Transparent data encryption should be enabled only after migration. If transparent data encryption is already enabled, the Contoso IT technician must move the certificate or asymmetric key to the master database of the target server.
- The Contoso IT technician can export the assessment in JSON or CSV format.
- Note: For large-scale assessments:
- Run multiple assessments concurrently and view the state of the assessments on the **All Assessments** page.
- Consolidate assessments into a **SQL Server database**.
- Consolidate assessments into a **Power BI report**.

Step 4: Preparing for VM assessment by using Azure Migrate

The Contoso IT technician needs to create a VMware account that Azure Migrate can use to automatically discover VMs for assessment, verify rights to create a VM, note the ports that need to be opened, and assign the statistics settings level.

- Setting up a VMware account: VM discovery requires a read-only account in vCenter Server that has the following properties:

User type: At least a read-only user.

Permissions: For the datacenter object, the Propagate to Child Objects checkbox must be selected. For Role, Read-only must be selected.

Details: The user is assigned at the datacenter level, with access to all objects in the datacenter.

To restrict access, the No access role with the Propagate to child object to the child objects (vSphere hosts, datastores, VMs, and networks) setting must be assigned

- Verifying permissions to create a VM: the Contoso IT technician verifies that it has permissions to create a VM by importing a file in .ova format.
- Verifying ports: the Contoso assessment uses dependency mapping. Dependency mapping requires an agent to be installed on VMs that will be assessed. The agent must be able to connect to Azure from TCP port 443 on each VM.

- Assigning the statistics settings level: before the deployment begins, the Contoso IT technician must set the statistics settings for the vCenter Server to level 3.

Note: After setting the level, the Contoso IT technician must wait at least a day before running the assessment. Otherwise, the assessment might not work as expected. If the level is higher than 3, the assessment works, but:

Performance data for disks and networking is not collected.

For storage, Azure Migrate recommends a standard disk in Azure, with the same size as the on-premises disk.

For networking, for each on-premises network adapter, a network adapter is recommended in Azure.

For compute, Azure Migrate looks at the VM cores and memory size and recommends an Azure VM with the same configuration. If there are multiple eligible Azure VM sizes, the one with the lowest cost is recommended.

To set the level:

In the vSphere Web Client, the Contoso IT technician opens the vCenter Server instance.

The Contoso IT technician selects Manage > Settings > General > Edit.

In Statistics, the Contoso IT technician sets the statistic level settings to Level 3.

Step 5: Discovering on-premises VMs by using Azure Migrate

To discover VMs, the Contoso IT technician creates an Azure Migrate project. The Contoso IT technician downloads and sets up the collector VM. Then, the Contoso IT technician runs the collector to discover its on-premises VMs.

Creating a project

- In the Azure portal, the Contoso IT technician searches for **Azure Migrate**. Then, the Contoso IT technician creates a project.
- The Contoso IT technician specifies a project name (**ContosoMigration**) and the Azure subscription, as well as creates a new Azure resource group (**ContosoFailoverRG**).
- Note:

You can create an Azure Migrate project in any of these geographies:

Geography	Storage location region
Asia	Southeast Asia or East Asia
Europe	North Europe or West Europe
Japan	Japan East or Japan West
United Kingdom	UK South or UK West
United States	Central US or West US 2
Canada	Canada Central
India	India Central or India South
Australia	Australia SouthEast

You can plan a migration for any target location.

The project location is used only to store the metadata that's gathered from on-premises VMs.

Downloading the collector appliance: Azure Migrate creates an on-premises VM known as the collector appliance. The VM discovers on-premises VMware VMs and sends metadata about the VMs to the Azure Migrate service. To set up the collector appliance, the Contoso IT technician downloads an OVA template, and then imports it to the on-premises vCenter Server instance to create the VM.

- In the Azure Migrate project, the Contoso IT technician selects **Getting Started > Discover & Assess > Discover Machines**. The Contoso IT technician downloads the OVA template file.
- Contoso copies the project ID and key. The project and ID are required for configuring the collector.

Verifying the collector appliance: before deploying the VM, the Contoso IT technician checks that the OVA file is secure:

- On the machine on which the file was downloaded, the Contoso IT technician opens an administrator Command Prompt window.
- Contoso runs the following command to generate the hash for the OVA file:
- C:>CertUtil -HashFile <file_location> [Hashing Algorithm]
- For example:
- C:>CertUtil -HashFile C:\AzureMigrate\AzureMigrate.ova SHA256
- The generated hash should match these settings (version 1.0.9.15):

Algorithm	Hash value
MD5	e9ef16b0c837638c506b5fc0ef75ebfa
SHA1	37b4b1e92b3c6ac2782ff5258450df6686c89864
SHA256	8a86fc17f69b69968eb20a5c4c288c194cdcffb4ee-6568d85ae5ba96835559ba

Creating the collector appliance: now, the Contoso IT technician can import the downloaded file to the vCenter Server instance and provision the collector appliance VM:

- In the vSphere Client console, the Contoso IT technician selects **File > Deploy OVF Template**.
- In the Deploy OVF Template Wizard, the Contoso IT technician selects **Source**, and then specifies the location of the OVA file.
- In **Name and Location**, the Contoso IT technician specifies a display name for the collector VM. Then, it selects the inventory location in which to host the VM. The Contoso IT technician also specifies the host or cluster on which to run the collector appliance.
- In **Storage**, the Contoso IT technician specifies the storage location. In **Disk Format**, the Contoso IT technician selects how it wants to provision the storage.
- In **Network Mapping**, the Contoso IT technician specifies the network in which to connect the collector VM. The network needs internet connectivity to send metadata to Azure.
- Contoso reviews the settings, and then selects **Power on after deployment > Finish**. A message that confirms successful completion appears when the appliance is created.

Runing the collector to discover VMs: now, the Contoso IT technician runs the collector to discover VMs. Currently, the collector currently supports only **English (United States)** as the operating system language and collector interface language.

- In the vSphere Client console, the Contoso IT technician selects **Open Console**. The Contoso IT technician specifies the language, time zone, and password preferences for the collector VM.
- On the desktop, the Contoso IT technician selects the **Run collector** shortcut.
- In Azure Migrate Collector, the Contoso IT technician selects **Set up prerequisites**. The Contoso IT technician accepts the license terms and reads the third-party information.
- The collector checks that the VM has internet access, that the time is synced, and that the collector service is running. (The collector service is installed by default on the VM.) the Contoso IT technician also installs VMware PowerCLI.

Note: it is assumed that the VM has direct access to the internet without using a proxy.

- In Specify vCenter Server details, the Contoso IT technician enters the name (FQDN) or IP address of the vCenter Server instance and the read-only credentials used for discovery.
- Contoso selects a scope for VM discovery. The collector can discover only VMs that are within the specified scope. The scope can be set to a specific folder, datacenter, or cluster. The scope shouldn't contain more than 1,500 VMs.
- In Specify migration project, the Contoso IT technician enters the Azure Migrate project ID and key that were copied from the portal. To get the project ID and key, the Contoso IT technician can go to the project Overview page > Discover Machines.
- In View collection progress, the Contoso IT technician can monitor discovery and check that metadata collected from the VMs is in scope. The collector provides an approximate discovery time.

Verifying VMs in the portal: when collection is finished, the Contoso IT technician checks that the VMs appear in the portal:

- In the Azure Migrate project, the Contoso IT technician selects **Manage > Machines**. The Contoso IT technician checks that the VMs that it wants to discover are shown.
- Currently, the machines don't have the Azure Migrate agents installed. Contoso must install the agents to view dependencies.

Step 6: Preparing for Dependency Analysis

To view dependencies between VMs that it wants to assess, the Contoso IT technician downloads and installs agents on the app VMs. The Contoso IT technician installs agents on all VMs for its apps, both for Windows and Linux.

Taking a snapshot: to keep a copy of the VMs before modifying them, the Contoso IT technician takes a snapshot before the agents are installed.

Downloading and installing the VM agents

- In Machines, the Contoso IT technician selects the machine. In the Dependencies column, the Contoso IT technician selects Requires installation.
- In the Discover Machines pane, the Contoso IT technician:

Downloads the Microsoft Monitoring Agent (MMA) and Dependency Agent for each Windows VM.

Downloads the MMA and Dependency Agent for each Linux VM.

- The Contoso IT technician copies the workspace ID and key. The Contoso IT technician needs the workspace ID and key when it installs the MMA.

- Installing the agents on Windows VMs

The Contoso IT technician runs the installation on each VM.

- Installing the MMA on Windows VMs

The Contoso IT technician double-clicks the downloaded agent.

In Destination Folder, the Contoso IT technician keeps the default installation folder, and then selects Next.

In Agent Setup Options, the Contoso IT technician selects Connect the agent to Azure Log Analytics > Next.

In Azure Log Analytics, the Contoso IT technician pastes the workspace ID and key that it copied from the portal.

In Ready to Install, the Contoso IT technician installs the MMA.

- Installing the Dependency agent on Windows VMs

The Contoso IT technician double-clicks the downloaded Dependency Agent.

The Contoso IT technician accepts the license terms and waits for the installation to finish.

- Installing the agents on Linux VMs

The Contoso IT technician runs the installation on each VM.

- Install the MMA on Linux VMs

The Contoso IT technician installs the Python ctypes library on each VM by using the following command:

sudo apt-get install python-ctypeslib

The Contoso IT technician must run the command to install the MMA agent as root. To become root, the Contoso IT technician runs the following command, and then enters the root password:

sudo -i

The Contoso IT technician installs the MMA:

The Contoso IT technician enters the workspace ID and key in the command.

Commands are for 64-bit.

The workspace ID and primary key are located in the Log Analytics workspace in the Azure portal. Select Settings, and then select the Connected Sources tab.

Run the following commands to download the Log Analytics agent, validate the checksum, and install and onboard the agent:

wget https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/scripts/onboard_agent.sh && sh onboard_agent.sh -w 6b7fcaff-7efb-4356-ae06-516cacf5e25d -s k7gAMAw5Bk8pFVUTZK-mk2lG4eUciswzWfYLDTxGcD8pcyc4oT8c6ZRgsMy3MmsQSHuSOcmBUsCjoRiG2x9A8Mg==

- Installing the Dependency Agent on Linux VMs

After the MMA is installed, the Contoso IT technician installs the Dependency Agent on the Linux VMs:

The Dependency Agent is installed on Linux computers by using InstallDependencyAgent-Linux64.bin, a shell script that has a self-extracting binary. The Contoso IT technician runs the file by using sh, or it adds execute permissions to the file itself.

The Contoso IT technician installs the Linux Dependency Agent as root:

wget –content-disposition https://aka.ms/dependencyagentlinux -O InstallDependencyAgent-Linux64.bin && sudo sh InstallDependencyAgent-Linux64.bin –s

Step 7: Running and Analyzing the VM Assessment

- The Contoso IT technician can now verify machine dependencies and create a group. Then, it runs the assessment for the group.
- Verifying dependencies and creating a group

To determine which machines to analyze, the Contoso IT technician selects View Dependencies.

For SQLVM, the dependency map shows the following details:

Process groups or processes that have active network connections running on SQLVM during the specified time period (an hour, by default).

Inbound (client) and outbound (server) TCP connections to and from all dependent machines.

Dependent machines that have the Azure Migrate agents installed are shown as separate boxes.

Machines that don't have the agents installed show port and IP address information.

For machines that have the agent installed (WEBVM), the Contoso IT technician selects the machine box to view more information. The information includes the FQDN, operating system, and MAC address.

The Contoso IT technician selects the VMs to add to the group (SQLVM and WEBVM). The Contoso IT technician uses Ctrl+Click to select multiple VMs.

The Contoso IT technician selects Create Group, and then enters a name (smarthotelapp).

Note: to view more granular dependencies, you can expand the time range. You can select a specific duration or select start and end dates.

- Running an assessment

In Groups, the Contoso IT technician opens the group (smarthotelapp), and then selects Create assessment.

To view the assessment, the Contoso IT technician selects Manage > Assessments.

The Contoso IT technician uses the default assessment settings, but you can customize settings.

- Analyzing the VM assessment

An Azure Migrate assessment includes information about the compatibility of on-premises with Azure, suggested right-sizing for Azure VM, and estimated monthly Azure costs.

- Reviewing confidence rating

An assessment has a confidence rating of from 1 star to 5 stars (1 star is the lowest and 5 stars is the highest).

The confidence rating is assigned to an assessment based on the availability of data points that are needed to compute the assessment.

The rating helps you estimate the reliability of the size recommendations that are provided by Azure Migrate.

The confidence rating is useful when you are doing performance-based sizing. Azure Migrate might not have enough data points for utilization-based sizing. For as on-premises sizing, the confidence rating is always 5 stars because Azure Migrate has all the data points it needs to size the VM.

Depending on the percentage of data points available, the confidence rating for the assessment is provided:

Availability of data points	Confidence rating
0%-20%	1 star
21%-40%	2 stars
41%-60%	3 stars
61%-80%	4 stars
81%-100%	5 stars

- Verifying Azure readiness

The assessment report shows the information that's summarized in the table. To show performance-based sizing, Azure Migrate needs the following information. If the information can't be collected, sizing assessment might not be accurate.

Utilization data for CPU and memory.

Read/write IOPS and throughput for each disk attached to the VM.

Network in/out information for each network adapter attached to the VM.

Setting	Indication	Details
Azure VM readiness	Indicates whether the VM is ready for migration.	Possible states: - Ready for Azure - Ready with conditions - Not ready for Azure - Readiness unknown If a VM is not ready, Azure Migrate shows some remediation steps.
Azure VM size	For ready VMs, Azure Migrate provides an Azure VM size recommendation	Sizing recommendation depends on assessment properties: - If you used performance-based sizing, sizing considers the performance history of the VMs. - If you used as on-premises, sizing is based on the on-premises VM size and utilization data is not used.
Suggested tool	Because Azure machines are running the agents, Azure Migrate looks at the processes that are running inside the machine. It identifies whether the machine is a database machine.	
VM information	The report shows settings for the on-premises VM, including operating system, boot type, and disk and storage information.	

- Reviewing monthly cost estimates

This view shows the total compute and storage cost of running the VMs in Azure. It also shows details for each machine.

Cost estimates are calculated by using the size recommendations for a machine.

Estimated monthly costs for compute and storage are aggregated for all VMs in the group.

Step 8: Cleaning up After Assessment

- When the assessment finishes, the Contoso IT technician retains the Azure Migrate appliance to use in future evaluations.
- The Contoso IT technician turns off the VMware VM. The Contoso IT technician will use it again when it evaluates additional VMs.
- The Contoso IT technician keeps the Contoso Migration project in Azure. The project currently is deployed in the ContosoFailoverRG resource group in the East US Azure region.
- The collector VM has a 180-day evaluation license. If this limit expires, the Contoso IT technician will need to download the collector and set it up again.

Checklist of Assessment Goals

Goal: Post Migration

After migration, apps in Azure should have the same performance capabilities that apps have today in Contoso's on-premises VMWare environment. Moving to the cloud doesn't mean that app performance is less critical.

Data Migration Assistant provides an assessment that allows Contoso assess the outcome of migrating its SQL Server environment to Azure SQL Database Managed Instance. The process generates a report listing recommendations supported by the target platform that can be used by the database after migration. The performance recommendations include such features as in-Memory OLTP and columnstore indexes.

- Note: As of December 2018, Data Migration Assistant does not support assessment for migrating to an Azure SQL Database Managed Instance. As a workaround, the Contoso can use SQL Server on an Azure VM as the supposed target for the assessment.

Azure SQL Database Managed Instance is available in the vCore-based purchasing model that allows independent scaling of compute and storage resources, facilitating matching on-premises performance levels. It also offers Contoso the choice of the hardware generation:

- Gen 4 - Up to 24 logical CPUs based on Intel E5-2673 v3 (Haswell) 2.4 GHz processors (where vCore is equal to a physical core), 7 GB per core, attached SSD
- Gen 5 - Up to 80 logical CPUs based on Intel E5-2673 v4 (Broadwell) 2.3 GHz processors (where vCore is equal to a hyperthread), 5.5. GB per core, fast eNVM SSD

Azure Migrate assesses performance of the VMware environment. Azure Migrate leverages an on-premises VM known as the collector appliance. The VM discovers on-premises VMware VMs and sends metadata about the VMs to the Azure Migrate service.An Azure Migrate assessment offers information about the suggested right-sizing for Azure VM. Sizing recommendation depends on the assessment approach:

- When using performance-based sizing, sizing considers the performance history of the VMs, including:

Utilization data for CPU and memory.

Read/write IOPS and throughput for each disk attached to the VM.

Network in/out information for each network adapter attached to the VM.

- When using as on-premises, sizing is based on the on-premises VM size and utilization data is not used.

In addition, Contoso installs Microsoft Monitoring Agent (MMA) and Dependency Agent on the app VMs in order to identify application dependencies. Any dependency might need to be considered for inclusion in the scope of migration in order to minimize negative performance impact resulting from increased latency in cross-premises connectivity scenarios.

Goal- Understanding Compatibility

Contoso needs to understand the compatibility of its applications and databases with Azure requirements. Contoso also needs to understand its hosting options in Azure.

In Azure, customers can run SQL Server workloads running in a hosted infrastructure (IaaS) or running as a hosted service (PaaS):

- Azure SQL Database: A SQL database engine, based on the Enterprise Edition of SQL Server that is optimized for modern application development. Azure SQL Database offers several deployment options:

A single database on a logical server.

A database in an elastic pool sharing resources with other databases on the same logical server.

An Azure SQL Database Managed Instances.

With all three versions, Azure SQL Database adds additional features that are not available in SQL Server, such as built-in intelligence and management. A logical server containing single and pooled databases offers most of database-scoped features of SQL Server. With Azure SQL Database Managed Instance, Azure SQL Database offers shared resources for databases and additional instance-scoped features. Azure SQL Database Managed Instance supports database migration with minimal to no database change.

- SQL Server on Azure Virtual Machines: SQL Server installed and hosted in the cloud on Windows Server or Linux virtual machines (VMs) running on Azure, also known as an infrastructure as a service (IaaS). SQL Server on Azure virtual machines is a good option for migrating on-premises SQL Server databases and applications without any database change. All recent versions and editions of SQL Server are available for installation in an IaaS virtual machine. The most significant difference from SQL Database is that SQL Server VMs allow full control over the database engine. You can choose when maintenance/patching will start, to change the recovery model to simple or bulk logged to enable faster load less log, to pause or start engine when needed, and you can fully customize the SQL Server database engine. With this additional control comes with added responsibility to manage the virtual machines.

Due to its requirement to minimize both management overhead and potential migration issues, Contoso wants to assess migration to Azure SQL Database Managed Instance.

Data Migration Assistant provides an assessment that allows Contoso assess the outcome of migrating its SQL Server environment to Azure SQL Database Managed Instance. The process generates a report that identifies compatibility issues affecting database migration. Compatibility Issues note changes that might break migration or that require a minor adjustment before migration. The report keeps Contoso informed about any features currently in use that are deprecated. Issues are organized by compatibility level. Compatibility levels map to SQL Server versions as follows:

- 100: SQL Server 2008/Azure SQL Database
- 110: SQL Server 2012/Azure SQL Database
- 120: SQL Server 2014/Azure SQL Database
- 130: SQL Server 2016/Azure SQL Database

- 140: SQL Server 2017/Azure SQL Database

An Azure Migrate assessment includes information about the compatibility of on-premises with Azure. Azure VM readiness indicates whether the VM is ready for migration. Possible states include:

- Ready for Azure
- Ready with conditions
- Not ready for Azure
- Readiness unknown

If a VM is not ready, Azure Migrate offers typically remediation steps.

Goal- Minimize Impact of Potential Compatibility Issues

Contoso's database administration should be minimized after apps move to the cloud. At the same time, Contoso would like to minimize impact of any potential compatibility issues of its SQL Server-based workloads.

By selecting Azure SQL Database Managed Instance as target for migrating its on-premises SQL Server database, Contoso considerably minimizes potential for any compatibility issues during migration. Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, Managed Instance preserves all PaaS capabilities, such as automatic patching and version updates, automated backups, and high-availability, effectively drastically reducing management overhead and TCO.

Goal- Costs Associated with the Infrastructure

Contoso wants to understand not only its migration options, but also the costs associated with the infrastructure after it moves to the cloud.

Azure SQL Database Managed Instance is available in the vCore-based purchasing model that will enable Contoso to choose the exact amount of storage capacity and compute needed for the migrated workload. Details regarding pricing for SQL Server Managed Instance are available at **https://azure.microsoft.com/en-us/pricing/details/sql-database/managed/**

An Azure Migrate assessment includes information about the estimated monthly Azure costs. The estimates include the total compute and storage cost of running the VMs in Azure as well as details for each machine. Cost estimates are calculated by using the size recommendations for a machine. Estimated monthly costs for compute and storage are aggregated for all VMs in the group.

In addition, with Software Assurance, Contoso will be able to leverage their existing Windows Server and SQL Server licenses for discounted rates on Azure VMs and SQL Database Managed Instances using the Azure Hybrid Benefit for Windows Server and SQL Server.