Migrate and Modernize with Azure Government

Azure for Government Playbook
About this Playbook

This playbook is intended for the leadership (technical and non-technical) for customers adopting Microsoft Azure Government.

Objectives

The goal of this playbook is to help you accelerate and optimize your Azure Government deployment by providing a clear roadmap and to help you understand best practices through your cloud journey. Our aim is not to re-write the existing body of detailed guidance on how to perform any given recommendation—instead we point you to resources that will help you.

For the non-technical side, this playbook provides valuable resources for envisioning new solutions and capabilities; as well as resources to help guide you through the process of reskilling and transforming your workforce to think and deliver in a cloud first mindset.

For the technical side, the playbook offers guidance on several topics that range from the technical skills your team will need, to resources that can accelerate learning. The playbook also describes some of the key opportunities for technical delivery to focus on as you get started and expand your Azure Government footprint.

How this playbook was made

This playbook was written by a Microsoft Partner, Opsgility, in conjunction with the Azure Government Engineering team. Subject matter experts at government agencies and Azure partners have volunteered their time to provide input and best practices to share with the rest of the government and partner community. A special thank you to Accenture, Applied Information Sciences, BrainScale, Planet Technologies, TechTrend and our Microsoft FastTrack for Azure team.
Using the playbook effectively

Quickly read through the playbook to familiarize yourself with the layout and content. Each section includes an executive summary and key actions for that specific topic. Review these summaries first to decide which areas to focus on. Go over the content several times, if needed, then share with your team.

TO GET THE MOST VALUE OUT OF THIS PLAYBOOK:

☑ Get your team together and discuss which pieces of the strategy each person is responsible for.
☑ Share the playbook with your technical and non-technical leadership.
☑ Leverage the resources available from Microsoft to help maximize your Azure investment.

WHAT TO PREPARE FOR:

☑ Developing a business strategy to capitalize on the Azure for government opportunity.
☑ Achieving compliance with government standards and obtaining an Authority To Operate.
☑ Integrating with government networks.
☑ Migrating and modernizing existing workloads and data platforms.
☑ Monitoring, management, security, and cost optimization

Share feedback on how we can improve this playbook by emailing AzureGovPlaybook@microsoft.com
# Table of Contents

**About this Playbook** ................................................. 2  
**Understanding Azure for Government** .......................... 6  
  Executive Summary .................................................. 7  
  What is Azure Government? ......................................... 8  
  Eligibility ............................................................. 11  
  Compliance and Certifications ..................................... 12  
  Azure Government Services ........................................ 16  
  Accessing Azure Government ....................................... 20  
  Network Integration .................................................. 23  
  Azure Government Support Options ............................... 26  
  Getting the Most Out of FastTrack for Azure .................. 28  
  Accelerating Authority to Operate ................................ 30  
**Cloud Leadership & Strategy** ...................................... 32  
  Executive Summary .................................................. 33  
  Government Challenges ............................................. 33  
  Digital Transformation for Government ........................ 35  
  Adopting a Cloud Mindset ......................................... 38  
  Creating a Cloud Strategy .......................................... 39  
  Bringing in the Right Stakeholders ............................... 40  
  Understanding the Migration Process ............................ 41  
  Understanding Agile and DevOps ................................. 42  
  Building a Center of Excellence .................................. 44  
  Reskilling for the Cloud ............................................ 45  
  Training & Readiness ............................................... 46  
  Azure Certifications ................................................ 48  
  Hiring and Job Description Resources ........................... 49  
**Migration Assessment** .............................................. 56  
  Executive Summary .................................................. 57  
  Discovery ............................................................. 58  
  Planning ............................................................... 62  
  Evaluation ............................................................. 65  
**Lift and Shift** ......................................................... 67  
  Executive Summary .................................................. 68  
  Building Out the Network ......................................... 69  
  Network Appliances .................................................. 72  
  The Virtual Data Center ............................................ 73  
  Enabling Hybrid Identity .......................................... 74  
  Planning for Storage ................................................ 75  
  File Shares ............................................................ 76  
  Choosing Virtual Machines ........................................ 77  
  Availability Options ................................................. 78  
  Customized Virtual Machine Images ............................. 79  
  Migrating to Virtual Machines .................................... 80  
  Migrating Disks ....................................................... 81  
  Migrating using Azure Site Recovery ............................. 82  
  Migrating VMware Workloads ..................................... 83  
  Migration Tools ...................................................... 84  
  Business Continuity ................................................ 86  
  Migrating Existing VMs to CSP ................................... 87  
  Migrating Databases ................................................ 88  
**Modernizing Apps** ................................................... 90  
  Executive Summary .................................................. 91  
  Modernizing Applications with Azure ........................... 92  
  Cloud-native Architecture and Design .......................... 94  
  Cloud Design Considerations ..................................... 95  
  Cloud Design Patterns ............................................. 97  
  Azure DevTest Labs ................................................ 98  
  Migrating Applications to Azure App Service .................. 101  
  Microservices and Containers ..................................... 103  
  What is Docker? ..................................................... 104  
  Modern Data Platform .............................................. 105  
  Cognitive Services and AI ......................................... 107  
**Optimize & Manage** .................................................. 108  
  Executive Summary .................................................. 109
INTRODUCTION

Cost Optimization ................................................................. 110
Azure Cost Management ....................................................... 111
Pre-purchasing ...................................................................... 114
Automatic Shutdown of VMs .................................................. 120
Monitoring and Alerting ....................................................... 122
Optimized Architecture ....................................................... 125
Azure Management Best Practices ......................................... 130
Azure Subscriptions ............................................................ 131
Resource Organization ....................................................... 134
Controlling access to Azure Resources .................................. 135
Security and Compliance .................................................... 136
Infrastructure as Code .......................................................... 137
Azure Resource Manager Templates ....................................... 138
Blueprints ........................................................................... 139
Automated Scripts .............................................................. 140
Azure SDKs and REST APIs .................................................. 141
Playbook Summary .............................................................. 142
Additional Resources ......................................................... 142
Why Choose Microsoft? ....................................................... 143
Troubleshooting Resources .................................................... 146
Best practices for running Azure projects ............................... 148

January 2020
Executive Summary

In this section, you will learn about Azure Government and the types of workloads that are appropriate to host within the Azure Government community cloud. This includes understanding the compliance position of the Azure public cloud, Azure Government, and Azure Government Secret.

While Azure Government is built using the same code as Azure public, there are some essential differences in the services, feature and management tools available. This section provides an overview of these differences allowing you to understand the constraints that are specific to Azure Government.

Secure network connectivity between Azure and government networks is a critical requirement for most government applications. We explain the available options to integrate networks while continuing to meet security and compliance requirements.

You’re not alone. The FastTrack for Azure team can help you with best practice guidance and reviews from experienced Microsoft experts. We’ll explain the FastTrack program, eligibility criteria and how to enroll.

Finally, we explain how best-practice guidance from Microsoft can help you accelerate the process of obtaining an Authority to Operate cloud-based workloads.

Top 5 things to do

You’re crafting your game plan to move to the cloud, make sure you nail down these 5 tasks as part of your plan.

- Choose the most suitable Azure environment for your workload
- Apply for access to Azure Government
- Review available Azure services and locations
- Engage FastTrack for Azure
- Plan for compliance and Authority to Operate
What is Azure Government?

US Government departments, agencies, or their partners can use Azure Government to benefit from cloud-based IT solutions while continuing to meet all relevant standards for security, protection and compliance.

Azure Government is purpose-built to meet the needs of federal, state and local, and tribal governments and their partners to include the defense industrial base (DIB). Using physically isolated, dedicated US data centers, Azure Government offers the following benefits:

- **Government exclusivity** – Only US federal, Department of Defense, state, local, and tribal governments and their partners have access to these dedicated Azure data centers, with operations controlled by screened US citizens.
- **Compliance** – Azure Government a very broad range of US Government certifications, simplifying compliance and onboarding. Two newly announced Secret locations offer enhanced security and isolation for hosting national security workloads.
- **DoD approval** – With six dedicated regions today, all granted an Impact Level 5 Provisional Authorization, Azure Government can host workloads for the US Department of Defense. Two additional regions, Azure Government Secret, are in private preview pending accreditation for DoD Impact Level 6.
- **Hybrid flexibility** – You can control not only the timing, but also the cadence of your organization’s adoption of the cloud. With hybrid connectivity between Azure and your existing environments, you can keep select data or functionality on-premises based on your requirements.
- **Innovation** – You’ll gain leading-edge capabilities including data analytics, AI/ML, Internet of Things and high-performance computing.

**Trusted** – Security is foundational for Azure. Use multi-layered, built-in security controls and unique threat intelligence from Azure to help identify and protect against rapidly evolving threats.
threats. Microsoft invests more than $1 billion annually on cybersecurity research and development and employs more than 3,500 security experts who are dedicated to your data security and privacy.

PUBLIC, GOVERNMENT AND SECRET

There are three options to choose between when deploying government services in Azure.

- **Azure Government**: The core of the offering, Azure Government comprises six Azure regions hosting a wide range of Azure services. These datacenters are dedicated facilities with operations controlled by screened US citizens. They offer FedRAMP Moderate and High provisional authorizations meeting DoD compliance standards at Impact Levels 2, 4, 5 and NIST 800-171 controls satisfy DFARS and ITAR requirements. Azure Government is suitable for most government workloads, including DoD.

- **Azure Government Secret**: Currently in Private Preview during the accreditation process, Azure Government Secret comprises an additional two Azure regions at undisclosed locations. With additional security controls, Azure Government Secret will provide extended support to meet Department of Defense Impact Level 6 (IL6) and Director of National Intelligence (DNI) Intelligence Community Directive (ICD 503) accreditation. Azure Government Secret is designed for Secret-classified workloads.

- **Azure**: Like Azure Government, the public Azure cloud service has also been accredited at the FedRAMP Moderate and High levels across a wide range of services, when using US data centers. This enables Azure public regions in the continental US to be used for government workloads that do not require the additional physical and logical isolation; guarantees around heightened screening of personnel; management exclusively by US citizens; and other important protections provided by Azure Government.

RESOURCES

- [Azure Government site](#)
- [Azure Government documentation](#)
- [Azure Government blog](#)
- [Azure Government videos](#)
- [Azure Government free trial](#)
- [Azure Government DC user community](#)
LOCATIONS

Azure Government offers dedicated instances of Azure that only US federal, state, local, and tribal governments and their partners have access to and that only screened US citizens control operations.

The current Azure Government regions are as shown in the map below.

Due to the sensitive nature of workloads that deal with secret data, the location of the two announced secret regions are undisclosed.

New regions are added as required and there are occasions where regions are retired as well. For example, US Gov Iowa will be retired on April 30, 2020 and any existing agency hosting workloads there will need to migrate them to another region.

There are also day-to-day needs to migrate applications between Azure regions, making the content of this playbook a valuable resource for understanding the business and technical capabilities and constraints when migrating workloads both to Azure from on-premises and even Azure-to-Azure.

Getting Started

See How to Buy Azure Government for information on how to purchase Azure Government, including pay-as-you-go subscriptions, Enterprise Agreements, and purchasing Azure Government through a partner using the Cloud Solution Provider program.

Azure Government Locations

- US DoD Central
- US DoD East
- US Gov Arizona
- US Gov Iowa*
- US Gov Texas
- US Gov Virginia
- US Sec East1 (announced)
- US Sec West1 (announced)

*US Gov Iowa will retire April 30, 2020.
Eligibility

Access to Azure Government is limited to approved US Government departments, agencies and their partners.

AGENCIES AND DEPARTMENTS

US government agencies or their partners interested in cloud services that meet government security and compliance requirements, can be confident that Microsoft Azure Government provides world-class security, protection, and compliance services. Azure Government delivers a dedicated cloud enabling government agencies and their partners to transform mission-critical workloads to the cloud.

Azure Government is suitable for a variety of government entities, including:

- **Federal Agencies**: Azure Government for federal agencies provides access to cloud services for hosting mission critical workloads for US government agencies and their partners.
- **State and Local Agencies**: Azure Government provides state and local governments the opportunity to do more with limited budgets, freeing up resources to focus on innovation and the delivery of services to citizens.
- **Department of Defense (DoD)**: For the DoD and its partners including the Defense Industrial Base (DIB) Azure offers access to the latest cloud services in an accredited environment where solutions can build stand-alone or integrated with other agencies through Azure’s hybrid cloud capabilities.
- **National Security**: Currently in Private Preview and pending accreditation, Azure Government Secret will offer DoD Impact Level 6 and Director of National Intelligence (DNI) Intelligence Community Directive (ICD 503) accreditation. These dedicated, air-gapped Azure regions are designed for classified workloads.

ELIGIBILITY

Azure Government is a unique cloud instance, exclusively for government customers and their solution providers. It’s offered to three distinct types of customers.

- **A US government entity** in its governmental capacity. Examples include federal agencies (e.g. bureau, agency, department, or other entity of the US government), state or local entities, tribal entities, regional or interstate government entities (but not international entities), and Federally Funded Research and Development Centers (FERDCs)
- **A partner** using Azure Government to provide a solution that, for example provides services or solutions to US government customers through direct or indirect contracts or serves US government customers through GSA or other contract vehicles.
- **A commercial private entity** with data that’s subject to US government regulations. Accepted government data types include:
  - International Traffic in Arms (ITAR)
  - Controlled Unclassified Information (CUI)
  - Department of Defense (DoD) Unclassified Controlled Nuclear Information (UCNI)
  - Department of Energy (DoE) UCNI
  - Criminal Justice Information (CJI)
  - Department of Defense Impact Level Data
  - Other data requiring Azure Government

An international commercial entity may qualify in certain circumstances, though to process regulated data they may be required to purchase the service through their US subsidiary.

Proof of membership in one of the groups listed above is required for access to Azure Government. For questions about eligibility for Azure Government, consult your account team. To sign up for trial, you can request a trial subscription.
Compliance and Certifications

Azure Government has the broadest compliance certifications of any cloud provider on the market. By being certified to meet these standards, Azure Government enables compliant and secure cloud deployments across a wide range of departments and agencies.

Azure Government delivers a dedicated cloud enabling government agencies and their partners to transform mission-critical workloads to the cloud. Azure Government services handle data that is subject to certain government regulations and requirements, such as Federal Risk and Authorization Management Program (FedRAMP), NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS. In order to provide you with the highest level of security and compliance, Azure Government uses physically segregated datacenters and networks (located in US only).

These accreditations are in addition to the accreditations found in Microsoft’s Azure public cloud offering. Azure public is also certified to FedRAMP Moderate and High levels in US data centers for a wide range of services, offering an alternative to Azure Government for workloads that do not require the additional isolation that Azure Government provides.

A detailed list of all of the Microsoft Azure compliance offers can be found in the Microsoft Trust Center and at https://aka.ms/AzureCompliance. The current list of FedRAMP-approved Azure services for both Moderate and High Impact Levels can be found in the FedRAMP marketplace.

The following sections discuss in further detail how Azure Government cloud services meet some of the most common regulatory requirements for the International Traffic in Arms Regulations (ITAR), the Criminal Justice Information Service (CJIS), and Department of Defense (DoD).

RESOURCES
- Overview of Azure compliance certifications
International Traffic in Arms Regulations (ITAR)

Microsoft provides certain cloud services or service features such as Azure that can support customers with ITAR obligations.

While there is no compliance certification for the ITAR, Microsoft operates and has designed in-scope services to be capable of supporting a customer’s ITAR obligations and compliance program.

Microsoft Azure Government and Microsoft Office 365 U.S. Government for Defense provide support for customers with data subject to the ITAR through additional contractual commitments to customers regarding the location of stored data, as well as limitations on the ability to access such data to US persons. Microsoft provides these assurances for the infrastructure and operational components of these government cloud services, but customers are ultimately responsible for the protection and architecture of their applications within their environments.

Customers must sign additional agreements formally notifying Microsoft of their intention to store ITAR-controlled data.

The ITAR has specific obligations to report violations. The Microsoft Enterprise Agreement Amendment contemplates that Microsoft and you work together in reporting such violations.

If you or your customers are seeking to host ITAR-regulated data, you should work with a Microsoft account representative and licensing teams to learn more, obtain proper agreements, and access relevant system architecture information.

RESOURCES

➔ ITAR Overview for Azure Government
➔ Microsoft Trust Center – ITAR
➔ Microsoft Trust Center – Compliance Overview
Criminal Justice Information Services (CJIS)

Microsoft Government in-scope services allow customers to adhere to CJIS standards, enabling criminal justice organizations to implement cloud-based solutions.

The CJIS Division of the US Federal Bureau of Investigation (FBI) gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI)—for example, fingerprint records and criminal histories. Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage, or processing of CJI complies with the CJIS Security Policy, which establishes minimum security requirements and controls to safeguard CJIS.

The CJIS Security Policy integrates presidential and FBI directives, federal laws, and the criminal justice community’s Advisory Policy Board decisions, along with guidance from the National Institute of Standards and Technology (NIST). The Policy is periodically updated to reflect evolving security requirements.

The CJIS Security Policy defines 13 areas that private contractors such as cloud service providers must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for the Federal Risk and Authorization Management Program (FedRAMP), a program under which Microsoft has been certified for its Government Cloud offerings.

Also, all private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. It also commits the contractor to maintaining a security program consistent with federal and state laws, regulations, and standards, and limits the use of CJI to the purposes for which a government agency provided it.

Microsoft government in-scope cloud services allow customers to adhere to the Criminal Justice Information Services (CJIS) Security Policy. Microsoft will sign the CJIS Security Addendum in states with CJIS Information Agreements. In the United States, 36 states and the District of Columbia currently have management agreements (see table).

Microsoft’s commitment to meeting the applicable CJIS regulatory controls allows Criminal Justice organizations to implement cloud-based solutions and be compliant with CJIS Security Policy V5.7. However, customers are ultimately responsible for the protection and architecture of their applications within their environments.

**RESOURCES**

- [Justice and Public Safety (JPS) in Azure Government](aka.ms/AzureGovPlaybook)
- [Microsoft Trust Center: CJIS](aka.ms/AzureGovPlaybook)

**STATES AND REGIONS WITH CJIS INFORMATION AGREEMENTS**

<table>
<thead>
<tr>
<th>Alabama</th>
<th>Florida</th>
<th>Kansas</th>
<th>Missouri</th>
<th>Oklahoma</th>
<th>Texas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
<td>Georgia</td>
<td>Kentucky</td>
<td>Montana</td>
<td>Oregon</td>
<td>Utah</td>
</tr>
<tr>
<td>Arkansas</td>
<td>Hawaii</td>
<td>Maine</td>
<td>New Jersey</td>
<td>Pennsylvania</td>
<td>Vermont</td>
</tr>
<tr>
<td>Arizona</td>
<td>Illinois</td>
<td>Massachusetts</td>
<td>New York</td>
<td>Rhode Island</td>
<td>Virginia</td>
</tr>
<tr>
<td>California</td>
<td>Indiana</td>
<td>Michigan</td>
<td>Nevada</td>
<td>South Carolina</td>
<td>Washington</td>
</tr>
<tr>
<td>Colorado</td>
<td>Iowa</td>
<td>Minnesota</td>
<td>North Carolina</td>
<td>Tennessee</td>
<td>West Virginia</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Washington, DC</td>
</tr>
</tbody>
</table>

If your state isn’t listed, contact ExpandAzureCJIS@azure.com
Department of Defense (DoD)


Azure Government is used by Department of Defense (DoD) entities to deploy a broad range of workloads and solutions, including those workloads covered by The DoD Cloud Computing Security Requirements Guide, Version 1, Release 2 at Impact Level 4 (L4), and Impact Level 5 (L5).

Azure Government is the first and only hyperscale commercial cloud service to be awarded an Information Impact Level 5 DoD Provisional Authorization by the Defense Information Systems Agency (DISA). In addition, Azure Government regions dedicated to US Department of Defense customer workloads are now generally available.

Azure Government Secret (currently in private preview pending accreditation) provides an additional level of security for US agencies and partners working with Secret US security classification level data. These dedicated regions are built to meet the regulatory and compliance requirements for Department of Defense Impact Level 6 (IL6) and Director of National Intelligence (DNI) Intelligence Community Directive (ICD 503) accreditation.

One of the key drivers for the DoD in moving to the cloud is to enable organizations to focus on their missions and minimize the distractions of building and managing in-house IT solutions. This allows for the realignment of critical IT resources to focus on application development, analytics, and cyber security.

The elasticity and flexibility delivered by Azure provides enormous benefits to DoD customers. It is frequently simpler, quicker, and more cost-effective to scale-up a workload in the cloud than it is to go through traditional hardware and services procurement processes when working on-premises, or in DoD data centers. For example, to procure new multi-server hardware, even for a test environment, may take many months, and require the approval of significant capital expenditure. By contrast, using Azure, a test migration for an existing workload can be configured in weeks or even days, and in a cost-effective manner (when the test is over, the environment can be torn down with no ongoing costs).

This flexibility is significant. By moving to Azure, DoD customers may not just save money; the cloud delivers new opportunities. For example, it is easy to spin up a test environment to gain insights into new technologies, you can migrate an application and test it in Azure before committing to a production deployment in the cloud. Mission owners can explore more cost-effective options easier, and with less risk.

Security is another key area, and although any cloud deployment requires proper planning to ensure secure and reliable service delivery, many properly configured cloud-based workloads (up to and including L4 workloads) in Azure Government will be more secure than many traditional deployments in DoD locations and data centers. This is because defense agencies have the experience and expertise to physically secure all assets; however, the IT surface areas present different challenges. Cyber security is a rapidly changing space, requiring specialist skills and the ability to rapidly develop and deploy countermeasures as required. The Azure platform, both commercial and government, now supports hundreds of thousands of customers, and this scale enables Microsoft to quickly detect evolving attack vectors and direct its resources onto rapid development and implementation of the appropriate defenses.

RESOURCES

- DoD Region Q&A
- Microsoft Trust Center – US Department of Defense (DoD) Provisional Authorization
Azure Government Services

Azure Government offers many of the same services as the Azure public cloud. However, not every service or feature is available, and releases often occur to a separate schedule.

The Azure services that provide compute, storage, networking, and more to Azure Government customers are deployed through the same code that is deployed in Azure public. However, there are differences in not just service availability, but also in the features available within a single service.

Just as in the commercial Azure regions, you should always review the services you are going to consume and their availability in the regions you plan to use. Service availability can vary across regions in everything from virtual machine size to the availability and features of PaaS services such as web sites and databases.

RELEASE CYCLES

To view the current list of available services in Azure Government and the regions in which they are available, see Azure Products by Region and filter the regions list to Azure Government.

When viewing availability, take note of the status of the service and whether it is:

- **Generally available** Services that have reached general availability are eligible for Azure support and many services carry a financially backed SLA.
- **In preview** Previews are provided “as-is,” “with all faults,” and “as-available,” and are excluded from the SLAs and all limited warranties in any legal agreements in place with Microsoft.
- **Available in the future** Services that are designated as “future availability” are currently on the roadmap, however there is no guarantee a given service will release on time or will ever release.

Azure services roughly follow a release cycle of private preview, public preview, and release to general availability. Private and public preview services should be considered as not fit for production use in most cases and there is no guarantee that a preview service will ever reach general availability. For more information, see the Supplemental Terms of Use for Microsoft Azure Previews and the Microsoft Online Subscription Agreement – US Government Cloud.

Service Differences in Azure Government
While Azure Government services run the same code as used in the Azure public cloud, there are some important configuration differences to consider.

As you consider the services you will consume in Azure Government, there are two important types of information you need to think about:

- **Variations** - Variations due to features that are not deployed yet or properties (for example, URLs) that are unique to the government environment.

- **Considerations** - Government-specific implementation detail to ensure that data stays within your compliance boundary.

The most common variation across services is differences in the endpoints that are used to connect to Azure services. For example, in Azure public, the domain suffix for Azure App Services is ‘azurewebsites.net’ while in Azure Government the suffix is ‘azurewebsites.us’. Similar domain name changes are required across many Azure services. There are also differences in how you connect to Azure Government to manage services, which is discussed in Connecting to Azure Government.

Another consideration which is applicable to almost every service is the constraints around metadata for the services you deploy (for example, the name of a resource or a setting or property of a service). Metadata often is not permitted to contain export-controlled data and typically applies to all configuration data. It’s critical to keep in mind the shared responsibility model for cloud in which customers are responsible for configuring, supporting and securing their applications via IaaS and PaaS.

In the following sections, we will review some of the major categories of services available in Azure Government and the variations and considerations for services within each category. For a detailed list of services available in Azure Government and their current release status, see available services in Azure Government or browse to a category from the links provided in the table.

### AVAILABLE SERVICES IN AZURE GOVERNMENT

<table>
<thead>
<tr>
<th>Compute</th>
<th>Networking</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web + Mobile</td>
<td>Azure Stack</td>
<td>Media Services</td>
</tr>
<tr>
<td>Databases</td>
<td>Data + Analytics</td>
<td>AI + Machine Learning</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>Integration Services</td>
<td>Security + Identity</td>
</tr>
<tr>
<td>Backup</td>
<td>Monitoring + Management</td>
<td>Developer Tools</td>
</tr>
</tbody>
</table>
**COMPUTE**

*Azure Compute* includes services such as Virtual Machines, Virtual Machine Scale Sets, Azure Batch, Azure Functions, and Azure Service Fabric. For most compute services, there are two primary considerations: virtual machine availability and data storage.

Virtual machine availability, including the available SKUs and sizes can vary based on region. You should always refer to the *Products Available by Region* documentation to verify machine families and sizes prior to deployment.

For data, you must be mindful of the Azure Government boundaries. While metadata cannot contain export-controlled data, data entered, stored, and processed within a VM can contain export-controlled data. This includes:

- Binaries running within Azure Virtual Machines.
- Static authenticators, such as passwords and smartcard PINs for access to Azure platform components.
- Private keys of certificates used to manage Azure platform components.
- SQL connection strings.
- Other security information/secrets, such as certificates, encryption keys, master keys, and storage keys stored in Azure services.

Services such as Azure Functions are offered in both a Consumption plan (on-demand compute) and App Service plan (pre-allocated compute) however in Azure Government the Consumption plan is only available in the US Gov Virginia region.

**NETWORKING**

Azure Government offers access to the robust *networking services* including ExpressRoute and the ability to connect to Azure over a VPN tunnel. It is strongly recommended that ExpressRoute is implemented to connect to Azure Government for the most secure and performant connection. If, however, a VPN is used instead, consider the following:

- Customers should contact their authorizing official or agency to determine whether private connectivity or other secure connection mechanism is required and to identify any additional restrictions to consider.
- Customers should decide whether to mandate that the site-to-site VPN is routed through a private connectivity zone. If so, customers should obtain either an MPLS circuit or VPN with a licensed private connectivity access provider.

ExpressRoute offers customers who have data classification levels up to FedRAMP High or IL5 a private and dedicated connectivity solution to Microsoft cloud offerings.
STORAGE

Every Azure region has a paired region for disaster recovery and resilience within the Azure platform. In this regard, Azure Government is no different than Azure public, but there are some nuances which affect services with native replication capabilities such as Azure Storage.

When choosing your Azure region, consider both the primary region and the secondary region used for disaster recovery and data replication. Azure SQL Database and CosmosDB let you choose your own primary and replica regions. However, when using Azure Storage, the replica is chosen for you, according to the table below.

<table>
<thead>
<tr>
<th>Primary Region</th>
<th>Paired Secondary Region (for Storage replication)</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Gov Iowa*</td>
<td>US Gov Virginia</td>
</tr>
<tr>
<td>US Gov Virginia</td>
<td>US Gov Texas</td>
</tr>
<tr>
<td>US Gov Texas</td>
<td>US Gov Arizona</td>
</tr>
<tr>
<td>US Gov Arizona</td>
<td>US Gov Texas</td>
</tr>
</tbody>
</table>

*US Gov Iowa will retire April 30, 2020.
Accessing Azure Government

Azure Government is managed much like the Azure public cloud. Learn how to configure tools to access Azure Government.

Azure Government runs the same code as Azure public cloud and is managed using broadly the same set of tools. To manage Azure resources in Azure Government, you must connect those tools to the Azure Government-specific management endpoints (also known as an environment). This applies whether you are managing your Azure resources through your browser via the Azure portal or using client-side command-line tools such as Azure PowerShell or the Azure CLI.

AZURE PORTAL

To connect to the Azure portal to manage resources in Azure Government, browse to https://portal.azure.us and sign in using the credentials for the directory associated with your subscription. The Azure Government portal is branded for Azure Government so you will know you are in the right place.
DEPLOYMENT OPTIONS

Azure provides multiple options and flexibility for you to deploy into the environment. Azure supports Azure PowerShell, Azure Resource Manager, Terraform, and others that conform with your local IT deployment practices.

By building a library of common PowerShell scripts, you can begin to build your own repository of re-usable scripts that can be used for multiple customers. Microsoft offers a library of sample scripts which partners and customers can use to begin building a script repository:

- Azure Virtual Machine PowerShell Samples - Linux Virtual Machines
- Azure Virtual Machine PowerShell samples - Windows Virtual Machines
- Web Apps
- SQL Databases
- azure-docs-powershell-samples on GitHub

Note that in Azure Government, there is no equivalent to Azure Cloud Shell that you can find in the Azure portal. To manage your resources in Azure Government, using Azure PowerShell you must first install PowerShell on your local machine. For more information, see Introduction to Azure PowerShell.

When you start PowerShell, you must tell Azure PowerShell to connect to Azure Government by specifying an environment parameter. The parameter ensures that PowerShell is connecting to the correct endpoints. The collection of endpoints is determined when you connect log in to your account. Different cmdlets require different versions of the environment switch, as detailed in the table.

<table>
<thead>
<tr>
<th>CONNECTION TYPE</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure commands</td>
<td>Connect-AzAccount -EnvironmentName AzureUSGovernment</td>
</tr>
<tr>
<td>Azure Active Directory commands</td>
<td>Connect-AzureAD -AzureEnvironmentName AzureUSGovernment</td>
</tr>
<tr>
<td>Azure (Classic deployment model) commands</td>
<td>Add-AzureAccount -Environment AzureUSGovernment</td>
</tr>
<tr>
<td>Azure Active Directory (Classic deployment model) commands</td>
<td>Connect-MsolService -AzureEnvironment UsGovernment</td>
</tr>
</tbody>
</table>
AZURE CLI

The Azure CLI 2.0 is Azure’s command-line experience for managing Azure resources.

As with Azure PowerShell, Azure Government has no equivalent to Azure Cloud Shell that you can find in the Azure portal. To manage your resources in Azure Government using the Azure CLI you will need to install it locally. You can install the Azure CLI on Linux, macOS, and Windows, and it can even be run from a Docker container.

Just as with Azure PowerShell, you can build a library of common scripts that can be re-used from client to client. There is an expansive library of Azure CLI samples which cover the management and configuration of multiple Azure services and resources:

- Azure Virtual Machine Azure CLI Samples - Linux Virtual Machines
- Azure Virtual Machine Azure CLI Samples - Windows Virtual Machines
- Web Apps
- SQL Databases
- azure-cli-samples on GitHub

To manage your resources in Azure Government using the Azure CLI, open a new instance of the CLI and set the cloud name to AzureUSGovernment. After setting the environment, you can login using the az login command. You can confirm you are connected to the right environment using the az cloud list command.

az cloud set --name AzureUsGovernment
az login
az cloud list --output table

<table>
<thead>
<tr>
<th>IsActive</th>
<th>Name</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>False</td>
<td>AzureCloud</td>
<td>latest</td>
</tr>
<tr>
<td>False</td>
<td>AzureChinaCloud</td>
<td>latest</td>
</tr>
<tr>
<td>True</td>
<td>AzureUSGovernment</td>
<td>latest</td>
</tr>
<tr>
<td>False</td>
<td>AzureGermanCloud</td>
<td>latest</td>
</tr>
</tbody>
</table>
Network Integration

Azure meets US Government standards for secure connectivity to government networks. Ensure your application is designed to connect securely.

Many cloud applications are hybrid applications, requiring the integration of Azure-based services with government-hosted systems. Network security is critical to the protection of US Government applications and data, and as such there are strict requirements for how US Government networks are connected to external networks. It’s important to make sure your Azure deployment is correctly designed to meet these requirements.

Trusted Internet Connections (TIC) Guidance

Background

In November 2007, the OMB established the Trusted Internet Connections program to improve federal network perimeter security and incident response functions. That policy was outlined in the Office of Management and Budget (OMB) Memorandum M-08-05 with the purpose to optimize and standardize the security of individual external network connections that are used by federal agencies.

TIC was designed to perform network analysis of all inbound and outbound .gov traffic to identify specific signatures and pattern-based data. TIC uncovers behavioral anomalies, such as botnet activity. Agencies are mandated to consolidate their external network connections and route all traffic through intrusion detection and prevention devices known as EINSTEIN. The devices are hosted at a limited number of network endpoints, which are referred to as TIC.

The objective of TIC is for agencies to know:

- Who is on my network (authorized or unauthorized)?
- When is my network accessed and why?
- What resources are accessed?

All agency external connections must currently route through an OMB-approved TIC. Federal agencies are required to participate in the TIC program as a TIC Access Provider (TICAP), or by contracting services with one of the major tier 1 internet service providers. These providers are referred to as Managed Trusted Internet Protocol Service (MTIPS) providers. TIC includes mandatory critical capabilities that are performed by the agency and MTIPS provider.

Looking ahead: TIC 3.0

In September 2019, OMB released an update to the TIC initiative in the OMB Memorandum M-19-26. This update aims to remove barriers to cloud by providing greater agility and flexibility to support cloud and emerging technologies in a secure way.

Most recently, on Dec. 20, 2020, the Department of Homeland Security’s Cybersecurity & Infrastructure Security Agency (CISA) announced its release of draft documentation to provide guidance for TIC 3.0. The new draft guidance documents consist of five volumes that should be read in sequential order to gain a thorough understanding of the updated initiative.

As of this publishing, and as more details become known, TIC guidance in Azure documentation will be updated. You can also view CISA’s draft of TIC 3.0 Service Provider Overlay Handbook.

aka.ms/AzureGovPlaybook
Recall that there are three main options to connect to Azure services:

- **Direct internet connection** - Connect to Azure services directly through an open internet connection. The medium and the connection are public. Application and transport level encryption are relied upon to ensure privacy. Bandwidth is limited by a site’s connectivity to the internet. Use more than one active provider to ensure resiliency.

- **Virtual private network (VPN)** - Connect to your Azure virtual network privately by using a VPN gateway. The medium is public because it traverses a site’s standard internet connection, but the connection is encrypted in a tunnel to ensure privacy. Bandwidth is limited depending on the VPN devices and the configuration chosen. Azure point-to-site connections are typically limited to 100 Mbps and site-to-site connections are limited to 1.25 Gbps.

- **Azure ExpressRoute** - ExpressRoute is a direct connection to Microsoft services. Because connectivity is through an isolated fiber channel, the connection can be public or private depending on the configuration used. Bandwidth is typically limited to a maximum of 10 Gbps.
To enable the connection from the Department or Agency (D/A) to Azure, without routing traffic through the D/A TIC, the D/A must use an encrypted tunnel or a dedicated connection to the cloud service provider (CSP). The CSP services can ensure connectivity to the D/A cloud assets isn’t offered to the public internet for direct agency personnel access.

For Azure, only the second option (VPN) and third option (ExpressRoute) can meet these requirements when they’re used in conjunction with services that limit access to the internet. Please consult with your Security Office as needed if your agency requires a site-to-site encryption in an ExpressRoute.


The Department of Defense mandates that commercial cloud services used for unclassified information (CUI) must be connected to customers through a Cloud Access Point (CAP). Therefore, the Azure DoD regions are connected to the Non-classified Internet Protocol (IP) Router Network (NIPRNet) through redundant connections to multiple geographically distributed CAPs. A DoD CAP is a system of network boundary protection and monitoring devices that offer protection to DoD information system network and services.

There are several considerations for routing and security rules in DoD environments. The DISA BGP routes will advertise a route for 0.0.0.0/0 which prevents some Azure services from communicating with their management plane. For example, App Service Environment (ASE) needs to route directly to the internet which requires removing the DISA BGP route from any subnets associated with an ASE and requires inbound network security rules allowing traffic from the Azure Government IP address space to the public VIP. Another example where you may need to override forced tunneling for an internet route is allowing Windows virtual machines to connect directly to the Azure KMS server as Azure VMs need to connect to the KMS server for activation and activation requires that the activation request comes from an Azure public IP address.

RESOURCES

- Outbound connections in Azure
- Virtual Network Service Tags
- Network Security Group Default Security Rules
- App Service Environment reference for DoD customers using a DISA CAP connection
- App Service Environment management addresses
- Windows activation fails in forced tunneling scenario
Azure Government Support Options

Choose between tailored support plans for Azure Government to get help when you need it.

Azure public is supported through Microsoft’s standard commercial support plans. These allow you to choose between tiered support levels tailored to the requirements of your workload. In addition, Microsoft provides dedicated support plans tailored specifically to the needs of Azure Government customers. These are based on similar tiered support levels, with additional features such as business-hours support provided by screened US staff.

Basic support services are included with every Azure subscription. This includes 24x7x365 access to Microsoft customer service, documentation, whitepapers, and support forums where you can troubleshoot issues with others. Most customers require more than basic support, especially when deploying business-critical workloads to the cloud.

In your considerations for the selection of a support model, you will need to understand your underlying requirements for basic needs like an SLA for response from Microsoft along with the criticality of the workloads you are deploying for customers are to them. The plan you select will directly drive the SLAs that you can offer to your customers.

Microsoft offers four support plans for Azure above the Basic tier. These are:

- **Gov Developer** Suitable for trial and non-production environments
- **Gov Standard** Suitable for non-critical production environments
- **Gov Pro Direct** For customers with a substantial dependence on Azure
- **Gov Premier** For customers with a business-critical, strategic dependence across multiple Microsoft products

As an introductory offer, all customers purchasing Microsoft Azure Government through an Enterprise Agreement will be eligible for Standard or ProDirect support, according to consumption, at no charge.

These support plans truly start to differ once you consider when you will need to interact with Microsoft support. The Developer support plan only includes business hours access to support, while the other plans include 24x7 access.

Once you have determined when you are going to interact with support, consider the response times for different case severities. Microsoft classifies severity at three levels:

- **Severity A** cases are reserved for issues that involve a significant loss or degradation of services and require immediate attention
- **Severity B** cases are for issues which exhibit a moderate loss or degradation of services but work can continue in a reasonable manner
- **Severity C** cases are for issues which have a minimal impact and there are only light impediments to service

The consideration becomes this: if you believe you will have a need to open a support case with Microsoft with a Severity A or Severity B, you will need to select a Standard support plan or higher. Severity A incidents include an initial response time SLA of less than 1 hour.

You may have noticed that there is no mention of an SLA for how quickly your issue will be resolved under any support plan. This is by design as the time it takes to troubleshoot and resolve an issue in Azure can vary widely based on the specifics of the issue. Microsoft does commit to working with you to resolve each issue as fast as possible.

**RESOURCES**

- [Azure Government Support Plans](aka.ms/AzureGovPlaybook)
<table>
<thead>
<tr>
<th>SUPPORT PLANS</th>
<th>INCLUDED</th>
<th>DEVELOPER</th>
<th>STANDARD</th>
<th>PROFESSIONAL DIRECT</th>
<th>PREMIER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best for</td>
<td></td>
<td>Gov Developer</td>
<td>Gov Standard</td>
<td>Gov Pro Direct</td>
<td>Gov Premier</td>
</tr>
<tr>
<td>Range of support</td>
<td></td>
<td>Microsoft Azure</td>
<td>Microsoft Azure</td>
<td>Microsoft Azure</td>
<td>All Microsoft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Government</td>
<td>Government</td>
<td>Government</td>
<td>products</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>Support provided by</td>
<td>Screened US persons</td>
<td>Business hours</td>
<td>Business hours</td>
<td>Business hours</td>
<td>Business hours</td>
</tr>
<tr>
<td></td>
<td></td>
<td>only</td>
<td>only</td>
<td>only</td>
<td>only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monthly cost</td>
<td>$40/mo</td>
<td>$125/mo</td>
<td>$1,250/mo</td>
<td>Contact licensing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Included with Azure Government subscription</td>
<td></td>
<td></td>
<td>service provider</td>
<td></td>
</tr>
</tbody>
</table>

1Two Azure online forum options: MSDN and Stack Overflow. MSDN is a Microsoft online property. Stack Overflow is not associated or affiliated with Microsoft.

2For the United States, business hours are 6:00 AM to 6:00 PM Pacific time, Monday through Friday excluding holidays.

3Initial response time (IRT) shown is for the maximum severity of each offering, and is the fastest IRT available for each offering. Lower severities have a longer IRT.

4StorSimple support is provided for the first year for the physical appliance until the customer’s next Enterprise Agreement anniversary, thereafter customers must purchase a StorSimple device support plan in addition to the Azure support plan; more information is available here.

5As of October 18, 2017 the Azure Government support model has changed; after hours support for Azure technologies might be provided outside of US.
Getting the Most Out of FastTrack for Azure

FastTrack for Azure provides direct assistance from Azure engineers, working hand-in-hand with customers & partners, to help customers build Azure solutions, quickly and confidently.

FastTrack for Azure is a Microsoft license benefit designed to help customers and partners accelerate their Azure projects by providing best practice assistance and guidance from Microsoft’s own expert engineers. The license benefit is available to government customers and partners using the Azure Public, Azure Government, or Azure Government Secret clouds. Best of all, FastTrack for Azure is a free license benefit for customers, so there’s no downside to taking full advantage.

**FASTTRACK FOR AZURE SERVICES**

FastTrack for Azure provides expert guidance to help you deliver your Azure projects more quickly, confidently, and successfully. Once approved, a dedicated project manager will be assigned to your project. They will be your point of contact throughout the project, working with you to understand your needs and how best to support you. The project manager will bring in Microsoft engineers with the appropriate expertise to support and guide your team to success.

FastTrack for Azure is available to support a wide range of project types, including infrastructure deployments, data center migration, data modernization, app modernization, business continuity, security, and more. For a full list, see the supported solutions section on the FastTrack site.

Services provided include architecture design reviews, technical knowledge transfers, operational guidance, and oversight assistance with proof-of-concept and dev/test deployments. FastTrack for Azure engineers can also direct you to appropriate documentation and samples to help accelerate your Azure journey.

Most FastTrack for Azure engagements are delivered remotely. However, for Azure Government customers, the FastTrack for Azure team also provides a secure facility for data import. This provides a quick and secure path for bulk data import to Azure Government.

FastTrack for Azure is not a consultancy service. They do not write custom code or scripts or develop other deliverables for you, nor do they help with envisioning for a new project. Rather, their role is to provide assistance so you can deliver your project more effectively.

**aka.ms/AzureGovPlaybook**
BENEFITS

There are many benefits to using FastTrack for Azure. Most important of these is direct assistance from Microsoft’s expert Azure engineers. These engineers bring a wealth of real-world customer experience to your project. In addition, FastTrack for Azure provides you access to proven tools and best-practice guidance and works with your team to understand your needs and provide tailored support.

Working with FastTrack for Azure helps your team deepen their skill set while delivering your projects more quickly, more confidently, and with reduced risk.

For partners, there are additional benefits. Working with the FastTrack for Azure team can reduce your costs, increasing your competitiveness. It also strengthens your brand and enables you to broaden your offerings.

ELIGIBILITY

FastTrack for Azure is available to support government customers and partners throughout the United States. Customers must have:

• A paid, active Azure subscription.
• A specific project identified
• A committed delivery plan expected to provide at least $5,000 USD of Azure consumption per month within 12 months.

For Partners, you must also demonstrate Azure competence, ideally through a Silver Cloud Platform or Gold Cloud Platform Microsoft Partner accreditation.

HOW TO ENGAGE

Government customers wishing to take advantage of FastTrack for Azure should start by asking their Microsoft account representative. Customers without a representative should click the ‘Check your eligibility’ option on the FastTrack site to self-nominate.

Microsoft Partners can engage the FastTrack for Azure team by nominating their customer at the FastTrack for Azure Partners site.

RESOURCES

• FastTrack for Azure
• FastTrack for Azure Partners
Accelerating Authority to Operate

Use security and compliance guidance from Microsoft to implement best practices that can significantly reduce the time required to obtain an Authority to Operate.

Microsoft’s government cloud services, including Azure Government, Office 365 US Government, and Dynamics 365 Government, meet the demanding requirements of the US Federal Risk and Authorization Management Program (FedRAMP), enabling US federal agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud.

The Joint Authorization Board (JAB) is the primary governance and decision-making body for FedRAMP. Representatives from the Department of Defense, the Department of Homeland Security, and the General Services Administration serve on the board. The board grants a Provisional Authorization to Operate (P-ATO) to cloud service providers that have demonstrated FedRAMP compliance. Azure was the first public cloud with infrastructure and platform services to receive a P-ATO from the JAB.

The JAB has granted Azure Government a P-ATO at the High Impact Level, the highest bar for FedRAMP accreditation, which authorizes the use of Azure Government to process highly sensitive data. The mandatory NIST 800-53 standards establish security categories of information systems—confidentiality, integrity, and availability—to assess the potential impact on an organization should its information and information systems be compromised. The FedRAMP audit of Azure and Azure Government included the Information Security Management System that encompasses infrastructure, development, operations, management, and support of in-scope services.

In addition, Azure also maintains a P-ATO for the Azure public cloud. Until recently, Azure public was accredited at the Moderate Impact Level, and Azure Government at the High Impact Level. As of May 2019, Azure public has also been certified at the FedRAMP High impact level.

Once a P-ATO is granted, a CSP still requires an authorization - an ATO - from any government agency it works with. In the case of Azure, a government agency can leverage the Azure P-ATO in its own security authorization process and rely on it as the basis for issuing an agency ATO that also meets FedRAMP requirements. It’s important to plan and prepare for your agency’s ATO success. See the FedRAMP Agency Authorization Playbook for guidance. To learn more about the benefits of FedRAMP on the Microsoft cloud, download the FedRAMP compliance backgrounder.

Microsoft government cloud services offer public sector customers a rich array of services compliant with FedRAMP, as well as robust guidance and implementation tools. These include the Azure Security and Compliance Blueprint for FedRAMP, which helps automate deployment and configuration of Azure resources in a FedRAMP environment.

SECURITY AND COMPLIANCE BLUEPRINTS ON AZURE

Azure Security and Compliance Blueprints are resources to assist you in building and launching cloud-powered applications that help you comply with stringent regulations and standards. With more certifications than any other cloud provider, you can have confidence deploying your critical workloads to Azure.

Blueprints include:

- Industry-specific overview and guidance
- Automated control implementation using Azure Policy and Azure Blueprint services
- Automated deployment of role-based access control and foundational architecture patterns tailored to the needs of the public sector
- Customer responsibility matrix

In the case of Azure Government, Microsoft offers a FedRAMP Blueprint. Additional Blueprints and deployment guidance include:

- DoD Blueprint
- NIST Cybersecurity Framework (CSF) Blueprint
- NIST 800-53 R4 blueprint

aka.ms/AzureGovPlaybook
For any Azure Security and Compliance Blueprint, Microsoft also makes a System Security Plan (SSP) High Baseline template available. The SSP is the main document in which a CSP describes all the security controls in use on the information system and their implementation. This document is intended to be used by service providers who are applying for a JAB P-ATO through FedRAMP. In some instances, US federal agencies may want to use it to document information systems security plans that are not part of the FedRAMP program.

FedRAMP Blueprint

FedRAMP Blueprint for Azure helps you accelerate your journey to Azure through templates which automate the deployment of resources to your Azure subscription that are focused on compliance and security, reference architectures, control implementation mappings, customer responsibility matrixes, and threat models.

DEPLOYMENT EFFICIENCY

Adopting blueprint guidance and automation, while utilizing the FedRAMP Blueprint helps enable you to deploy more secure and compliant applications in less time, and at a lower cost. The process improvements associated with the FedRAMP Blueprint also may save expenses related to misconfigurations, compliance uncertainty, and infrastructure management.

CONTROL COVERAGE

Understanding inherited, shared, and owned controls are vital to deploying compliant workloads in Azure. Microsoft provides a Customer Responsibility Matrix (CRM) that delineates each control and associated responsibility. Additionally, the Control Implementation Matrix (CIM) provides a clear explanation of how each control is managed in Azure.

REFERENCES

- FedRAMP Blueprint
- Blueprints and compliance on Azure Government
Cloud Leadership & Strategy

Migration and Modernization with Azure Government
Executive Summary

A cloud mindset is the key that unlocks the potential of digital transformation.

This section of the playbook frames the motivation for government agencies to adopt cloud-based services, and the motivation for Microsoft to supply these services by creating the Azure Government cloud. This section will help set the context as to how leadership at every level is impacted and can critically impact the success of cloud adoption.

We start by reviewing the common challenges shared by government leaders as they strive to deliver high-quality, value-for-money services to their citizens. These reflect both the evolving user expectations for multi-channel service engagement together with the continuous drive to improve internal process efficiency and deal with challenges such as legacy infrastructure and skills.

We then look at digital transformation for government. Digital transformation is already transforming the world of business by enabling powerful new customer experiences with dramatically streamlined processes and increased staff productivity. We discuss how this revolution applies to the public sector and show how public services can also be transformed to take advantage of new technologies.

We then discuss how digital transformation is enabled by the cloud. We discuss the value proposition delivered by cloud technologies, and how these technologies provide a step-change in flexibility, agility, and productivity when compared with traditional IT. Cloud technologies therefore form the foundation of digital transformation.

Understanding how digital transformation is critical to your agency, we'll discuss how to get started, by building cloud strategy. A cloud strategy includes the business case, budgets, and engaging the right stakeholders. It also includes planning at an organizational level to hire or reskill your existing staff to be cloud enabled.

Resources from the Microsoft Azure Cloud Adoption Framework are referenced throughout this section.

Top 5 things to do

Transform your organization to take full advantage of the cloud. These are the top 5 things you should do to enable digital transformation powered by Azure Government.

- Understand the importance of a cloud mindset
- Build a cloud strategy that aligns stakeholders across your organization
- Adopt agile processes for faster delivery
- Leverage the GSA Centers of Excellence
- Train your team with effective cloud skills
Government Challenges

Government agencies are continually seeking ways to meet complex demands while doing more and with less. With these challenges come new possibilities to capitalize on the promise of technology to create more efficient, transparent, and productive government.

Government agencies and leaders face continual challenges from an ever-changing world. Emerging technologies create new opportunities to deliver government services in new ways, and to transform internal operations for greater efficiency. Here are some of the key challenges faced by government leaders today:

- **Citizen expectations for multi-channel, digital services:** With the ubiquity of smartphones and shift to mobile-first browsing behavior, users expect government services to be accessible across multiple channels, from desktop to tablet to mobile.
- **Cross-agency collaboration:** Providing unified experiences across government streamlines the citizen experience and increases efficiency. However, this can require integration of applications, data and processes across agencies and departments.
- **Streamlining internal operations:** As internal processes adapt to new services they can easily become complex and inefficient. Streamlining operations to increase efficiency is essential.
- **Security, privacy and regulatory requirements:** For any government service, accreditation with applicable government standards for security and privacy is a non-negotiable requirement.
- **Managing legacy technology:** Many long-running government services carry a burden of legacy technology, increasing maintenance costs and acting as a brake on innovation. Transforming services requires transforming this infrastructure foundation.
- **Recruiting and retaining technical talent:** Attracting and retaining top technical talent is always challenging, especially when competing with the private sector. Legacy technologies and a slow pace of change make this even harder.

As we shall see in the coming pages, Azure and Azure Government provide a comprehensive suite of cloud technologies help that enable you to meet these challenges.
Digital Transformation for Government

Azure Government has been designed to make sure US Government agencies and departments can take full advantage of digital transformation to benefit citizens, services, public workers and the economy.

Truly embracing digital technologies has the potential to affect all aspects of how government delivers services to citizens, from streamlining internal processes to delivering new engagement models via digital channels. Microsoft models these changes in four pillars:

**ENAGE YOUR CITIZENS**

Engage citizens through web, mobile and other channels for greater connection and participation

- Provide 24/7 access to services through multiple digital delivery channels
- Streamline citizen engagements by improving collaboration and information sharing

**EMPOWER YOUR EMPLOYEES**

Boost productivity with flexible workstyles and mobile solutions that enable a data-driven culture.

- Enable workers to interact and communicate more easily and effectively
- Enable smarter citizen interactions by empowering field workers, case workers, inspectors and community leaders with secure mobile apps

**OPTIMIZE YOUR OPERATIONS**

Streamline and accelerate service delivery by transforming legacy processes.

- Eliminate paper-based processes for next level of efficiency
- Optimize service delivery costs with the flexibility and elastic scale of cloud-based services

**TRANSFORM YOUR SERVICES**

Use cloud technologies to deliver new services benefiting society and the economy

- Harness the data explosion to gain insights and deliver better decision making
- Leveraging digital platforms to reduce delivery timeframes

**FURTHER READING**

- [Case Study: Veterans Affairs](#)
- [Government cloud adoption case studies](#)
- [Microsoft Digital Transformation eBook Series](#)
- [Designed to Disrupt: Reimagine your apps and transform your industry](#)
The Cloud Enables Digital Transformation

Digital transformation helps you connect people, data, and processes in new ways, creating new opportunities for service delivery and efficiency. Cloud technologies are at the center of the digital transformation revolution.

The cloud has changed more than the way we implement and manage IT; it's changing the services themselves. With ready access to data, and intelligent new ways to view, analyze and use the information, the cloud has engendered powerful new capabilities. There are many advantages to adopting the cloud. These benefits fall into four broad categories: cost, agility, service quality, and new capabilities:

- **Cost**: Cloud computing offers significant potential cost-savings over on-premises infrastructure, especially considering the full cost of the latter. In addition, cloud computing may help enable organizations to move IT spending from capital expenditure (CapEx) to operational expenditure (OpEx). Since the fixed costs associated with shared infrastructure are avoided, the cloud also provides much greater visibility into the true cost of individual applications.

- **Agility**: Where traditional on-premises infrastructure can take weeks or even months to deploy, Azure offers near-instant provisioning of resources. This helps enable Azure projects to move much more quickly, without the need to over-provision resources in advance or spend considerable time on infrastructure planning. To take full advantage of this new flexibility, organizations are accelerating the adoption of new ways of working, such as using agile software development methodologies, continuous integration and deployment (CI/CD), and modern PaaS-based application architectures.

- **Service quality**: Azure’s infrastructure has been designed to support some of the world’s most demanding workloads. These workloads continuously raise the bar on the quality of service Azure must provide. As a result, migration to Azure often offers significant improvements in performance and reliability compared to traditional infrastructure. Azure Government has been designed to meet or exceed the security and compliance requirements for government services.

- **New capabilities**: Azure enables new application scenarios which may simply not be possible, or would be prohibitively expensive to deliver, using on-premises infrastructure, such as big data storage and analytics, and machine learning. These technologies are enabling new services and driving innovation only available in the cloud.
These benefits are all central to a successful digital transformation strategy. Reduced costs and the shift from CapEx to OpEx dramatically lowers the cost of innovation, and service delivery. This is supported by the increase in agility that lowers innovation cost still further. The scale, performance, and reliability of the cloud enables small development teams to develop critical services for national audiences.

Most of all, new technologies including big data, IoT, machine learning, and AI empower the insight and user focus upon which digital transformation depends. These technologies are often only available in the cloud or are prohibitively expensive on-premises. Moreover, competition between major cloud providers is driving a tidal wave of innovation within the cloud itself. New features and services provide an ever-richer platform to continue to experiment, innovate, reduce cost and deliver improved services.

Embracing the cloud is not simply the easiest, or cheapest, or fastest way to drive digital transformation—it is the only way. In many cases, the first step on this journey is to migrate existing applications to the cloud.

The US Government is Embracing the Cloud

The federal government recognizes the potential for cloud services to transform government services and delivery. This is reflected in several initiatives:

- The Modernizing Government Technology Act allows federal agencies to repurpose unused IT budget to fund modernization projects. This gives agencies new opportunities to resource cloud migration and modernization projects.
- The Office of Management and Budget Cloud Smart Strategy supports cloud adoption in federal agencies. It is intended to promote best practices, security and faster service delivery.
- The President’s Management Agenda establishes cross-agency priority goals for each of three key areas: IT modernization, data accountability and transparency, and modernizing workforce skills.
- GSA’s IT Schedule 70 Cloud Special Item Number 132-40 makes it easier for agencies to acquire cloud services by providing centralized, streamlined access to services.
- GSA’s Cloud Information Center (CIC) is a collaborative community and central repository for all things cloud.
Adopting a Cloud Mindset

Taking full advantage of the digital transformation opportunities of the cloud requires a cultural change, with implications across the organization. It’s not simply another IT project.

Adopting the cloud is a far-reaching change, with implications beyond simply the way IT projects are implemented and delivered. The implications of the cloud extend far beyond IT, impacting other parts of the organization. To take full advantage of the digital transformation opportunities offered by cloud technologies, an organizational cultural change may be required to adopt what we call a cloud mindset. Conversely, without a cloud mindset, the full benefits of cloud adoption cannot be realized.

What is a Cloud Mindset?

What is a cloud mindset? In part, it’s about letting go of received wisdom regarding traditional IT. It’s a new and positive can-do way of thinking about services and service delivery, unencumbered by past restrictions. With near-instant provisioning and easy reconfiguration, developing services in the cloud is fast, agile, and reactive to user needs. However, if cloud projects are delivered using waterfall development processes designed for the era of multi-month provisioning schedules, then the benefits of fast provisioning are lost. Processes must be updated to take advantage of cloud agility.

The impact of cloud, and the need for a cloud mindset, extends beyond the IT department. Service owners can become more deeply engaged in how IT delivers those services since service improvements can be delivered rapidly, and the cost of experimentation is low. Finance for IT must adapt to the shift from capital to operational expense. Human resources must deliver the skills and career paths necessary to deliver in the cloud.

A cloud mindset is also about recognizing new possibilities. An automated chatbot that helps citizens navigate thousands of pages of information by asking natural-language queries can improve user experiences while reducing support costs. IoT and big data analytics analyzing weather data from government vehicles enables more accurate, targeted road treatment reducing accident rates. Smart mobile apps for field workers that transform productivity. The potential is huge, but requires a creative approach to embracing new possibilities, and letting go of previous beliefs about what IT is for and what it can do.

Adopting cloud requires a fundamental change. It’s not simply new skills that must be acquired in addition to the old. Cloud requires people to work and think differently. People need to challenge themselves and others to question existing practices and revisit past experiences.

Management have a critical role to play. Culture change at this level requires a growth mindset, which needs to be promoted and modelled by the leadership.

Staff must also understand the rationale and benefits of the cloud and embrace change as an opportunity for both the organization as well as for them personally. Also, developing new, in-demand skills, cloud enables technical staff to operate more efficiently and deliver greater value.

Overall, it is important to present these changes in a positive context. Cloud is a huge opportunity for both the organization and each individual to succeed and grow. Change at this level is not without risk and mistakes are inevitable. For people to feel safe stepping outside of their comfort zones, a culture of learning rather than blame is required to handle the inevitable missteps and issues that will arise on the way.

FURTHER READING

➔ Embracing the cloud mindset with Scotia Bank (YouTube)
Creating a Cloud Strategy

Resources

A good start on your cloud journey is to define your cloud strategy.

Developing a cloud strategy should not be scoped purely at the IT level, since without engagement from service teams and other stakeholders such as finance, the full benefits of the cloud cannot be achieved. This means the team charged with developing your cloud strategy will require executive sponsorship if it is to be successful.

Key stakeholders across the organization must be identified and engaged. This first requires that they are educated and informed on the capabilities and benefits of cloud adoption, and on the extent of the changes that will be required, so they fully appreciate why their engagement is essential.

What does a cloud strategy look like? At a high level, it is a document describing the vision and goals of your cloud adoption. It should include high-level timelines, and an overview of the approach that will be used to adopt the cloud and migrate existing applications. The impact to each stakeholder group should be articulated, as well as the expected benefits.

The cloud strategy forms the foundation for executive sponsorship going forward. Your Cloud strategy requires clear top-level commitment to executing against the plan, together with broad alignment across all stakeholders. This includes commitment to making the necessary changes, at an organizational and process level as well as at the technical level. It must also be appropriately funded and staffed.

Creating the strategy is just the beginning. The next stage is to make sure everyone understands the cloud strategy, and how it supports the broader digital transformation goals. The strategic rationale and benefits must be broadly understood. Everyone should be able to answer the question, 'why cloud?'

Be clear about how each team and individual contributes, and the growth opportunities for each individual and team. Explain the plans to ensure staff can develop the skills they will need to be successful. IT has always been evolving, and successful IT careers are not forged by standing still.

This is not a one-time conversation. A growth mindset must be cultivated and promoted continually though ongoing behaviors, and leaders need to lead by example.
Bringing in the Right Stakeholders

A cloud strategy is an organization wide effort and will require many stakeholders committed to its success.

Bring in key stakeholders early in the planning process and ensure expectations are clear on who is responsible for what outcome.

Many organizations build a core cloud strategy team with representatives from each area impacted by the cloud. This team may grow or shrink in size as strategy is executed.

EXAMPLE STAKEHOLDERS AND HOW THEY ARE IMPACTED

• **Institutional Leadership** – provide the executive sponsorship and overall vision that aligns the rest of the cloud strategy team and ensures funding and accountability.

• **IT Leadership** – provides the technical decision making and implementation teams to deliver on the cloud vision.

• **Legal** – contracts with cloud provider, implementation contractors, existing data center agreements.

• **Finance / Procurement** – moving from capital expenditure to operational expenditure model, purchasing negotiations, license optimization.

• **Human Resources** – new role descriptions, acquiring new talent, reskilling existing talent.

• **Security and Compliance** – identifies and overcomes risks associated with how authorization and identity in the cloud. Helps navigate regulations and to ensure compliance.

All stakeholders should have a base level of knowledge of Azure and its capabilities and the various cloud operating models. Microsoft Learn provides a free on-demand course, Azure Fundamentals, that is specifically designed for technology and business professionals that teaches these core competencies.

The [Cloud adoption using the Microsoft Cloud Operating Model whitepaper](aka.ms/AzureGovPlaybook) is another great resource to leverage as part of this early planning phase.
Understanding the Migration Process

Before you focus on defining your strategy it’s helpful to understand at a high level what the migration process is. It can be broken down into three key phases:

**ASSESS**

The assessment phase is where your team will use a mixture of software tools and consultancy best practices to discover what applications and services can be migrated, what their current configurations are, and the people that will be impacted by the migration, as well as identify any dependencies of the application. The output of your assessment will include a comprehensive plan for what to do with the application and the expectations on availability and functionality.

**MIGRATE**

The migration phase is when the recommendations in your assessment plan are put into place. The following steps are usually taken:

- Setup Azure subscriptions using best practices for security, connectivity, policies and general governance prior to migration to ensure you are using Azure correctly from the start.
- Perform the migration using the prescribed method identified in the assessment plan.
- Evaluate and test to ensure the migrated application meets the criteria outlined in your assessment.
- Cut over production traffic to the migrated service.

**OPTIMIZE**

In the optimization phase, you will use Azure security and management resources to govern, secure, and monitor your cloud applications in Azure. This is also the time to look for opportunities to optimize spending. Common tasks at this stage are:

- Review Azure Cost Management and Azure Advisor to track spending and identify areas for cost savings.
- Evaluate migrated applications for opportunities to right size over provisioned virtual machines and services.
- Implement automation to resize or stop based on a utilization schedule.
- Identify applications that could benefit from optimization with platform as a service (PaaS) services or containers.

Learn more in the Azure Migration Center

The Azure Migration Center provides detailed information to help you with planning small scale to large scale migrations. There are resources for tools, best practices, and webinars to help you quickly get up to speed on the different options such as rehosting, refactoring, rearchitecting, available to move your workloads to Azure.

FastTrack for Azure White Glove Migration

For federal customers, FastTrack for Azure has a White Glove Migration service that provides access to Azure engineers and a 10G ExpressRoute, located at our Chevy Chase office in Maryland, directly into Azure Government. This engagement allows you to quickly and confidently migrate your data leveraging your own hardware or Azure’s Data Box family of products. Learn more about the program and its eligibility criteria by visiting FastTrack for Azure or by speaking to your account team.
Understanding Agile and DevOps

A DevOps approach to software development leverages the agility of Azure Government for faster, more efficient delivery.

Traditional IT projects use ‘waterfall’ development methodologies. These are characterized by distinct planning, development, testing and deployment phases with strict quality gates controlling progression from one phase to the next. Projects typically take several months or even longer to complete.

This approach to IT was evolved to provide clear timelines and enable traditional IT hardware provisioning, which can frequently take several months from placing an order to having the hardware available. Without the up-front planning of a waterfall process, the hardware would not be available when the project needs it.

However, waterfall development has several shortcomings. Any changes to the project requirements, design or scope can cause significant disruption to the plan. Working software is only available for review late in the process, magnifying the risk of misunderstandings in requirements. IT work is notoriously difficult to estimate, and schedule slips are common. And most importantly, there is a long delay between identifying a requirement and delivering a solution to meet that requirement.

AGILE DEVELOPMENT

Recognizing this, a number of alternative software development methodologies have emerged over several decades. These are characterized by short development cycles and rapid feedback loops, in which software is developed in short, iterative ‘sprints’, each delivering incremental value to production. This is a fundamentally different approach to software development favoring a reactive, iterative approach instead of relying on large up-front plans. Collectively, these approaches are known as agile development methodologies, and their principles are captured in the Manifesto for Agile Software Development, first published in 2001.

A challenge faced by these agile methods is that IT hardware still required long provisioning times, and once purchased was highly inflexible. While application software could be evolved rapidly, the same was not true of hardware.

This changed with the advent of the cloud. Cloud computing provides flexible computing infrastructure with provisioning times measured in minutes instead of months. In addition, developing applications to run on platform-as-a-service cloud platforms greatly reduces the requirements for on-going maintenance. Cloud technologies also provide streamlined, integrated tools for rapid development, testing and deployment with no more than a few clicks of a mouse.

Cloud computing therefore enables a new wave of agile development. In the cloud, both the software and the underlying infrastructure evolve as one. An ‘infrastructure as code’ approach treats the infrastructure for a service simply as a cloud configuration file, managed alongside the code, allowing one-click deployment of entire application environments.

DEVOPS AND DEVSECOPS

Recognizing the productivity potential offered by agile software development, some organizations have restructured not just their processes, but also their teams. Traditional IT has a separation between development, testing, and operations teams, with code passed ‘over the wall’ between teams. To increase agility, these walls are being torn down and teams integrated, with the development, test and operations disciplines being combined into a single ‘DevOps’ team.

In a DevOps model, a single team owns the service, from design through implementation, testing, deployment and into production. The same team who wrote the code are now responsible for keeping it running 24x7 and are on-call when it fails. This leads to a greater emphasis on
quality, reliability, and serviceability, since the developers prioritizing changes and fixes are directly affected by the consequences of those choices. It also creates greater efficiency by breaking down communication barriers. The net result is higher quality services and greater efficiency.

Taking this theme of shared execution and accountability further, a more recent trend is the emergence of a ‘DevSecOps’ approach. This integrates security responsibilities into the DevOps team, and every step of the development and operations process. Since security is hard to retrofit, this approach can be particularly relevant in Azure Government projects where security is especially critical.

**FURTHER READING**

- [Open source DevOps in Azure Government](#)
- [Azure Government developer blog](#)
- [Azure Government YouTube playlist](#)
Building a Center of Excellence

Lower your costs, reduce risk, and deliver cloud projects more quickly and efficiently by taking advantage of the GSA Cloud Adoption Center of Excellence.

In the Enterprise sector, establishing a Center of Excellence is a proven technique for helping to accelerate cloud adoption while reducing risks. The US Government is adopting a similar approach, with the creation of the cloud adoption Center of Excellence within the GSA.

The role of the Center of Excellence is not to deliver your cloud projects for you. Rather, they are a supporting organization that enables your cloud teams to move more quickly and with greater confidence. The Center of Excellence offers expert advice and best practice guidance based on industry and government experience. These are available to your cloud teams across the following areas:

- End-to-end migration planning and modernization assessments
- Migration strategy and approach
- Migration roadmap and execution timelines
- Security and governance models
- Acquisition and oversight support services.

The Cloud Adoption Center of Excellence is just one of a number of IT Centers of Excellence with the GSA. Other Centers of Excellence include Contact Center, Customer Experience, Data Analytics and Infrastructure Optimization. All of these can play an important role in the digital transformation of Government services. These Centers of Excellence can help your projects minimize risk and cost, reduce completion time, and ensure compliance.

The USDA have been early adopters of the Centers of Excellence program. As well as taking advantage of the Center of Excellence services, the USDA has embedded 10 of its own key staff members within the Centers of Excellence, creating a deeper working relationship. In phase 1, the agency has realized around $26 million in cost avoidance and savings as a result of the Centers of Excellence this program.

FURTHER READING

- GSA Centers of Excellence
- Cloud Adoption Center of Excellence
Reskilling for the Cloud

As part of embracing a cloud-based world, you should understand some of the steps needed to manage acquiring and growing the technical experts you need.

**Mapping Existing Staff** - the cloud requires new skills, but this doesn’t mean that your existing staff is not up the challenge! A successful reskilling exercise will require identifying the needed skills and roles your practice will need going forward and then mapping your existing team to those roles. Once identified, an onboarding plan will be identified to help guide your new experts on their chosen path.

**Interviewing/Hiring New** - in many cases, the cloud offers capabilities that no one on your team has an appropriate background for. In those cases, you may need to hire new talent. You should start off with a defined role and the needed soft and technical skills for the role and then move forward with a recruitment plan to find the best fit for your organization. We’ll discuss some options for finding new talent later in this section.

**Onboarding** - Every existing team member or new hire will need an onboarding plan to be successful. This means a list of external and internal training to take, to learn not only the technology they will use on a day-to-day basis but also the systems your organization has created to deliver solutions consistently for your users. A good onboarding plan will also involve a method for ongoing training such as access to on-demand training and lab environments, as well as access to a technical community.

**Building a Technical Community** - Technical communities can be an incredibly beneficial way of increasing the technical expertise within your organization. Putting subject matter experts on tools such as Yammer, Microsoft Teams, Slack (and many others) has the benefits of spreading their expertise across the organization as well as providing easy access to often asked questions and scenarios your teams may face.

**Rewarding Assistance** - Giving your team the ability to communicate with each other and help others in the organization is a big step in building a learning and helping culture. The leaders of your practice should be encouraged to publicly praise or reward team members when they go out of their way to help each other.

**Retaining your staff** - Hiring and onboarding is only the first step among many to build a rock solid technical and business delivery team. Ensure frequent communication about the company’s goals, and about expectations of your team are essential. Working with your human resources team to establish an employee retention plan is key, there are many low cost and low impact techniques to ensure a happy workforce.
Training & Readiness

Preparing and Training Technical Staff for the Cloud

Follow a learning curriculum to build the skills you need most to stay relevant.

Suggested resources to help onboard your team for training success are available in this section. This includes a range of online learning resources for self-paced learning, as well as options for instructor-led training for rapid technology adoption.

Use the following resources as part of your Azure onboarding for new and existing staff:

- **Microsoft Learn** is a free, online training platform that provides interactive learning including [Azure Training and Certifications](https://aka.ms/AzureGovPlaybook). Become proficient with fun, guided, hands-on, interactive content that's specific to your role and goals.

- **Microsoft Azure Hands-on Labs** provides free, self-paced labs to help you stay current with Azure. The live environments are fully self-contained. You do not need your own Azure subscription to complete the labs, just login with a remote desktop (RDP) client and get started.

- **Microsoft Learning** offers a wide variety of official curriculum on-demand, as well as [edX courses that are taught by Microsoft experts](https://aka.ms/AzureGovPlaybook), and help you learn through hands-on experiences with a broad reach of Azure technologies.
Additional Resources

MICROSOFT CONFERENCE RECORDINGS
Even if you missed the annual live event, Microsoft provides many of its sessions as on-demand recordings—no conference pass required.

- **Microsoft Build** focuses on latest trends and future looking technology innovations for leading architects, developers, start-ups and student developers
- **Microsoft Ignite** focuses on innovative ways to build solutions and migrate and manage your infrastructure. There are also hands-on experiences to help you innovate in areas such as security, cloud, and hybrid infrastructure and development.
- **Microsoft Inspire** is a partner-to-partner networking event to connect, collaborate and celebrate as one community. Informed and inspired by shared experiences and insights that will help grow your business with Microsoft.

MICROSOFT LEARNING PARTNERS
Microsoft Learning Partners are available worldwide to help enable your team for Microsoft Azure via live instructor-led training. This can be scheduled as a dedicated delivery at your location or virtually using remote learning technologies. Many courses are scheduled as open-enrollment courses, which doesn’t require you to schedule a dedicated class.

- **Opsgility** is a key Microsoft partner that offers Azure and Office 365 training. Find more than 200+ online classes focused on Azure with full learning paths for Azure certification. Opsgility also offers a full set of instructor-led Azure trainings that focus on architects, developers, DevOps, operations, sales, and decision makers.
- **Pluralsight** is a key Microsoft partner that offers Azure training. Gain the know-how and confidence your job demands through these free online courses, delivered in partnership with Pluralsight.
- **O’Reilly Safari** provides subscription access to more than 40,000 books, videos, and interactive tutorials from over 200 of the world’s best publishers, including O’Reilly, Pearson, Harvard Business Review, and Packt. It also offers live online training courses led by instructors from O’Reilly’s network of tech innovators and expert practitioners.
- **FastTrack for Azure** can also help you accelerate your learning and cloud adoption via workshops.
Azure Certifications

There are numerous certifications your team may want to consider as additional motivation for advancing their skills.

Microsoft role-based Azure certifications may be a useful way to identify skills, measure progress and motivate your team.

**MICROSOFT ROLE-BASED CERTIFICATIONS**

**MICROSOFT CERTIFIED AZURE FUNDAMENTALS**

Prove that you understand cloud concepts, core Azure Services, Azure pricing and support, and the fundamentals of cloud security, privacy, compliance, and trust.

- [Exam AZ-900: Microsoft Azure Fundamentals](#)

**MICROSOFT CERTIFIED AZURE ADMINISTRATOR ASSOCIATE**

Azure Administrators implement, monitor, and maintain Microsoft Azure solutions, including major services related to compute, storage, network, and security.

- [Exam AZ-103: Microsoft Azure Administrator](#)

**MICROSOFT CERTIFIED AZURE DEVELOPER ASSOCIATE**

Microsoft Azure Developers design, build, test, and maintain cloud solutions, such as applications and services, partnering with cloud solution architects, cloud DBAs, cloud administrators, and clients to implement these solutions.

- [Exam AZ-203: Developing Solutions for Microsoft Azure](#)

**MICROSOFT CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT**

Microsoft Azure Solutions Architects must have expertise in compute, network, storage, and security so that they can design solutions that run on Azure.

- [Exam AZ-300: Microsoft Azure Architect Technologies](#)
- [Exam AZ-301: Microsoft Azure Architect Design](#)

**MICROSOFT CERTIFIED AZURE DEVOPS ENGINEER EXPERT**

Azure DevOps professionals combine people, process, and technologies to continuously deliver valuable products and services that meet end user needs and business objectives.

- [Exam AZ-400: Microsoft Azure DevOps Solutions](#)

**RESOURCES**

[Microsoft Role-based Certifications](#)
Hiring and Job Description Resources

The following tables provide detailed job description examples you can leverage to hire key technical resources.

Use these job descriptions as starting points when hiring your cloud team. All technical skills, non-technical skills, certifications, and technologies listed are potential items a candidate should have, but no candidate will have all the items listed.

### CLOUD ARCHITECT

A Cloud Architect (CA) drives high-priority customer initiatives in collaboration with customers and your sales team. The CA is a technical, customer-facing role that is accountable for the end-to-end cloud experience. CAs own the Azure technical user engagement including architectural design sessions, specific implementation projects and/or proofs of concepts. The ideal candidate will have experience in customer-facing roles and success leading deep technical architecture and application design discussions with senior customer executives to drive cloud deployment. Bachelor’s degree in computer science or related field preferred.

#### Technical Skills

- Solid understanding of modern authentication protocols and a background in cyber security.
- Deep understanding of cloud computing technologies, business drivers, and emerging computing trends.
- Deep technical experience in enterprise mobile, identity and access control, & security solutions.
- Understanding of cloud governance technologies for cost management and control.
- Understand how to define SLAs and design systems to meet those SLAs.
- Understanding of common database technologies such as SQL Database/Server, Oracle, MySQL
- Working knowledge with AGILE development, SCRUM and Application Lifecycle Management (ALM) with one or more of the following programming languages: PowerShell, Bash, .NET, C++, Java, JSON, PHP, Perl, Python, Ruby on Rails, HTML, CSS, JavaScript, Responsive Web Design.

#### Non-Technical Skills

- Proven track record of building technical relationships at all levels.
- Proven track record of driving decisions collaboratively, resolving conflicts & ensuring follow through.
- Presentation skills with a high degree of comfort with both large and small audiences.
- Prior work experience in a consulting/architecture position within a software & services company.
- Problem-solving mentality leveraging internal and/or external resources.
- Exceptional verbal and written communication.

#### Certifications

- Exam priorities: [AZ-300 Microsoft Azure Architect Technologies](https://aka.ms/AzureGovPlaybook), [AZ-301 Microsoft Azure Architect Design](https://aka.ms/AzureGovPlaybook).
Project Experience Types/Qualities

- 5+ years of architecture, design, implementation, and/or support of highly distributed applications (i.e. having an architectural sense for ensuring availability, reliability, etc.).
- Experience of 2+ significant Azure migration projects.
- 5+ years of success in consultative/complex technical and deployment projects (where necessary, managing various stakeholder relationships to get consensus on solution/projects).
- Oversight experience on major transformation projects and successful transitions to implementation support teams.

Technologies

CLOUD INFRASSTRUCTURE ENGINEER

The Cloud Infrastructure Engineer delivers technical solutions and support to users allowing them to maximize their investment in cloud technology. The ideal candidate will have experience and success implementing cloud-based solutions, migrating workloads to the cloud, and experience with connecting and managing hybrid cloud environments.

Building upon solid IT project experience relative to their level, cloud infrastructure engineers are responsible for:

- The delivery of high-quality engagements around Microsoft’s solution areas, technologies and products in diverse client environments.
- The design and development of integrated solutions using the latest Microsoft products and technologies.
- Understanding the relevant application development, infrastructure and operations implications of the developed solution.

Technical Skills

- Deep understanding of cloud computing technologies, business drivers, and emerging computing trends.
- Deep technical experience in infrastructure design including private and public cloud, networking, virtualization, identity, security and storage.
- Understanding of how to build resilient multi-site architectures.
- Experience with Windows, Linux and OSS technologies.
- Experience with configuration management and automation technologies such as PowerShell DSC, Chef, ARM Templates, and Puppet.
- Experience with deploying and managing the infrastructure for databases such as SQL Server, Oracle, Maria, Cassandra
- Working knowledge with AGILE development, SCRUM and Application Lifecycle Management (ALM) with one or more of the following programming languages: PowerShell, Bash, .NET, C++, Java, JSON, PHP, Perl, Python, Ruby on Rails.

Non-Technical Skills

- Services project management.
- Building cross-organizational relationships.
- Proven track record of driving decisions collaboratively, resolving conflicts and ensuring follow through.
- Presentation skills with a high degree of comfort with both large and small audiences.
- Problem-solving mentality leveraging internal and/or external resources.
- Exceptional verbal and written communication.

Certifications

- Microsoft Certified Azure Administrator Associate, AWS Certified SysOps Administrator
- Exam priorities: AZ-103 Microsoft Azure Administrator
Project Experience Types/Qualities

- 3-5+ years senior (Tier 3) level support with cloud infrastructure as part of responsibilities.
- 5+ years of architecture, design, implementation, and/or support of highly distributed applications (i.e. having an architectural sense for ensuring availability, reliability, etc.)
- 2+ years of experience in “migrating” on premise workloads to the cloud.
- 5+ years of success in complex technical and deployment projects (where necessary, managing various stakeholder relationships to get consensus on solution/projects.
- Oversight experience on major transformation projects and successful transitions to implementation support teams.

Technologies

A Senior Software Developer has a history of designing, owning and shipping software, as well as excellent communication and collaboration skills. With a focus on cloud-based application development, the candidate must have demonstrable experience architecting and deploying applications to cloud platforms, the ability to effectively integrate disparate services as needed, and decide when to implement IaaS, SaaS, and PaaS components. As a mentor to junior developers, the senior software developer should have a solid understanding of the software development cycle, from architecture to testing. They should have a passion for quality and be a creative thinker. A senior developer will write secure, reliable, scalable, and maintainable code, and then effectively debug it, test it and support it live. This person should also be comfortable owning a feature and making decisions independently, and should have leadership experience with agile methodologies, such as the Scrum approach to agile software development.

A Senior Software Developer can also effectively gather customer requirements and ask clarifying questions when needed. This person must be able to translate these requirements to actionable tasks they will perform, or delegate to members of the team. The ideal candidate will have experience in customer facing roles and success leading deep technical architecture and design discussions with senior executives.

Eight plus years of experience with deep understanding of web technologies, API consumption/development, full lifecycle application development, database development (relational and/or NoSQL), and enterprise/cloud architecture. Technical BS degree in Computer Science desirable, and experience in:

- The delivery of high-quality engagements around Microsoft’s solution areas, technologies and products in diverse environments.
- Stabilizing developed solutions using Microsoft methodologies in complex environments.
- The design and development of integrated solutions using the latest Microsoft products and technologies.
- Understanding the relevant application development, infrastructure and operations implications of the developed solution.

Bachelor’s degree in computer science or related field preferred.

**Technical Skills**

- Distributed application and database design and development including scalability and performance, API management, RESTful services
- Database architecture, design, and lifecycle management, data modelling, data transformation
- High availability, disaster recovery, data replication, health checks, resiliency and backup
- Cloud-native architecture, design patterns and implementation
- Application modernization, refactoring, and migration including microservices and containers
- Cloud operations, DevOps, monitoring, diagnostics, reporting, governance
- Cloud security and compliance
Non-Technical Skills

- Collaboration, stakeholder management, relationship management, technical oversight, technical recommendations, problem solving, risk management, architecture design session, program management, proof of concept design, technical demonstration, excellent communication skills.

Certifications

- Microsoft Certified Azure Developer Associate, Certified ScrumMaster, AWS Certified Developer.

Project Experience Types/Qualities

- API consumption and development, coordinate and execute pilots, prototypes or proof of concepts, provide validation on specific scenarios, document and share technical best practices, further customer investment, hybrid solutions on premises or in the cloud, industry-visible, CI / Continuous Deployment, large project relative to size of customer, lift and shift, migrations and upgrades (SQL, etc.), on-premises to cloud, production environment, projects where data is born in the cloud, cross-platform SQL Server migration, server-side/desktop development, service architecture, size of project team (complexity), significant challenges, source code repository implementation support teams.

Technologies


- **Programming/Scripting Languages**: .NET (C#, F#, VB.NET), Java, Python, JavaScript, Scala, Go, Ruby, PHP, SQL, T-SQL, PowerShell

- **Platforms**: Linux (Red Hat, Ubuntu, Debian, etc.), Windows.
## PROJECT MANAGER

The Project Manager is responsible for the overall success of the project. They are responsible for ensuring the initial vision and goals of the project are clearly defined and aligned with all relevant stakeholders and executing the project to meet those goals. This includes building project plans, tracking and managing risks, analyzing dependencies, and communication within the team, with management, and with the customer.

Throughout the project, the Project Manager will need to make scoping and prioritization decisions as issues arise. Making good decisions is only possible if the Project Manager can fully understand each issue. In addition, a good Project Manager can anticipate issues before they arise and take pre-emptive corrective action. In addition to strong project management skills, the Project Manager should also have a strong technical background.

### Technical Skills
- Solid technical background in IT infrastructure and application architectures.
- Solid understanding of cloud computing technologies, business drivers, and emerging computing trends.
- Solid understanding of cloud migration approaches and supporting tools.

### Non-Technical Skills
- Strong project management skills including experience of a variety of project management methodologies such as Agile, SCRUM, waterfall methodologies, etc.
- Demonstrated success in driving complex projects with multiple stakeholders and dependencies.
- Proven track record of building deep technical relationships with senior executives and growing cloud consumption share in large or highly strategic accounts.
- Proven track record of driving decisions collaboratively, resolving conflicts & ensuring follow through.
- Strong written and spoken presentation skills with a high degree of comfort with senior audiences.

### Certifications
- A relevant Project Management qualification such as PMP, Certified ScrumMaster or PRINCE 2.
- Microsoft Certified Azure Fundamentals, Microsoft Certified Azure Administrator Associate.

### Project Experience Types/Qualities
- 5+ years technical project management experience leading complex projects on critical IT systems.
- 3+ years in hands-on technical IT role (e.g. developer, operations engineer).
- Experience of delivering projects through the FedRAMP ATO process.

### Technologies
- Project Management and issue tracking tools (VSTS, MS Project, or similar).
- Infrastructure, Networking and Storage technologies (including MS SQL or other databases).
- Azure IaaS, Azure Backup, Azure Site Recovery.
Migration Assessment

Migration and Modernization with Azure Government
Executive Summary

A Migration Assessment Plan provides the foundation for a successful cloud migration. Any issues not identified during planning risk derailing your migration project.

The first step to migrating or modernizing a workload with Azure is to build a Migration Assessment Plan. The migration assessment should answer the following questions:

- What applications and infrastructure am I currently running?
- Of these applications, which should be migrated, modernized, retired, replaced, or maintained on-premises?
- What are the risks associated with a migration, and how long will it take?
- What are the costs associated with the migration?
- What additional benefits will cloud migration deliver for my service?

Creating the Migration Assessment Plan should be an iterative process. Identify applications for migration, create the assessment plan, and migrate. This allows improvement in future assessments as well as increased velocity as you identify areas that can be improved in your process. Planning normally follows the following three phases:

1. A **discovery** phase, in which the current applications and infrastructure are documented, as well as the business context and overall goals for the migration.
2. A **planning** phase, in which a detailed cloud design and migration plan are constructed.
3. An **evaluation** phase, which builds the business case for the migration for review and sign-off by the final decision makers.

Top 4 things to do

A migration assessment is the foundation for successful migration project. Here are the top 4 things for successful migration assessments.

- Develop a comprehensive migration assessment methodology
- Choose your migration assessment tools
- Learn how to accurately calculate return on investment
- Build migration roadmaps, prioritizing the simplest migrations
Discovery

The goal of the discovery phase is to fully understand the existing infrastructure and applications, and the context and goals surrounding those applications and their move to the cloud. This informs the planning and evaluations phases which follow.

A full discovery process requires you to analyze the existing workload from several viewpoints and using a variety of methods and tools.

APPLICATION CONTEXT

It’s important to understand the service which each application provides. What does it do? Who uses it? What is the impact of an outage? Placing the existing applications in their correct context is essential to making informed decisions regarding prioritization, design, and indeed every aspect of the migration project.

Equally important is an understanding of the end users and how they use the application. In many cases, cloud migration will be a seamless change, of which users will be unaware. In other cases, migration is used as an opportunity to upgrade the user experience, so users may need to access applications differently, or perform specific tasks in new ways. To help users embrace rather than resist this change, it’s important to understand the user experience, and to keep stakeholders informed and engaged throughout the migration process.

Existing pain points (such as reliability, performance, or issues with functionality) should be identified. Migration to cloud is often an opportunity to reduce or remove such problems. These kinds of positive changes make it easier to get buy-in from both decision-makers and end users.

REQUIREMENTS

As with any IT project, a clear understanding of requirements is vital. Since this is a migration project, the functional requirements of the system—what it does—will be largely unchanged from the existing system. Your focus should be on capturing non-functional requirements.

Non-functional requirements, such as reliability, performance, and forecasted scale must be understood so they can be factored into the design. The cloud offers far greater flexibility than on-premises infrastructure and is therefore able to adapt quickly to changes in demand. Even so, some requirements—such as very high availability delivered through redundancy across more than one Azure region—have design and cost implications that need to be captured up-front.

Likewise, security and compliance requirements must be captured. As we have seen, Azure Government offers a comprehensive portfolio of security and compliance accreditations. Delivering an application that is compliant with a specific set of standards requires that the design be reviewed against the Azure guidance for those standards.

ON-PREMISES IMPLEMENTATION AND DEPENDENCIES

Of course, the discovery phase must also capture the details of the existing application implementation. The hardware, network, and storage infrastructure must be documented. It is important to capture the actual usage as well as the physical specifications. Traditional infrastructure is often over-provisioned to handle expected future demand or worst-case scenarios, and the agility and elastic scale of the cloud offers the opportunity to optimize significantly on this approach. Usage should be measured at both normal and peak expected load. Data should be gathered on CPU, memory, network (latency and bandwidth) and storage (capacity, IOPS, and throughput).

Any dependencies between components and systems, such as between application servers and databases, must be identified and mapped. Understanding these dependencies is important when grouping and sequencing migrations during the planning phase.

Capture the current version of all software, and all operating systems—in some cases, updating the software to more recent, supported versions may be required as a pre-requisite to migration. Where software is developed in-house, the availability of source code and skilled staff familiar with the code must be established. Where
software is licensed, vendor support for cloud technologies must be understood. For example, does the vendor already offer a cloud-based version of the software? If the software uses Microsoft SQL Server, has the vendor certified use with Azure SQL Database?

**METHODS AND TOOLS**

A variety of methods must be employed to gather all this information. First, it is important to identify key stakeholders, such as service delivery owners and technical staff. Interviews with each stakeholder will be necessary to understand their perspectives and priorities, and to gather their input on the topics listed above.

Various tools are also available to assist with gathering technical data on the existing infrastructure, from both Microsoft and third parties. In many cases, these tools can also help with the subsequent migration planning, costing, and even with the migration execution.

Examples of available tools, from both Microsoft and third-party vendors, are given in below. These are all supported in the Azure public cloud, check with the individual vendors for Azure Government support. You can also consult the [Azure Migration Center](#) for more information.

<table>
<thead>
<tr>
<th>MICROSOFT OFFERINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Migrate</strong>: The Azure Migrate tool can be used to assess on-premises workloads for suitability, as well as offering advice on performance-based VM sizing and cost estimations. The initial release of Azure Migrate only supports assessment for VMware VMs. Support for Hyper-V assessment and VMware migration is coming soon. Azure Migrate offers the following capabilities:</td>
</tr>
</tbody>
</table>
| • Discover and assess on-premises VMs  
• Confidently plan your migration  
• Easily migrate your workloads to Azure |
| More resources: |
| • [Assess on-premises workloads for migration to Azure](#)  
• [Watch a Demonstration of Azure Migrate](#)  
• Azure Migrate hands-on lab |
<p>| <strong>Azure App Service Migration Assistant</strong>: The Azure App Service Migration site is a dedicated site to support migrating application to Azure App Service. For Internet-facing sites, an online assessment provides an initial migration compatibility report in seconds. You can then download the App Service Migration Assistant for an in-depth assessment of both on-premises and Internet-facing applications, and automated migration of most modern ASP.NET applications. |
| <strong>Azure Database Migration Service</strong>: The Azure Database Migration Service is a fully managed service designed to enable seamless migrations from multiple database sources to Azure Data platforms with minimal downtime. |
| <strong>SQL Server Data Migration Assistant (DMA)</strong>: Enables you to upgrade to a modern data platform by detecting compatibility issues that can impact database functionality in your new version of SQL Server and Azure SQL Database. DMA recommends performance and |</p>
<table>
<thead>
<tr>
<th>MIGRATION ASSESSMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>reliability improvements for your target environment and allows you to move your schema, data, and uncontained objects from your source server to your target server.</td>
</tr>
<tr>
<td>Azure SQL Database DTU Calculator: A Database Transaction Unit (DTU) is a blended measure of CPU, memory, and I/O used by an Azure SQL Database. Within each SQL Database service tier, Microsoft guarantees performance in terms of DTUs. The SQL Database DTU Calculator can be used to analyze the performance of existing on-premises databases, to calculate the number of DTUs (and hence service tier) required after migration to Azure SQL Database.</td>
</tr>
<tr>
<td>THIRD-PARTY OFFERINGS</td>
</tr>
<tr>
<td>Turbonomic</td>
</tr>
<tr>
<td>Turbonomic plans reflect what your workloads actually need to run in the cloud—no more, no less. Get to the cloud quickly and safely, while avoiding cost-overruns or performance issues.</td>
</tr>
<tr>
<td>Cloudamize</td>
</tr>
<tr>
<td>The Cloudamize cloud infrastructure analytics platform helps you make data-driven decisions with ease and confidence throughout your entire cloud journey.</td>
</tr>
<tr>
<td>• Assess: Which cloud is right for me and what will it cost?</td>
</tr>
<tr>
<td>• Plan: How do I prioritize my applications for migration?</td>
</tr>
<tr>
<td>• Migrate: How do I ensure my migration execution is right on the first try?</td>
</tr>
<tr>
<td>Movere</td>
</tr>
<tr>
<td>More than just a point-in-time assessment, Movere enables a depth of monitoring, analysis and optimization unseen in any other platform. Movere organically scans environments globally at a rate of up to 1,000 servers per hour and multiple instances/environments in less than one day.</td>
</tr>
<tr>
<td>RISC Networks</td>
</tr>
<tr>
<td>RISC Networks CloudScape provides IT professionals with the most relevant infrastructure performance analysis needed to properly prepare for cloud, data center, and infrastructure projects. Agentless discovery of Network Devices, routers, switches, Windows and Linux Servers and more. Review the Asset Report in the RISC Networks Portal or download an excel spreadsheet.</td>
</tr>
<tr>
<td>BitTitan Azure Assessments</td>
</tr>
<tr>
<td>Provide detailed readiness reporting using cost analysis and planning tools to convince your customers to adopt Azure. Take advantage of massive opportunities to move data out of SQL servers at end of life or support. Even uncover security concerns in customer infrastructure.</td>
</tr>
<tr>
<td>• Readiness check</td>
</tr>
<tr>
<td>• Cost analysis</td>
</tr>
<tr>
<td>• Detailed planning</td>
</tr>
<tr>
<td><strong>TSO Logic</strong></td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>The TSO Logic Platform provides the industry’s most accurate data-driven analysis of total cost of ownership and cost modelling for your ideal future state. It ingests millions of data points from your current environment, including age, generation and configuration of all hardware and software they’re running and each instance’s historical utilization. The Platform creates a fine-grained statistical model of compute patterns for all OS instances, showing how much you’re spending, where you’re over-provisioned, and where there are opportunities to realize significant savings both now and in the future.</td>
</tr>
</tbody>
</table>

**BMC Discovery for Multi-Cloud**

BMC Discovery for Multi-Cloud automates asset discovery and application dependency mapping to build a holistic view of all your data center assets, multi-cloud services, and their relationships.
Planning

The purpose of the planning phase of the Migration Assessment Plan is to build a proposal of what to applications to migrate, how to migrate each application, and when each migration should take place.

Having understood the various workloads and their underlying architectures during the discovery phase, the first step in the planning phase is to logically group the infrastructure and application components, and to prioritize their migration. This prioritization will be based on several factors: simplicity of application and infrastructure, number of dependencies, application criticality, limitations of existing hardware, and hardware and license refresh cycles.

Once the applications and infrastructure have been grouped and prioritized, a migration plan should start to emerge. Depending on the number and complexity of applications, your migration plan may range from a relatively straightforward application migration schedule or may be a complex multi-year strategic migration roadmap, with detailed application-level planning taking place iteratively as the roadmap is executed.

A pragmatic approach is advisable, prioritizing simpler, non-critical services for the early migrations. These are less risky and likely to be quicker to migrate and to present fewer issues. Early success builds confidence and allows demonstrable return on investment. It also builds experience, which reduces the risks associated with migrating the more complex workloads which follow.

COMMON MIGRATION APPROACHES

When designing the migration for a specific workload, there are a number of choices available.

- **Retire**: Some applications may be end-of-life and can more easily be retired than migrated.
- **Replace**: Many common business workloads (such as Exchange or SharePoint) have equivalent SaaS offerings. Migrating to SaaS services offers an alternative to running application infrastructure in the cloud, typically with higher availability and lower TCO.
- **Rehost**: A lift-and-shift approach, in which applications are migrated to IaaS virtual machines, offers a fast migration path with a high level of compatibility with existing software. SQL Managed Instances is another option when rehosting SQL Servers, offering compatibility benefits of virtual machines, but the manageability benefits of PaaS.
- **Rearchitect**: Converting applications to run as PaaS services offers significant advantages over a simple rehosting in IaaS virtual machines, due to the lower ongoing management complexity and costs. However, converting to PaaS may take longer and require greater technical skills, and the level of change—from minor refactoring to a complete application re-write—will depend on the existing codebase and the choice of PaaS technology adopted. As a result, while some applications may be converted to PaaS services as part of a migration project; more commonly they are first rehosted to IaaS and then evolved to take advantage of PaaS.
• **Retain on-premises:** For some applications, continuing to run on-premises may be best option, for example for critical applications

**IAAS OR PAAS?**

The choice between IaaS and PaaS is not all-or-nothing. A range of blended options exists, combining both IaaS and PaaS components in a single application architecture. For example, a traditional 3-tier application may see the application tier migrated to IaaS VMs, while the front-end tier is migrated to Azure App Service and the database tier is migrated to Azure SQL Database.

Where third-party software is used, licensing and support agreements must be reviewed to ensure that cloud-based deployments are fully supported, and to evaluate which cloud-based services may be used. For example, some software may support SQL Server running in IaaS, but not be validated with Azure SQL Database. In such cases it may be worthwhile to contact the software vendor to understand the cloud roadmap for the product.

While PaaS migrations may be more time-consuming and require greater initial investment, this cost is frequently outweighed by the benefits of reduced management overhead. This benefit is especially appealing to managed service providers. In addition to the efficiency gains of a PaaS approach, a modern application architecture also creates a foundation for higher-value customer offerings such as data analytics for increased business insight.

Many organizations adopt a ‘PaaS-first’ approach, preferring PaaS solutions where possible, recognizing that use of IaaS is inevitable in many cases, during a transition to PaaS or due to technical constraints such as the use of third-party software. In many cases, migration takes a phased approach, with initial migration executed as a ‘lift and shift’ to IaaS VMs, followed by additional phases to convert the application to make greater use of PaaS services.

**OPPORTUNITY TO CLEAN UP LEGACY DEPLOYMENTS**

In addition, cloud migration is often used by an organization as an opportunity to clean up legacy infrastructure and applications. It may be necessary to modernize certain infrastructure in-place before it can be migrated, for example, upgrading a legacy database or OS to a more modern version. Another common example is to consolidate on-premises databases prior to migration. Similarly, converting applications to PaaS may be an opportunity to combine several related applications into one.

**WHICH AZURE SERVICES AND TOOLS**

Having decided on the overall approach to migration, the design for the migrated application can be completed. This design describes in detail which Azure services are to be used, and how they will be configured. This includes:

- The design for identity, such as whether Azure AD will extend an on-premises Active Directory or not, and whether to adopt hybrid identity.
- The design for **subscription and resource governance**, including the **resource naming convention**.
- The list of Azure services and resource types used, their deployment region, and the SKU or service tier in each case.
- The network design, including virtual networks and subnets, peering, network security groups, routes, connectivity to existing networks, and use of virtual appliances.
- The storage design, accounting for capacity, IOPS, and data throughput requirements.
- The design for backup, high availability and disaster recovery.
- The tools used for the initial deployment to Azure and on-going updates.
- Plans for on-going operations, including monitoring, alerting, reporting, patching, and scaling.

Remember when specifying the compute, network, and storage capacity of the migrated service not to simply copy the hardware specification of the on-premises system. Instead, scale the system based on the actual usage data gathered during the discovery phase, and design the system to scale as needed in future.

**MINIMIZE DOUBT AND RISK WITH PROOF-OF-CONCEPTS**

Technical uncertainties impacting the design can be resolved using Proof-of-Concept implementations, which can reduce the risk of unexpected discoveries impacting the migration schedule during the execution phase.
With the goal state of the migrated application in place, the design for the initial deployment and application migration can be completed. This describes in detail how each application will be migrated from the on-premises environment to Azure. This includes:

- How existing application data will be transferred.
- How traffic will be switched to new application endpoints.
- The nature and duration of any user impact during migration.
- Details of how the migration will be monitored and verified.
- The process for roll-back should the migration fail.

- Details of any supporting tools, such as Azure Migrate or Azure Site Recovery, that will be used.

**PROJECT SCHEDULE**

Finally, the Planning phase includes creating the schedule for executing the migration. PaaS migration projects typically follow traditional software development phases and milestones for coding, testing, user acceptance, staging, and production deployment, followed by additional milestones for data migration, verification, and endpoint cut-over. IaaS ‘lift and shift’ projects may forego the coding phase, but the other phases are still typically required.
Evaluation

In the last phase of the migration assessment plan—Evaluation—you will review the migration plan and expected benefits, before approving the migration execution.

Earlier in this playbook, we discussed the different objectives and priorities that different organizations have when moving to Azure—from cost optimization, to increased agility, to improved citizen services, to enabling new scenarios. Understanding the motivations behind each migration is crucial to evaluating whether the proposed migration will deliver those benefits. In addition, reviewing the migration plan is an opportunity to make sure best practices are being followed and service risks are addressed appropriately.

**FORECASTING AND OPTIMIZING COSTS**

Cost is a universal concern. The discovery phase should already have captured an accurate picture of the existing on-premises application costs. To complete the picture, an accurate forecast of Azure costs is required. When computing these costs, consider the following points:

1. The choice of SKU or service tier is important since it can make a significant difference to pricing. A direct translation of existing on-premises hardware specifications into Azure Virtual Machine SKUs may not be optimal, since on-premises hardware may be under-utilized, and Azure hardware is typically newer, and hence faster, than on-premises hardware with a similar number of CPU cores. The **Optimize and Manage phase** is a key talking point in this discussion.

2. Remember to account for the hours each service will run. It may be possible to scale back usage of Production environments at times of low usage, especially when using PaaS. Non-production environments such as Dev/Test should only be deployed when they are in active use.

3. The Azure Hybrid Benefit allows existing Windows Server software licenses (with Software Assurance) to be re-used on Azure Virtual Machines. This allows existing licensing investments to be leveraged, so the Virtual Machine is only charged at the ‘bare metal’ (Linux) rate. This can result in significant reductions in your Azure bill of 40% or even more. This benefit is also available for SQL Server licensees, allowing them to reuse their SQL Server licenses without paying the premium rate as well as significant cost savings for using Azure SQL Database. See **Azure Hybrid Benefit** for further details.

4. Similarly, the License Mobility program enables Microsoft Windows Server application licenses (with Software Assurance) to be used in Azure, again allowing existing licensing investments to be leveraged in Azure. See **License Mobility through Software Assurance on Azure** for further details.

5. Some costs, such as Virtual Machine SKU, are relatively easy to predict. Other costs, such as bandwidth or storage access charges, vary according to application usage and can be difficult to predict without accurate data. Usage may need to be estimated based on transaction logs or other available usage information.

6. Where appropriate, take advantage of **Azure Reserved Instances** to further reduce Azure subscription costs.

These approaches, when used in combination, can offer very substantial cost savings. Azure Migrate provides cost estimates as part of a migration assessment. These estimates can be tailored based on a wide range of parameters, such as the VM family and size, use of discount plans, and hours of operation. The **Azure pricing calculator** is another useful tool for predicting Azure costs based on expected usage and service tiers. Many third-party tools also offer pricing estimation.

On-premises infrastructure has the advantage of well-understood up-front pricing. By comparison, cloud costs can be more difficult to predict, and may vary over time, for example as usage changes, or as the service is optimized, or as the unit cost of Azure resources changes.
It is generally better to slightly overestimate rather than underestimate what future costs will be.

Once the costs of the migrated service have been fully understood, they can be compared with the costs of the existing service as captured during the discovery phase of the migration assessment. This comparison is useful for budgeting purposes, but remember that cost savings alone are only a small part of the cloud value proposition, and the migration project may have many other cloud benefits.

COMMON CONCERNS

There are several common questions or concerns that may be raised in the context of an Azure migration. Common concerns include:

- **Security and compliance**: Requirements should be captured during the discovery phase and addressed in the proposed design, which should explicitly address security concerns and the Azure technologies used to mitigate common threats. This design should use recommended solutions to ensure the relevant accreditations will be awarded.

- **Service availability**: The proposed design should address the requirements for backup, availability and disaster recovery, consistently with the published Azure SLAs.

- **Functionality, compatibility and performance**: A proof of concept is a common way to address functionality and performance concerns and build confidence in the proposed solutions.

- **Cost and cost variability**: A sound understanding of fully-loaded costs for the existing application implementation, together with a complete costing for the Azure implementation, should be presented. While a high-level overview of cost approximation may provide a clear business case, providing additional detail can improve forecasting and confidence.

RESOURCES

➔ Microsoft Cloud Adoption Framework for Azure
Lift and Shift

Migration and Modernization with Azure Government
Executive Summary

Now the actual work of migrating workloads studied during the assessment phase begins. In this section, we’ll consider ‘lift and shift’ migrations to Azure infrastructure services.

Migrating applications to Azure using Infrastructure-as-a-Service is often the quickest way to move applications to Azure, as well as requiring the least work and presenting the fewest risks.

For some applications, and some customers, migrating to Azure infrastructure is the end goal, and the application will continue to be operated in that way indefinitely. In many cases however, an infrastructure migration is used as a starting point, after which a longer-term program of application modernization begins. In this case, the end goal is for the application to be operated using Platform-as-a-Service technologies, giving lower management overhead and greater agility. Application modernization is the topic of the next chapter of this playbook.

The foundation of an Azure infrastructure deployment comprises:

- **Identity** – how will users authenticate and how resources are secured
- **Compute** – configuring virtual machines for availability, scale and performance
- **Network** – designing the network for current and future connectivity requirement
- **Storage** – planning for performance, durability, scalability and archival

This section discusses how to design and build this foundation and provides several resources to help.

We then discuss how to migrate the existing application servers—physical or virtual—to Azure. We provide guidance on how to choose the right Azure virtual machine and the various tools and methodologies to execute the migration itself.

Finally, we’ll present some key topics that are important for Azure infrastructure migrations:

- Migrating VMware workloads
- Configuring backup and disaster recovery for migrated workloads
- Migrating existing Azure applications to Cloud Solution Provider (CSP) subscriptions
- Using Azure Stack as a migration target for customers that cannot migrate to the public cloud
- Migrating data and databases

Top 5 things to do

Here are the top 5 things to focus on during an Azure infrastructure migration.

- Deploy your network, compute and storage infrastructure
- Implement user identity
- Understand the available tools and approaches for server migration
- Configure high availability and backup
- Understand how to migrate data
Building Out the Network

The network forms the backbone of any application, both on-premises and in the cloud. It is the doorway to the end users, the glue that enables the application to function, and the security boundary against outside attacks. Establishing the right network architecture is a critical step in designing any cloud migration.

Designing the network can be one of the most technical and challenging aspects of a cloud migration project. The network design must consider a range of requirements and security threats. Common considerations include:

- Designing network topologies with the right connectivity for application access and internal traffic
- Creating hybrid networks connecting on-premises and Azure-based resources
- Routing traffic for scale, resilience and high availability
- Securing the network against outside threats, including DDoS
- Monitoring and trouble-shooting networking issues

Microsoft Azure offers an extensive range of networking services and features, enabling almost any networking topology to be created in Azure. This enables existing network topologies to be reproduced in Azure as part of a migration. Migration to the cloud is also an opportunity to align the network design with current best practices for performance and security.

In addition to designing your Azure network, remember to consider the existing on-premises network. What changes—temporary or permanent—are needed to make the existing network compatible with and extensible to the cloud?

**AZURE NETWORKING**

Azure provides a comprehensive range of networking services to support a wide range of network topologies. These are built using Microsoft’s software defined networking technology, which offers cloud scale, fast provisioning, and virtual isolation of network traffic in the multi-tenant Azure environment.

This guide gives a short overview of the core Azure networking services. Microsoft publishes substantial additional documentation on each of these services online. For further reading, we recommend the [Azure Networking Overview](#).

**VIRTUAL NETWORKS**

Virtual networks are the most fundamental resource in Azure networking. A virtual network allows you to create a dedicated, private network space (for example, 10.0.0.0/16) within the Azure cloud. Resources, such as Azure virtual machines, can be allocated private IP addresses within this space, and use those addresses to communicate with each other.

Each virtual network can be divided into subnets, and virtual networks can be connected with each other using peering connections. You can configure user-defined routes and network security groups (NSGs), which are like firewall rules, to control traffic in, out, and between subnets.

Inbound Internet traffic is supported by creating a public IP Address, which can be either IPv4 or IPv6 (many IPv6 networking features are currently in preview). These IP addresses can be statically or dynamically assigned. Outbound Internet traffic is supported both with and without the presence of a public IP Address (and can be blocked using an NSG if required).

**LOAD BALANCING OPTIONS**

There are three alternative load-balancing technologies available in Azure. It is important to understand all three, and to design your application appropriately.

- **Azure Load Balancer** is a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy virtual machines or other service instances. It can be used for both Internet-facing and internal application endpoints.
• **Azure Application Gateway** is a Layer 7 load-balancer with security and routing features, such as web application firewall, SSL off-loading, URL path-based routing and cookie-based session affinity. It is an example of a network appliance; a range of third-party appliances is also available via the Azure Marketplace.

• **Azure Traffic Manager** is a DNS-based global traffic management service. It provides a range of traffic-routing capabilities, based on end user geo-location, endpoint proximity (based on network latency), and endpoint availability. Traffic Manager can be used to direct traffic between endpoints in different Azure regions, or between Azure and non-Azure endpoints.

Note that all three load-balancing services include endpoint health probes for back-end instances, and the ability to deliver high-availability by automatically removing failed instances from service and restore them once they return to health.

### DNS SERVICES

Azure supports a range of DNS services and features, for use by both Internet-facing and internal applications:

• **Azure DNS** allows you to host your DNS domain. It provides a global network of authoritative DNS name servers for high availability and low latency and supports all common DNS record types. Azure DNS is generally available for Internet-facing domains; Intranet-facing **private domain support is available in the Azure public cloud**.

• **Azure-provided DNS** is the name given to the recursive DNS service provided by default to all Azure virtual machines. You can override the virtual machine DNS settings at either the virtual network or individual virtual machine level to specify your own recursive DNS server; the most common scenarios are to specify the DNS service of your Active Directory deployment when using domain joined virtual machines, or to enable DNS lookup for on-premises servers when using hybrid networking.

• Reverse DNS lookup is used to create a mapping from an IP address to a DNS name. Azure lets you **configure the reverse DNS name** assigned to the public IP addresses assigned to your virtual machines. You can also **host the reverse lookup zone** for your own IP address block using Azure DNS.

### SECURITY, MONITORING AND TROUBLESHOOTING

• **DDoS Protection**: Azure provides two levels of DDoS protection. The basic level, which is free of charge, provides always-on traffic monitoring and real-time mitigation against common attacks. The paid-for standard-level service provides policies tuned using machine learning and real-time telemetry.

• **Azure Firewall** provides a central, fully scalable firewall-as-a-service for Azure-based applications. It can be used to filter all Azure traffic (inbound, outbound, between on-premises and Azure, and between networks in Azure). This is primarily for infrastructure as a service. There are similar options for platform-as-a-service workloads such as **Azure Application Gateway**.

• **Network Watcher** provides a central hub for a range of tools to view network settings across your deployment. It also provides several very useful tools for investigating network issues, such as the ability to run packet captures, and to verify connectivity from a virtual machine to a given endpoint.

• **Azure Security Center** provides its ability to both detect and help protect against threats. Using machine learning to process trillions of signals across Microsoft services and systems, Security Center alerts you of threats to your environments, such as remote desktop protocol (RDP) brute-force attacks and SQL injections. And it provides actionable recommendations for mitigating these threats. Turn on Security Center to strengthen your security posture and protect against threats. ASC has **two options**: a Free Tier, which you must enable in the portal to utilize; and the upgraded Standard Tier.

### HYBRID NETWORKING

It may be necessary for some parts of an application (typically the application database) to reside on-premises, whilst the other tiers of the application are moved to Azure. In these so-called ‘hybrid’ networks, a secure and robust connection is required between the database in the on-premises environment and the rest of the application in Azure. We call this connectivity between Azure and on-premises networks ‘hybrid networking’.

Another example is Intranet applications. Even if the entire application stack is moved to Azure, some organizations will prefer to access Intranet applications over their internal network, rather than a public IP address. Here again, a secure connection between the on-premises network and the Azure network is required.
There are strict requirements that control how any external system connects to US Government networks. These are discussed in the earlier section on Network Integration. Azure for Government supports these standards using both Virtual Private Networks (VPNs) or dedicated connections (ExpressRoute).

**Virtual Private Networks**

In a Virtual Private Network (VPN), traffic flows over the public Internet through a secure, encrypted tunnel, but appears from a networking perspective to be between two private networks.

Azure supports two types of VPN:

- **Site-to-Site VPN**: Used to join on-premises networks to Azure, for example to connect application servers with database servers. At the Azure end, a VPN Gateway is deployed into a dedicated subnet in your virtual network. The on-premises network endpoint is a VPN gateway device. These devices form a VPN tunnel over which traffic between the networks flows.

- **Point-to-Site VPN**: Used to join individual machines to the Azure network, for example to connect remote worker laptops to an Azure application, or for Dev/Test purposes. Once again, a VPN Gateway is deployed in Azure, in this case connecting to a VPN client deployed on the remote machine.

**ExpressRoute**

Microsoft Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. ExpressRoute connections do not go over the public Internet; offering a higher level of performance and reliability compared to traditional VPN connections.

Where VPN connections provide connectivity only to a single Azure virtual network in a single region, ExpressRoute connectivity supports all Azure regions in a given geopolitical region, or all regions worldwide with the ExpressRoute Premium add-on.

VPN connections only provide connectivity to Azure resources. With ExpressRoute, you can establish connections to all Microsoft cloud services, including Microsoft Azure, Office 365, and Dynamics 365. For guidance on using ExpressRoute to access Office 365 visit [http://aka.ms/ExpressRouteOffice365](http://aka.ms/ExpressRouteOffice365).

ExpressRoute offers a choice of **connectivity models**:

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

- **Any-to-any (IPVPN) networks** You can integrate your WAN with the Microsoft cloud. IPVPN providers (typically 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 like any other branch office. WAN providers typically offer managed Layer 3 connections.

- **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.

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

**RESOURCES**

➔ [Reference Architecture: Hybrid Networking](http://aka.ms/AzureGovPlaybook)
Network Appliances

Using Network Virtual Appliances can improve application security, help meet existing security policies, leverage existing licensing investments, and re-use existing skills.

Many on-premises applications make use of third-party network appliances, for example to provide additional security, availability, or custom routing features. Many of these appliances are available as ‘network virtual appliances’ (NVAs) in the Azure Marketplace. Having identical or similar functionality available in Azure makes it much easier to migrate existing applications that use these devices.

Customers may have made a significant investment in these appliances, in terms of hardware and licensing, and also in the configuration of the appliance to support their security policy and in training their staff. Minimizing change and maximizing re-use of existing investments can be an important way to remove obstacles from a migration project. Using a virtual appliance from the customer’s existing vendor makes it easy to re-use existing configurations and policies, as well as providing a familiar interface to existing staff. Moreover, in many cases the virtual appliances support ‘bring your own license’, so existing license investments can be re-used.

Microsoft provides its own network appliance, Azure Application Gateway. Third-party network virtual appliances are available in the Azure Marketplace from a wide range of vendors, including Cisco, Barracuda, Check Point, Citrix, F5, and many more. For a full list, see the Azure Marketplace.

RESOURCES

➔ Reference Architecture: Networking DMZs with Network Virtual Appliances
The Virtual Data Center

Azure Virtual Datacenter is an approach to making the most of the Azure cloud platform’s capabilities while respecting existing security and networking policies. When deploying workloads to the cloud, IT organizations and business units must balance governance with developer agility. Azure Virtual Datacenter provides models to achieve this balance.

Unlike an existing on-premises datacenter environment, the Azure public cloud operates using shared physical infrastructure and a software-defined environment abstraction. The Azure Virtual Datacenter model allows you to structure isolated workloads in the Azure multi-tenant environment that meet existing governance policies.

With this approach, a set of shared services, access controls and policies are deployed and managed independently of the actual application workloads. These services include shared components such as load balancers, hybrid network connections, network security appliances, and management jump-boxes. Policies ensure that all traffic is routed through this shared infrastructure, which is responsible for implementing and enforcing governance standards.

Individual application workloads are then deployed separately into this infrastructure. Each workload uses a dedicated virtual network, integrated with the shared infrastructure using peering and routing rules. The resulting network is a ‘hub and spoke’ model, with a central hub of shared components, with each application workload isolated in separate spokes.

With this approach, you can deliver a flexible and agile and yet also highly secure and compliant infrastructure, with the aim of meeting any customer security policy requirements and assuaging security concerns. By sharing network security infrastructure, you can also demonstrate significant cost savings over siloed application deployments. These advantages will be especially important for large agencies who typically have more demanding requirements and a larger number of applications to migrate.

FURTHER READING

Deploying and configuring an Azure Virtual Datacenter requires a deep understanding of a broad range of Azure technologies. Fortunately, the Microsoft Azure Global Customer Engineering (AGCE) and FastTrack for Azure have published extensive guidance, based on their experience of helping Microsoft’s largest customers on their Azure journeys. For more information, see the Azure Virtual Datacenter portal on the Azure Architecture Center, the Azure Virtual Datacenter White Paper and the Mesh and Hub-and-Spoke Networks on Azure White Paper.
Enabling Hybrid Identity

As organizations move from using on-premises applications to cloud-based services, controlling access to those services becomes a challenge. Azure Active Directory provides the solution.

Controlling access to cloud-based services poses multiple challenges. How do you know which services your employees are using? How do you ensure access is authorized and authenticated? And how do you manage authentication credentials across all those services?

Azure Active Directory is a cloud-based directory and identity management service designed to address these challenges. It enables a single set of credentials to be used to authenticate access to thousands of common cloud-based services. By integrating with on-premises directories, this enables a common set of credentials to be used for both corporate and cloud applications. We call this hybrid identity. Enabling hybrid identity is a foundational step for most migrations.

When migrating applications to the cloud, it is important to understand how user identity will be managed. This should be designed early before any migration efforts have taken place beyond a proof-of-concept.

- You can run Windows Server Active Directory (commonly referred to as AD) in the cloud using virtual machines created with Azure Virtual machines. This approach makes sense when you’re using Azure to extend your on-premises datacenter into the cloud.
- You can use Azure Active Directory to give your users single sign-on to Software as a Service (SaaS) applications. Microsoft’s Office 365 uses this technology, for example, and applications running on Azure or other cloud platforms can also use it.
- Applications running in the cloud or on-premises can use Azure Active Directory Access Control to let users log in using identities from Facebook, Google, Microsoft, and other identity providers.

Organizations already using Office365 or Azure will already be using Azure Active Directory since it’s the authentication mechanism behind both services. In some cases, where different directories are in use, it’s useful to transfer ownership of their subscription to another account.

SERVICE PRINCIPAL ACCOUNTS

As well as supporting user authentication, applications use Azure Active directory to authorize access to the resources they need. They do this using special types of accounts, called service principal accounts which can be created using the Azure portal, PowerShell, or CLI.

Service principal accounts should be configured with just enough permissions to run the tasks needed by the application, and no more. It’s important that applications do not run in the context of user accounts. This breaks the principles of least privilege and individual accountability.

MANAGED IDENTITY

Managed identity enables service principal accounts to be created automatically for Azure resources such as virtual machines. Credentials for the account are automatically provisioned into the virtual machine using a virtual machine extension. Applications running on the VM can use those credentials to request access tokens used to authenticate requests to other Azure resources.

Managed identities automate the full credential management lifecycle—from initial provisioning, through rollover, to deleting the Service Principal account when the resource is deleted. This greatly reduces the management overhead associated with credential management, whilst also increasing security. To learn more, see managed identity overview.

Note: Every environment is unique. If you plan to use Office 365 and HSPD12, consult Microsoft for guidance.

RESOURCES

➔ What is Azure AD?
➔ Deploying a Hybrid Identity Solution
➔ How to Deploy ADFS in Azure
➔ Azure AD Domain Services
➔ Azure Active Directory Proof of Concept Playbook

aka.ms/AzureGovPlaybook
Planning for Storage

Data storage is a critical feature of any application. Choosing the right storage technology will help create performant, cost-effective cloud deployments.

There are a wide range of data storage technologies available in Azure. Each offers different features, performance, resiliency and cost characteristics. It’s important to understand the options before choosing the storage for your applications.

When using native Azure Storage, consider the following:
How do you plan to implement SAS key rotation, logging, and firewall rules to secure content. Engage with your Microsoft team for recommendations.

In this section, we’ll discuss the storage options available to Azure Virtual Machines, considering both the disks attached to the virtual machines themselves, and shared file shares.

To add, Azure supports a wide range of database options. These are considered later in this playbook: see sections on Migrating Databases and Modern Data Platform.

VIRTUAL MACHINE DISKS

With the right storage combination, you can achieve up to 2 PiB of storage per virtual machine, with up to 80,000 IOPS (input/output operations per second) and up to 2 GB per second disk throughput, with extremely low latencies for read operations. However, achieving this performance requires a large (and costly) deployment. While Azure supports extreme levels of disk performance, it’s key to right-size your design to avoid unnecessary cost.

The first step in planning disk storage is to identify storage requirements—capacity, throughput, and read/write operations per second. This information should be gathered in the assessment phase, using tools such as Azure Migrate or Azure Site Recovery Deployment Planner. This helps determine the storage architecture to use, for example the size, type and number of disks.

There are two technologies available for virtual machine disks in Azure. The original approach, which is still supported, is to store the disk image in a ‘blob’ in Azure storage. The current approach, called Managed Disks, abstracts the disk as a first-class resource in its own right. Managed Disks offer numerous advantages over blob storage and is the recommended approach for all new deployments.

When planning your disk storage, you will need to choose an appropriate storage tier:

- **Standard HDD disks** are the lowest-cost storage tier. It uses traditional spinning disks, which offer higher latency than SSDs. Throughput and transaction rates are also lower than for SSDs, except for the smallest disk sizes. They are suitable for less performance-critical workloads and are ideal for Dev/Test environments.

- **Standard SSD disks** use solid-state drives to offer significantly lower latency rates than Standard HDD disks. Reliability is also higher, although the SLA is the same. Throughput and transaction rates are similar to Standard HDD disks, with some variation depending on disk size. Standard SSDs are suitable for Web servers, low IOPS application servers, lightly used applications, and Dev/Test workloads.

- **Premium SSD disks** also use solid-state drives to deliver low latency and offer much higher transaction and throughput rates than Standard disks. They are suitable for database servers, file servers and interactive applications that require high throughput and low latency. They are also required to take advantage of the Azure SLA for single-instance virtual machines.

- **Ultra SSD disks** (in preview) offer the highest levels of throughput and IOPS, with consistent low-latency in the sub-millisecond range. They are designed for data-intensive workloads such as SAP HANA and critical databases.

In each case, it is important to understand the capacity, IOPS and throughput options available, and to choose a storage design that meets your requirements. In some cases, to meet the required performance, it will be necessary to stripe data across multiple disks.
File Shares

Cloud file shares make sharing files across cloud and on-premises servers easy.

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol (also known as Common Internet File System or CIFS). Azure File shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS. Additionally, Azure File shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Azure File shares can be used to:

- **Replace or supplement on-premises file servers:** Azure Files can be used to completely replace or supplement traditional on-premises file servers or NAS devices. Popular operating systems such as Windows, macOS, and Linux can directly mount Azure File shares wherever they are in the world. Azure File shares can also be replicated with Azure File Sync to Windows Servers, either on-premises or in the cloud, for performance and distributed caching of the data where it’s being used.

- **Lift and shift applications:** Azure Files makes it easy to lift and shift applications to the cloud that expect a file share to store file application or user data. Azure Files enables both the classic lift-and-shift scenario, where both the application and its data are moved to Azure, and the hybrid lift-and-shift scenario, where the application data is moved to Azure Files, and the application continues to run on-premises.

- **Simplify cloud development:** Azure Files can also be used in numerous ways to simplify new cloud development projects, for example for shared application settings, diagnostics, or shared tools including third-party appliances such as NetApp.

Azure Files are a fully managed service, requiring no patching or on-going management, and have built-in resiliency.
Choosing Virtual Machines

Choosing the right virtual machines family and size, with the correct availability options, is an important part of the design process.

Migrating existing servers—whether physical, VMware or Hyper-V—comprises two main steps. First, an appropriate Azure virtual machine must be selected and provisioned. Secondly, the application files (executables, configuration and local data) stored on the disks associated with the existing servers must be migrated.

In this section, we’ll focus on the first step—choosing the right the virtual machines and choosing the right high availability design for their deployment.

VIRTUAL MACHINE FAMILIES

Azure supports a wide range of virtual machine families, with a wide range of compute and memory capabilities. The family and size of each virtual machine used should be determined during the planning phase of the discovery process, based on the analysis of the existing application and hardware. For example, database servers and web servers may have very different memory requirements, and so use different virtual machine families.

Many of the assessment tools can help with this right sizing exercise. Even so, having intimate knowledge of the available options will undoubtedly be required.

Remember that the Azure public cloud may offer a wider range of virtual machine sizes than Azure Government, and that availability varies by region. Be sure to check your VM family choices match your choice of region using the Products available by Region page.
Availability Options

Beyond choosing the right family and size of virtual machine, choosing the right availability option will also be integral to the project at hand.

In addition to understanding the native availability requirements for the workload (for example: SQL Server Always On) you will have to plan and choose the right level of availability with Azure Virtual Machines, backed by a suitable virtual machine availability SLA.

**SINGLE INSTANCE VM**

When any Azure virtual machine is backed by Azure Premium Storage (for all disks), Microsoft provides a 99.9% availability SLA.

**AVAILABILITY SETS**

Azure Availability Sets are a logical grouping capability that you can use in Azure to ensure that the virtual machines you place within it are isolated from each other when they are deployed within an Azure datacenter.

Using availability sets helps protect against outages caused by local failures, such as a top-of-rack network switch, or by rolling system updates such as host OS patching.

Availability sets offer a 99.95% availability SLA. This requires that at least two virtual machines are deployed.

**AVAILABILITY ZONES**

Azure Availability Zones are fault-isolated locations within an Azure region, designed with independent power, cooling, and networking. They help protect your mission-critical applications from failures of entire datacenters, caused by events such as power or cooling failures, fire, or flood.

Availability zones are designed to be sufficiently isolated to protect against coordinated failures, yet close enough for low network latency between zones, so that write operations to zone-redundant storage take place synchronously.

Availability zones also support zone-redundant networking. Zone-redundant load-balancers can be used to distributed traffic across virtual machine instances, both within and across availability zones. Zone-redundant public IP addresses enable a single public IP address to be shared across all zones, with traffic routed away from failed zones automatically.

Availability zones were made generally available as of March 30, 2018. They offer a 99.99% availability SLA. They are not yet supported in all Azure regions including Azure Government. See Azure Regions for latest details.

**REGION PAIRS**

Deploying your application to more than one Azure region helps protect you against large-scale region-wide disasters (such as hurricanes) with the potential to impact all availability zones within a region. However, this comes at a significant cost—as well as the increased Azure consumption arising from the larger deployment footprint, the application design must account for data consistency between regions and traffic routing, both before and during a disaster.

Cross-region data replication can be achieved using a range of database technologies, including Azure SQL Database. Cross-region traffic routing and failover is provided by Azure Traffic Manager, which supports a variety of traffic-routing policies.

When deploying an application to more than one Azure region, you should take advantage of Azure region pairs. Each Azure region has a ‘paired’ region, and Azure avoids deploying system updates to both regions at the same time. Spreading your load across paired Azure regions helps protect against unexpected outages caused by Azure system updates.

For guidance when planning, please consult Microsoft.

**RESOURCES**

➢ Azure Resiliency
Customized Virtual Machine Images

Take advantage of custom virtual machine images to optimize your deployment time

Many customers use virtual machine images in their existing virtualization environment complete with third-party and custom software ready for deployment. These images can be used in Azure as well, which can accelerate deployments by removing the need to change configuration settings and deploy software after the virtual machine is created.

CUSTOM IMAGES FOR WORKING TOOLS

Many Azure customers create custom images (based on Windows and Linux) that contain their custom applications and third-party tools they commonly use as part of a migration or modernization project.

With this approach, they get the additional benefit of a common working environment which allows for consistent behavior and a common set of tools. New teams can get started much faster and with less confusion since all the environments have the expected set of tools and services when they start.

CREATING YOUR OWN IMAGES

A first step should be to browse the Azure Marketplace, to see if there is an existing virtual machine image available that meets your needs. Using an existing image saves you valuable time in creating your own. However, if you can’t find a suitable image in the Marketplace, you can also create a custom image as a baseline for your virtual machines.

The easiest way to create a new image is to start by provisioning a VM from the Azure Marketplace and then customizing it by installing software and services. After the VM is configured you must run sysprep.exe with the generalize and shutdown options selected. Once the VM is shutdown you can use the Azure capture command to store the image for later use. For more information, see Creating Custom VM Images.

You can also use the open source tool ‘Packer’ to create custom virtual machine images. To build images, you define a Packer template file specifying the build process for the image. Packer supports integration with Azure, allowing you to define Azure resources such as service principal credentials. Running Packer will then deploy a virtual machine to Azure, perform the necessary build steps, create the image, and then clean up the virtual machine. This image can then be used as a baseline for more virtual machines. For more information, see How to use Packer to create Windows virtual machine images in Azure.

UPLOADING EXISTING IMAGES

Using the Azure Command line tools or Storage Explorer you can upload existing VHD files and register them as managed images that can be used to create new virtual machines in Azure.

For details, see the Migrating Disks section in this playbook.
Migrating to Virtual Machines

A critical step in any migration to Azure infrastructure is the migration of the servers themselves. Over the following pages, we’ll learn about the migration approaches you can use and the tools available to help you.

There are two main approaches to migrating the application files to virtual machines in Azure:

1. Start with a clean Azure virtual machine and re-install and re-configure the application software, OR
2. Port the existing machine disks, so that the virtual machine in Azure continues where the on-premises machine left off.

A clean installation on a new virtual machine has the advantage of leaving behind any legacy issues associated with the existing machine, such as patching history and device drivers. It creates a clean, up-to-date disk image and a clean install of the application software. It is also repeatable, which helps with reliable testing.

However, a clean install is only possible where the application installers and the knowledge to configure the application are available. For legacy applications, in practice, this is frequently not the case. For these applications, porting the existing disks to Azure may be the only practical option. Even when porting disks, some application and system configuration will be required to adapt to the new environment.

In the following sections, we’ll discuss a variety of ways of implementing the second migration approach—porting existing disks to Azure. First, we’ll consider the simplest possible approach of simply copying the disks. Next, we’ll look at how migration can be streamlined using Azure Site Recovery. Finally, we’ll discuss the features and resources available specifically to support VMware to Azure migrations.
Migrating Disks

Take care to configure the machine correctly when copying an OS disk to Azure.

The simplest way to migrate existing servers to Azure is simply to migrate their disks to Azure and then attach those disks to new Azure virtual machines. This is straightforward for data disks but requires some careful OS configuration when porting OS disks.

By using snapshots, disks can be exported from existing servers and imported into Azure while those servers are running. For stateless servers, this works well. However, for stateful servers (such as databases), any changes after the snapshot is created will be lost during the migration. In this case, to avoid loss of data, the service will need to be stopped during the migration process. Migrating disks in this way therefore incurs a longer system downtime than other migration approaches, such as using Azure Site Recovery. However, the simplicity of disk migration means it may be a good choice where this downtime is acceptable.

**MIGRATING HYPER-V OR VMWARE VIRTUAL MACHINES TO AZURE**

Importing Hyper-V disks to Azure only supports the VHD disk format, which must be a fixed-size disk no larger than 1,023GB. In addition, only ‘Generation 1’ VMs are supported. You can convert from the VHDX format to VHD, and from a dynamically expanding disk to a fixed-size disk. However, you cannot change the VM’s generation, and will therefore need to use a different migration approach with Generation 2 VMs, such as Azure Site Recovery.

Converting Hyper-V disks from VHDX to VHD format, and to fixed size, can be achieved using either Hyper-V Manager or PowerShell. For details, see [Prepare a Windows VHD or VHDX to upload to Azure](https://aka.ms/AzureGovPlaybook). You can also convert the VMware VMDK disk format to VHD using the [Microsoft VM Converter](https://aka.ms/AzureGovPlaybook). For more information, see the blog article [How to Convert a VMware VMDK to Hyper-V VHD](https://aka.ms/AzureGovPlaybook).

You will have to choose whether to ‘sysprep’ your VM. You typically do this if you want to create a template from which you can deploy several other VMs that have a specific configuration. This is called a **generalized image**. If, instead, you want only to create one VM from one disk, you don’t have to use sysprep. In this situation, you can just create the VM from what is known as a **specialized image**.

There is a long list of additional OS changes that are required. For example, any static persistent routes must be removed, WinHTTP proxy removed, the SAN disk policy configured, the time zone set to UTC, and the power profile set to High Performance. For Windows, the full list is documented at [Prepare a Windows VHD or VHDX to upload to Azure](https://aka.ms/AzureGovPlaybook). For Linux, see [Information for Non-endorsed Distributions](https://aka.ms/AzureGovPlaybook) and the additional per-distro guidance pages. Once complete, the VHD file can be uploaded as a blob in Azure Storage. From there, you can use the VHD blob either to create a Managed Disk (in the case of a specialized image) or to create a Managed Image (in the case of a generalized image). These can then be used in your Azure virtual machines.

**MIGRATING AWS EC2 INSTANCES TO AZURE**

Migrating AWS EC2 instances to Azure follows a similar process as used for Hyper-V or VMware, as described above. First, you export the EC2 instance to a VHD file in an Amazon S3 bucket, using the instructions provided in [Exporting an Instance as a VM using VM Import/Export](https://aka.ms/AzureGovPlaybook). This VHD file is then transferred to Azure and used to create a Managed Disk or Managed Image (both specialized and generalized VHDs are supported).

For further information, see [Move a Windows VM from AWS to Azure using PowerShell](https://aka.ms/AzureGovPlaybook).

**MIGRATING PHYSICAL SERVERS TO AZURE**

Physical servers can be migrated to Azure by converting their disks to VHD files, then following a similar process as described above. This can be done using the [Disk2vhd utility](https://aka.ms/AzureGovPlaybook). This uses the Windows Volume Snapshot capability to create consistent point-in-time disk snapshots, allowing the VHD to be created without system downtime.
Migrating using Azure Site Recovery

Azure Site Recovery (ASR) is an Azure service designed initially to enable customers to deliver high availability applications by enabling automatic failover to Azure infrastructure in the event of failure. By treating an application migration as a controlled failover without failback, it can also be used to migrate applications to Azure.

The requirements for failover to a backup site are similar to the requirements for a migration. Key concerns focus on data replication and integrity, re-directing the network traffic, and minimizing downtime. While initially designed for failover, Azure Site Recovery supports both failover and migration scenarios.

Azure Site Recovery for Migration supports migration from physical machines and both VMware and Hyper-V virtual machines to Azure. The ASR Deployment Planner can be used to help assess the workload to be migrated and determine details of the migration such as the network capacity needed and Azure virtual machines to use.

Once installed and configured, the migration starts by copying data (disks) from each machine to be migrated. Once completed, continuous incremental data transfers are used. This all occurs while the on-premises application is fully operational, prior to any application migration work window.

Data synchronization integrates with a wide range of common application workloads to ensure the synchronized snapshots are application consistent. Common workloads supported by Azure Site Recovery include SQL Server, Active Directory, Exchange and Oracle Data Guard. For a full list of supported workloads, see What workloads you can protect with Azure Site Recovery.

During application cut-over, virtual machines in Azure are booted using the replicated data. A final incremental data transfer is used to ensure the Azure virtual machines are fully up to date. Azure Site Recovery supports an RPO (Recovery Point Objective) as low as 30 seconds, enabling the work window during which applications are unavailable to be kept as small as possible.

The application traffic is then switched to the Azure-based service. For Internet-facing applications, the Azure service will have a new IP address, hence this switchover happens at the DNS level. Azure Site Recovery integrates with Azure Traffic Manager, enabling this transition to happen quickly and easily. For Intranet applications, there are two possible approaches: changes to the internal IP address require the internal DNS record to be updated; alternatively, the internal IP address can be preserved, with switchover by changing the IP subnet routing tables. This last approach is useful if application dependencies require that existing internal IP addresses be preserved.

If you are using a Trusted Internet Connection, please consult with your agency.
Migrating VMware Workloads

Many services use VMware to run virtualized servers. The overall process of migrating VMware virtual machines to Azure follows a similar sequence to any other migration. However, there are some considerations that are specific to VMware.

Migrating VMware virtual machines to run in Azure is one of the most common migration scenarios. Microsoft has published a detailed Migrating VMware to Microsoft Azure TCO Guidance document to help demonstrate the value proposition that underpins these migrations.

The overall process for migrating VMware workloads to Azure follows a similar path to other workloads, using tools we have already seen such as Azure Migrate and Azure Site Recovery. To help support VMware customers on their migration journey, these services are designed and tested specifically with VMware workloads in mind. Existing VMware administrators unfamiliar with Azure may appreciate free online training to introduce Azure VMs to existing VMware vSphere administrators.

There are many technical compatibility issues to consider when planning a VMware to Azure migration, such as firmware version, OS version, VMware version, disk size, disk format, network capacity, etc. The Azure Migrate and Azure Site Recovery Deployment Planner tools can be used to automatically assess an existing VMware environment prior to migration, giving a report of issues that needs to be addressed.

There are a variety of approaches available for VMware workload migration, summarized below.

**AZURE MIGRATE**

As well as supporting VMware migration assessment, Azure Migrate also provides migration of VMware workloads. Using Azure Migrate for both assessment and migration provides an integrated experience, streamlining the overall migration process.

Support for VMware migration is currently in preview, and requires you to register in advance. The preview is offered with full support for production workloads. Be sure to check the current status and availability in Azure Government.

**AZURE SITE RECOVERY**

As described in the previous section, Azure Site Recovery is a powerful tool for migrating existing applications to Azure virtual machines.

Microsoft publishes step-by-step guidance on how to prepare and configure VMware migration to Azure using Azure Site Recovery. To protect running workloads, make sure the vCenter access account used by the Azure Site Recovery configuration server only has the correct access permissions.

**PORTING VMWARE DISKS**

Instead of using Azure Site Recovery, an alternative approach for VMware to Azure migration is to simply port the existing disks to Azure and assign them to a new VM. A number of steps are required to properly configure the OS for Azure, and to convert the disks to the correct format. For details, see the Migrating Disks section of this playbook.

**RESOURCES**

- Azure VMWare Solutions
Migration Tools

Following is a list of the most common migration tools and services used when migrating servers to Azure Virtual Machines. See also the tools listed under Discovery, many of which can also support migration. These tools are all supported in the Azure public cloud, check with the individual vendors for Azure Government support. You can also consult the [Azure Migration Center](https://aka.ms/AzureGovPlaybook) for more information.

- **Azure PowerShell** and **Azure CLI**
  
The Azure command line tools are some of the most frequently used tools with migration. Tasks range from uploading images to Azure Storage, to automating Azure infrastructure during a failover from **[Azure Site Recovery with a recovery plan](https://aka.ms/AzureGovPlaybook)**.

- **Azure Migrate**
  
  Azure Migrate support for VMware migration is in preview, and requires you to [register in advance](https://aka.ms/AzureGovPlaybook). The preview is offered with full support for production workloads.

- **Azure Site Recovery**
  
  As well as offering a Disaster Recovery solution for failover to Azure VMs, **[Azure Site Recovery](https://aka.ms/AzureGovPlaybook)** can also be used to replicate and migrate VMs to Azure at scale. Azure Site Recovery can be used with **[Azure Migrate](https://aka.ms/AzureGovPlaybook)** (which helps with migration assessments).

- **CloudEndure**
  
  CloudEndure® provides an automated migration solution that utilizes block-level continuous replication, application stack orchestration, and automated machine conversion to ensure data integrity during migrations to, between, or within the cloud.

- **ATADATA**
  
  ATADATA’s automates the migration of workloads and also auto-provisions multi-tiered live workloads directly into Hyper-V, Azure Classic or Azure Resource Manager environments. The agentless architecture is managed through the ATADATA Console which installs entirely behind client firewalls, or via a hosted/SaaS deployment.

- **Datometry**
  
  Datometry Hyper-Q simplifies enterprise management of existing applications and develops new applications on cloud databases.

- **Unittrends**
  
  Automatically remodel VMs to native cloud virtual machines in low cost AWS S3 or Azure Blob storage. This free tool even handles the transformation of networking differences between VMware and AWS.

- **Attunity**
  
  Attunity Replicate empowers organizations to accelerate data replication across a wide range of heterogenous databases.
CloudAtlas

CloudPilot’s static code analysis ensures a deep understanding of applications and data to successfully migrate them with no code changes to Azure Containers, Azure Virtual Machines, or Azure App Service (PaaS). Migrate in minutes, not months. CloudPilot checks applications for security, governance, and regulatory compliance, and with coding best practices to reduce migration risks and costs.

ZeroDown Software

ZeroDown enables companies to move applications from their data center or other hosting platform to Azure with no interruption of service. The tool automatically synchronizes the source and target environments and is transparent to the migrated application’s users with no cutover problems or loss of in-flight transactions.
Business Continuity

Providing guaranteed continuity of service even in the event of failures is a key requirement of any business application. Services in Azure are no exception.

Business continuity requires that services keep running, or recover quickly, even when disaster strikes. That could be a large-scale IT failure, or a data loss event.

This presents both a challenge, and an opportunity. You can use Azure services to enhance your offerings to support business continuity for customers. In designing your business continuity service, be prepared to answer common customer questions, such as:

- Will you help me restore my data when it is corrupt or lost? Will you take care of my data’s long-term retention compliance requirements?
- Will you protect my mission critical applications? Will you make DR and recovery plans and run DR drills?
- Will you ensure business continuity in case of any interruption? What kind of SLAs will you provide?

To protect against IT failures, Azure Site Recovery enables critical workloads to replicate their running state to Azure, and to rapidly fail over to an Azure-based infrastructure when needed. Whilst this creates data redundancy, it does not protect against data corruption, accidental data deletion, or ransomware, and thus additional data backups, as provided by Azure Backup, are also essential.

These services can be used to protect both cloud workloads and on-premises deployments. Providing additional resilience to on-premises applications by integrating these Azure services can be a ‘quick win’, helping to build confidence prior to a full Azure migration.

Microsoft Azure offers a rich set of services to backup workloads and fail over critical workloads, in addition to hybrid storage support.

- **Azure Backup** supports file and folder-based workloads, virtual machine backup, as well as workload specific support such as Hyper-V, VMware, SharePoint, and Active Directory straight to Azure, removing the need for physical backups like tape. Azure Backup also provides backup for SQL Server running in Azure VMs (without requiring any backup infrastructure) and for Azure Files shares.
- **Azure StorSimple** is an appliance (physical and virtual) that provides hybrid tiered storage to automatically offload data to the cloud.
- **Azure Site Recovery** protects important applications by coordinating the replication and recovery of physical or virtual machines. You can replicate to your own datacenter, to a hosting service provider, or even to Azure to avoid the expense and complexity of building and managing your own secondary location. Azure Site Recovery continuously monitors service health and helps automate the orderly recovery of services in the event of a site outage at the primary datacenter.
Migrating Existing VMs to CSP

The Azure Cloud Solution Provider (CSP) program is a Microsoft Reseller program enabling Microsoft Partners to re-sell Azure services and provide additional support for their customers. It is available in both Azure Public and Azure Government clouds.

In some cases, a customer may have an existing Azure-based application, which they wish to transfer to the Managed Service Provider (MSP) for ongoing maintenance and monitoring. Migrating an existing application to an MSP may require that the Azure resources that implement that application be migrated to a different Azure subscription. This will typically be a CSP subscription managed by the MSP on behalf of the customer.

Azure supports moving resources between subscriptions. However, there are a small number of limitations to be aware of.

First, Azure only supports resource move where both source and destination subscriptions reside under the same Microsoft tenant (directory). The existing subscription may use a different Azure AD tenant or may use a Microsoft account. In either case, it must be transferred to the tenant created when the customer account is created in the CSP portal.

Second, not all Azure resources are available in CSP subscriptions. The Azure CSP Migration Assessment Tool can be used to identify any existing resources that are not currently supported in CSP subscriptions, or which do not support resource move. In some cases, the tool will specify modifications which are required prior to migration; in other cases, the tool may identify existing resources which cannot currently be migrated. In this case, changes to the application may be required to remove this component.

Third, CSP subscriptions only support the Azure Resource Manager deployment model, and not the Azure Service Management (‘classic’) model. Resources using the ‘classic’ model will be identified by the Azure CSP Migration Assessment Tool, and will need to be migrated in-place to the Azure Resource Manager deployment model before continuing.

Finally, the resources can now be migrated to the new subscription. Cross-subscription migrations require resources and all their dependencies to be moved at once. For example, if you have VM resources in one resource group, and that VM’s disks are stored in a storage account in another resource group, first move all dependent resources to a single resource group. You can then migrate the entire resource group at the same time.

The links given in the Resources section below provide detailed step-by-step instructions for each step of the migration process.

RESOURCES

- CSP for Azure Government
- Migrating resources from an EA subscription to CSP
- Migrating resources from a PAYG subscription to CSP
- Azure CSP Migration Assessment Tool
- Upgrade resources from Classic to Resource Manager
- Moving resources between Azure subscriptions
- ASR Capacity Planning guide for migration to CSP
Migrating Databases

Migrating databases is a crucial step in any migration project. Fears over application downtime or data loss are common, so it’s important to have a well thought-through and proven approach.

Alongside migrating servers to virtual machines, migrating the application database is perhaps the most critical step in any Azure workload migration. Maintaining integrity and availability of data is critical, and the time taken to synchronize data between old and new systems may determine the duration of any service disruption during migration.

Your migration team will need to:
- Understand compatibility issues between existing databases and new databases in Azure, including running a compatibility assessment tool.
- Choose an appropriate database hosting technology in Azure.
- Create new databases and migrate any existing database schema and objects.
- Execute data migration.
- Cut over the production system to use the new database.

There are two main options for running a database in Azure: either as a database installed on an Azure VM or using Azure Platform as a Service. In both cases, a range of database technologies is supported, including Microsoft SQL Server, PostgreSQL, MySQL, NoSQL, Cassandra, MongoDB and more.

In many cases, even where an infrastructure-only migration strategy is being followed, the database will be migrated directly to Azure Platform as a Service, rather a database hosted on a VM. The motivation is to take advantage of the PaaS benefits of Azure such as lower management overhead for underlying infrastructure, quick provisioning and service scaling, and integration with other PaaS services.

For customers who have SQL Server on premise then Azure SQL Database also offers SQL Database Managed Instances for near 100% compatibility with on-premises SQL Server. This provides you with all the advantages of a PaaS deployment along with the ease of migration inherent in a SQL Server on IaaS deployment. This makes SQL Database Managed Instances an ideal target for database migrations.

A key goal of migration is to avoid any loss of data. In some cases, a real-time synchronization between old and new databases is possible, enabling migration without service impact. In many cases however, the most pragmatic approach is to accept that the application may be unavailable (or available as read-only) during the migration work window during which the data will be replicated. The duration of this window can be kept to a minimum by performing an initial data transfer prior to
migration, followed by an incremental sync containing only subsequent changes during the migration work window. Migrations should be approached with the same rigor and processes as a full software or hardware project – a solid methodology is required for success.

**KEY SERVICES**

- **Azure Database Migration Service**: The Azure Database Migration Service is a fully managed service designed to enable seamless migrations from multiple database sources to Azure Data platforms with minimal downtime. The service uses the Data Migration Assistant to generate assessment reports that provide recommendations to guide you through the changes required prior to performing a migration, and performs all of the associated steps, taking advantage of best practices as determined by Microsoft.

- **Data Migration Assistant**: The Microsoft Data Migration Assistant tool can be used to assess a Microsoft SQL Server database in preparation for migration, identify compatibility issues, and to execute the migration, either to SQL-on-IaaS or to Azure SQL Database.

- **Third-party tools**: A range of third-party tools is available to assist with data migration. See the Database Migration Guide for a list of tools.

**RESOURCES**

- Azure Database Migration Hub
- Data Migration Blog
- Azure Blog post: Migrating to Azure SQL Database with zero downtime for read-only workloads
- Azure SQL Database Managed Instance Azure Blog post: Migrating to Azure SQL Database with zero downtime for read-only workloads
- Azure SQL Database Managed Instance
Executive Summary

Modernizing applications to use Azure platform services maximizes the value of migrating to the cloud. Which applications should you modernize, and how?

In the previous chapter, we looked in depth at how to migrate workloads to the cloud using a ‘lift and shift’ approach (rehosting) to Azure’s infrastructure services. In this chapter, we’ll study how to migrate applications to Azure’s platform services (rearchitecting).

While a lift-and-shift migration to Azure infrastructure services can offer significant benefits, it does not take advantage of everything the cloud has to offer. Virtual machines still need to be patched, services cannot scale automatically based on usage, software updates have to be managed, and many of the higher-level services offered by the cloud are not available.

To take full advantage of the cloud requires a migration to Azure platform services. Here, the full benefits of the cloud can be realized: patching and many other maintenance tasks are handled automatically by the platform, streamlined workflows support rapid software updates, services can auto-scale based on usage, and the full power of all Azure services is available.

Earlier in this playbook, we discussed the various motivations behind a cloud migration, and the different ways that migration can deliver value for a business. To recap, the four main cloud benefits are: cost saving, agility, service quality, and the new scenarios that cloud-based technologies can enable. Only a platform-based architecture can take full advantage of these benefits.

In this chapter, we will discuss migrating applications to Azure platform services. We will start by taking a closer look at the platform services available in Azure, the benefits of a platform-based approach, and we will provide some best practices and design considerations for ‘cloud-native’ application architectures.

We will then go on to discuss the most commonly used approaches, focusing firstly on Azure App Service, and then on microservices and containers. We’ll also look at the various technologies available for storing and processing data, including ‘big data’ technologies used to extract insight and value from large data volumes.

Finally, we’ll discuss higher-level platform services for machine learning and artificial intelligence. These cloud-only services are increasingly used to light up new application scenarios, delivering competitive advantage beyond cost savings and agility.

Top 4 things to do

Cloud-native designs offer the greatest cloud benefits. Here are the top 4 things to get you started.

- Understand the benefits of platform vs infrastructure approaches to the cloud
- Build technical expertise in cloud-native design
- Choose which platform services your practice will use
- Build experience at migrating existing applications to platform services
Modernizing Applications with Azure

One of the most effective ways to realize the benefits of migrating applications and system architectures to the cloud is to utilize PaaS (Platform as a Service) services.

Platform as a Service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable the delivery of everything from simple cloud-based apps to sophisticated, cloud-enabled applications. Like IaaS (Infrastructure as a Service), PaaS includes infrastructure (servers, storage, and networking) but also middleware, development tools, business intelligence (BI) services, database management systems, and more. PaaS is designed to support the complete application lifecycle.

**BENEFITS OF USING PAAS**

Here are the biggest benefits of using PaaS services to modernize and host applications in the cloud:

- **Managed Virtual Machines (VMs):** PaaS hosting is provided by Managed VMs that do not require the traditional maintenance and updates required by traditional IaaS VMs. This provides an abstraction that automates Operating System updates and patches, so the development team only needs to be concerned with the application, data, and deployment rather than infrastructure maintenance.

- **Cut coding time:** PaaS development tools can cut the time it takes to code new apps with pre-coded application components built into the platform, such as workflow, directory services, security features, search, and so on.

- **Add development capabilities without adding staff:** PaaS components can give your development team new capabilities without your needing to add staff having the required skills.

- **Develop for multiple platforms—including mobile—more easily:** Some service providers give you development options for multiple platforms, such as computers, mobile devices, and browsers making cross-platform apps quicker and easier to develop.

- **Use sophisticated tools affordably:** A pay-as-you-go model makes it possible for individuals or organizations to use sophisticated development software and business intelligence and analytics tools that they could not afford to purchase outright.

- **Support geographically distributed development teams:** Because the development environment is accessed over the Internet, development teams can work together on projects even when team members are in remote locations.

- **Efficiently manage the application lifecycle:** PaaS provides all the capabilities that you need to support the complete web application lifecycle: building, testing, deploying, managing, and updating within the same integrated environment.
MIGRATING APPLICATIONS TO PAAS

Using Azure platform features is not all-or-nothing. You can combine infrastructure and platform services in a single deployment. For example, it is common for an infrastructure migration to run application servers using infrastructure virtual machines, but to use the Azure SQL Database platform service as the data tier, rather than running SQL Server on virtual machines. Many other combinations as possible.

While it is most convenient to build “cloud-native” applications from the start, that is often not possible with many applications. There is often a significant investment in “legacy” applications that make it cost prohibitive to start over from a blank slate to benefit from the cloud. For this reason, it’s most feasible with many systems to refactor the applications to include cloud-native design considerations and leverage PaaS technologies.

To support this, Azure provides a range of platform services, each offering a range of benefits and each requiring a different degree of application modernization. For example, an application might be migrated to Azure App Service, or converted to run in containers, with relatively few changes. At the other extreme, a fully serverless architecture utilizing Azure Functions and higher-level Azure services may require the application to be re-written. Choosing the right approach to application modernization requires an understanding of the suitability, cost and migration complexity of each of the platform approaches available.

KEY CHALLENGES

- Focus on building applications and business logic, instead of managing infrastructure, reliability, scalability, and latency.
- Quickly build powerful web, mobile, and API apps using multiple languages / frameworks (.NET, .NET Core, Java, Ruby, Node.js, etc.).
- Reliably deploy, update and scale applications effortlessly across many virtual machines, using either Windows or Linux.
- Globally deliver content to any device with low latency.

KEY SERVICES FOR THIS OFFERING

- **Virtual Machine Scale Sets**: Apply autoscaling to virtual machines for high availability. Create thousands of identical virtual machines in minutes.
- **Azure App Service**: Quickly create powerful cloud apps using a fully managed platform.
- **Azure Container Services (AKS)**: Simplify the deployment, management, and operations of Kubernetes
- **Service Fabric**: Build and operate always-on, scalable, distributed apps. Simplify microservices development and application lifecycle management.
- **Azure Functions**: Build apps faster with a serverless architecture. Accelerate your development with an event-driven, serverless compute experience.
Cloud-native Architecture and Design

Most of the traditional application designs and architectures that are commonplace in on-premises datacenters can run in the cloud without change. However, the cloud brings with it many new capabilities and features. Applications that make use of cloud capabilities are often referred to as cloud-native applications.

On the surface, designing applications for the cloud is not very different than designing for on-premises. All the same development tools, language, and frameworks can be used in the cloud. This enables all the familiar tools and existing skillsets of the development team to be used.

However, the cloud also offers a range of additional capabilities, and taking advantage of these requires some design changes. In addition, there are a wide range of cloud services and features available, and a variety of design approaches available. When migrating to a cloud-native application architecture, you are responsible for:

- Choosing the right cloud-native application architecture for your application.
- Incorporating proven best practices into your cloud designs.
- Optimizing implementation by leveraging existing deployment templates for common architectures.

You’re not on your own. Microsoft has published extensive guidance on designing applications for the cloud. This guidance can be found in the Azure Architecture Center, and provides a wealth of resources and proven cloud architecture best practices, based on real-world experiences gained from working directly with the largest Azure customers. Using this guidance can accelerate your design process, as well as ensuring that your designs follow proven best practices. Amongst other resources, the Azure Architecture Center includes:

- The Azure Application Architecture Guide, which presents a number of common architecture styles, technology choices, and design principles for Azure applications.
- Azure reference architectures, which demonstrate recommended practices and include deployable solutions which can be used as the basis of your own deployments.
- Azure architecture best practices for a wide range of common topics, including API design and implementation, autoscaling, use of background jobs, monitoring, fault handling, and more.
- Design review checklists for Availability, Resiliency and Scalability, which can be used to validate and improve your own designs, enabling you to catching potential problems early and avoid expensive re-work later.
Cloud Design Considerations

Cloud-native applications are designed differently from conventional applications.

There are a few design considerations necessary when building software to be “cloud-native” and utilize PaaS services. These design considerations address many of the key differences to resource allocations and availability with PaaS services and IaaS resources. Here are the key design considerations for building "cloud-native" applications, or migrating existing applications, using PaaS services:

- **Scale Out over Scale Up**: One of the traditional methods of scaling to meet increased load in on-premises environments is to Scale Up; simply add more CPU power, Memory capacity, or storage capacity to the server. This is a common practice on-premises with both Single Server and Multi-Server hosting solutions. In the cloud, server resources are more of a readily available commodity. In the cloud, you can basically provision a new server VM when it’s needed. For this reason, it’s much easier to add more servers when extra capacity is needed. An additional benefit of Scaling Out (adding more servers / VMs) is an increases resiliency to the application deployment. If a 1 server out of 10 goes down, it affects the overall performance of the application and SLA to the company’s clients and users much less than if 1 server out of 2 goes down. Scaling Out and spreading load across server instances has many benefits, including: higher availability, higher resilience against failure, as well as the ability to tweak server resources to optimize cost when comparing pricing tiers.

- **Graceful Fault Handling**: Every software system has failures. When distributing load across multiple server instances, or integrating a distributed / microservices architecture, an application needs to be coded to gracefully handle all error when possible. These errors can even include transient failures, such as not being able to connect to a database or service, isolated network outage on a single VM, or any other sort of error that occurs at random times for a short period of time and then goes away. When a call to an external service fails, the application can be coded with Retry Logic to re-initiate making the service call 1 or more times before throwing an exception. Another possible implementation is to cache a user’s request using some type of message queue, so the user can continue with their work while the system handles the error and performs the requested work in the background.
• **Multi-Zone and Multi-Region Deployment:** One of the aspects to hosting application in on-premises environments that can easily become cost prohibitive is the ability to deploy to multiple datacenters for redundancy and increased resiliency. In the cloud, Microsoft Azure is made up of 54 announced Azure Regions spread across continents and geographies that can be utilized for any cloud application deployment. Availability Zones are being introduced in Azure and Azure Government. Check for availability in your region. Availability Zones can be utilized to enable application instances to be deployed to specific datacenters within the Region. Application deployments that utilize Zones and Regions have the capacity to be globally resilient against Regional or Datacenter failures. This extra resiliency can be combined with scaling out to host applications with a much greater level of resiliency and availability than is possible in most on-premises datacenter environments.

• **Do Not Write to Local File System:** When using PaaS services like Azure App Service to host an application, it’s important to not write anything persistent to the local file system. The reason for this is that multiple instances of the application running in the service do not share the same local file system as they are hosted on different VMs. Instead of writing to the local file system, any files and/or data that needs to be accessed across application instances should be written to a shared storage service like Azure Blob Storage, Azure Redis Cache, or another database service.

• **Stateless Design:** When designing applications to scale out, instead of scale up, the design to share state across instances can prove to be difficult depending on the overall application architecture. Modern application architecture is to design applications to remain Stateless. This has become the modern standard in web application and Rest API design. It’s common to use Cookies with an HTTP-based application to remain Stateless, but another option is to use a cache service like Azure Redis Cache to share state across instances for applications that still require state.

• **Serverless:** Serverless computing, such as Azure Functions, takes the benefits of PaaS even further by adding an additional abstraction layer that enables for an individual function of code to be deployed and hosted without requiring a full application to be maintained. This larger abstraction of Azure Functions is integrated with Input and Output Bindings that provide built-in capabilities to integrate with other Azure services, as well as third-party services and applications. Using Serverless compute decreases the overall development and maintenance costs that enable faster time to delivery and easier production support. Learn more about [Serverless in Azure Government](#).

• **PaaS Services:** Where a specific service is available for a task, using that service is usually a better choice than building your own using lower-level platform components. These services have already been designed to deliver the availability, performance, security and scale required by Microsoft’s most demanding customers—saving significant work and providing a service level that would be difficult and expensive to match. Using services built specifically for the cloud enhances the development team’s capacity to deliver value, in addition to providing an abstraction that removes many of the monotonous and time-consuming aspects of Server and Virtual Machine maintenance.
Cloud Design Patterns

Use proven design patterns to accelerate and improve your cloud-native application designs.

Among the multitude application design challenges your developers will face, many have already been solved and documented as cloud design patterns. These patterns provide proven out-of-the-box solutions to challenges involved in designing applications to make best use of the cloud. Using proven, established patterns streamlines development by saving the development team from having to design solutions for these common scenarios on their own.

Here are some of the most commonly used cloud design patterns used to build “cloud-native” applications:

- **Retry Pattern**: Enable the application to handle transient failures when it tries to connect to a service or network resource, by transparently retrying a failed operation. This can improve the stability of the application.
- **Circuit Breaker Pattern**: Handle faults that might take a variable amount of time to recover from, when connecting to a remote service or resource. This can improve the stability and resiliency of an application.
- **Competing Consumers Pattern**: Enable multiple concurrent consumers to process messages received on the same messaging channel. This enables a system to process multiple messages concurrently to optimize throughput, to improve scalability and availability, and to balance the workload.
- **Priority Queue Pattern**: Prioritize requests sent to services so that requests with a higher priority are received and processed more quickly than those with a lower priority. This pattern is useful in applications that offer different service level guarantees to individual clients.
- **Queue-Based Load Leveling Pattern**: Using a Queue that acts as a buffer between a task and a service it invokes in order to smooth intermittent heavy loads that can cause the service to fail or the task to time out. This can help to minimize the impact of peaks in demand on availability and responsiveness for both the task and the service.
- **Cache-Aside Pattern**: Load data on demand into a cache from a data store. This can improve performance and help to maintain consistency between data held in the cache and data in the underlying data store.
- **Throttling Pattern**: Control the consumption of resources used by an instance of an application, an individual tenant, or an entire service. This can allow the system to continue to function and meet service level agreements, even when an increase in demand places an extreme load on resources.
- **Command and Query Responsibility Segregation (CQRS)**: This design pattern segregates operations that read data from operations that update data by using separate interfaces. This can help maximize performance, scalability, and security. It also supports the evolution of the software system over time through higher flexibility and prevents update commands from causing merge conflicts at the domain level.

The Microsoft Architecture Center includes an additional list of cloud design patterns, as well as a list of cloud “anti-patterns”—common mistakes that can negatively impact the performance of cloud-native applications.
Azure DevTest Labs

DevTest is probably the only workload that doesn’t have corporate issues slowing down its migration. Aside from the security and backup of a company’s source code, there’s no reason for IT managers to balk nor are there regulatory or compliance rules that are stopping the march of DevTest to the cloud.

Microsoft Azure DevTest Labs provides an end-to-end experience to address the testing environment needs of modern development teams. Before looking at the benefits of DevTest labs, let’s first review the challenges of building and maintaining DevTest environments.

DevTest Challenges

Skills and Effort Required to Build Out DevTest Environments

Many development shops build an infrastructure from scratch as their companies haven’t moved any workloads to the cloud yet, and that can be overwhelming for developers. Even though they are leveraging cloud tools, solving mundane issues such as designing Virtual Networks, IP address spaces, subnetting, DNS for name resolution, Virtual Machines templates, file shares, storage connections to DevOps package repositories will all need to be designed and implemented. This requires skills in all areas of IT, many of which are outside of a developer’s expertise.

Augmenting Previously Deployed Continuous Integration and DevOps Tools

Many development and testing teams have invested in continuous integration and DevOps tools that are heavily utilized for their operations. When migrating DevTest environments from on premise to the cloud, these investments must be leveraged and augmented to ensure their investment is extended to the cloud.
Customizing the Environment to Meet the Needs of Developers and Testers

Developers and testers need their environments to be exactly right to ensure efficiency and to minimize bugs. Development teams have become very detail-oriented to ensure that each environment being developed can be replicated quickly and can be the same every time, no matter what. Often, this means building Virtual Machine (VM) templates and scripts to ensure configurations with DevOps tools. Cloud solutions must allow for this type of very precise customization and ease of use.

Providing a “Ready to Test” Solution

“Ready to test” is all about efficiency. Testing teams need to focus on their role in the development cycle, which is ensuring the highest quality of the application. Oftentimes, testers must build their environment by hand, which takes time away from testing the application and can also introduce human error. When testers show up for work, they should login and start their test, nothing else. The bits they are testing, and all their tools should already be installed on the VMs they are working with to ensure they catch every issue, instead of installing software over and over.

Ensuring Access Control and Isolation from Production Environments

A development and testing environment is meant just for that – development and testing – and those who use these environments should only have access to leverage the cloud for such activities. It’s important to provide them with the access they need to be successful in their role without risking the safety of production systems.

Accidental shutdowns of systems should never happen, and sufficient isolation between DevTest and production should be in place to ensure proper change control practices are followed. Moving to the cloud doesn’t mean pioneering to the Wild West. Governance must be in place to ensure that all teams are playing their roles properly while utilizing the resource.

Leveraging the Cost Efficiencies of the Cloud via “Pay-As-You-Go” While Capping Costs and Staying on Budget

One of the most interesting aspects of moving to the cloud for DevTest is the idea that costs are only incurred while developing and testing. Some companies can dip as low as 0% utilization of on premise DevTest environments at times during the year. Leveraging the flexibility of the pay-as-you-go model is one of the most compelling reasons to move to the cloud. If the users of the resources aren’t cognizant of how many resources they are using or when those resources are being used, the scalability of the public cloud can turn into some very large bills. Just think of an electric bill if everything in a home was left on 24 hours a day, seven days a week; the bill would be astronomical. IT projects are known for always being over budget, so there needs to be a way to ensure that the resources required don’t put a project over budget.
Azure DevTest Labs

To solve these problems and let developers and testers do what they do best, Microsoft has developed a turnkey solution for DevTest in the cloud: **Azure DevTest Labs.** This service addresses the above problem by means of the following features.

**Quickly be “Ready to Test”**
DevTest Labs provides multiple options to help developers and testers to get their environments ready quickly. It offers three different types of VM bases that developers and testers can use to create the Dev/Test environments:

- **Marketplace images:** VM images directly from Azure Marketplace.
- **Custom images:** leveraging a VHD file built by the customer.
- **Formulas:** a reusable base where VM creation settings (such as VM image, VM sizes, virtual network, etc.) are pre-defined, so that environments can be created without requiring any more input.

Reusable artifacts in the DevTest Labs allow users to run VM extensions and install tools, deploy applications or execute custom actions on demand once a lab VM is created.

**Worry-free self-service**
DevTest Labs enables a team self-service model where developers and testers go to the Azure portal directly to create environments, instead of going through a complicated “request” process. In this case the DevTest Lab is leveraging Azure Role-Based Control (RBAC), which empowers teams to use the portal to build VMs as needed on their own.

Lab policies makes it easier to control costs by allowing lab owners to set boundaries and standard operating procedures around what is spend on the project. By using policies Development and Testing teams can ensure they won’t go over and have an unexpected bill at the end.

Using Lab policies and Azure Role-Based Access Control (RBAC), DevTest Labs enables a sandbox environment for developers and testers to provision their own environments without unexpected accidents that can introduce a big bill.

**Create once, use everywhere**
DevTest Labs resources (labs, custom images, formulas, artifacts, etc.) are reusable across labs, so that you don’t need to re-create the same thing from scratch.

DevTest Labs fully supports Azure Resource Manager (ARM) and follows the best practice of using resource groups. You can create multiple labs with the same settings/policies by deploying the same ARM template.

ARM templates are fully supported to deploy labs and resources in a lab. Reusable custom images and formulas can be created from an existing VM, and artifacts loaded from VSTS Git or GitHub repositories can be used cross different labs.

**Integrates with existing toolchain**
Azure DevTest Labs provides pre-made plug-ins, command-line tool and APIs that allow you to integrate your Dev/Test environments from labs to the release pipeline.

In addition to APIs and command line tools, **Azure DevTest Labs Tasks** are available in Visual Studio Marketplace to better support your release pipeline.
Migrating Applications to Azure App Service

Azure App Service is a powerful and flexible platform for hosting web applications in Azure. Migrating applications to Azure App Service is often the simplest and quickest way to take advantage of the benefits of PaaS.

Azure App Service is a fully managed platform to run and scale both Internet-facing and Intranet web applications and services, on both Windows and Linux. It supports a wide range of development languages and offers a high level of developer productivity with features such as such as CI/CD, easy and safe application updates, and integration with Azure Repos, BitBucket, Docker Hub and GitHub. Azure App Service also supports auto-scaling of the infrastructure supporting your app, enabling significant cost savings.

Review the following considerations before you consider migrating your applications to Azure App Service:

- **Port Bindings**: Azure App Service support port 80 for http and port 443 for HTTPS traffic. If you have sites using any other port after migration to Azure App Service, do remember that these are the only ports that will be used.
- **Usage of assemblies in the GAC (Global Assembly Cache)**: This is not supported. Consider bin placing the assemblies in the local bin.
- **IIS5 Compatibility Mode**: IIS5 Compatibility Mode is not supported. In Azure App Service each Web App and all the applications under it run in the same worker process with a specific set of application pool settings.
- **IIS7+ Schema Compliance**: One or more elements and/or attributes are being used which are not defined in Azure App Service IIS schema. Consider using XDT transforms.
- **Single Application Pool Per Site**: In Azure App Service each Web App and all the applications under it run in the same application pool. In case you have applications with different application pool in IIS, consider establishing a single application pool with common settings or creating a separate Web App for each application.
- **COM and COM+ components**: Azure App Service does not allow the registration of COM components on the platform. If your site(s) or application(s) make use of any COM components, these would need to be rewritten in managed code and deployed with the site or application.
- **ISAPI Extensions**: Azure App Service can support the use of ISAPI Extensions, however, the DLL(s) need to be deployed with your site and registered via the web.config.

Once the above limitations have been taken into consideration, you will need to migrate your applications. The easiest way to migrate is by using the Azure App Service Migration Assistant, which can assist with both migration assessment and migration execution.

The App Service Migration Assistant tool is downloaded and run on the application web server. This provides an in-depth assessment of the application configuration. For modern applications without migration blockers, the tool can also be used to
migrate the application itself to the Azure Web Apps service.

The App Service Migration Assistant tool can be used with both public and Intranet sites. A current limitation is that only ASP.NET applications are supported. The App Service team intends to support more platforms in future, so check the web site for the current support matrix.

Once you have decided to migrate, the following areas need to be considered for migrating applications to Azure App Service. You should also review the considerations for migrating databases to Azure listed earlier in this playbook.

- **On-premises integration**: In case your applications are communicating with other applications which will not be migrated to Azure, you must consider how the communication will happen when your application moves to cloud. One solution is to enable the other application to communicate over the internet using REST. This may require changes in both the applications, not to mention the additional risk of exposing the server onto internet. Another approach would be to establish a secure connectivity to your on-premises server from Azure App Service, where your application is hosted. This can be done in any of the following ways depending on your requirement – Deploying your apps in an App Service Environment using an Isolated App Service Plan; enabling virtual network integration with an Azure VNet, establish a Site to Site VPN between this Azure virtual network and on-premises, and then enable routes between your App Service and the on-premises server; and establishing hybrid connections.

- **Authentication**: When on-premises, using no authentication or Windows authentication may be acceptable as there was mutual trust with AD. When you migrate to Azure, you will need to enable authentication with Azure Active Directory. This means modifying some of your configuration to be able to authenticate your users via Azure AD.

- **Session State**: In an ideal case, you can make your application stateless to scale/switch at will. In case it is not possible, have your session state configured to be persisted in Azure Redis Cache.

- **File Persistence**: Usually, websites might require uploading files that need to be persisted. On Azure App Service, it is recommended to persist any files outside of the App Service into something like a blob store. Modify the application to now use either the Azure Storage SDK or the REST APIs for saving and accessing files.

- **App Settings and Connection Strings**: There will be App Settings and Connection Strings that will change based on environment, whereas some will stay same. For the ones that change based on environment, also define them on the portal or deployment template so that they can be overridden for different deployment slots.

- **Logging**: If your logging framework is logging to files saved locally you will need to update them to either log in to Azure Diagnostics or to a centralized blob store. You can also include Azure App Insights to get deeper insights into how your application is performing.

- **Certificates**: Certificates are not migrated directly. You will need to explicitly upload your certificates to be able to work on Azure, as detailed in this Bind SSL Certificate documentation. You can also purchase certificates directly from Azure, as detailed in this buy SSL cert documentation.

- **Custom Domains**: Custom domains can be associated to Azure Web Apps via a CNAME record change. You also need to update App Service to validate the DNS. Details are available in this map custom domain documentation.

- **Email**: Sending Emails requires an SMTP server. App Service does not provide you with the same and there is no way that you can configure it within App Service. While you can setup a SMTP server to send emails on Azure IaaS VMs, we do put in restrictions. We recommend using relay services to send email, such as Office 365.

- **LDAP Queries**: If you are building internal applications that are querying your LDAP store such as AD, those may not work on Azure App Service. Specifically, in the case of Active Directory, you can move AD to Azure AD and then use the graph APIs to make the necessary queries to Azure. For this, you will need to register your application with Azure AD to permit querying Directory Objects. A complete list of graph APIs is here.
Microservices and Containers

The microservices architecture has become an important part of building distributed mission-critical software systems.

Traditional application architectures build applications in large, monolithic components. These large components are deployed as a single unit, making it hard to maintain strict separation between internal components. This results in long integration, test and release cycles, which slow development, reduce agility and increase costs.

The primary design principle of a microservices architecture is to design an entire software system to be built using smaller software components, called microservices. Each microservice performs a single function of the overall system that can be developed, deployed, and scaled independently. This independence enables accelerated development by enabling individual component teams to work more independently, thereby avoiding long integration, test and release cycles. For more information, see the article Why a microservices approach to building applications?

Containerization is an approach to deployment and application management that combines an application with its dependencies and configurations (via manifest files) into a container image. Due to their highly efficient resource consumption, containers are an ideal platform for the development of microservices. Each microservice is built into a dedicated container image, and can then be more easily deployed, scaled, and managed as a single package. Using microservices and containers reduces the effort required to manage the deployment and scalability of an application.

Azure supports several services to support microservices and containers:

- **Azure Kubernetes Services (AKS):** Kubernetes is the leading platform for orchestrating container deployments. AKS simplifies the deployment, management, and operation of Kubernetes.
- **Azure Container Instances (ACI)** provides a fully managed service in which you can run your containers, without any need to deploy or manage the underlying infrastructure. This service enables you to easily run containers on Azure with a single command, and with per-second billing.
- **Azure Container Registry** is a fully managed Docker Registry service. Container registries can be used to store and manage container images across all types of deployments.
- **Azure Service Fabric** is a platform for deploying and operating always-on, scalable, distributed, microservice-based applications. Service Fabric enables you to simplify microservices development and application lifecycle management.
- **Web App for Containers** allows you to easily deploy and run containerized web apps that scale with your business and provides a fully managed platform for infrastructure maintenance.
What is Docker?

Docker has become the de-facto standard for containers.

Docker is an open-source project for automating the deployment of applications as portable, self-sufficient containers that can run on the cloud or on-premises. Docker is also a company that promotes and evolves this technology. Docker works in collaboration with cloud, Linux, and Windows vendors, including Microsoft.

Docker image containers run natively on Linux and Windows. Windows images run only on Windows hosts and Linux images run only on Linux hosts. The host is a server or a virtual machine.

You can develop on Windows, Linux, or macOS. The development computer runs a Docker host where Docker images are deployed, including the app and its dependencies. On Linux or macOS, you use a Docker host that is Linux-based and can create images only for Linux containers (on macOS you can edit code or run the Docker CLI, but as of the time of this writing, containers do not run directly on macOS). On Windows you can create images for either Linux or Windows containers.

For further reading, see:

- Introduction to Containers and Docker
- .NET Microservices: Architecture for Containerized .NET Applications
Modern Data Platform

The cloud has driven rapid changes in how applications handle data. Whatever your data needs, Azure offers a service to suit.

Modern data platforms are designed to ingest and process petabytes of data for a variety of purposes. These systems are capable of ingesting and storing data in nearly any format and at any scale. Data may be structured like a relational database or unstructured such as a web log. These modern data platforms enable a variety of applications types such as large scale cognitive and AI applications and high throughput IoT data ingestion.

There are several options for running a modern data platform in Azure. There are big data stores such as Azure Data Lake Store and Azure Storage and there are compute technologies such as HDInsight and Data Lake Analytics. There are also more focused database options such as Azure SQL Data Warehouse and Cosmos DB that can also operate on large amounts of data.

Choosing a data platform solution will require you to understand the variety of data platform services available and choose the most suitable services for the given application. Once chosen, further work will be needed to choose the correct configuration, for example assessing and optimizing the cluster and storage size.

Transferring large data volumes to the cloud can be another challenge. Online transfers, either via the Internet or an ExpressRoute connection, are the default approach, enabled by tools such as AzCopy. For very large volumes, you can use disks or the Azure Data Box appliance (currently in Preview) to ship data to Microsoft data centers.

A common scenario is data analytics, perhaps from incoming telemetry or using existing data stores. Azure offers several services to help, such as Azure Analysis Services for data modelling and analytics to Azure Event Hubs and Stream Analytics for real-time processing of incoming data streams.

In many on-premises environments, it is common to configure a single monolith Hadoop cluster to handle all types of data ingestion and processing. The architecture we use in the cloud allows us to store all of our data in the same location such as an Azure Data Lake Store and then spin up any number of compute clusters to operate on that data. This separation of compute and storage buys us two things:

- **Decoupled compute and storage scale.** We can scale compute and storage independently of each other. If we need more processing power, we can simply increase the size of our HDInsight cluster.
- **Optimized spending.** We can now have multiple, purpose-built compute clusters allowing us to optimize cluster size and runtime based on a single workload rather than all workloads in aggregate.

**DATA SERVICES IN AZURE**

A summary of the Modern Data Platform services offered by Microsoft is given below:

- **Azure HDInsight:** Azure HDInsight is a fully managed cloud service that makes it easy, fast, and cost-effective to process massive amounts of data. Use popular open-source frameworks such as Hadoop, Spark, Hive, LLAP, Kafka, Storm, R & more. Azure HDInsight enables a broad range of scenarios such as ETL, Data Warehousing, Machine Learning, IoT and more
- **Azure Data Lake Analytics:** Develop and run massively parallel data transformation and processing programs in U-SQL, R, Python, and .NET over petabytes of data with zero infrastructure.
- **Azure Data Lake Store:** Store your unstructured, semi-structured and structured data with no limits on size or throughput. Secure, massively scalable, and built to the open HDFS standard, allowing you to run massively parallel analytics.
- **Azure Cosmos DB:** A low latency, horizontally scalable and globally distributed multi-model database. Support for many APIs such as SQL, JavaScript, Gremlin (Graph), MongoDB, Cassandra and Azure Table storage. Cosmos DB was formerly known as DocumentDB.
MODERNIZING APPLICATIONS

- **Azure SQL Database**: A fully managed database service for structured, relational data.
- **Azure SQL Data Warehouse**: A massively parallel processing server with independent compute and storage scalability, allows you to integrate with big data stores, and create a hub for your data marts and cubes—to drive highly tailored, enterprise-grade performance, while leveraging your existing SQL and BI skills.
- **Azure Data Factory**: Fully managed ETL service in the cloud. Connect all of your data sources and orchestrate your data workflows wherever your data lives.
- **Azure Storage**: Offering fast and scalable blob, table and queue storage, and shared file storage for Azure virtual machines
- **Azure Storage Import/Export Service** and **Azure Data Box**: Use physical disks or a custom-built appliance to ship large data volumes to Azure
- **Azure Analysis Services**: A fully-managed service enabling you to combine data from multiple sources into a single semantic model, enabling reporting through client tools such as Power BI and Excel.
- **Azure Stream Analytics**: A managed event-processing engine for real-time analysis on streaming data.
- **Azure Event Hubs**: A hyper-scale telemetry ingestion service supporting real-time and batch processing.

For more information on the Microsoft Data Platform, see the Microsoft partner [Data Platform & Analytics Playbook](aka.ms/AzureGovPlaybook).
Cognitive Services and AI

Microsoft’s AI and cognitive services allow you to process data in new and exciting ways, extracting patterns and meaning that would previously have required human input. These services enable a wealth of new scenarios.

One of the business benefits of cloud migration is the ability to enable new scenarios that would be impossible (or at least, prohibitively expensive) previously. This concept is at the heart of the digital transformation paradigm shift, and Microsoft’s cognitive and AI services are at the heart of this capability.

You can use the unique data that you generate by operating their services to enhance your applications in new and unexpected ways, for example by interpreting service and customer data in real-time and large scale, including text, docs, images, video, and voice.

The Microsoft AI Platform provides a comprehensive set of flexible AI services and enterprise-grade AI infrastructure that runs AI workloads anywhere at scale. The Microsoft AI Platform accelerates the development of AI solutions with high-level services. Modern AI tools designed for developers and data scientists help you create AI solutions easily, and with maximum productivity.

Machine Learning enables computers to learn from data and experiences, and apply that learning to sense, process and act on information in future. There are many applications for this technology. A common use case is predictive analytics—using historical data to predict future behavior, for example using telemetry data from machines in a factory to predict forthcoming hardware failure and enable pro-active maintenance, thereby reducing downtime.

Microsoft’s suite of Cognitive Services enable insight from human interactions, from facial expressions, to speech, and natural language processing. For example, extracting the positive or negative sentiment from comments on a review forum or twitter feed can enable you to respond more rapidly to a service quality issue, thereby improving the overall citizen experience.

Enhancing existing applications to take advantage of these services is one of the ways to provide additional value to your users.

Core services of Microsoft’s AI platform include:

- **Microsoft Cognitive Services**: Use AI to solve existing problems. Infuse your apps, websites, and bots with intelligent algorithms to see, hear, speak, and understand natural methods of communication.
- **Azure Machine Learning**: Model AI algorithms and experiment with ease. Customize based on your requirements.
- **Azure Bot Service**: Accelerate development for conversational AI. Integrate seamlessly with Cortana, Office 365, Slack, Facebook Messenger, and more.

For further information on how to take advantage of AI, see the Azure AI Platform overview and the AI Practice Development Playbook.
Optimize & Manage

Migration and Modernization with Azure Government

Microsoft Azure Government
Executive Summary

After a successful migration, the workload will be handed off to the Operations team, who must provide a whole new set of services such as monitoring, patching, cost optimization and support.

In this section, we will focus first on cost optimization. Azure offers a wide range of possibilities for reducing running costs and creating cost savings, which we’ll discuss in depth. Taking advantage of these is key to delivering services as efficiently as possible, making responsible use of taxpayer dollars.

Next, we’ll review some best practices for managing services in Azure. We’ll consider subscription management, resource organization, and how to protect Azure resources against unauthorized or accidental changes. We’ll also look at the security and compliance tools and guidance that are available from Microsoft.

Last, we’ll discuss how to automate the deployment and management of Azure services using Infrastructure as Code. Consider both the advantages of this approach, and the variety of technologies available in Azure to deliver, including how to develop your own custom tools.

Top 3 things to do

Here are 3 top tips to increase your efficiency and differentiate your practice.

- Learn how to understand, forecast and optimize costs
- Use best practices for Azure resource management
- Automate using Infrastructure as Code
Cost Optimization

Taking full advantage of Azure’s cost saving and cost management features can help you control costs and deliver your services more efficiently.

With the pay-as-you-go nature of the cloud there are many ways to overspend; even when being careful. A common fear when it comes to adopting the cloud is the fear of runaway spending. Azure provides a range of cost management features and cost optimization opportunities to enable government customers and partners to effectively manage and optimize their spend.

It is always a good idea to design and deploy Azure-based systems that are designed for optimization from the start. Then, by analyzing application performance and cloud spend, and by taking advantage of new Azure features, optimize spend over time.

Additionally, since each Azure service is listed as a separate line item on your Azure bill, you can attribute the spend to different projects, departments, teams, applications and cost centers. This provides superb transparency, allowing services owners to properly understand and manage their service delivery costs.

The key challenges for cost management and optimization include:

• Understanding current cloud spend and forecasting future spend
• Gaining the most value from cloud spend
• Guarding against unexpected costs
• Optimizing deployments for cloud efficiency

In this section, we’ll look at how the cost management and cost savings features available in Azure can help you meet these challenges.
Azure Cost Management

You can’t optimize what you can’t measure. Effective cost management starts with understanding your costs, at a granular level.

Azure Cost Management is an Azure service designed to help you understand and manage your Azure costs. It supports cost analysis, forecasting, budgets, and alerting. It also provides cost optimization recommendations. This service is available within both the Azure public cloud and Azure Government.

VISIBILITY

Azure Cost Management provides a view into the costs of the Azure environment. These reports can be analyzed and the subscription or resource group level. They can also be aggregated across subscriptions or filtered using resource tags to create a wide range of views.

Tracking usage and costs trends is provided by the Cost Analysis area of the tool, which provides a report of costs against time. When first used, the report will have no groups or filtered applied, so this shows the all-up cost for the entire Azure environment. The report can be filtered by the various Azure services consumed by this subscription or by groups that you can add. Some examples of groups are departments or applications that you have identified using Azure Tags.

Access control helps manage costs by ensuring that users and teams access only the cost management data that they need.

MONITORING AND ALERTING

Monitoring usage and spending is critically important for cloud infrastructures because organizations pay for the resources they consume over time. When usage exceeds agreement thresholds, unexpected cost overages can quickly occur.

There are a few important factors which can make ad-hoc monitoring difficult. First, projecting costs based on average usage assumes that your consumption remains consistent over a given billing period. Second, when costs are near or exceed the budget, it’s important to get
notifications proactively as to allow for planning or to adjust Azure spending.

Azure Cost Management allows you to alert stakeholders automatically to spending anomalies and overspending risks. Various reports support alerts based on budget and cost thresholds.

**OPTIMIZATION (RIGHT-SIZING)**

An important aspect to any cloud deployment is ensuring that the right resources are being used for the job at hand. Azure Cost Management provides right-sizing recommendations, for example on switching from on-demand to pre-purchase VMs, or to reveal underutilized VMs which can be moved to a lower cost VM family or size. These recommendations are surfaced via Azure Advisor.

**TRANSPARENCY AND ACCOUNTABILITY**

Prior to moving to the cloud, most service owners don’t have a true idea of what their services cost to run. Often the IT department is seen as overhead or even a black hole that is difficult to understand. With the cloud, this model is turned up-side down, as IT can now see the exact cost of each and every resource.

Azure Cost Management enables cloud accountability by providing accurate cost allocation and chargeback across the organization. These costs can be rolled up and reported on to different entities that can be defined including subscriptions, accounts, departments and cost centers.

This could be as simple as tagging Azure resources for simplified cost allocation. More complex models can also be implemented with different types of cost allocation such as blended/average/normalized rates, compute pre-purchase rates, or any other policy of your choice.

Alerting helps manage costs by notifying you automatically when unusual spending or overspending occurs. Alerts can also notify other stakeholders automatically for spending anomalies and overspending risks.
## Third-Party Cost Management

These are just some of the third-party tools offering cost management functionality for Azure. As with other third-party tools, these are available for the Azure public cloud. Check with the vendor for Azure Government support.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APPTIO Cost Transparency</strong></td>
<td>Apptio Cost Transparency allows you to view all your public cloud costs across providers like AWS and Azure. It can monitor public cloud spend and trends by service type, such as compute, storage, network, and understand which departments are consuming cloud services to help proactively manage spend.</td>
</tr>
<tr>
<td><strong>CloudCheckr</strong></td>
<td>CloudCheckr is a multi-cloud management platform enabling enterprises and service providers to save money, reduce risk, and ensure governance at scale.</td>
</tr>
<tr>
<td><strong>Corent SurPaaS®</strong></td>
<td>SurPaaS® is a platform for migrating and operating applications. It has monitoring and metering features that collect usage data for the Azure infrastructure, and to examine the actual application transactional activity on a tenant basis in order to create customized tenant cost allocations and billing.</td>
</tr>
<tr>
<td><strong>SCALR</strong></td>
<td>Cost is affected by all other aspects of cloud usage, and cost control doesn’t stop with visibility. Gain insights you can turn into financial guardrails that encourage smart behavior.</td>
</tr>
<tr>
<td><strong>HANU Insight</strong></td>
<td>Hanu Insight is a Continuous Financial Governance product that provides end-to-end visibility of your Azure spend and optimizes your consumption to maximize your Azure investments.</td>
</tr>
</tbody>
</table>
Pre-purchasing

Making an up-front commitment to Azure can deliver significant cost savings. There are a variety of programs available to take advantage.

A move to the cloud is a shift in mindset with respect to purchasing technology. Traditionally, hardware and software are purchased upfront using capital expenditures with no ongoing commitment to the platforms chosen beyond support. With a migration to the cloud this relationship changes, due to the pay-as-you-go nature of the cloud. This means there are new strategies that you, as a cloud customer, must bring to the table both in terms of licensing and implementation. This guidance and optimal deployment of Azure features can make or break the success of a migration.

You will need to understand how the transition will impact your budget and existing investments. In addition, you will require input into strategies for saving on a long-term commitment to Azure as your cloud platform.

Pre-purchasing Azure is a great way to manage those costs and make the most out of every dollar that is spent on the platform. In this section, we’ll look at five pre-purchase or credit schemes which you can use to significantly reduce Azure spend.

**ENTERPRISE AGREEMENT (EA) WITH AZURE MONETARY COMMITMENT**

The Enterprise Agreement offers large customers the distinct benefit of having one contract to purchase all of their Microsoft products and services. Any Enterprise Agreement customer can add Azure to their agreement by making an upfront monetary commitment to Azure. This is essentially a dollar amount that the customer expects to spend on Azure over the course of each year during the EA. EAs do allow a customer to negotiate their rates based on their commitment to Microsoft which is one attractive reason for entering into this type of contract.

When an EA is signed, the customer will make an upfront payment to cover the cost of Azure for the first year. Each subsequent year another payment is made to Microsoft. That commitment is consumed throughout the year by using any combination of the wide variety of cloud services Azure offers from its global datacenters. Microsoft will also extend the same rates that were negotiated for services consumed beyond the commitment. This allows customers to use Azure even with this unplanned growth, so they can meet their organization’s needs. Enterprise Agreement customers can pay Microsoft at the end of the year for unplanned growth, as long as use is within certain thresholds. If the customer doesn’t use all the pre-purchased budget for the year it is forfeited and can’t be rolled over to the next year.

Azure can be added to an EA at any time, although the anniversary or expiration of an existing EA commitment is a great time to evaluate usage and future plans for the platform.

Azure, via the EA, also gives customers access to the Enterprise Portal, a great resource for customers managing multiple accounts or subscriptions. Subscriptions can be grouped into accounts, and accounts into departments. These departments can correspond to organizational departments or other groupings such as geographic location or application group. Settings budgets at the department level is a great way to gain visibility and accountability for Azure consumption across an organization. See the section on Azure Subscriptions for further information.

**SERVER AND CLOUD ENROLLMENT**

Server and Cloud Enrollment is an enrollment under the Microsoft Enterprise Agreement that enables customers to commit to one or more key server and cloud technologies from Microsoft. In exchange, they get the best pricing and terms, plus other benefits such as cloud-optimized licensing options and simplified license management.

The following are some of the benefits of Server and Cloud Enrollment:

**Best value**

- Get the best pricing, discounts, and added benefits designed to support server and cloud technologies.
• Best pricing and terms for server and cloud products, including discounts on new licenses and Software Assurance
• Full Software Assurance benefits for all deployed licenses, including new version rights
• Unlimited Problem Resolution Support for qualifying customers

Flexible
Move to the cloud as needed and grow organically without losing the value of your existing investments.

• Application license mobility to the cloud through Software Assurance
• New subscription-based licensing gives you more flexibility when you need to retire workloads, consolidate, or migrate to the cloud

Manageable
Adopt the latest technologies while simplifying deployment and license management.

• Simplified licensing management streamlines overall deployment and management
• Standardized terms, conditions, and discounts
• A standardized management platform across on-premises and Microsoft Azure comes with commitment to the Core Infrastructure Suite (CIS) in Server and Cloud Enrollment

The program is available to Government customers. To enroll, customers must make an installed-base commitment to one or more of the following four Server Cloud Enrollment components:

• **Core Infrastructure**: Windows Server and System Center
• **Application platform**: SQL Server, BizTalk Server, and SharePoint Server
• **Developer platform**: Visual Studio Enterprise
• **Microsoft Azure**: All Azure cloud services

This means committing to full Software Assurance coverage across the installed base of a Server and Cloud Enrollment component. For the Core Infrastructure component, however, customers can commit to full System Center coverage on the Windows Server installed base through the Core Infrastructure Suites (CIS). Microsoft Azure is automatically available when enrolling in any of the other three components, and it can also be licensed standalone.

**HYBRID BENEFIT**

When creating a Windows Server virtual machine in Azure there are two components that make up the cost per minute:

• **Base compute cost**: cost for the hardware of the VM, comprising the CPU, memory, and temp disk (OS and data disks are managed separately)
• **Windows OS license**: cost of the Windows operating system

If a customer already has Windows OS licenses with Software Assurance, then Microsoft extends a benefit which can help them save up to 40 percent on Windows Server VMs. This is known as the [Azure Hybrid Benefit for Windows Server](https://aka.ms/AzureGovPlaybook). This allows customers to use their on-premises Windows Server licenses with Software Assurance or Windows Server Subscriptions to save when migrating to Azure. With this benefit, for each license Microsoft will cover the cost of the OS, while the customer is only charged for the base compute costs (which are the same as the Linux VM costs).

The Azure Hybrid Benefit helps customers get more value from their Windows Server licenses for machines that are migrated to the cloud since the investment in that software isn’t lost.

Hybrid Benefit is also available for running SQL Server workloads in Azure. Existing SQL Server licenses with Software Assurance can be used to offset the license costs.
of either SQL Server running in Azure VMs, or the Azure SQL Database service.

Hybrid Benefit for Windows Server VMs

Customers can use the benefit with Windows Server Datacenter and Standard edition licenses covered with Software Assurance that they own. Depending on the edition, customers can convert or re-use their licenses to run Windows Server virtual machines in Azure and pay a lower base compute rate (Linux virtual machine rates).

Each 2-processor license or each set of 16-core licenses are entitled to two instances of up to 8 cores, or one instance of up to 16 cores. Customers can also use multiple licenses to cover licensing for a large VM in Azure. For example, a virtual machine with more than 16 cores can be covered with HUB by "stacking licenses". With two 2-processor licenses or two 16-core licenses, the customer would have the HUB to cover the OS license for a VM up to 32 cores. There is a 90-day assignment rule for Windows Server, which requires licenses to stay assigned to the same hardware for a minimum of 90 days and this rule does apply to Azure virtual machines.

For every 2-processor Windows Server license or Windows Server license with 16-cores covered with Software Assurance, you will receive either of the following:

- Up to two virtual machines with up to 8 cores, or
- One virtual machine with up to 16 cores

There are a few differences on how the HUB can be used based on the type of license that you customer owns:

- **Standard Edition Licenses** can only be used once either on-premises or in Azure. Once you assign the Azure Hybrid Benefit to Azure you cannot use the Standard Edition license on-premises again.
- **Datacenter Edition Licenses** allow simultaneous, indefinite usage both on-premises and in Azure.

Hybrid Benefit for SQL Workloads

Azure Hybrid Benefit for SQL Server can be used with both SQL Server Enterprise Core and SQL Server Standard Core licenses. In both cases, Software Assurance is required.

For SQL Server running in Azure VMs, these licenses transfer directly to Azure, core-for-core. That is each Enterprise Core license qualifies you for one core of SQL Server Enterprise Core in Azure VMs, and similarly for Standard Core licenses. In both cases, you must allocate a minimum of four core licenses per VM.

With Azure SQL Database, the licensing is a little more complicated. The SQL Database can use any of the Managed Instance, Elastic Pool or Single Database deployment models. However, the database must use the vCore pricing model, not the DTU-based pricing model.

Each SQL Server license provides the following Azure SQL Database license rights:

- **SQL Server Enterprise Edition**: 1 core on-premises license entitles you to either 1 core at the Business-Critical tier, or 4 cores at the General-Purpose tier.
- **SQL Server Standard Edition**: 1 core on-premises license entitles you to 1 core at the General-Purpose tier only.

Each license can only be used either on-premises or in the cloud. However, there is a 180-day grace period during which you can use the same license both on-premises and in the cloud, to facilitate migration.

Deployment Options

For Windows Server, there are several ways you can deploy your VMs to take advantage of Hybrid Benefit pricing:

- You can deploy Windows Server virtual machines pre-configured with the Azure Hybrid Benefit straight from the Azure Portal, using ARM Templates, PowerShell, or the Azure CLI. Windows Server Datacenter Azure Platform images are made available via in the Azure Marketplace. There are no Windows Server Standard images in Azure, so Microsoft allows Windows Standard licenses to be used with the Windows Datacenter Azure Platform images at no additional cost.
- Another option is to upload OS images to the customer’s subscription and use these as the basis for your deployments. These images should be generalized to ensure that they don’t have issues as duplicates in the environment. Windows VMs should have the sysprep tool run on them using the Out of Box Experience. The image should then be uploaded to Azure Storage and then made into a Managed Image. For more information on how to use PowerShell to complete this for your customer view this article on uploading on-premises VMs. All VMs created using this image will be charged at the base
compute rate and the OS licensing will be covered under the Hybrid Benefit scheme.

- Another option is to upload a current Windows Server virtual machine disk (VHD) to Azure and create an Azure VM using this disk. You can upload the VHD using PowerShell cmdlets, but only after the VM has been prepped for Azure. The process to prepare a VM to upload to Azure can be reviewed in this article on preparing a Windows VHD or VHDX to upload to Azure. Once this VM is up and running in Azure it will be charged at the base compute rate and the OS licensing will be covered under the Hybrid Benefit scheme.

- Another option is to migrate an existing workload to Azure using Azure Site Recovery. Once migrated, the virtual machine in Azure will be running as a custom image and thus will be charged at the base compute rate and the OS licensing will be covered under the Hybrid Benefit scheme.

AZURE RESERVATIONS

Another way to save on Azure costs is through pre-purchasing compute capacity using Azure Reservations. Azure Reservations are available for Azure Virtual Machines, Azure SQL Database, Azure Cosmos DB and Azure SQL Data Warehouse.

Azure VM Reserved Instances

Reservations for Azure VMs are called Azure Virtual Machine Reserved Instances. Customers can reserve virtual machines in advance and enjoy cost savings of up to 72% on pay-as-you-go prices. When combining the cost savings gained from Azure Reserved Instances with the added value of the Azure Hybrid Benefit, customers can save up to 80 percent on their Windows workloads.

Reserved VM Instances provide price predictability, as well as the flexibility to exchange or cancel to get pro-rated refund, should their needs change. Discounts for Reserved Instances are determined based on the customers commitment to a one-year or three-year term on Windows and Linux virtual machines (VMs). Reserved Instances also help customers improve their budgeting and forecasting with a single upfront payment, making it easy to understand their investment and avoiding unexpected overages.

You can lower your total cost of ownership by combining Reserved Instances with On-Demand instances to manage costs across predictable and variable workloads. In customer environments, there will be different types of systems, some of which have known requirements for their VMs. An example of a system with known requirements would be an SAP implementation where the exact specifications for the VMs are locked and are not expected to change during the next three years. This is a great example of how Reserved Instances could be used to maximize the savings. In this same environment, you could have a public e-commerce web application that has variable needs and leverages the ability to scale out and scale in based on the number of visitors on the website. This workload would be best suited to the on-demand pricing leveraging standard the pay-as-you-go model.
Reserved Instance Purchasing and Billing

Reserved Instances are purchased in one-year or three-year terms with a single upfront payment. Purchasing can be completed very easily using the Azure portal in three steps:

- Specify the Azure region
- Select the Virtual Machine type
- Chose a term (one year or three years)

For Enterprise Agreement (EA) customers, Azure Monetary Commitment can be used to purchase Azure Reserved VM Instances. In scenarios where EA customers have used up their monetary commitment, Reserved Instances can still be purchased, and those purchases will be invoiced on their next overage bill. Reserved Instances can be assigned at the enrollment or subscription level, so you can manage Reserved Instance usage at an organizational or individual department level. Assignments are easy to change post-purchase.

For customers purchasing via Azure.com, at the time of purchase, the credit card on file will be charged for the full upfront payment of the Azure Reserved Instances. To see Reserved Instance purchase details, use the Azure portal and select the Reservations menu on the left side of the Azure Portal to view all Reserved Instances associated with the account. All Reserved Instances will be displayed on the right.

The Reserved Instance will apply immediately to any existing running VMs that match the one-year or three-year terms of the Reserved Instance, depending on if you scope the Reserved Instance to a specific subscription or apply it at the enrollment level. In both cases, the period of the Reserved Instance starts immediately after purchasing.

The Reserved Instance purchase can be assigned to a subscription or enrollment and can be changed as necessary.

Assignment allows you to decide whether the reservation is applied at the Azure account/enrollment or at the subscription level. This provides flexibility for how to leverage the savings. For example, to simply buy reservations to save money for the entire customers organization, you can assign all reservations to the account level. If the customers wishes to apply the Reserved Instance savings to a particular business unit, such as finance, you could provision a subscription for that department and then assign the Reserved Instance to their subscription. Then only they would be able to take advantage of the Reserved Instance commitment savings.

Azure Reserved Instances provide a single price for each VM size in a region. There is no requirement to choose Windows or Linux VMs for the Reserved Instance purchase. If Windows Server VM is selected, there is an option to use the Azure Hybrid Benefit or pay the Windows Server rate.

There are two options for adding Windows Server licenses to an Azure Reserved VM Instance. The first option is to use your Azure Hybrid Benefit. If you have Windows Server with Software Assurance on-premises, you can assign these licenses to the Azure Reserved Instance. The second option is to add Windows Server using the Windows Server hourly meter. If you cannot take advantage of the Azure Hybrid Benefit, Windows Server will be charged when the VM is active, based on the number of cores the VM is using.

Availability of Reserved Instances

Azure Reserved Instances are available for all VM families other than A-series, A_v2 series, or G-series, or any VM series in Preview. Microsoft does offer to exchange Reserved Instances to a different region or VM family, but there is no guaranteed availability of capacity in a given region or VM family.

Reserved Capacity for Database Workloads

Azure reservations are also available for Azure SQL Database, Azure Cosmos DB, and Azure SQL Data Warehouse. This is known as Reserved Capacity.

As with Reserved Instances for Azure VMs, Reserved Capacity is based on a one-year or three-year pre-purchase. The reservation is purchased separately from the service, and service billing is discounted against matching reservations.

For each service, the reservation is purchased in the following units:

- For Azure SQL Database, each reservation specifies the number of vCores (minimum 8 vCores)
• For Cosmos DB, each reservation specifies the capacity as a number of Request Units per Second (minimum 20,000 RU/S)
• For Azure SQL Data Warehouse, each reservation specifies the number of Data Warehouse Units (cDWU), in multiples of 100.

As with Azure VM Reserved Instances, each reservation must specify the Azure region and whether it is scoped to a single subscription or shared across subscriptions in an EA or account.

**Exchanges and Cancellations**

Azure reservations for both VMs and databases require making upfront commitments on compute capacity, but Microsoft allows for flexibility should the customer’s business needs change. An exchange allows the customer to receive a prorated refund based on the unused amount which applies fully to the new purchase price. A cancellation terminates the contract and Microsoft will provide a prorated refund based on unused amount minus early termination fee of 12 percent. Customers can cancel a reservation at any time (up to $50,000 per year).

**DEV/TEST PRICING**

Microsoft provides discounted rates on Azure for ongoing development and testing needs. These benefits include:

• No Microsoft software charges on Virtual Machines
• Significant dev/test pricing discounts on a variety of other Azure services
• Exclusive access to Windows 10 Virtual Machines

There are also Dev/Test pricing discounts on the services that these teams consume in Azure, including significant discounts on VMs, SQL VMs, Azure App Service, HD Insight amongst others.

There are two methods for customers to receive these benefits and discounts, and it is based on the type of client that you are working with on their Dev/Test workload in Azure.

**Small Development Teams**

Small teams are best suited to leverage Visual Studio subscriptions which include benefits for Azure. Each subscription includes a monthly Azure credit which is dependent upon the level of the subscription and ranges from $50 to $150 (full details at Azure credits for Visual Studio subscribers).

The monthly Azure credit for Visual Studio subscribers is ideal for experimenting with and learning about Azure services. When you activate this benefit, it creates a separate Azure subscription with a monthly credit balance that renews each month while you remain an active Visual Studio subscriber. Any overage above the credit would be billed to a credit card that the developer would put in file with Microsoft. If no credit card is on file, then Azure services are suspended if the credit balance is exceeded.

**Large Development Teams**

Development and Test subscriptions for large teams are purchased via an EA and require that each user be an active Visual Studio Online subscriber. Unlike the small team these do not include a credit each month, but instead are eligible for the discounted rates on Azure services. This is a significant benefit due to the nature of how these teams work on their projects. For example, if a group of developers were writing code that requires SQL Server Enterprise Edition, they won’t be charged for that software running on their development VMs. Only the production SQL Server would have this charge—which is a very large savings over time.
Automatic Shutdown of VMs

One of the most attractive attributes of the cloud is the pay-as-you-go nature of the services. Take full advantage by only using resources when you need them.

In many environments, there are times of day when certain services aren’t needed and thus there is no reason for them to be running. This is particularly true of Azure Virtual Machines, which can be shut down and later re-started with no loss of data.

Non-production cloud servers need to be online only when employees are actively working on them. In some cases, non-production environments can be turned off, or de-allocated, over 70 percent of the time, which translates into a direct 70 percent cost reduction.

It’s important to understand the requirements placed on each virtual machine that will be deployed. Understanding which virtual machines only provide useful service during certain hours of a workday or even days of the week is critical to maximizing your potential savings. This could also change over time as the application evolves or as new workloads are onboarded to the cloud.

It’s important to understand that there are two ways to stop a virtual machine:

- Shutting down the virtual machine from within the virtual machine OS puts the virtual machine into the ‘Stopped (allocated)’ state. In this state, the underlying infrastructure (CPU, memory) is still reserved for the virtual machine, and hence the virtual machine is still billed
- Stopping the virtual machine from the Azure portal or other Azure tools (PowerShell, CLI, etc.) puts the virtual machine into the ‘Stopped (deallocated)’ state. The virtual machine is no longer billed, resulting in significant potential savings (although other resources such as VM disks associated with the VM may still be charged)

A stopped virtual machine can be re-started at any time and will continue where it left off since its disks have not been affected. Note that if the virtual machine is associated with a Public IP Address, then stopping and re-starting the virtual machine may result in a new Public IP Address being allocated. To preserve the same Public IP Address, a static Public IP Address should be used.

Azure supports several ways to implement automatic shut-down of virtual machines. We’ll now look at each in turn.

**AUTO SHUT DOWN OF VMS**

Automatic shut-down of virtual machines is one of the ways that Microsoft helps customer to optimize their costs, by automatically shutting down a virtual machine at a given time.

This feature was originally introduced as a feature of DevTest Labs and was widely adopted used by customers. Because of this success, auto shut down was added to all Azure Resource Manager virtual machines.

Customers can schedule a time each day (local time is supported) when a VM will be stopped. At this time, the virtual machine is stopped and deallocated, and Microsoft stops billing the subscription for the compute time until it is re-started.

Auto shutdown is available via the Azure portal. This method is simple to use for individual virtual machines.
and can be configured while the virtual machine is being provisioned or after it has been created. The settings configured include the local time zone, the time to shut down and the option to notify the shut-down 15 minutes in advance, via email.

It is also possible to set the auto shut-down settings when deploying virtual machines by other methods, such as Azure Resource Manager templates. To do so, you need to create a separate resource of type Microsoft.DevTestLabs/schedules, specifying the target virtual machine and auto shut-down settings. This configuration will have the same result as configuring the Auto Shutdown in the portal during the provisioning of a virtual machine and is how the portal configures them behind the scenes. The configurations can later be changed using the portal just as if they were provisioned there.

It is important to note that the auto shut-down feature has no corresponding auto start-up, so the virtual machines will need to be started manually. As an alternative, consider using one of the other approaches to auto shutdown described below.

POWERSHELL VIA AZURE AUTOMATION RUNBOOKS

It is also possible to automatically shut down and restart Azure virtual machines using a ‘runbook’ executed using Azure Automation. This is different than the Auto shutdown feature using the Microsoft.DevTestLabs resource provider. This is fully dependent upon the partner or customer to configure and leverages the Azure PowerShell cmdlets. For a packaged solution, see the next option, ‘Start/stop VMs during off hours.’

START/STOP VMS DURING OFF-HOURS

There is an Azure Marketplace solution known as ‘Start/stop VMs during off-hours’. You can find this solution by clicking ‘+ Create a resource’ in the Azure portal, then entering ‘start stop vms’ in the search field.

This solution allows you to start and stop Azure Virtual Machines automatically, using a schedule or based on utilization. Solution relies on two Azure services and a SendGrid service:

- **Automation**: starts and stops your virtual machines.
- **Log Analytics**: visualizes the successful start and stop of your machines.
- **SendGrid**: sends email notifications of stop and start activities.

This solution is more complex, but more robust in that it is a full strategy for achieving auto start and stop for an entire subscription rather than targeting individual virtual machines. For further information, see the [start/stop VMs during off hours documentation page](#).
Monitoring and Alerting

Effective monitoring is a critical component of any service. Azure provides a broad range of features to enable effective monitoring of cloud workloads.

An effective monitoring strategy helps you understand the detailed operation of the components of your applications. It also helps you increase your uptime by proactively notifying you of critical issues so that you can resolve them before they become problems.

Azure includes multiple services that individually perform a specific role or task in the monitoring space. Together, these services deliver a comprehensive solution for collecting, analyzing, and acting on telemetry from your application and the Azure resources that support them. They can also work to monitor critical on-premises resources in order to provide a hybrid monitoring environment. Understanding the tools and data that are available is the first step in developing a complete monitoring strategy for your application.

Many of the monitoring tools in Azure are integrated, offering you a suite of shared capabilities such as alerts, dashboards, and metrics aggregation along with specific solutions for deep infrastructure and application monitoring.

In this section, we will first review some fundamental monitoring concepts, then describe the tools available in Azure to implement effective monitoring.

Azure Monitoring Concepts

AZURE SERVICE AND RESOURCE MONITORING

In Azure, your monitoring and metrics are often available at multiple levels, including the service and resource level. For instance, your virtual machines will rely on multiple Azure services like storage and networking.

The health of the platform services will need to be monitored for overall platform health and proactive maintenance notices while the health and metric of deployed resources (e.g., the storage account your virtual machine VHD is stored in) will also need to be monitored to understand resource health and perform reactive alerting.

Consider that you are responsible for monitoring your own Azure resources and developing a strategy for coverage of proactive and reactive alerting. For example, if you host a database in an IaaS server like Microsoft SQL Server, you will want to proactively monitor the CPU consumption of the server itself and generate reactive alerts when that CPU consumption passes a threshold, so your operations staff and database administrators can address any issues before they affect users.

APPLICATION MONITORING

You must also consider that the applications and workloads you deploy will also have application level audit and event logs. This means your strategy must account for not only the Azure platform and resource level health, but also for the application level audit logs and their potential ingestion into a centralized logging service such as Log Analytics.

SECURITY MONITORING

The deployment of virtual machines will bring with it the baseline monitoring you perform today. However, the logging plane and tooling will most likely change or be augmented with cloud-friendly monitoring tools.

For your Windows and Linux virtual machines, you will need to monitor your operating system event logs, including security logs, administrative logs, antimalware, and service specific logs. In addition to monitoring, you should be mindful of maintaining compliance by performing regular vulnerability scanning and watching for configuration drift where possible.

To improve your security posture and make monitoring easier, you can leverage native gallery images when you deploy your virtual machines which are consistently updated with the latest security patches and bug fixes. You can also use these images to develop your own baselines, adopting services such as Azure Automation and Desired State Configuration (DSC) to perform configuration management as we discussed earlier.
helping to maintain your baseline and prevent configuration drift.

**Azure Monitoring Tools**

**ALERTS**

*Azure alerts* proactively notify you of critical conditions and potentially take corrective action. Alert rules can use data from multiple sources, including metrics and logs. They use action groups, which contain unique sets of recipients and actions in response to an alert. Based on your requirements, you can have alerts start external actions by using webhooks and integrate with your ITSM tools.

**METRICS EXPLORER**

*Metrics* are numerical values generated by an Azure resource to help you understand the operation and performance of the resource. By using Metrics Explorer, you can send metrics to Log Analytics for analysis with data from other sources.

**DASHBOARDS**

You can use *Azure dashboards* to combine different kinds of data into a single pane in the Azure portal. You can then share the dashboard with other Azure users.

For example, you can create a dashboard that combines:

- Tiles that show a graph of metrics
- A table of activity logs
- A usage chart from Application Insights
- The output of a log search in Log Analytics

You can also export Log Analytics data to *Power BI*. There, you can take advantage of additional visualizations. You can also make the data available to others within and outside your organization.

**AZURE MONITOR**

*Azure Monitor* enables core monitoring for Azure services by allowing the collection of metrics, activity logs, and diagnostic logs. For example, the activity log tells you when new resources are created or modified.

Metrics are available that provide performance statistics for different resources and even the operating system inside a virtual machine. You can view this data with one of the explorers in the Azure portal and create alerts based on these metrics. Azure Monitor provides the fastest metrics pipeline (5 minutes down to 1 minute), so you should use it for time critical alerts and notifications.

You can also send these metrics and logs to Azure Log Analytics for trending and detailed analysis or create additional alert rules to proactively notify you of critical issues as a result of that analysis.

**AZURE ADVISOR**

*Azure Advisor* constantly monitors your resource configuration and usage telemetry. It then gives you personalized recommendations based on best practices. Following these recommendations helps you improve the performance, security, and availability of the resources that support your applications.

**SERVICE HEALTH**

The health of your application relies on the Azure services that it depends on. *Azure Service Health* identifies any issues with Azure services that might affect your application. Service Health also helps you plan for scheduled maintenance.

**ACTIVITY LOG**

Activity Log provides data about the operation of an Azure resource. This information includes:

- Configuration changes to the resource.
- Service health incidents.
- Recommendations on better utilizing the resource.
- Information related to autoscale operations.

You can view logs for a particular resource on its page in the Azure portal. Or you can view logs from multiple resources in Activity Log Explorer.

You can also send activity log entries to Log Analytics. There, you can analyze the logs by using data collected by management solutions, agents on virtual machines, and other sources.

**APPLICATION INSIGHTS**

You can use *Azure Application Insights* to monitor availability, performance, and usage of your application, whether it’s hosted in the cloud or on-premises.
By instrumenting your application to work with Application Insights, you can achieve deep insights and implement DevOps scenarios. You can quickly identify and diagnose errors without waiting for a user to report them. With the information that you collect, you can make informed choices on your application’s maintenance and improvements.

Application Insights has extensive tools for interacting with the data that it collects. Application Insights stores its data in a common repository. It can take advantage of shared functionality such as alerts, dashboards, and deep analysis with the Log Analytics query language.

**LOG ANALYTICS WORKSPACES**

Log Analytics workspaces play a central role in Azure monitoring by collecting data from a variety of resources (including non-Microsoft tools) into a single repository. There, you can analyze the data by using a powerful query language.

Application Insights and Azure Security Center store their data in the Log Analytics data store and use its analytics engine. Data is also collected from Azure Monitor, management solutions, and agents installed on virtual machines in the cloud or on-premises. This shared functionality helps you form a complete picture of your environment.

**NETWORK MONITORING**

There are several tools that work together to monitor various aspects of your network, whether in Azure or on-premises.

- **Network Watcher** provides scenario-based monitoring and diagnostics for different network scenarios in Azure. It stores data in Azure metrics and diagnostics for further analysis. It works with the following solutions for monitoring various aspects of your network.

- **Network Performance Monitor (NPM)** is a cloud-based network monitoring solution that monitors connectivity across public clouds, datacenters, and on-premises environments. Check for availability in Azure Government.

- **ExpressRoute Monitor** is an NPM capability that monitors the end-to-end connectivity and performance over Azure ExpressRoute circuits.

- **DNS Analytics** is a solution that provides security, performance, and operations-related insights, based on your DNS servers.

- **Service Endpoint Monitor** tests the reachability of applications and detects performance bottlenecks across on-premises, carrier networks, and cloud/private data centers.

**SERVICE MAP**

Service Map provides insight into your IaaS environment by analyzing virtual machines with their different processes and dependencies on other computers and external processes. It integrates events, performance data, and management solutions in Log Analytics. You can then view this data in the context of each computer and its relation to the rest of your environment.

Service Map is similar to Application Map in Application Insights. It focuses on the infrastructure components that support your applications.
Optimized Architecture

Your choice of application architecture can have a significant impact on running costs. Incorporating cost as a design goal can result in significant savings.

A common problem that affects organizations when they initially move resources into the cloud is their virtualization strategy. They often use an approach like the one used when creating virtual machines for the on-premises virtualization environment. And, they assume that costs are reduced by moving their on-premises VMs to the cloud, without any thought to changing how it is deployed and the resources (CPU & RAM), that are assigned. However, this approach is not likely to reduce costs.

The problem with this approach is that the existing on-premises infrastructure was already paid for. Users could create and keep large VMs running if they liked—idle or not and with little consequence. Moving large or idle VMs to the cloud is likely to increase costs. Cost allocation for resources is important when customers enter into agreements with cloud service providers.

Using the features of Azure with a new mindset is required to gain efficiencies from the cloud, and not end up with additional costs by moving. There are features in Azure which allow for autoscaling of compute infrastructures and thus when coupled with the Pay as you Go model can provide for the savings customers desire. These strategies often have the added benefit of high-availability given that they scale the compute out and in instead of up and down. This means more nodes provide the service rather than one larger node providing the service.

Moving to a PaaS platform for services is also a common strategy to change the architecture of a service and gain cost savings. Web applications that were traditionally running on VMs in a customer’s datacenter can now be moved to the Azure App Service and will run just as today, but with much less overhead in terms of cost and management responsibility.

In this section, we'll discuss the following approaches to optimizing your application architecture to reduce costs:

AZURE PAAS SERVICES OVER IAAAS

PaaS over IaaS is the default stance that customers and partners should take as a best first approach.

IaaS deployments require almost the same amount of effort as deploying and managing VMs in a customer datacenter without the hardware and facilities cost and complexity. The cloud computing service provider manages the infrastructure, while customers must purchase, install, configure, and manage their own software, operating systems, middleware, and applications. IaaS does provide the advantages of no upfront capital commitment and the customer needs to rent a VM for as long as it is needed.

aka.ms/AzureGovPlaybook
PaaS is a complete development and deployment environment in the cloud, with resources that enable customers to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled services.

Like IaaS, PaaS includes infrastructure—servers, storage, and networking, but also middleware, development tools, business intelligence (BI) services, database management systems, and more. PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating.

PaaS allows you to avoid the expense and complexity of buying and managing software licenses, the underlying application infrastructure and middleware or the development tools and other resources. You operate and manage the applications and services, while Azure manages everything else.

A common strategy for cloud adoption is to take a ‘PaaS-first’ approach. This means that where possible, a Platform-as-a-Service architecture should be used, only backing away to an IaaS deployment if there are specific reason(s) why the deployment can’t leverage a PaaS service.

There are times when a complete PaaS offering might not make sense, but you should use a cloud mindset when evaluating these circumstances. For example, if a web server must remain on a VM in Azure IaaS the question should be asked: “Can the images and data files that are downloaded to the client be offloaded from the VM to Azure Storage?” Azure Storage is a HTTP web server at scale that can easily host all of the applications images, PDFs or other binary files that will be sent to the clients while the app is in use. A simple change to the HTML code of the app to reference a different URL for these files and the application is now leveraging a PaaS service. In the customer’s datacenter those downloads would be left to the VM, but with Azure Storage all the files could be placed on that service which would free up the burden of loading these files from the VM to the client. This could mean a difference in the size of the VM and thus reduce the bill each month for that application.

**AUTO SCALE VM SCALE SETS & AZURE WEB APPS**

Auto-scale is a built-in feature of many Azure services to meet the changing needs of applications. Typically, these are in the form of websites with fluctuating compute requirements based on network traffic. When autoscaling Azure will add more nodes to service the application and then remove nodes when the traffic spike diminishes. This is known as scaling-out and scaling-in to meet the performance demands. Of course, performance means different things for different applications. Some apps are CPU-bound, others memory-bound. For example, a web app that handles millions of requests during the day and relatively few at night. Auto-scale can scale a service by any of these or via a custom metric defined by the customer or partner.

Be proactive and build autoscaling into your migrations. It’s not wise to wait for a traffic spike to take down your app or site and scale the VM size to meet the demand. With scheduled auto-scale, you can respond before anything ever happens. If a scheduled event means you know a spike in traffic is coming, simply using auto-scale to add 10x more virtual machines in advance to handle the load. Another example would be for a website that traffic always skyrockets at 9 a.m. Monday through Friday. This can be handled with an autoscaling rule that triggers a scale out during those hours, but contracts during the offer hours. By using this simple approach to better understand the application, you are ensuring a high level of service quality in an optimized manner.

**Azure App Service** is a great example of using a PaaS service that can auto-scale. This service is used for hosting web applications, REST APIs, and mobile back ends. It supports by Windows and Linux along with many programming languages including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python.
Web Apps not only adds the power of Microsoft Azure to the application, such as security, load balancing, autoscaling, and automated management. It also has DevOps capabilities without the need to provision and build other VMs or services. These capabilities include continuous deployment from Azure DevOps, GitHub, Docker Hub, and other sources, package management, staging environments, custom domain, and SSL certificates.

With App Service, the customer pays for the Azure compute resources they use. The compute resources used is determined by the App Service plan that is implemented during the migration. Keep in mind that as the provider you need to give guidance on the size of the App Service plan just as you would for VM sizes. Each size and type of App Service place provides different capabilities from the number of cores and RAM to storage space and ability to host custom domain names for their site.

For deployments that require an IaaS deployment, but also need the ability to auto-scale partners will need to leverage Virtual Machine Scale Sets (VMSS). VMSS is an Azure compute resource that can be used to deploy and manage a set of identical VMs. With all VMs configured the same, scale sets are designed to support true auto-scale, and no pre-provisioning of VMs is required. So, it’s easier to build large-scale services that target big compute, big data, and containerized workloads.

VMSS should be used for applications that need to scale compute resources out and in, and are highly available given that they are deployed behind the Azure load balancer and balanced across fault and update domains.

The VMs that are part of the VMSS can be configured using the VM Custom Script extension, via Azure Automation Desired State Configuration (DSC) or other VM exertions such as CHEF or Puppet. By using automation to configure the application on the VMs that are created by the VMSS there is no need for the administrator to take any actions during a scaling event. The required VMs will be created by the autoscaling rule and then we then boot for the first time they will be configured with the application.

**REGION PRICING DIFFERENCES**

With 54 announced regions, more than any other cloud provider, Azure makes it easy to choose the datacenter and regions that’s right for you and your customers. Within each of these regions there are services that are made available and each have a cost associated with them.

With that in mind, it is important to understand that there are two variables to these services:

- **Availability**: not all services are available in every region
- **Cost**: service costs vary by Azure Region

**Availability** of services is based entirely on when Microsoft provides the service to a region. For example, there are many different Virtual Machine families in Azure which are named using letters from the alphabet such as A, B, D, M amongst others. These VM types aren’t always available in every region when they are released by Microsoft. Some VM types are available in many regions while others are only available in a few. The D series of VMs is an example of almost full coverage across all of Azure. This contrasts with the M series VMs which are only available in selected regions. There are also availability differences between the Azure public cloud and the Azure Government cloud.

**Cost** is of course an important factor in any project, and Azure migrations are no exception. Each of these regions has their own price list and these prices do fluctuate over time. In some cases, the cost difference between a service in one region as compared to another may be relatively insignificant. In other cases, it can become a critical concern.
Using the Azure Calculator, you can see the standard pricing by region for a VM (not all regions are supported in the calculator).

For more information on pricing see the Azure Price FAQ.

**AZURE SQL DATABASE ELASTIC POOLS**

Azure SQL Database elastic pools help customers manage and scale multiple Azure SQL databases. SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands. The databases in an elastic pool are on a single Azure SQL Database server and share a set number of resources (elastic Database Transaction Units (eDTUs) at a set price. Elastic pools in Azure SQL Database enable SaaS developers to optimize the price performance for a group of databases within a prescribed budget while delivering performance elasticity for each database.

Pools are well suited for many databases with specific utilization patterns. For a given database, this pattern is characterized by low average utilization with relatively infrequent utilization spikes.

The more databases you can add to a pool the greater your savings become. Depending on your application utilization pattern, it is possible to see savings with as few as two S3 tier databases.

Elastic Pools automatically scale performance and storage capacity for elastic databases on the fly. You can control the performance assigned to a pool, add or remove elastic databases on demand, and define performance of elastic databases without affecting the overall cost of the pool.

There are built-in sizing recommendations that proactively identify databases which would benefit from pools and allow "what-if" analysis for quick optimization to meet your performance goals. Rich performance monitoring and troubleshooting dashboards help you visualize historical pool utilization.

There are three different performance and pricing tiers: Basic, Standard, and Premium. Each of these pools offer a broad spectrum of performance, storage, and pricing options. Pools can contain up to 400 elastic databases. Elastic databases can auto-scale up to 1,000 elastic database transaction units (eDTUs).

**AZURE BLOB STORAGE (HOT, COLD & ARCHIVE)**

Azure Blob Storage is a Microsoft-managed cloud service providing storage that is highly available, secure, durable, scalable, and redundant. Microsoft takes care of maintenance and handles critical problems that may arise.

Azure Blob Storage is a service for storing large amounts of unstructured object data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data
publicly to the world, or to store application data privately. Common uses for Azure Blob Storage include:

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

Azure storage offers three Access Tiers for Blob object storage. This enables customers to choose the most cost-effective storage option, depending on usage patterns.

Access Tiers for Blob object storage:

- **Hot**: optimized for storing data accessed frequently
- **Cold**: optimized for storing data that is infrequently accessed and stored for at least 30 days
- **Archive**: optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours)

Data stored in the cloud is growing at an exponential pace. To manage costs for your expanding storage needs, it’s helpful to organize your data based on attributes like frequency-of-access and planned retention period to optimize costs. Data stored in the cloud can be different in terms of how it is generated, processed, and accessed over its lifetime. Some data is actively accessed and modified throughout its lifetime. Some data is accessed frequently and modified over its lifetime. Some data is accessed frequently early in its lifetime, with access dropping drastically as the data ages. Some data remains idle in the cloud and is rarely, if ever, accessed once stored.

Each of these data access scenarios benefits from a different storage tier that is optimized for an access pattern. With hot, cool, and archive storage tiers, Azure Blob storage addresses this need for differentiated storage tiers with separate pricing models.

**Hot**

Hot storage has higher storage costs than cool and archive storage, but the lowest access costs.

Example usage scenarios for the hot storage tier include:

- Data that is in active use or expected to be accessed (read from and written to) frequently
- Data that is staged for processing and eventual migration to the cool storage tier

**Cool**

Cool storage tier has lower storage costs and higher access costs compared to hot storage; and is intended for data that will remain in the cool tier for at least 30 days.

Example usage scenarios for the cool storage tier include:

- Short-term backup and disaster recovery datasets
- Older media content not viewed frequently but is expected to be available immediately when accessed
- Large data sets that need to be stored cost effectively while more data is being gathered for future processing. (*For example*, long-term storage of scientific data, raw telemetry data from a manufacturing facility)

**Archive**

Archive storage has the lowest storage cost and higher data retrieval costs compared to hot and cool storage. This tier is intended for data that can tolerate several hours of retrieval latency and will remain in the archive tier for at least 180 days.

While a blob is in archive storage, it is offline and cannot be read (except the metadata, which is online and available), copied, overwritten, or modified. Nor can you take snapshots of a blob in archive storage. However, you may use existing operations to delete, list, get blob properties/metadata, or change the tier of your blob.

Example scenarios for the archive storage tier include:

- Long-term backup, archival, and disaster recovery datasets
- Original (raw) data that must be preserved, even after it has been processed into final usable form. (*For example*, Raw media files after transcoding into other formats)
- Compliance and archival data that needs to be stored for a long time and is hardly ever accessed. (*For example*, Security camera footage, old X-Rays/MRIs for healthcare organizations, audio recordings, and transcripts of customer calls for financial services)

To read data in archive storage, you must first change the tier of the blob to hot or cool. This process is known as rehydration and can take up to 15 hours to complete. Large blob sizes are strongly recommended for optimal performance.
Azure Management Best Practices

There are a range of best practices that should be adhered to when migrating or operating any workload in Azure. Following these established patterns helps avoid common pitfalls and makes it easier to maintain your deployments in the long term.

Often, new Azure deployments start off as an experiment from a learning exercise or a proof of concept that was converted into a production workload. When these ad-hoc type deployments occur, it is easy to get started on the wrong foot and implement anti-patterns accidentally.

In the following sections we’ll review several key strategies that can kick your migration projects off on the right foot and avoid future problems.

First, we’ll take a detailed look at Azure subscriptions. Avoiding subscription bloat while enforcing clear management and security boundaries requires a subscription management strategy. We’ll review several different models for subscription management.

Next, we’ll consider how resources are organized and named within each subscription. Resources are organized using resource groups, and the correct resource grouping as a large impact on how the resources are deployed and managed. Resource naming, and the use of naming conventions, is also important to promote consistency and reduce human error during resource management operations.

Organizing resources at deployment is just the start. It’s also important to consider how resources will be managed throughout their lifecycle. Accidentally deleting a production resource can create a catastrophic application outage. It’s also important to control resource creation, if you are to control costs. With this in mind, we’ll review the technologies in Azure that enable you to control the resource lifecycle.

Finally, we’ll consider security and compliance, and provide links to valuable resources provided by Microsoft that can help you ensure your deployments are secure and meet any applicable government regulations.
Azure Subscriptions

An Azure subscription is the most fundamental entity used to organize Azure resources.

Before you can use Azure, you need an Azure subscription. The subscription is the boundary for several independent Azure concepts:

- **Security boundary** - each subscription forms an administrative security boundary. A subscription administrator has full control over resources within that subscription and controls the subsequent configuration of role-based access control and policies within the subscription. Where controls must be applied to more than one subscription, they must be applied to each subscription independently—there is no control mechanism that spans subscriptions.

- **Service limits** - The subscription is the boundary at which many of the Azure Service Limits are applied. Resource utilization forecasts need to be made at the subscription level to ensure they stay within these limits. For further details on Azure subscription limits, see https://docs.microsoft.com/azure/azure-subscription-service-limits

- **Billing** - the subscription forms the billing boundary. All Azure resources within a subscription are billed at the subscription scope. Different billing schemes (such as pay-as-you-go, CSP, or Enterprise Agreement) are applied at the subscription level.

With these points in mind, you need to choose how to organize resources across subscriptions. A common model is to use a separate subscription for each application, and to use separate subscriptions for production vs non-production deployments. A single subscription can contain more than one non-production deployment, in separate resource groups. Keep the subscription model simple, whilst retaining essential flexibility.

**MANGEMENT GROUPS**

Organizations typically manage multiple subscriptions. For example, different applications are typically deployed to separate subscriptions. Similarly, different environments, such as development, staging, and production, are often separated by using separate subscriptions. In addition, developers often have individual subscriptions for experimentation and learning.

Each subscription requires appropriate governance. This governance includes role-based access controls for team members, control over how each subscription is used (for example, the size and type of VM that can be created), and cost management.

A large organization may have hundreds of subscriptions. Applying and managing governance controls consistently and at scale across multiple subscriptions can require significant effort.

Management Groups are an Azure feature designed to help address this challenge. Management Groups allow you to group subscriptions into a hierarchy. Governance controls can be applied to nodes in the hierarchy in a single operation, and flow down from there into every
subscription. The root of the Management Group hierarchy is the tenant root Management Group, of which there is exactly one for each Azure Active Directory tenant. All Azure subscriptions within this tenant must sit within the Management Group hierarchy under this root.

This provides a simple and powerful way to efficiently apply and update governance across Azure subscriptions at scale. As well as being used to apply governance, several other Azure features now support management groups. This includes Azure Cost Management, Azure Advisor and Azure Security Center, allowing you to see costs, recommendations, and security reports spanning multiple subscriptions.

**SUBSCRIPTIONS WITH AN ENTERPRISE AGREEMENT**

The Azure Enterprise Agreement portal allows large enterprise customers of Azure to manage Azure subscriptions and associated licensing information from a central portal. Enterprise Agreement (EA) customers can add Azure to their EA by making an upfront monetary commitment to Azure. That commitment is consumed throughout the year by using any combination of the wide variety of cloud services Azure offers from its global datacenters. Within a given enterprise enrollment, Microsoft Azure has several roles that individuals play.

**The Enterprise Administrator** has the ability to add or associate accounts and departments to the enrollment, can view usage data across all accounts and departments, and is able to see the monetary commitment balance associated to the enrollment. There is no limit to the number of Enterprise Administrators on an enrollment.

**Department Administrators** can manage department properties, manage accounts under the department they administer, download usage details, and view monthly usage and charges associated to their department if the Enterprise Administrator has granted permission to do so.

**The Account Owner** can add subscriptions for their account, update the Service Administrator and Co-Administrator for an individual subscription, view usage data for their account, and view account charges if the Enterprise Administrator has provided access. Account Owners will not have visibility of the monetary commitment balance unless they also have Enterprise Administrator rights.

**SUBSCRIPTIONS WITHIN A CSP**

The CSP model does not have the concept of departments and accounts. Instead, each CSP subscription is created within a customer. The customer entity contains all the services that you have sold such as Office 365, Dynamics CRM, as well as Azure subscriptions.

Within each CSP customer, a Management Group hierarchy can be used enabling consistent governance across subscriptions. However, there is no such facility that spans multiple customers, so each customer will need to be managed separately.

Azure CSP subscriptions are also subject to a small number of technical limitations. See Migrating existing VMs to CSP for more information.
COMMON SUBSCRIPTION MANAGEMENT STRATEGIES

Common considerations when creating a subscription creation strategy:

- **Subscription Service Limits** – will the migration be impacted by service limits such as number of virtual networks, or ExpressRoute connectivity? What about future growth?
- **Virtual Network Connectivity** – how will resources in each subscription connect to each other? Site-to-Site, ExpressRoute, Virtual Network Peering?
- **Security** – role-based access control is setup per subscription. How will this impact your subscription creation strategy?
- **Chargeback** – how will you report and group Azure consumption costs?

The following are some common strategies that you can take when creating subscriptions. The key to understand is there is not a single model, each approach comes with its own caveats that you as the provider should understand and plan for.

**Subscription per Environment**

In this model, each environment contains the different types of applications and workloads.

Pros:
- Minimized risk of running into subscription limit issues
- Virtual network address spaces can be tailored per application
- Minimized risk of impacting one environment by changing the other

Cons:
- New ExpressRoute circuit required per 10th application unless you are using ExpressRoute Premium which has larger limits depending on circuit bandwidth
- More subscriptions to manage (RBAC, Policies, Tagging, Chargeback)

**Subscription per Application**

Each application uses a different subscription.

Pros:
- Minimal subscription limit issues since each application is in a subscription
- Per application RBAC model

Cons:
- Higher risk of running into cross subscription connectivity limits unless applications are isolated from each other
- More subscriptions to manage (RBAC, Policies, Tagging, Chargeback)

RESOURCES

- [Azure Onboarding Guide](aka.ms/AzureGovPlaybook)
- [Azure Subscription Service Limits](aka.ms/AzureSubscriptionServiceLimits)
Resource Organization

Consistent naming and tagging schemes help organize your Azure resources, making management easier and reducing mistakes.

Even a simple application can involve a substantial number of Azure resources, such as virtual machines, network interfaces, IP addresses, storage accounts, virtual networks, subnets, network security groups, etc. Without disciplined and intuitive resource organization, administrative mistakes are inevitable.

NAMING CONVENTIONS

Adopting a systematic and descriptive naming convention for each Azure resource is a useful way of making the purpose of each resource and the relationships between resources clearer. This increases manageability and reduces the likelihood of administrative mistakes.

Well-designed naming conventions enable you to identify resources in the portal, on a bill, and within scripts. Most likely, your customer will already have naming conventions for their on-premises infrastructure. When migrating to Azure, you should extend those naming standards to your Azure resources where possible. Naming conventions facilitate more efficient management of the environment at all levels.

Designing a naming convention is not entirely straightforward. Different Azure resource types have different limitations on what names are permitted (alphabet, case sensitivity, and length). Microsoft has documented these rules and published a baseline recommendation for a naming convention which can be used as a starting point.

RESOURCE GROUPS

A resource group is a container that holds related resources for an application. The resource group could include all the resources for an application, or only those resources that are logically grouped together. The service designer decides how to allocate resources to resource groups based on what makes the most sense for the organization. Since resource groups are commonly used as a security boundary for role-based access permissions, a good general principle is to group resources that share the same management lifecycle.

With Resource Manager, application designers can create a simple template (in JSON format) that defines deployment and configuration of entire application. This template is known as a Resource Manager template and provides a declarative way to define deployment. By using a template, you can repeatedly deploy the application throughout the app lifecycle and have confidence that resources are deployed in a consistent state. We’ll cover more about writing templates later. Since each template must be deployed to a single resource group, the resource groups structure also impacts your deployment template design. Deployment to multiple resource groups can be achieved at the expense of the additional complication of breaking your deployment into separate, nested templates.

TAGGING RESOURCES

In addition to a naming convention, resource tags can also be used to organize Azure resources. Tags are key-value pairs, with a maximum of 15 tags per resource or resource group. Tags can be used for multiple purposes—common scenarios include:

- **Azure billing** - supports filtering and grouping using tags, enabling tags to be used to implement internal chargebacks or billing codes (‘billTo=IT-Chargeback-1234’)
- **Associating resources** - for a particular application across resource groups (‘application=payroll’)
- **Resource owner** - Identifying the owner of a particular resource (‘managedby=joe@contoso.com’).
- **Environment** – Identifying the environment of a particular deployment (‘environment=staging’)

aka.ms/AzureGovPlaybook
Controlling access to Azure Resources

With great power, comes great responsibility. Just as the cloud allows services to be provisioned in minutes, critical services can just as easily be changed or deleted. Fortunately, Azure provides comprehensive features to enable you to control access without losing agility.

A typical application will only use a small subset of the wide range of resource types available in Azure. Allowing unrestricted creation of resources allows consumption of resources far beyond what was planned. This can cause unexpectedly high bill or even affect the correct operation of the application (for example, by causing subscription limits to be breached).

Similarly, incorrectly modifying or accidentally deleting a resource can cause an application outage. It is therefore important to control who has access to Azure resources, especially those supporting production applications, and to control what operations are permitted by those who do have access.

To summarize, the main governance challenges faced by an organization running production services in Azure are:

- Prevent unexpected costs by controlling which resources are deployed
- Control who has access to Azure resources, and what changes they are permitted to make
- Separate the control of production from non-production environments
- Prevent accidental resource changes or deletions that are potentially service impacting

Azure provides three complementary mechanisms to control what resource management operations are permitted in a subscription, who has permission to perform those operations, and to prevent accidental mistakes. These are known as policies, role-based access control, and resource locks.

- **Azure Resource Manager Policy** allows you define rules or conventions that must be applied to resources within a subscription. For example, a policy may block the use of certain types of resources or limit the SKUs or service tier of another resource type or enforce or prevent the use of a particular Azure region. Policies can also be used to enforce rules, such as the inclusion of a tag to enable billing cross-charging or enforcing a naming convention. Policies can be applied to the entire subscription or scoped to a resource group or resource.

- **Role-based access control (RBAC)** allows control over the actions of a user or group of users. Each role defines what actions are permitted, or not permitted, on what types of resource. Once a role has been defined, it can be applied to specific users or groups of users (as defined in Azure AD), and applied at the subscription, resource group or individual resource scope.

- **Resource Locks** allow certain potentially damaging management operations to be blocked. There are two types of lock: ‘DoNotDelete’, which permits all actions except deletion, and ‘ReadOnly’, which permits read operations but blocks any updates or deletes. For example, a ‘DoNotDelete’ lock may be applied to a storage account containing critical data to prevent accidental deletion, regardless of the role-based access permissions granted to the user. The operation can only proceed if the lock is first removed, which provides a useful checkpoint to verify that the operation really is intended. Adding and removing locks themselves are controlled by separate RBAC permissions, thereby providing role separation and enabling operator activities to be reviewed. Whilst a single lock can be applied at the subscription or resource group scope, they are typically applied to individual resources, allowing more fine-grained control.

Azure Policy, RBAC and locks are complementary. Policies focus on the resources in a subscription, regardless of the user initiating each request. RBAC works at the user level, controlling which operations are available to each user. Resource locks prevent accidental modification or deletion of individual resources. These three mechanisms work together to provide a powerful toolkit to control resource access whilst permitting necessary management operations under suitable controls.
Security and Compliance

Security is a critical requirement for government applications and compliance with government standards is a must. Applications cannot be migrated to Azure unless there is a high degree of confidence in the security and compliance of the solution.

Security in the cloud is a shared responsibility between Microsoft and the Azure customer developing and hosting applications in Azure. Microsoft makes substantial investments in the physical, logical and operational security of its infrastructure, networks, and software. This also includes the dedicated Azure Government datacenters operated by screened US citizens. Meeting CJIS, FedRAMP and DOD regulations is a key part of this ongoing dedication to meet the needs of federal, urban, regional, and state governments and law enforcement agencies in the US. Microsoft is an industry leader across hyper-scale cloud providers in helping agencies achieve compliance.

Azure provides a wide range of features and tools which can be used to secure applications hosted in Azure. It is the responsibility of the customer to understand and make appropriate use of Azure so that the applications they manage are properly protected.

Security is a specialist topic, requiring both broad and deep technical skills. Technical teams require appropriate experience and training to properly design, implement, and manage secure Azure solutions. Both the threat landscape and the security features available in Azure are continually evolving. On-going investment should be made to review and update the security protections of existing applications, and to ensure staff skills stay up to date.

Microsoft Azure supports an extensive range of features and services which can be used to secure Azure-based applications, and to provide secure connectivity to on-premises environments where required. In addition, Microsoft publishes extensive guidance on security best practices.

Use the following resources to deliver secure and compliant customer solutions:

- **Azure Government Security and Identity** provides guidance on security features available in Azure Government. These include Azure Security Center (ASC), a service designed to review all resources in your Azure environment and provide reports and guidance on how to improve their security to meet Azure best practices. ASC is a free service that you must turn on. This will help strengthen your security posture and protect against threats. ASC also has an optional paid tier with additional supports reporting for resources outside of Azure.

- The **Microsoft Trust Center** is a hub for security, compliance and privacy guidance from Microsoft. This includes all aspects of Microsoft's software portfolio (both on-premises and cloud), and guidance for third parties on how to develop their own applications securely. It also has a section for Azure Security.

- The **Azure Trust Center** provides links to additional resources on security, compliance and privacy.

- The **Azure Security documentation hub** contains both an overview of the full suite of security features available in Azure, as well as comprehensive guidance on specific areas such as networking, storage, compute, identity, and operations. Best practice guidance is also included, as well as links to additional resources.

- The **Security best practices for IaaS workloads in Azure documentation page** contains further useful guidance on secure Azure deployments.

- The **Microsoft Cloud Architecture resources** includes a series of posters providing a technical overview of core Azure features areas aimed at architects. This includes guidance on networking, hybrid cloud, storage, identity, mobility, and security.
Infrastructure as Code

Automate infrastructure deployment and management through declarative or imperative scripts.

Infrastructure as Code (IaC) is the process of writing scripts to automate the deployment and configurations management of infrastructure. Using automation to manage your infrastructure enables you to:

- Increase accuracy and reliability of resource deployment and configuration.
- Automate the process of replicating environment configurations across dev, test, and production environments.
- Add version control to infrastructure configuration management.

Automation is also a key component to implementing DevOps practices, and Infrastructure as Code fits in well with the other aspects of DevOps such as Continuous Integration (CI) and Continuous Deployment (CD).

There are two methods to writing scripts for implementing Infrastructure as Code: Imperative and Declarative. The imperative approach utilizes traditional command-line scripts to define the step-by-step process to modify current state to the desired end-state. The declarative approach utilizes a definition file that declares what the desired end-state is, and the tooling automatically figures out how to modify the current state to reach the desired end-state.

With the infrastructure deployment and configuration automated with scripting, these scripts can then be checked into Source Control, such as Git or Azure DevOps in Azure public cloud. This integration with Source Control adds the ability to affectively track infrastructure version changes over time in the same manner that all other source code is tracked. It also enables Infrastructure as Code (IaC) to be integrated into the release pipeline through Continuous Integration (CI) and Continuous Deployment (CD); alongside the source code for the enterprise applications that may run on the infrastructure being automated.

In this section, we'll review several approaches to automating infrastructure provisioning and management:

- **Azure Resource Manager Templates**: Declarative templates formatted in JSON to define the configuration of an Azure deployment.
- **Blueprints**: Declarative management of entire environments, from initial deployment to ongoing updates. Each blueprint combines Resource Manager templates, role-based access control assignments and Azure policy assignments into a single declarative object.
- **Automated scripts**: Create imperative scripts using Azure PowerShell and Azure CLI for managing Azure resources.
- **Azure SDKs and REST APIs**: Build your own management tools by leveraging the Azure SDKs and REST APIs to automate Azure resource management.
Azure Resource Manager Templates

Implement declarative Infrastructure as Code using Azure Resource Manager

Azure Resource Manager templates offer a **declarative** method of implementing Infrastructure as Code (IaC) for deploying and maintaining infrastructure and application deployments. Put simply, a template consists of a text file, in JSON format, specifying the resources in each deployment.

Templates can be parameterized, allowing a small number of inputs to control the type, number and size of resources deployed. This allows the same template to be used for multiple deployments in different environments, such as Test, Pre-Production and Production.

Consistency across the Azure ecosystem allows for Resource Manager Templates to be written that can deploy applications to both the Azure public cloud and Azure Stack without requiring any changes to the template.

Templates can be authored using a plain-text editor, or a variety of IDEs (Integrated Development Environments), such as Visual Studio 2019 and Visual Studio Code. These editors enhance the authoring experience with syntax highlighting, code completion, and other common IDE features.

Templates can be easily deployed, either directly from Visual Studio, using the Azure portal, PowerShell or CLI, or even integrated into a Continuous Integration / Continuous Delivery (CI/CD) pipeline using Visual Studio Team Services, Jenkins, or some other automated build and deployment tool.

Templates support two deployment modes, incremental and complete. In both modes, all resources specified in the template are deployed. The differences are in what happens to pre-existing resources that are **not** specified in the template—in incremental mode, they are unchanged, whereas in complete mode, they are deleted. This enables templates to be used both for clean deployments and to update existing deployments.

Developing Azure Resource Manager templates is a skill. The template language supports a wide range of features, some of them quite advanced such as conditionals and nested templates. Learning to use the full power of Templates is a highly worthwhile investment for any team making significant use of Azure. Several guides and samples are available to help you—see the links in the Resources section below.

**TEMPLATE AUTHORING TOOLS**

- **Azure Resource Manager Tools for Visual Studio Code.** Visual Studio Code (VS Code) is a free code IDE from Microsoft. The Azure Resource Manager Tools is an Extension to VS Code that adds syntax highlighting, autocomplete, and other features to the IDE for authoring ARM Templates with ease.

- **Visual Studio Azure Resource Group project** The Azure Resource Group project (deployed as part of the Azure SDK) template adds full IDE support to Visual Studio 2015 and 2017 for authoring and deploying ARM Templates directly within Visual Studio.

- **Azure portal** Templates can also be loaded into the Azure portal for easy deployment. The portal also supports editing templates online and downloading templates for editing offline. In fact, every deployment you make using the Portal uses a template, and you can download these templates from the portal as a starting point for creating your own.

**RESOURCES**

- [Azure Resource Manager Overview](#)
- [Authoring Azure Resource Manager Templates](#)
- [Azure Quickstart Templates](#)
- [Sample templates from the Azure Resource Manager team](#)
- [Create and deploy your first Azure Resource Manager template](#)
Blueprints

Automated deployment entire environments, with full lifecycle version management.

As we have just seen, Azure Resource Manager Templates provide a powerful means of deploying applications to Azure. By using a declarative model of all the required Azure resources, they enable the engineer to focus on the goal state of the deployment, letting Azure take care of the deployment process. Integrating these templates into source control enables automated deployment as part of a Continuous Integration / Continuous Delivery pipeline.

However, templates also have their limitations. First, the template itself is created and managed outside Azure. There is no central repository where all templates must be stored. Second, there is no tracking of deployments, no way to answer the question ‘where has this template been deployed?’. Third, there is no version control, no way to ask ‘which version of this template was deployed here?’ Fourth, there is no control over the resources deployed by the template once the deployment completes. For example, a template might define the best-practice configuration for a VPN gateway, but nothing stops the gateway being modified and diverging from this best practice.

BLUEPRINTS

Azure Blueprints are designed to address all these concerns. Like templates, blueprints are a declarative model for defining an Azure deployment. However, there are some important differences. Whereas templates are designed to deploy an application, blueprints are designed to deploy an entire environment. This environment can comprise multiple resource groups, resources (specified using templates), role-based access control assignments and Azure policy assignments. All these elements are included in the Blueprint.

TRACKING AND VERSIONING

Blueprints are stored in Azure, with a full version lifecycle. Each deployment (or assignment) of each blueprint is tracked, so you can easily identify every current blueprint deployment. This tracking includes the blueprint version that is currently deployed. Upgrades are managed by creating new blueprint versions and then updating a blueprint assignment to use that new blueprint version.

BLUEPRINT LOCKS

Blueprints also support resource locking. As with Resource Manager resource locks, there are two lock types: DoNotDelete and ReadOnly. However, the locking implementation with blueprint locks is quite different. Resource Manager locks protect against accidental changes, requiring the administrator to first remove the lock before making a change. Blueprint locks are stricter—the lock cannot be overridden, even by the subscription owner. The only way to modify the resources is by updating or removing the blueprint assignment. This makes blueprint locks suitable for publishing best practice deployments safe in the knowledge that the best-practice configuration will always be preserved.

RESOURCES

→ Azure Blueprints Overview
Automated Scripts

Implement Imperative Infrastructure as Code (IaC) using Command-Line scripts

Azure PowerShell and Azure CLI (cross-platform command-line tool) offer an imperative method of implementing Infrastructure as Code (IaC) for deploying and maintaining environment and infrastructure deployments with the Microsoft Azure ecosystem. These tools are designed for managing and administering Azure resources from the command-line, and for building automation scripts that work using Azure Resource Manager.

Automation scripts written using either tool can easily be checked into Source Control, such as Git or Visual Studio Team Services, for added version control. The scripts can even be integrated into a Continuous Integration / Continuous Delivery (CI/CD) pipeline using Visual Studio Team Services, Jenkins, or some other automated build and deployment tool.

Azure PowerShell and Azure CLI can both be downloaded and installed from the Azure downloads page. They are also available via the Microsoft Web Platform Installer. The tools are frequently updated, and it’s worthwhile always making sure you have an up-to-date copy to access the latest Azure features.

In addition to executing commands at the command-line of the local machine, the Azure Cloud Shell within the Azure Portal can be used to execute Azure PowerShell and Azure CLI scripts directly within a web browser from any machine. The Cloud Shell is accessed by clicking the Cloud Shell icon in the toolbar at the top of the portal, or as a standalone page at https://shell.azure.com. Cloud Shell is currently available for Azure Public, but not yet for Azure Government.
Azure SDKs and REST APIs

Custom code can be built to automate Azure resources, too.

The Azure SDKs (Software Development Kits), in addition to templates and command-line tools, can be used for both working with Azure Resources, as well as implementing the automation of deployment, configuration, and management of Azure Resources. These tools help add additional automation capabilities to grant the capacity to work with and automate resources in Microsoft Azure.

The Azure Development SDKs are a set of reusable libraries built by Microsoft that work with Azure Resource Manager to manage Azure resources. These SDKs enable any custom automation scenario to be built out, in addition to the integration of Azure services with custom code. This allows you to use or build exactly the right tool to solve the problem at hand.

These libraries support a wide array of programming languages and platforms, including:

- .NET Framework
- .NET Core
- Java
- Node.js
- PHP
- Python
- Ruby
- Android
- iOS

You can also manage Azure resources by calling the Azure Resource Manager REST APIs directly, using your own code instead of the SDKs. These APIs are the foundation of all resource management in Azure—indeed, the Azure portal, PowerShell, CLI and SDKs all use these Azure REST APIs. Using the REST APIs gives you direct access to all Azure resource management features.

RESOURCES

- [Azure SDK Downloads](aka.ms/AzureGovPlaybook)
- [Azure REST API Reference](aka.ms/AzureGovPlaybook)
Playbook Summary

We hope this playbook has helped you understand Azure for Government, and how it can help deliver a fundamental transformation of government services. We also hope you feel more confident in your next steps to adopt Azure Government, migrate existing workloads, and transform your organization.

Our goal, when creating this playbook, was to organize resources and provide insight that you can use to accelerate or optimize your cloud journey with Azure Government. To this end, we laid out the opportunity of digital transformation, followed by a roadmap of how you can adopt Azure Government successfully.

In the first section, **Understanding Azure Government**, we focused on understanding the Azure Government cloud. This included an overview of the Azure public, Azure Government and Azure Government Secret clouds, their security accreditations, and how to choose between them. We also reviewed the eligibility criteria for Azure Government, and how to get started with Azure Government, including support options and assistance from the FastTrack for Azure team.

The second section, **Cloud Leadership & Strategy** started by helping you to understand the potential for digital transformation to revolutionize government services. We explained how Azure Government acts as the foundation for digital transformation and explained how taking full advantage of Azure Government is much more than an IT project. It requires cultural change at an organizational level to envision new ways of working unencumbered by legacy IT practices. We showed how you can take advantage of cloud adoption best practices, and take advantage of a range of free and paid-for training opportunities to help build your cloud team.

We then moved to the technical content, which forms the bulk of this playbook, starting with a chapter on **Migration Assessment**. This included detailed guidance on the three stages of the assessment process—discovery, planning and evaluation—, and the expected contents of the resulting migration assessment plan.

In the fourth section, **Lift & Shift**, we discussed how to migrate workloads at scale using the Lift & Shift approach. This covered everything from setting up the network to using services such as Azure Migrate to move servers to Azure Virtual Machines.

In the fifth section, **Modernizing Apps**, we discussed how you can leverage platform as a service components and new technologies such as containers to modernize applications to make them cloud native for a lower total cost of ownership and easier scale.

In the sixth section, **Optimize & Manage**, we discussed how you can keep track of and even cut your cloud spending, along with applying governance controls to your cloud workloads.

In the appendix to this playbook, **Additional Resources**, we provide some references on why to choose the Microsoft cloud, troubleshooting, and best practices.

**FEEDBACK**
Share feedback on how we can improve this playbook by emailing AzureGovPlaybook@microsoft.com
Why Choose Microsoft?

A trusted global leader, committed to customers, a leading cloud platform.

More than 86% of Fortune 500 companies have the Microsoft Cloud, which offers a fully integrated stack for any kind of data from on-premises, hybrid or fully in the cloud, with an open cloud platform that supports a wide variety of operating systems and programming languages.

54 REGIONS AND COUNTING

To help organizations meet data residency, sovereignty and compliance requirements, Microsoft has a worldwide network of 54 announced Microsoft-managed datacenter regions, offering services in 140 countries. Microsoft continues to make significant investments in geo-expansion through our local and sovereign offerings.
WHY CHOOSE THE MICROSOFT CLOUD

No other company has such a complete portfolio, from IaaS to PaaS and SaaS, from productivity and social solutions to ERP, from smartphones to PPIs. Microsoft offers the most connected, comprehensive set of cloud solutions (Azure, Office 365, Microsoft Dynamics), with an unmatched breadth and depth of capabilities from platform to productivity apps to business solutions. Our integrated portfolio of cloud services works across devices and is supported by one of world’s largest developer and partner ecosystem. From a customer perspective, this means a lower cost and complexity associated with the product/services integration, IT provider management and support.

THE ONLY CLOUD: ENTERPRISE LEVEL, HYPER SCALE, AND TRUE HYBRID

Microsoft is the only cloud provider that combines a hyperscale cloud offering, a truly hybrid platform, and an enterprise level support for your cloud workloads with enterprise level SLAs.

COMPLETE SET OF INTEGRATED CLOUD OFFERINGS

Microsoft has a complete set of integrated cloud offerings, from infrastructure as a service (IaaS), to Platform as a Service (PaaS) and all its Software as a Service (SaaS) offerings. As an example, a PaaS development can easily integrate with a VM on Azure IaaS and easily integrate with app services like SharePoint and CRM Online.

COMMITMENT TO OPEN SOURCE

With Azure, you have choices. [Choices that help you maximize your existing investments](#). Get support for infrastructure as a service (IaaS) on Linux and Java and PHP Web application platforms. Develop and test your Linux and open source components in Azure. You bring the tools you love and skills you already have, and run virtually any application, using your data source, with your operating system, on your device. [Much of the Azure tooling and frameworks your technical teams use is open source and hosted in GitHub](#).

NATIVE SSO AMONG SERVICES AND ON-PREMISES

Being able to offer Single Sign On is key among multiple cloud services and on-premises apps is key for employee productivity and IT management. Microsoft natively offers SSO among its cloud services, offers REST API for custom apps and federation and directory sync services with AD and other directories.

BROADEST PARTNER ECOSYSTEM

Microsoft Partner Network includes over 430,000 organizations worldwide. By working with this broad partner ecosystem, we can offer better solutions and better services to our customers.

BEST AND MOST INNOVATIVE ENTERPRISE CLOUD PRODUCTIVITY SOLUTION

No other cloud provider offers such a complete suite of productivity services. Office 365 is recognized as the leading cloud productivity platform. Our customers can access the productivity platform through the browser or through the Office application, used by 1B users worldwide.

INTEGRATED BUT SEPARATED ENTERPRISE AND CONSUMER CLOUD OFFERINGS

Not all cloud solution providers in this space offer consumer solutions. Others have only one consumer platform that they extend to the enterprise, mixing SLAs and involving the greater risk of sharing private information in a public environment.

ENTERPRISE MOBILITY

The Enterprise Mobility Suite (EMS) is the first comprehensive offering in the industry to recognize that success in enterprise mobility is not just about devices. A complete mobility strategy requires the cohesive management of data, identity, and devices. With an integrated platform for universal device management, identity/access management, and data protection, EMS reduces licensing complexity and makes it easier to extend your existing productivity infrastructure to the cloud.
MICROSOFT CLOUD COMPLIANCE CERTIFICATIONS & ATTESTATIONS SEPT 2016

All of Microsoft's services are independently verified to meet legal and compliance requirements, are financially backed, and offer transparent information on their availability. Microsoft was the first cloud provider that adhere to ISO 27018 and ISO 22301.

FURTHER READING

➔ Azure Government enables digital transformation for Veterans Affairs
➔ More Microsoft in Government cloud blogs
➔ Government cloud adoption case studies
➔ Public Safety and Justice cloud adoption case studies
Troubleshooting Resources

To assist your support team, we have compiled several resources to assist with troubleshooting the related services your team may use as part of delivering services in this practice.

**MSDN SUPPORT FORUMS**

MSDN support forums are moderated by Microsoft staff and others in the community. This is a great location for asking troubleshooting questions for Azure.

Direct links to EMS forums:

- Azure Active Directory (AAD)
- Advanced Threat Analytics (ATA)
- Cloud App Security (CAS)

**STACK OVERFLOW**

Stack Overflow is the largest online community for programmers to learn, share their knowledge, and advance their careers. This a great community-based resource for assisting developers with troubleshooting code related issues on Azure.

**SERVER FAULT**

Server Fault is a question and answer site for system and network administrators. This a great community-based resource for assisting IT Professionals with troubleshooting infrastructure related issues on Azure.

---

**AZURE TROUBLESHOOTING RESOURCES**

**TROUBLESHOOTING AZURE ACTIVE DIRECTORY**

- Azure AD Connectivity
- Microsoft Azure AD Domain Services

**TROUBLESHOOTING MICROSOFT INTUNE**

- Device Enrollment
- Client Setup
- Conditional Access
- Company Resource Access Problems
- Exchange Connector
- Lookout Integration

**TROUBLESHOOTING INFORMATION PROTECTION**

- Troubleshooting Azure AD Connectivity
- Troubleshooting Azure AD Domain Services

- Troubleshooting Password Management
- Troubleshooting Azure AD Connect Synchronization Issues

aka.ms/AzureGovPlaybook
### TROUBLESHOOTING ADVANCED THREAT ANALYTICS

- Troubleshooting using Known Errors
- Troubleshooting using performance counters
- Troubleshooting ATA using Logs
- Troubleshooting using the ATA Database

### TROUBLESHOOTING AZURE INFRASTRUCTURE AS A SERVICE

- Troubleshooting RDP Connections
- Troubleshoot Creating a new VM
- Troubleshoot restarting or resizing a VM
- Troubleshoot Allocation failures on Windows
- Troubleshooting Application Access on Linux
- Troubleshooting Resource Manager Deployment issues with Linux
- Troubleshooting ARM Template Deployment Errors
- Troubleshooting Specific RDP errors
- Troubleshoot Application Access
- Troubleshooting SSH connections
- Troubleshooting Allocation issues on Linux
- Redeploying a Virtual Machine
- Troubleshooting and monitoring Azure Storage

End-to-End Storage Troubleshooting
Best practices for running Azure projects

Deploying or creating a solution in Azure can cover a broad surface area of technologies and services that are used.

A common problem for customers implementing solutions on their own is not following established best practices and existing reference architectures. It is our recommendation to ensure that your team is aware of and takes advantage of established best practices from Microsoft where possible. We have compiled a list of best practices resources as it relates to deploying infrastructure in Azure or for hybrid deployments.

### DOCUMENT

- **Pricing Azure Services with the Calculator**
- **Azure Guidance from Patterns and Practices**
- **Azure Reference Architectures**
- **Best practices for running a Windows Virtual Machine on Azure**
- **Performance Best Practices for SQL Server running in Azure**
- **Azure Resiliency Technical Guidance**
- **Azure Security Best Practices and Patterns**
- **Best Practices for Network Security**
- **Patterns for Designing ARM Templates**
- **OMS Architecture**
- **Asymmetric Routing with Azure ExpressRoute**
- **Best practices for Azure App Services**
- **Instrumenting applications using Application Insights**

### OVERVIEW

- Pricing calculator to price out services used in your Azure project.
- Checklists for availability, scalability, security for a broad list of topics and services in Azure.
- A collection of documented best practices for deploying virtual machines and VPN connectivity in Azure.
- Configuring storage, availability, performance, and connectivity.
- Performance tuning SQL Server in Azure Virtual Machines.
- Best practices for building resilient solutions in Azure.
- Best practices and patterns.
- Best practices for protecting networks using virtual appliances, network security groups and hybrid connectivity solutions.
- Best practices with template design and deployment.
- Reference Architectures for Operations Management Suite components.
- Best practices for asymmetric routing using Azure ExpressRoute.
- Best practices for deploying, monitoring and troubleshooting Azure App Services.
- Using Application Insights to instrument applications for troubleshooting, monitoring and telemetry capture.