SEVEN STEPS TO GET STARTED WITH MICROSOFT AZURE
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>STEP 1: DON’T START WITH A PRODUCTION WORKLOAD</td>
<td>3</td>
</tr>
<tr>
<td>STEP 2: CONSIDER ANY CORPORATE POLICIES AND COMPLIANCE ISSUES</td>
<td>3</td>
</tr>
<tr>
<td>STEP 3: DEFINE YOUR GOALS FOR THE CLOUD</td>
<td>4</td>
</tr>
<tr>
<td>STEP 4: CALCULATE YOUR FINANCIAL RETURN ON AZURE</td>
<td>5</td>
</tr>
<tr>
<td>STEP 5: DETERMINE YOUR CLOUD IDENTITY STRATEGY</td>
<td>5</td>
</tr>
<tr>
<td>STEP 6: CONSIDER HOW TO SECURE YOUR CLOUD ENVIRONMENT</td>
<td>6</td>
</tr>
<tr>
<td>STEP 7: REALIZE IT’S NOT AS EASY AS IT LOOKS</td>
<td>7</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>7</td>
</tr>
</tbody>
</table>
INTRODUCTION

Ready to start using Microsoft® Azure®, but not sure how to get started?

Have teams within your organization opened Azure accounts that you need to consolidate? Maybe you inherited some Azure workloads through a merger or acquisition? Or perhaps you’ve concluded that working with Microsoft’s offering is the best way to move to the cloud?

Good news. Getting started with Microsoft Azure can be easier than you imagine. And moving to the cloud with Azure creates the potential for some serious rewards, including lower costs, more strategic use of IT resources and a competitive edge.

This white paper describes seven proven steps to help you gain those rewards. These steps cover everything from planning and budgeting to choosing the best strategy to secure your cloud environment.

What is Microsoft Azure?

Azure is Microsoft’s cloud computing platform for building, deploying and managing applications and services through a global network of Microsoft data centers. Azure consists of a growing collection of integrated services, including identify management, analytics, computing, database, mobile, networking, storage and web.

STEP 1: DON’T START WITH A PRODUCTION WORKLOAD

Here’s the first tip: Don’t jump in too fast with Azure. Instead, slow down and make an effective plan, following these steps.

Start by choosing to move a workload that you can afford to have fail a little as you learn.

“The most successful companies today will be those that are able to embrace failure in all of its forms. They must fail fast, fail early and fail often,” writes digital thinker Dominic Basulto in The Washington Post.

He defines this approach as “making rapid, iterative adjustments that uncover tiny failures and then correct them more quickly than one’s competitors.”

The same mantra applies to getting familiar with Azure. Small failures are OK, as long as they lead to ultimate success. So, use workloads that can fail without any devastating results.

Rank your apps

If you haven’t done this exercise before, it’s time to rank all your applications by how much they impact your core mission.

For example, you can use the grid shown in Table 1:

<table>
<thead>
<tr>
<th>More Critical</th>
<th>Medium priority</th>
<th>Low priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top priority</td>
<td>Includes all applications that are not mission-critical, but harder to move to the cloud</td>
<td>Includes all mission-critical applications that are easier to move to the cloud</td>
</tr>
<tr>
<td>Less Critical</td>
<td>Medium priority</td>
<td>Low priority</td>
</tr>
<tr>
<td>Top priority</td>
<td>Includes all applications that are not mission-critical or in production and are easier to move to the cloud</td>
<td>Includes all mission-critical applications that are easier to move to the cloud</td>
</tr>
</tbody>
</table>

For your first field test of the Azure cloud, pick a workload in the lower-left quadrant. For most enterprises, the best place to start is with a dev/test workload. That way, as you learn and experiment, there will only be minor consequences for any failures.

STEP 2: CONSIDER ANY CORPORATE POLICIES AND COMPLIANCE ISSUES

Next, research any internal policies or compliance regulations that touch on moving data or apps to the cloud.

Sectors such as finance, government, healthcare and retail all have special rules defined for data security, handling personally identifiable information (PII) and so on. For instance, HIPAA requires any documents containing PII to be encrypted prior to migration to the cloud.

Regulations in other sectors may vary, so make sure you understand the data security requirements that apply to your market space.

If you’re a publicly traded company, there are certain regulations you must follow. And these rules vary by country, so also check up on any divisions and subsidiaries of your enterprise around the world.
The best way to get started is to ask your corporate compliance team or legal counsel for clarification. But don’t worry. Most IT leaders now find they can do everything they need to in the cloud — without breaking any rules.

Third-party certifications pave the way

“If you’re like most organizations, you’ll probably find that you can do more than you thought you could in the cloud, while still complying with the necessary regulations,” notes David Chappell, an industry expert on Azure and cloud computing. Third-party certifications make compliance even easier.

The laws are being modernized, and the situation is getting clearer, he says. And Azure has now gained many third-party certifications that make compliance even easier.

“Azure meets a broad set of international and industry-specific compliance standards,” states the Azure website, “such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards like Australia IRAP, UK G-Cloud and Singapore MTCS.”

For more details, visit the Azure Trust Center at https://azure.microsoft.com/en-us/support/trust-center/

STEP 3: DEFINE YOUR GOALS FOR THE CLOUD

Now that you have a handle on what’s allowed, think hard about what you’re really trying to achieve in the cloud.

In general, the most likely business benefits you can gain will be lower costs and higher reliability for infrastructure, and better support for mobile app users.

More specifically, are you seeking to

• Save money on IT overall?
• Shift costs from capital expenses (capex) to operating expenses (opex) for a better bottom line?
• Gain from a faster, more flexible model for provisioning IT?
• Shift computing to another region to speed up response rates for employees or customers in that part of the world?
• Learn about the cloud for yourself, or get access to more knowledge about it?
• Launch custom apps faster to give your enterprise a competitive edge?

Your goals determine how much you will need of each type of cloud resource:

• Infrastructure-as-a-Service (IaaS)
• Platform-as-a-Service (PaaS)
• Software-as-a-Service (SaaS)

Source: Rackspace website https://support.rackspace.com/en-us/support/trust-center/
A simpler explanation

If you need to explain these concepts to a non-technical colleague, here's a simple metaphor you can try.

IaaS is the fundamental layer that enables everything else to happen. So, in transportation, IaaS is like the highways, city streets, road signs and traffic lights.

PaaS uses that IaaS layer to actually do something, similar to a truck on the road loaded with packages.

And SaaS is something a user can see and use, like a package that the PaaS truck delivers to a consumer.

Like any analogy, this isn’t perfect. But it gets across some of the main points about the three different service levels — without talking about servers, operating systems or networking.

STEP 4: CALCULATE YOUR FINANCIAL RETURN ON AZURE

Now that you've defined the benefits you're seeking, it's time to give your plans a financial reality check.

Start with your current IT budgets and your existing roadmaps to project IT spending. Then consider some fresh scenarios.

What would it cost, and what could you save, by moving these workloads to the cloud:

- Backup, restoration and disaster recovery
- Calendaring
- CRM and sales force automation

- Data storage and archiving
- Dev/test
- Email
- Marketing content
- Office apps for creating and sharing documents
- Training apps and content
- User-generated content
- Various websites and portals

In many scenarios, Azure will cost dramatically less, offering pay-per-use for compute, pay-per-gig-per-hour for storage and inexpensive bandwidth, including free data uploads to the cloud.

For example, if you continue to add more workloads to your existing data center, you will simply extend all of your current capex for hardware and infrastructure, payroll for IT labor and ongoing monthly costs for power, HVAC and other operating expenses.

But if you add new workloads to the cloud instead of your data center, and begin to transfer workloads to the cloud, you will benefit from a pay-as-you-go model. Those costs come out of your operating budgets (opex), and you should see a clear reduction in payroll and other ongoing costs.

For IT leaders approaching the physical limits of their hardware facilities, Azure offers a compelling alternative. By migrating compute resources to a private cloud running Azure, firms can avoid tying up precious capital in bigger buildings and more server rooms.

Consider what it would cost you NOT to move to the cloud

Then look at it another way. What if you could develop, test and roll out a new mobile app 20% faster by using Azure? What would you gain in better revenue and customer service?

What if you could develop a more cloud-aware app that required 20% fewer calls to tech support? What savings would you see? How many added sales would result?

And by using the cloud, what if you could reallocate IT personnel to more strategic tasks than simply “keeping the lights on”? How many people could you reassign? What could that team achieve? How much could ROI increase?

Running these calculations for the first time can seem daunting. As companies move to the cloud, the benefits fall into some typical industry categories. A seasoned partner can help you identify these categories and figure out your likely bottom line.

STEP 5: DETERMINE YOUR CLOUD IDENTITY STRATEGY

After you know your projected bottom line, there’s a technical issue you’ll have to deal with: how to handle your authentication in the cloud.

Once upon a time, when everyone used desktop PCs behind the enterprise firewall, everyone used Active Directory® (AD) for all authentication. It was rock-solid and slow-changing. But it was designed in an era before the cloud and today’s vast array of mobile devices.

More recently, Microsoft created Azure Active Directory (AAD), an updated approach designed for the cloud and today’s mobile devices. Table 2 sums up the key differences between these two technologies.
You likely want to use a hybrid approach: integrating your existing AD and Office 365® users with AAD to create one big pool of users.

At this point, you’ll need to choose between synchronization and federation. If you’re moving slowly to the cloud, you can start by authenticating through synchronization, which enables users to log in to your cloud with their existing credentials. In effect, you gain single sign-on (SSO) functionality for both on-premises applications and your unique enterprise applications.

Eventually, you may need more reach and flexibility, such as controlling individual access to many SaaS apps from any device. At that point, you can add on federation. Just as a federation brings together states into a larger whole — while each state retains much of its own authority — Azure identity federation does the same with various SaaS providers.

Azure operates as a federation hub that’s already connected to most SaaS services, such as Citrix® GoToMeeting®, Dropbox, Salesforce®, WebEx® and hundreds more. Using federation with AAD gives your users convenient and secure access to a vast range of SaaS services, while saving your IT team the effort of manually linking to dozens of different cloud services.

**Profound implications for your business**

Your cloud identity strategy has some profound implications for your business.

Consider your full range of users:

- On-premises
- Mobile BYOD users
- IT admins
- Trusted B2B partners
- B2C customers

AAD enables your enterprise to do more for each type of user. With AAD, you gain flexibility in how each type of user can access any SaaS apps, Azure cloud-based apps or on-premises applications. For example, you can:

- Enable BYOD access for your mobile workforce
- Allow trusted B2B partners to log in to supply chain applications to update shipments or invoice
- Enable B2C customers to sign on to your website using Facebook credentials

But you have to get it right. If your cloud identity strategy is too strong, you risk frustrating users by blocking their access when they need it. On the other hand, if it’s too weak, you risk making it too easy for an experienced cybercriminal to break in and steal sensitive data.

Authentication in the cloud is far too complicated to leave to anyone without training and experience in AAD. Because when authentication fails, everything fails.

A seasoned partner can help you do the AD analysis, remediation and integration work required to implement your chosen cloud identity strategy.

**STEP 6: CONSIDER HOW TO SECURE YOUR CLOUD ENVIRONMENT**

As an IT leader, security is always on your mind, whether you’re thinking about the cloud or not.

As you get started with Azure, you’ll want to consider these three levels of security:

1. **Authentication**: As touched on earlier, how do you determine that someone really is who they say they are — an authorized user, sys admin, B2B business partner or B2C consumer?
2. **Role-based access controls**: How do you make sure that authorized users can only access the apps they need and the data they’re supposed to see?
3. **Network-level threat detection and removal**: What if an unauthorized or malicious user does manage to penetrate a cloud app, or exploit a hole inadvertently left open in your firewall? How can you detect and remove that threat?

### Table 2: Microsoft Active Directory and Azure Active Directory

<table>
<thead>
<tr>
<th>Active Directory</th>
<th>Azure Active Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed for on-premises devices and software</td>
<td>Designed for the cloud</td>
</tr>
<tr>
<td>Works best with single-platform Windows</td>
<td>Works cross-platform with any browser</td>
</tr>
<tr>
<td>Mainly used for directory services via DNS</td>
<td>Mainly used for identity services via HTTP and HTTPS</td>
</tr>
<tr>
<td>Queried with LDAP</td>
<td>Queried with APIs</td>
</tr>
<tr>
<td>Hierarchical structure: forests, trees, organizational units (OUs) and group policy objects (GPOs)</td>
<td>Flat structure: no forests, no trees, no OUs, no GPOs; does have domains, users and groups</td>
</tr>
<tr>
<td>Authentication mainly through Kerberos</td>
<td>Authentication through various protocols</td>
</tr>
</tbody>
</table>

You may want to use a hybrid approach: integrating your existing AD and Office 365® users with AAD to create one big pool of users.

At this point, you’ll need to choose between synchronization and federation. If you’re moving slowly to the cloud, you can start by authenticating through synchronization, which enables users to log in to your cloud with their existing credentials. In effect, you gain single sign-on (SSO) functionality for both on-premises applications and your unique enterprise applications.

Eventually, you may need more reach and flexibility, such as controlling individual access to many SaaS apps from any device. At that point, you can add on federation. Just as a federation brings together states into a larger whole — while each state retains much of its own authority — Azure identity federation does the same with various SaaS providers.

Azure operates as a federation hub that’s already connected to most SaaS services, such as Citrix® GoToMeeting®, Dropbox, Salesforce®, WebEx® and hundreds more. Using federation with AAD gives your users convenient and secure access to a vast range of SaaS services, while saving your IT team the effort of manually linking to dozens of different cloud services.

**Profound implications for your business**

Your cloud identity strategy has some profound implications for your business.

Consider your full range of users:

- On-premises
- Mobile BYOD users
- IT admins
- Trusted B2B partners
- B2C customers

AAD enables your enterprise to do more for each type of user. With AAD, you gain flexibility in how each type of user can access any SaaS apps, Azure cloud-based apps or on-premises applications. For example, you can:

- Enable BYOD access for your mobile workforce
- Allow trusted B2B partners to log in to supply chain applications to update shipments or invoice
- Enable B2C customers to sign on to your website using Facebook credentials

But you have to get it right. If your cloud identity strategy is too strong, you risk frustrating users by blocking their access when they need it. On the other hand, if it’s too weak, you risk making it too easy for an experienced cybercriminal to break in and steal sensitive data.

Authentication in the cloud is far too complicated to leave to anyone without training and experience in AAD. Because when authentication fails, everything fails.

A seasoned partner can help you do the AD analysis, remediation and integration work required to implement your chosen cloud identity strategy.
The reality is that every IT manager must now address this third possibility, whether for workloads in the cloud or behind your own firewall.

“No locale, industry, or organization is bulletproof,” says the 2016 annual report on data breaches from Verizon, which summed up 64,199 well-documented attacks from 2015. As usual, incidents were reported in every sector, from accommodation to utilities. And while most attacks were from outside, about one in five came from an employee or partner with permission to pass through the firewall. And these insider breaches take the most time and effort to detect.

Fortunately, Azure can take care of the most common intrusion attempts, like spoofing or DDoS attacks. Outside of those scenarios, you need a security plan. For example, what if a guest OS gets through the firewall on a VPN? Do you automatically send an alert and shut them down? Or do you monitor them until they do something suspicious?

Microsoft Azure imposes and enforces strict operational best practices, including disciplined patch and configuration management. As you know, many attacks that use known vulnerabilities can be blocked through diligent patch management.

And if you still feel unsure about trusting workloads and data to anyone outside your firewall, ask yourself this: Who can manage a data center better — your team, or the Microsoft team?

“If you think your data center is more secure than an Azure data center, you’re probably mistaken,” notes David Chappell. "Microsoft very likely has more resources than you do to build and operate state-of-the-art security technologies, to carefully vet the people who work in its data centers and more.”

**STEP 7: REALIZE IT’S NOT AS EASY AS IT LOOKS**

Some people think Azure is “just Windows in the cloud” or that “it’s all Microsoft, so it all works together.” They need to think again. The cloud doesn’t run itself.

It’s true that AD, Azure and AAD all come from Microsoft. But they don’t all automagically work together. You have to decide how you want them to interoperate, then set them up correctly.

The first time you do that, it’s not simple. There are tricks and traps that people only learn from experience working with Azure.

Although the cloud changes the game, it still requires rigor and understanding. And you’ll still need “cloud operations” people, although they may need different skill sets.

**Tedious, error-prone administration**

Azure has many features to learn and configurations to adjust. For example, here are some of the many tasks that Azure still requires:

- Architecture design
- Backup configuration and monitoring
- Database administration
- Firewall rules management
- Load balancer configuration and monitoring
- Network management
- Operating system configuration and patching
- Security
- Troubleshooting
- Virtual machine monitoring

Do you have the in-house resources to handle all those tasks?

One of the biggest reasons CIOs outsource workloads to the cloud is to save on tedious, error-prone administration. Configuration and optimization are better left for certified experts who do these tasks every day.

If this is your first time working with Azure or moving any workloads to the cloud, you would be prudent to seek out a knowledgeable partner who can help manage this for you.

**CONCLUSION**

Microsoft Azure provides a vast suite of features and capabilities. The complexity and ongoing evolution of Azure can make it a challenge to adopt, operate and manage.

This white paper describes seven steps to get started with Microsoft Azure. At every step, you can benefit from the help of an experienced guide who’s been there before.

By outsourcing management to a seasoned partner, you can reduce your risk and shorten your time to value while getting more value from Azure faster, with less risk of mistakes.

To find out more about how Rackspace can help you get started with Azure, visit rackspace.com/azuredirect.
Microsoft Azure, visit our Azure website at https://www.rackspace.com/azure

FOOTNOTES


5. Verizon, page 7

6. Verizon, page 35

7. Chappell, pages 3-4

ABOUT RACKSPACE

Rackspace, the #1 managed cloud company, helps businesses tap the power of cloud computing without the complexity and cost of managing it on their own. Rackspace engineers deliver specialized expertise, easy-to-use tools, and Fanatical Support® for leading technologies developed by AWS, Google, Microsoft, OpenStack, VMware and others. The company serves customers in 120 countries, including more than half of the FORTUNE 100. Rackspace was named a leader in the 2015 Gartner Magic Quadrant for Cloud-Enabled Managed Hosting, and has been honored by Fortune, Forbes, and others as one of the best companies to work for.

Learn more at www.rackspace.com or call us at 1-800-961-2888

© 2016 Rackspace US, Inc.