



Cloud Operations and Management

Microsoft Practice
Development
Playbook



aka.ms/practiceplaybooks

About this Playbook

This playbook is intended for the business and technical leadership for new and existing Microsoft partners that are adding a new practice to their business focused on delivery of services for Microsoft Azure related to Azure operations, security, and management.

Objectives

The goal of this playbook is to help you accelerate or optimize your Azure operations and management-focused practice.

For the business side, this playbook provides valuable resources for driving new revenue opportunities, strategies for marketing, selling, and lead capture, as well as building deeper and longer-term engagements with your customers through potential new service offerings like managed services.

For the technical side, the playbook offers guidance on a number of topics that range from the technical skills your team will need, to resources that you can use to accelerate learning as well as an explanation of some of the key opportunities for technical delivery to focus on as you get started and grow your practice.

How this playbook was made

This playbook is part of a series of guidance written by Microsoft Partner [Opsgility](#), in conjunction with the Microsoft One Commercial Partner group and 22 other successful Azure partners that have volunteered time to provide input and best practices to share with the rest of the partner community.

To validate the guidance provided in these playbooks, we conducted a survey of 1,136 global Azure partners with MDC Research. In this survey, we gathered insights on a range of topics, including how partners hire, compensate and train resources; their business model, revenue and profitability; what practices and services they offer; and what skillsets they have in place to support their offers. The results of this survey are provided in-line with the guidance found within this playbook.

CONTRIBUTING PARTNERS

[Artis Consulting](#)

[Atea](#)

[AwareComm](#)

[Blue Meteorite](#)

[DEFTeam Solutions](#)

[Dimension Data](#)

[Empired](#)

[Equinix](#)

[Frama Data Systems](#)

[Hanu Software](#)

[Kloud Solutions](#)

[Mirabeau](#)

[New Signature](#)

[OpenSistemas](#)

[PC Solutions](#)

[Perficient](#)

[PlainConcepts](#)

[Slalom](#)

[Softjam](#)

[SpanishPoint](#)

[SQL Services Ltd.](#)

[Theta](#)





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 sales, marketing, support, technical, and managed services teams.
- Leverage the resources available from Microsoft to help maximize your profitability.
- Share feedback on how we can improve this and other playbooks by emailing playbookfeedback@microsoft.com.

Table of Contents

The Azure Operations and Management Opportunity	5	Managing Azure Subscription Access.....	81
Define Your Strategy	7	Identity and Access Management (IAM).....	82
Executive Summary.....	8	Security and Networking	86
Identify Target Customers.....	9	Configuration Management	92
Define Engagement Process.....	11	Availability and Business Continuity	94
Define Service Offerings.....	12	Compliance and Monitoring	100
Azure Security and Management	13	Support and Incident Management.....	103
Define Your Pricing Strategy	24	Automation and DevOps.....	106
Calculate Your Azure Practice Costs	28	Continuous Integration / Continuous Deployment.....	109
Understanding Managed Services	29	Go to Market & Close Deals	110
Accelerate your Managed Service Model.....	31	Executive Summary	111
Understanding Intellectual Property	38	Managed Services Transition	112
Hire & Train	45	Marketing Your Offerings	113
Executive Summary.....	46	Consultative Selling and Technical Pre-Sales.....	114
Hire, Build, and Train Your Team	48	Guide: Go-to-Market and Close Deals.....	115
Job Descriptions for Your Service Delivery Team.....	51	Optimize & Grow	116
Reskilling Your Existing Technical Resources.....	63	Executive Summary	117
Recruiting Resources.....	66	Guide: Optimize and Grow	118
Training & Readiness	67	Playbook Summary.....	119
Competencies and Certifications	71	Additional Resources	119
Operationalize	76	Why Choose Microsoft?	120
Executive Summary.....	77	Troubleshooting Resources	123
Azure Virtual Datacenter.....	78	Common Objections	125
Managing Azure Subscription Creation	79	Case Studies.....	127

March 2019

The Azure Operations and Management Opportunity

As companies embrace the opportunities presented by cloud computing to connect with customers and optimize operations, they take on new challenges. One of the biggest challenges in the adoption of cloud computing is ensuring the customers have the right skillset to manage the underlying technologies as well as an understanding of how to manage and automate the Microsoft Azure platform.

CHANGING BUSINESS NEEDS WITH THE CLOUD

In the new world of digital transformation, technology has become the source of competitive differentiation and customers are asking themselves how their current organizations need to change to adapt into delivering a successful and sustainable digital business. With IT organizations becoming the primary means of meeting the needs of the business they need to evolve from supporting the business to being a part of the business by delivering value through services hosted in the cloud.

As IT organizations become more closely aligned with the business, their roles and responsibilities will also evolve. Many customers see IT staff transitioning directly into business units which takes away from core IT. While a greater partnership and knowledge of the business is built, this leaves an opportunity for partners to step in and assist customers in the areas of Operations and Management. Partners should understand and embrace this fundamental change so that they can become strategic partners and trusted advisors as they lead their customers on this journey.

BUSINESS VALUE AND AGILITY IN THE CLOUD

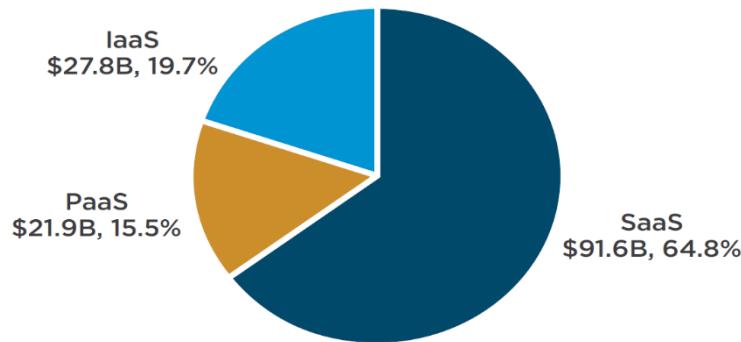
As customers transition to cloud computing platforms, they are faced with managing not just a new set of technologies, but also a new way of approaching the management and operations of their digital estate. While the cloud can bring greater business value and agility, it can also bring new concerns, including cloud sprawl.

PC Sprawl (1995+)	Server Sprawl (2000+)	Cloud Sprawl (2015+)
Active Directory	Management suites	SaaS management
Patch, asset, mobile management	Virtualization, monitoring, patch, backup	Security, threats
Secure access	Identity, workload	Monitoring, backup

Partners must be prepared to help customers understand how to manage, automate, and optimize their digital estate hosted in Microsoft Azure. In addition, partners should be positioned to ensure that customers have a solid foundation on which to execute their cloud strategy.

IDC forecasts that worldwide public IT cloud services revenue (i.e., SaaS, PaaS, and IaaS) will reach \$141.2B USD by 2019, a 19.4% compounded annual growth rate (CAGR): almost six times the rate of overall IT spending growth! SaaS still makes up the majority of spending, though PaaS and IaaS are expected to grow at almost twice the rate of SaaS over the next 5 years.

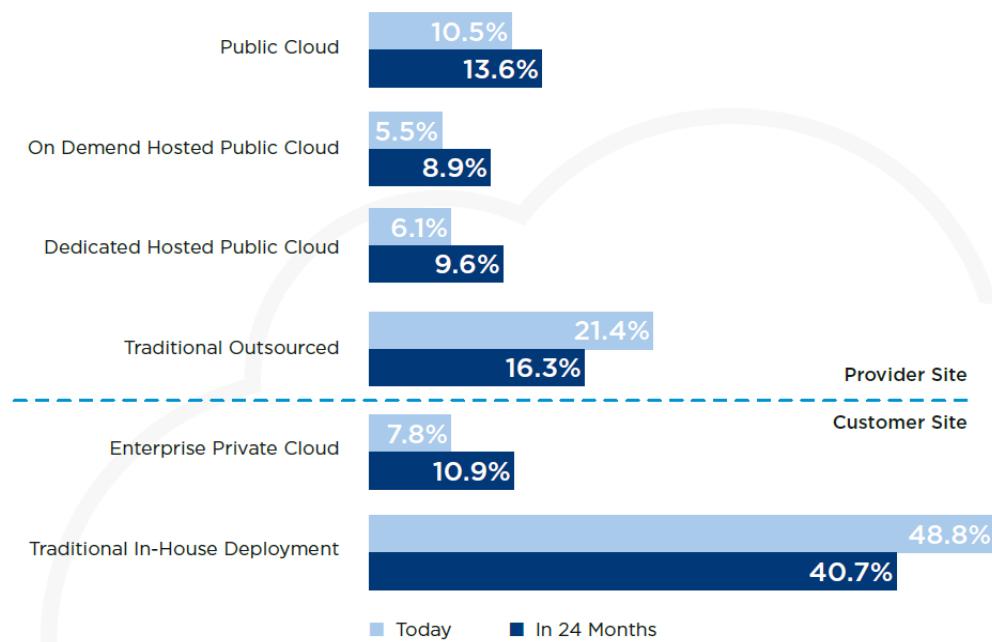
PUBLIC IT CLOUD SERVICES, 2019



This cloud spend also leads to two major shifts in budgets:

- A 44% growth in the move from non-cloud to cloud delivery (e.g., on-demand, elastic, self-service, resource pooling, measured service)
- An 11% growth in the move from customer site to provider site. (e.g., traditional outsourced, hosting provider, and public cloud)

AVERAGE IT BUDGET DISTRIBUTION OVER THE NEXT 2 YEARS



These shifts lead directly to revenue generating activities and additional opportunities for partners to delivery services on the Microsoft Azure platform.

Microsoft
Partner
Network

Define Your Strategy

Cloud Operations & Management

aka.ms/practiceplaybooks



Executive Summary

Now that you understand the opportunity before in building a practice focused on the delivery of Azure operations and management, the first step is to define the strategy you will use to build your practice. Like the foundation of the house, thinking though your strategy is critical to the long-term success of your practice — and it is worth it to take the time to think this strategy through.

We begin by showing you to identify your target customers by identifying your customers' needs and understanding their existing technology stack. This will allow you to offer the right services and focus on selling services within your defined areas of expertise.

Then we will guide you through the process of defining your service offerings. With your service offerings defined, we'll move on to defining your pricing strategy, and explore strategies you can use to incentivize your customers to use your services for more Azure initiatives which directly drives consumption.

We will then help you understand the building blocks for putting together a practice.

With your customers identified, your service offerings and pricing model defined, and your practice in place, we will next explore how to land a customer.

With your first customers in place, we will also explore how you can leverage re-usable IP and build a repeatable delivery model.

If you are not yet a Microsoft Partner, we will give you a walking tour of the Microsoft Partner Network, the programs you can leverage to grow your practice, how to earn competencies that yield additional benefits, and how to maximize the benefits you get from the program.

After that, we'll give you a head start in how to identify potential customers when starting your practice, as well as potential service offerings.

We'll conclude this section by helping you understand support — how to support your customers, Microsoft's support offerings, and the support-related benefits you get from establishing competencies in the Microsoft Partner Network.

Let's get on to defining your practice strategy.

TOP 5 THINGS TO DO

Measure twice and cut once. Here are the top 5 things you should absolutely do when defining the strategy for your practice.

- Define your focus & value proposition
- Understand the operations and management opportunity
- Develop a business plan
- Define and design the solution offer
- Define your pricing strategy

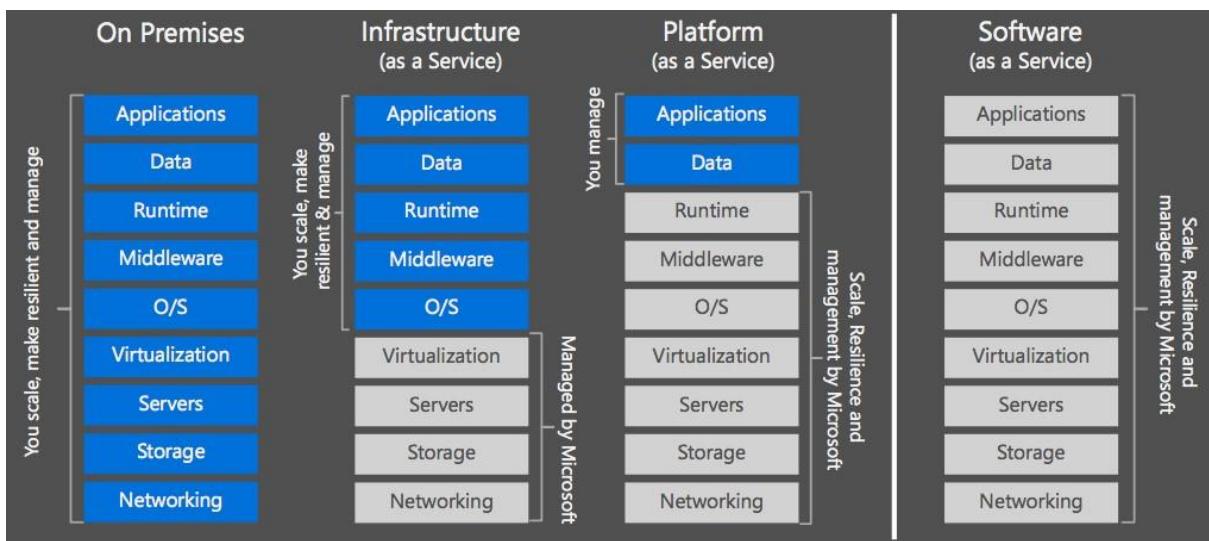
Identify Target Customers

With your Azure Operations and Management practice, you can help keep your customers both productive and secure across multiple technical disciplines. Your technical expertise allows your customers to focus on their business and not day-to-day operations.

IDENTIFY CUSTOMER NEEDS

Customers will have varying needs based on how far they have come in their digital transformation journey and how established their digital estate is today. Some customers will already have one or more Azure subscriptions, application deployments, and cloud-ready applications in use day. Other customers will be at the start of their journey, looking to you as a trusted advisor to guide them on their journey and implementation of Azure within their organization.

Customers may have existing on-premises deployments today which are targeted to be migrated to an Infrastructure-as-a-Service (IaaS) environment, or current applications which are being transformed for hosting in a Platform-as-a-Service (PaaS) offering. The needs of your customers and the services you can offer will be highly dependent upon their existing technological stack as well as their future goals for when that stack is hosted in Microsoft Azure.



If your customers are targeting an IaaS environment, you'll have the opportunity to focus on several Azure services, including monitoring and maintaining the security posture of Virtual Machines, Networks, and Storage. As customers mature and begin to entrust their PaaS workloads to you, additional opportunities will surface such as the ability to monitor application builds and deployments as well as offer additional automation services.

IDENTIFY TARGET MARKET

It is more important now than ever that partners have a well-defined target market. Having a well-defined target market will allow your sales representatives and marketing personnel to focus on selling services to the right customers. As you consider your target demographics, think about:

- What is my ideal customer size?
- Are there specific technology stacks we should stay away from?
- Do I want to target specific market segments (e.g. Financial Services, Government, Healthcare, etc.)?
- Will you market to customers in specific geographic regions?

Build your prospect hit list

Your goal is to build the list of prospects that could potentially turn into customers. To accomplish this, create an awareness campaign to draw attention to your Azure practice, highlight your service offerings, and use your success to earn additional business with your customers and the industry at large.

Use these awareness activities to help generate new customers:

WEBINARS AND PODCASTS

A great way to transfer knowledge, establish yourself as an expert, and pique the interest of potential customers.

REFERRALS

Ask for referrals in email and phone calls when talking with existing customers, partners, and vendors who might know someone who is ready for your services.

WHITE PAPERS

These are a great way to build credibility with decision makers. Technical staff often expect a white paper to help them understand underlying architecture and technology of your solutions.

NEWS ARTICLES

Leverage public relation efforts to drive publicity around your technology, things your company is doing in the market, and other topics of current interest.

SOCIAL MEDIA

Social media such as Twitter, LinkedIn, etc., is a place to build awareness, reputation, and customer satisfaction — and gain new customers.

Also, consider offering your services as a pilot project to your prospects. With a pilot project, the customer receives two important values. First, they get to better understand how the project goals will be successful. Second, they have a production-grade starting point for their larger efforts.

It is important to keep the distinction between proof-of-concept (PoC) and pilot clear. A PoC should never be considered for direct deployment into production; whereas a pilot should be constructed with a production release in mind.

Case Study

BRISTOW GROUP

For many enterprises, mobility is one of a number of strategies used to help create a competitive business environment. For Bristow Group, the leading provider of industrial aviation services in the world, mobility is the whole point. More than half of the company's nearly 5,000 employees are either flying or maintaining helicopters on any given day.

[Read the case study](#)

Define Engagement Process



Pre-Sales, Post-Sales, and Support

For your practice, you should define the technical effort required before the sale (pre-sales), after the sale (post-sales), and in support of the sale. You will need to decide on the technical pre-sales and post-sales requirements for your solution offer.

PRE-SALES

The technical effort required to make the sale involves:

- Discuss the customer requirements and address their objections.
- Develop technical pitch decks. Leverage the [Cloud Adoption Framework](#).
- Technical demo: This demo may be generic or may need customization to better meet the requirements of the customer. The goal of the technical demo is to inspire confidence in your ability to deliver the desired solution by demonstrating you have "already done something like it before."

POST SALES

The technical effort required after the sale includes:

- Addressing follow-on customer concerns about the technology or implementation.
- Providing training to increase awareness of the solution that will be implemented.

- Providing a technical demo more customized for the customer to better understand their needs before moving on to the next phase of the project.
- Following up with the customer to ensure implementation is on track and meeting expectations.

For guidance with sales efforts, consider the learning paths available in the Microsoft Partner Network [Learning Portal](#).

SUPPORT

Define your customer support program and processes. This includes:

- Defining your support model
- Provisioning your support infrastructure
- Defining and implementing your escalation process
- Selecting and enabling your support options for Azure

Microsoft also provides support for technical presales and deployment services.

Define Service Offerings

It is important to understand the cloud business models and that not all revenue streams are equal.

THERE ARE FOUR WAYS TO MAKE MONEY SELLING CLOUD:

- Resale
- Project Services
- Managed Services
- Packaged IP

Partners that focus almost entirely on product revenue have the biggest barrier, and typically see margins in the range of 5–20%. This is because the margins for this revenue line are tied to vendor incentives. These partners are subject to changes in strategy and the desire to fund programs, and have the least control over their own destiny.

Project services typically drive a range of approximately 35% gross margin, but this has been under pressure for some time. This is a result of little differentiation in the channel, which has caused billable price points to hold steady over the past five or more years. Concurrently, increasing salary and benefit costs of consultants and inflation have eroded profitability.

As a result, aggressive and entrepreneurial members of the channel have adapted and gone after the higher margin opportunities of managed services, which

generate on average 45% gross margin and packaged IP, which often exceeds 70%.

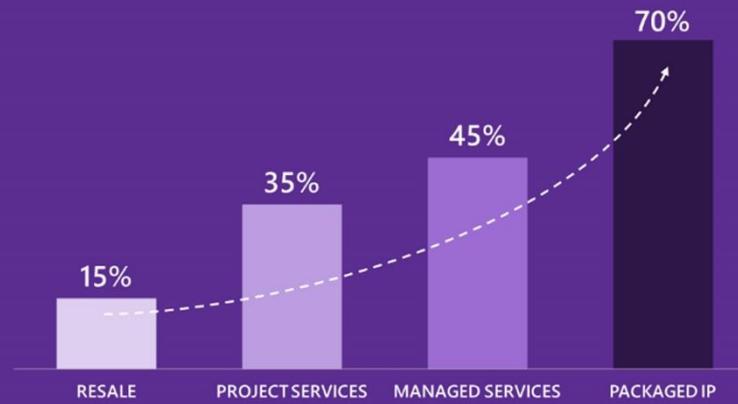
It is these partners who are setting themselves up to be rewarded. The mergers and acquisitions space is quite active. The partners who gravitated toward the recurring revenue lines and realized healthy growth are being presented with much higher valuations. This can have a dramatic increase in the cash event of the company and overall shareholder value — far higher than what a traditional partner focused on product and billable services can realize.

A business plan is a critical asset that can help you envision and think through the details of your practice, identify gaps you will need to address, and explain the fundamentals of your practice to others. Leverage the [Cloud Practice – Develop a Business Plan](#) guide for details, profitability scenario overviews, business plan templates, and financial models.

Read on to understand what types of project services, managed services, and intellectual property you should be considering in your operations and management practice, and leverage the [Define and Design Your Solution Offer guide](#) to understand how to define your value proposition, solution and vertical offerings, and partnership opportunities.

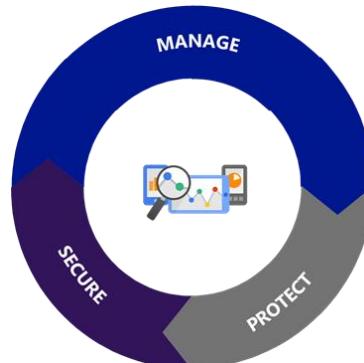
Not all revenue streams are created equal

AVERAGE GROSS MARGINS



Azure Security and Management

Azure offers many services for visibility and control across your customers environment – from their on-premises datacenter to the cloud. Partners can offer services that help their customers manage, protect, and secure their workloads no matter where they reside.



MANAGE

Azure Monitor, Log Analytics, Application Insights, and Azure Automation are the core Azure services which comprise the management stack. Each of these services can help customers gain visibility into their environments, reduce mean time to resolution when errors do occur, and improve the performance and usability of the applications that they deploy in Azure.

COMPREHENSIVE VISIBILITY



Comprehensive visibility across platform, apps and workloads
Collect and correlate data from multiple sources incl. multi-vendor solutions
Gain insights to act on using machine learning and advanced analytics



REDUCED MEAN TIME TO RESOLUTION

Visualize and alert on the health, performance and utilization
Discover app and network components and map their connections
Detect and respond to issues before they impact your users



IMPROVED PERFORMANCE AND USABILITY

Learn, iterate, and improve the performance and usability of your apps



CHANGE AND UPDATE MANAGEMENT

Install OS patches
Track virtual machine changes
Automatically track inventory changes

Azure Monitor

All the monitoring data you need to operate and maintain your Azure resources is centrally available through Azure Monitor.



Azure Monitor provides base-level infrastructure metrics and logs for most services in Microsoft Azure. Azure Monitor is one of several core monitoring services in Azure and provides fundamental, required monitoring across Azure resources allowing you to:

- Monitor your Azure resources with detailed logs
- Set up alerts and take proactive, automated actions
- Use flexible configuration and data consumption options
- Integrate with analytics and notification tools that are familiar to you and your customers

VIEW AND MANAGE MONITORING DATA

With Azure Monitor, you get detailed, up-to-date performance and utilization data, accessing to the Azure activity log that tracks every API call, and diagnostic logs that help you debug issues for your customers in their Azure resources.

ALERTING AND AUTOMATED ACTIONS

In addition to providing access to your customers performance and utilization data, you can also configure Azure Monitor with alerts and take automated actions based on them. This allows you as partner to be proactive

with your customers workloads that are hosted in Azure by detecting issues before they affect their business. With Azure Monitors automated actions, you can auto-scale resources, start Automation runbooks, and even call webhooks.

DIAGNOSE OPERATIONAL ISSUES QUICKLY

Not all events can automatically be remediated, so Azure Monitor also gives you the tools you need to analyze and diagnose operational issues in your customers' environments so you can resolve them efficiently. You can even create dashboards with graphs of performance metrics, search through subscription activity, and share your insights with your customers.

INTEGRATE WITH EXSTING TOOLS

Azure Monitor also integrates directly with many of the other solutions you'll learn about in this playbook, including Application Insights and Log Analytics. Azure Monitor also integrates with a variety of partner tools, potentially allowing you and your customers to leverage existing vendor relationships and technology investments. As a partner, you can even build your own custom integrations by using REST APIs and webhooks.

Log Analytics

Centralize log data from multiple systems and environments, including those external to Azure, in a single data store.



Log Analytics will allow you to transform both yours and your customer's Azure activity data and managed data resources across different subscriptions into actionable insights. Through Log Analytics, you'll gain deeper insights into your customer's environments hosted in Azure or on-premises with its hybrid capabilities.

- Quickly connect and collect log data from multiple sources
- Correlate and analyze using powerful machine learning constructs
- Search and query interactively using an expressive language
- Develop deep insights use purpose-built management solutions

COLLECT AND CORRELATE DATA FROM MULTIPLE SOURCES

Log Analytics will allow you to correlate data in new ways using powerful joins and a rich query language. With these deep insights, you will be able to concentrate on the data that is important to you, performing advanced date-time analysis. Through Log Analytics near real-time capabilities, you'll be able to quickly identify the root cause of operational issues in your customer subscriptions.

SMART ANALYTICS

Log Analytics interactive query engine also offers one-click diagnosis of performance issues from the advanced analytics portal. With machine learning, partners have access to advanced learning algorithms to detect and mitigate potential issues before they impact your customers.

RICH EXPLORATION WITH INTERACTIVE QUERIES

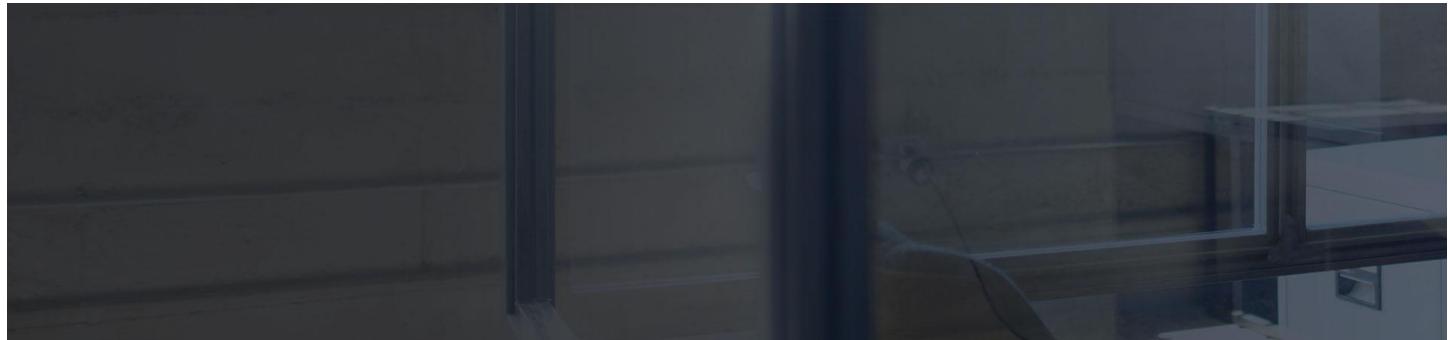
As you build your queries and visualizations, you'll have the ability to combine that data with the data from resources such as Azure Monitor, offering your customers a rich view of the performance of their environments while allowing your operations resources to understand performance and activity in each environment.

BUILT-IN NOTIFICATION AND AUTOMATION

The data that is stored in Log Analytics becomes actionable in the same ways as the data in Azure Monitor, including the ability to natively integrate with service management solutions such as ServiceNow and provides for the correlation of alerts from various sources. The data that is stored in Log Analytics can even be automated, with the ability to trigger remediation through Azure Automation, Logic Apps, and Azure Functions.

Application Insights

Get rich performance monitoring, powerful alerting, and easy-to-consume dashboards to help your customers ensure their applications are available and performing as they expect.



Application Insights allows partners to offer customers a cloud-first and cloud-ready application performance management suite. With Application Insights rich data sets, you will be able to know about issues before they become larger problems, understand who and what are affected, and performance root cause analysis to find and fix issues.

- Detect and diagnose exceptions and application performance issues
- Monitor Azure websites, including those hosted in containers, plus websites on-premises and with other cloud providers
- Seamlessly integrate with your DevOps pipeline using Visual Studio Team Services, GitHub, and our webhooks
- Get started from within Visual Studio, or monitor existing apps without redeploying

APPLICATION PERFORMANCE MANAGEMENT

Data stored in Application Insights can be used show trends in application performance and behavior, identity usage patterns, and get quick answers to questions about website performance. By using the same query engine as that in Log Analytics, partners can leverage the same skillset for operators across multiple solutions.

INTERACTIVE DATA ANALYTICS

The data in Application Insights is powerful on its own, but like many other Azure services, it can be combined with Log Analytics, offering partners the ability to aggregate

application performance data, Azure activity logs, and operational data from Azure virtual machines in a single data set.

MACHINE LEARNING

Application Insights includes smart detection capabilities, leveraging machine learning and service analytics which continually analyze application telemetry. Through this continual analysis, the Application Insights service can provide anomaly detection, failure counts, performance changes, and even platform behavior analysis. This data can be actioned through the same notification and alerting mechanisms as Azure Monitor and Log Analytics, again providing a familiar interface for operations to interact with Azure.

DEVOPS INTEGRATION

Application Insights can be easily integrated into you or your customers existing DevOps processes. This allows you to bring Application Insights rich monitoring to your continuous integration and continuous delivery pipelines. This includes integrations with Visual Studio Team Services or GitHub for issue tracking and resolution.

GET STARTED QUICKLY

Application Insights is not just for your customers bespoke applications – it can also be used to instrument and understand existing websites hosted in IIS, offering partners the opportunity to onboard customers into the service early in their cloud journey.

Azure Automation

Automate, configure, and install updates across hybrid environments



Azure Automation delivers a cloud-based automation and configuration service that provides consistent management across your Azure and non-Azure environments. It consists of process automation, update management, and configuration features. Azure Automation provides complete control during deployment, operations, and decommissioning of workloads and resources.

- Control hybrid environments
- Integrate management systems using serverless runbooks
- Ensure consistent management for Windows and Linux

LOWER COSTS THROUGH AUTOMATION

By automating your operations, including tasks for you and your customers, partners can focus on work that drives value for their customers. Azure Automation allows partners to automate all of their frequent, time-consuming, and error-prone cloud management tasks. This leads to lower operational costs.

UPDATE MANAGEMENT

Azure Automation can be combined with Log Analytics to offer a cloud-hosted patch and update management services for both Windows and Linux operating systems. With Azure Automation's hybrid capabilities, update management and compliance can be managed across Azure, on-premises, and even other cloud platforms. The rich orchestration engine also provides for defined maintenance windows, exclusions, and more.

CONFIGURATION MANAGEMENT

Azure Automation offers a first-party virtual machine configuration service hosted in Azure with support for Desired State Configuration (DSC). Along with DSC, the automation service also allows you to author and manage PowerShell configurations, import existing scripts, and generate node configurations – all in the cloud.

INVENTORY MANAGEMENT

Through Azure Automation's inventory and change tracking functions, partners can provide customers full inventories of operating system resources, including installed applications and even custom configuration items. A rich reporting interface with powerful search allows operators to quickly find detailed information on everything that is configured within an operating system – both Windows and Linux.

Inventory changes can also be tracked across Windows services, Linux daemons, software, registry, and individual files to promptly investigate issues. Inventory and change tracking is built on Log Analytics, allowing partners to configure automated alerts to track unwanted changes.

INTEGRATE WITH SERVICES

In addition to configuration management, Azure Automation also offers a rich automation and scheduling service based on runbooks that can be authored in PowerShell or Python. This allows partners to integrate not just other Azure services, but also any public systems that customers require for deploying, configuring, and

managing the end-to-end lifecycle of resources deployed in Microsoft Azure.

These runbooks can be triggered from systems outside of Azure, bringing integrations with existing ITSM, DevOps, and monitoring systems to fulfill requests and ensure continuous delivery and management.

PROTECT

Azure Backup and Azure Site Recovery will allow your customers to experience the benefits of high availability, disaster recovery, and backup. These Azure services allow partners to offer a full suite of services around business continuity and disaster recovery.



REDUCED COST

- No need to purchase additional hardware
- No secondary site resource costs
- Pay for what you use



REDUCED COMPLEXITY

- Faster onboarding with cloud services
- Simpler execution for testing and failover
- Integrated business continuity as a service



INCREASED COMPLIANCE

- Industry-leading certification portfolio
- Deploy in one of Azure's 38 global datacenters
- Increase your coverage of applications to meet your compliance requirements

Azure Backup

Protect your customers data with a cloud-based backup-as-a-service



Azure Backup is the Azure-based service you can use to back up, protect, and restore your customer's data in the Microsoft cloud. Azure Backup replaces existing on-premises or off-site backup solutions with a cloud-based solution that is reliable, secure, and cost-competitive. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure.

- Keep your data in Azure and on-premises safe
- Backup supports all machines, including VMware and Hyper-V virtual machines running on Linux and Windows, as well as physical Windows Servers

REDUCE COSTS

Azure Backup is a pay-as-you-go service, giving partners and customers the flexibility to choose the data that they want to protect for as long as they need to protect it. Azure Backup is designed to be cost-effective for both short-term and long-term data retention scenarios. Virtual machines and individual files or folders can be restored – in Azure or on-premises – as needed, for free.

QUICK ONBOARDING AND DEPLOYMENT

Azure Backup enables hybrid deployment and management of customers environments quickly and

easily. Backup can be used to protect Azure and on-premises workloads and comes with support for Windows, Linux, VMware, and Hyper-V. When deployed into virtualization environments such as VMware, Backup can automatically detect your virtual machines and connect them to Azure.

All of your customer's backup information is surfaced in a centralized dashboard, allowing partners to quickly decide what to restore in an event which generates unexpected data loss. Backup reports can also be exported to Power BI, offering partners richer visualizations and data analysis, along with the ability to share deeper insights with their customers.

RANSOMWARE PROTECTION

In the age of ransomware, customers can never be too careful with their data. Azure Backup allows partners to offer customers piece of mind that their backups are secured through limited access controls, automated notifications if suspicious activity is detected in a Recovery Services vault, and unauthorized deletions are kept for days, providing ample time to secure the environment and start the recovery process.

**RANSOMWARE ATTACKS
OCCUR EVERY 40 SECONDS**

**4,000 DAILY ATTACKS SINCE
2016**

300% INCREASE OVER 2015

**\$5 BILLION DAMAGES
PREDICTED IN 2017**

15X INCREASE OVER 2015

Sources: <https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/>, <https://www.justice.gov/criminal-ccips/file/872771/download>, <https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/>

Azure Site Recovery

Reduce application downtime during IT interruptions, without compromising compliance. Azure Site Recovery supports applications in Azure and on-premises, providing comprehensive coverage across Linux, Windows, VMware and Hyper-V virtual machines, and physical servers.

Azure Site Recovery (ASR) contributes to the business continuity and disaster recovery services you will be able to offer your customers. The Site Recovery service helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines from a primary site (Azure or on-premises) to a secondary location (Azure or on-premises). When an outage occurs at your primary site, you fail over to secondary location, and access hosted workloads from there. After the primary location is running again, you can fail back to it.

REDUCE INFRASTRUCTURE COSTS

As a partner you can offer your customers lower on-premises infrastructure costs by using Azure as a secondary site for conducting business during outages. Or, you can help your customers eliminate their on-premises costs altogether by moving their workloads to Azure and setting up recovery between Azure regions. ASR allows you to perform discovery on your customer environments so you can pre-assess network, storage, and compute resources needed to replicate and run applications all while paying for only compute and networking resources needed to run customer workloads in Azure during outages (while running).

SIMPLE DEPLOYMENT AND MANAGEMENT

Replicating applications and workloads between Azure regions can be accomplished in just three steps. When it comes to orchestrating a failover, there are often multiple steps and sequencing issues. ASR integrates with Azure Automation, offering partners and customers a wide range of automation options and integrations to orchestrate the recovery of even the most complex multi-tier applications.

TRUSTED RECOVERY

Recovery and backups are only good when they are tested and vetted on a regular basis. ASR makes it easy to test failovers and integrity of failover solutions with isolated recovery options. This allows you to test your recovery scenario end-to-end without impacting production workloads or end-users.

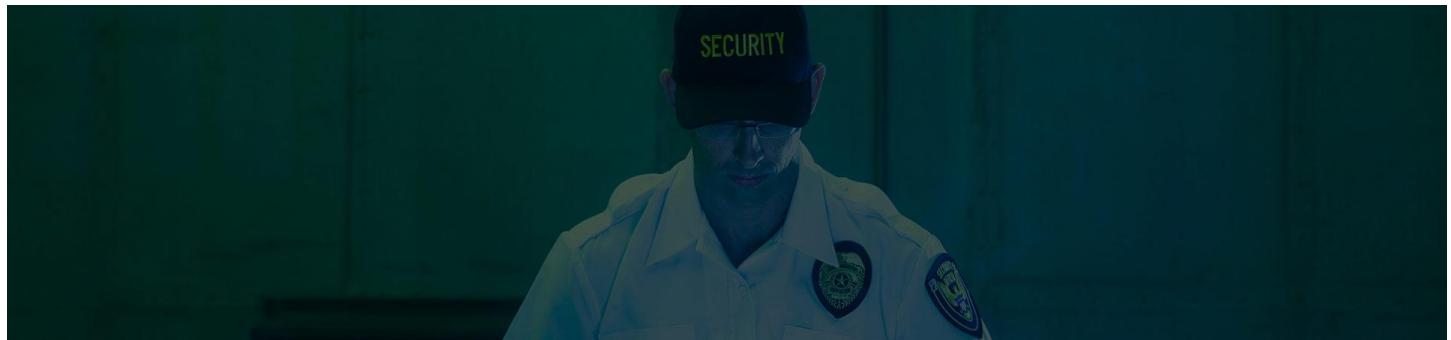
AUTOMATED RECOVERY

After ASR has been deployed, configured, orchestrated, and tested, you can configure automated recovery of applications to Azure with minimal downtime. ASR is backed by a 99.9 percent SLA and 24x7 support to ensure your partners can offer customers the confidence that their applications will be available and compliant.

"Before, it could take months and potentially millions of dollars to replicate infrastructure and recover data after a disaster, in addition to suffering disruption of business operations. Now we can recover instantly and at no cost" - Jim Slattery, Chief Financial Officer, Capstone Mining

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks.



Azure Security Center offers partners the ability to ensure their customers' deployments are secured with centralized policy management, continuous security assessment, actionable recommendations, advanced cloud defenses, prioritized alerts and incidents, and integrations with connected solutions.

- Monitor security across on-premises and cloud workloads
- Apply policy to ensure compliance with security standards
- Find and fix vulnerabilities before they can be exploited
- Use access and application controls to block malicious activity
- Leverage advanced analytics and threat intelligence to detect attacks
- Simplify investigation for rapid threat response

UNDERSTAND SECURITY POSTURE

Azure Security Center (ASC) brings a unified view of security across your customer's on-premises and Azure-hosted workloads. ASC integrates with Log Analytics, offering automated onboarding of new Azure virtual machines and automated discovery of other Azure resources like Azure Storage and Application Insights. The collected data can include other solutions as well, including next-generation firewalls and other marketplace solutions.

ENSURE COMPLIANCE AND SECURITY STANDARDS

ASC can help you make sure compliance with your customer's or regulatory security requirements by centrally managing security policies across all of their hybrid cloud workloads. Security policies define the desired configuration of your customer workloads and can be tailored to the type of workload or the sensitivity of the data hosted within those workloads.

FIND AND REMEDIATE VULNERABILITIES

By continuously monitoring the security of your customer's machines, networks, and Azure services ASC can surface vulnerabilities quickly and, in many cases, offer automated remediation. In cases where automatic remediation is not available, ASC will guide you through the steps to remediate vulnerabilities and ensure your customer environments are secure.

LIMIT THREAT EXPOSURE

Go beyond the basics and offer your customers advanced protection, including adaptive threat protect and application whitelisting that allow you to block malware and other unwanted code. Powered by machine learning, these application controls are constantly monitored for compliance.

In addition, you can enable advanced networking and virtual machine management features such as just-in-time

access, allowing you to control access to management ports on Azure-hosted virtual machines to drastically reduce the surface area exposed to brute force and other network attacks.

RESPOND QUICKLY TO ATTACKS

Partners and their customers can leverage the Microsoft Security Graph to get ahead of evolving cyber-attacks, including denial of service attacks and botnets. The built-in behavioral analytics and machine learning can automatically identify attacks and zero-day exploits and make you aware immediately. ASC also bridges pre and post-breach activity by monitoring your networks, machines, and cloud services.

SECURE

Azure Security Center, network security appliances, and advanced networking features of Azure allow partners to secure customer workloads and offer on-going management services around the Azure security stack.

GAIN VISIBILITY AND CONTROL



- Unified view of security across your Azure resources
- Central management of security policies
- Integrate with existing processes and tools like SIEM

PROTECT AGAINST ATTACKS



- Remediate vulnerabilities with ongoing assessment and recommendations
- Rapidly deploy built-in security controls and integrated partner solutions
- Reduce attack surface with predictive analytics

DETECT THREATS AND RESPOND EARLY



- Identify real threats with advanced analytics
- Gain insight into attack campaign with Intelligent Security Graph
- Remediate quickly with prioritized alerts and recommendations

Azure Network Appliances

Use your favorite network virtual appliances in Azure

Azure includes a rich networking stack, with security built-in from the ground up from design, development, monitoring, threat intelligence, and response. Network access control lists (ACLs) can be configured to restrict access on public endpoint IP addresses. ACLs configured on endpoints can further restrict the traffic to only specific sources IP addresses.

Network Security Groups (NSGs) control network access to virtual machines in virtual networks. This collection of network ACLs allows a full five-tuple (source IP address, source port, destination IP address, destination port, protocol) set of rules to be applied to all traffic that enters or exits a subnet or a virtual machine's network interface. The NSGs, associated to a subnet or VM, are enforced by Azure's networking stack.

To further bolster network security, a large number of solution providers offer network virtual appliances (NVAs) in the Azure Marketplace. NVAs bring next-general firewalls, intrusion prevention and intrusion detection systems, web application firewalls, and more to Azure.

- Industries best-of-breed appliances
- Easy to configure and manage
- Easily scalable and highly available

SIMPLIFY CUSTOMER MIGRATIONS

The Azure Marketplace allows partners and customers to use the brands you already know and leverage existing vendor relationships to bring familiar network appliances to Azure. These virtual machine images allow you to bring the networking security, and other functions of the providers your teams already know.

DEPLOY ADVANCED NETWORK SCENARIOS

Existing customer environments can be complex, but NVAs allow partners to build and maintain complex configurations which keeps customers security and compliance requirements front and center. By combining NVAs with core Azure networking features like user-defined routes and forced tunneling in hybrid scenarios, partners can offer customers similar network controls as they have on-premises today and in many cases improve their security posture.



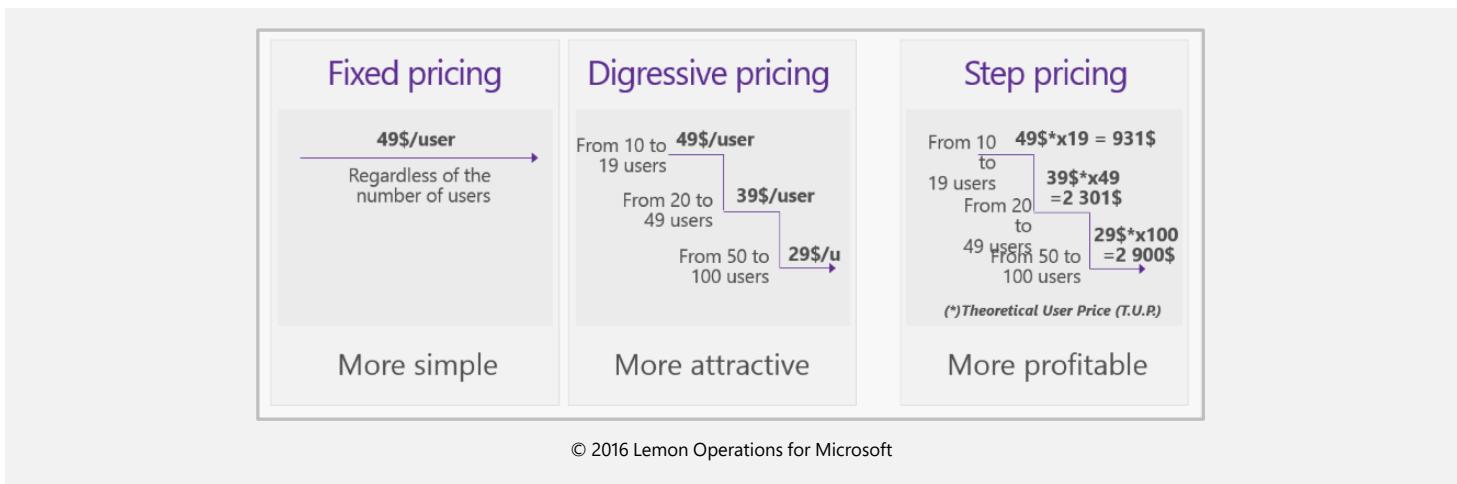
Check Point
SOFTWARE TECHNOLOGIES LTD.



Define Your Pricing Strategy

Pricing your offer is no longer determined simply by cost plus margin.

Pricing a product or offering is different in today's marketplace. Increasingly it is about return on value (ROV) — the added benefits (e.g., better per-unit price, improved service characteristics) your customer gets by being a better customer of yours (e.g., buying contracts with longer durations, making upfront payments, etc.). Customers will only pay as much as the value they estimate they will get from the offering. Price is rarely mentioned on service provider websites. The sales copy speaks of partnerships and the price is often revealed only after speaking to a sales representative. In an offer-based strategy, this will not work. In the business of cloud, price is always disclosed up front. Because price is part of your value proposition and solution offer, your pricing is something you can be proud of and share. Remember you are in a race against yourself and the competition. Be proud and show your price early, removing any customer concerns. Pricing is now a result of the product, and it begins with your value proposition. To understand how to price your offers, let's review the pricing strategies to see the benefit they bring to your solution offer.



STANDARD PRICING

Pricing is the consequence of the product and aligns to the accepted industry/application standard. Think of this as reference pricing; as in customers have seen similar products sold for this amount, so you price your offer so that it is similar. What's the standard price for a mobile phone app? \$0.99. If you charge more, you are breaking from the industry accepted, standard pricing. This is an old way to look at pricing. Buyers today will accept this model, but they do not prefer it and it provides minimal help in getting your offer purchased.

VIRTUOUS PRICING

Virtuous pricing is about using the price as a sales weapon. The goal of virtuous pricing is to create a virtuous sales cycle within your customers, where each sale encourages the next sale within the customer organization. It fosters product adoption and proliferation. Let's begin with a counter example of what is not virtuous pricing — a fixed price per user. Here, you have a simple pricing structure (which is important), but there is nothing to encourage more aggressive purchasing by the customer.

Enter digressive pricing, which drops the per-unit price with the purchase of more units. Your customers get a discount per unit price the more they buy. This can help create a virtuous sales cycle within the customer because now the customer is looking for ways to bring their cost per unit (e.g., user) down.

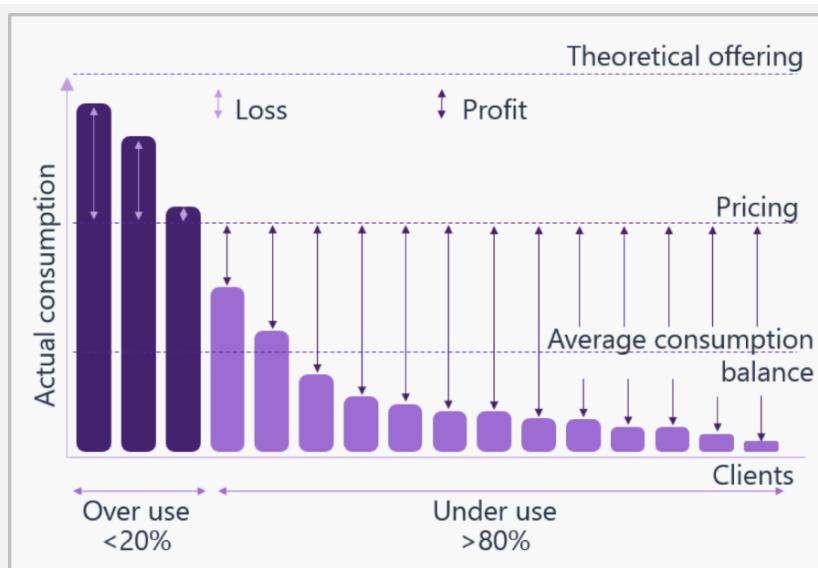
For example, assume one line of business has already purchased 19 users from you at \$49 per user. Now, there are discussions within another line of business within the same customer organization to purchase a similar product from a competitor or to purchase yours. Your existing customer is incentivized to lobby on your behalf because if the other line of business purchases your product, their cost per user will drop to \$39 per user. And the cycle can continue as each new group evaluates your solution offering.

There is a way to adjust digressive pricing slightly to make it significantly more profitable — step pricing. This method sets the price for each step as the top number of users in the range. Building on the example from digressive pricing, let's say that the customer purchased 15 users. They would pay for the equivalent of 19 users since that is the price for this range of units. Why is this more profitable? Because your customer is effectively paying you for the 4 users they are not using (yet) — which goes straight into your profits. What's more is you have amplified the virtuous sales cycle because the customer wants to get as close to the maximum number of users for the step as possible in order to get the lowest possible cost per unit within the step.

FLAT RATING PRICING

This is one of the most powerful business pricing strategies.

You have probably already experienced it, although you may not have realized. Flat rating pricings is leveraged by banks, insurance, etc., every time you pay premiums. While it can have varying levels of sophistication (banks and insurance firms use sophisticated versions of this based on significant work by their actuaries), the model can be described and implemented in a simple fashion. The basic idea is that you provide a certain quantity of value for a set cost that all customers pay. Some customers may come close to (or even exceed) using the full value of what they pay for, while the rest are nowhere close. A well-crafted model identifies the average consumption across all of your customers, and creates a situation where over 80% of the customers are using less than what they are paying for (and ideally less than the average consumption) and fewer than 20% are using more. You set your price to be above the average consumption. By doing so, clients in the 80% who use less than what they pay for generate your profit. The further they are below the average consumption, the more profit they generate. For the 20% who use more than they pay for, you might take a loss on them individually. However, in the aggregate, the long tail represented by the 80% of customers who do not fully use what they pay for more than covers the cost of your heavy consumers, and these heavy consumers are likely to be your biggest champions. So, there are tangential benefits to supporting their cost. Pricing models built around flat rate pricing have shown between 1.5 and 3 times as much profit as traditional models.



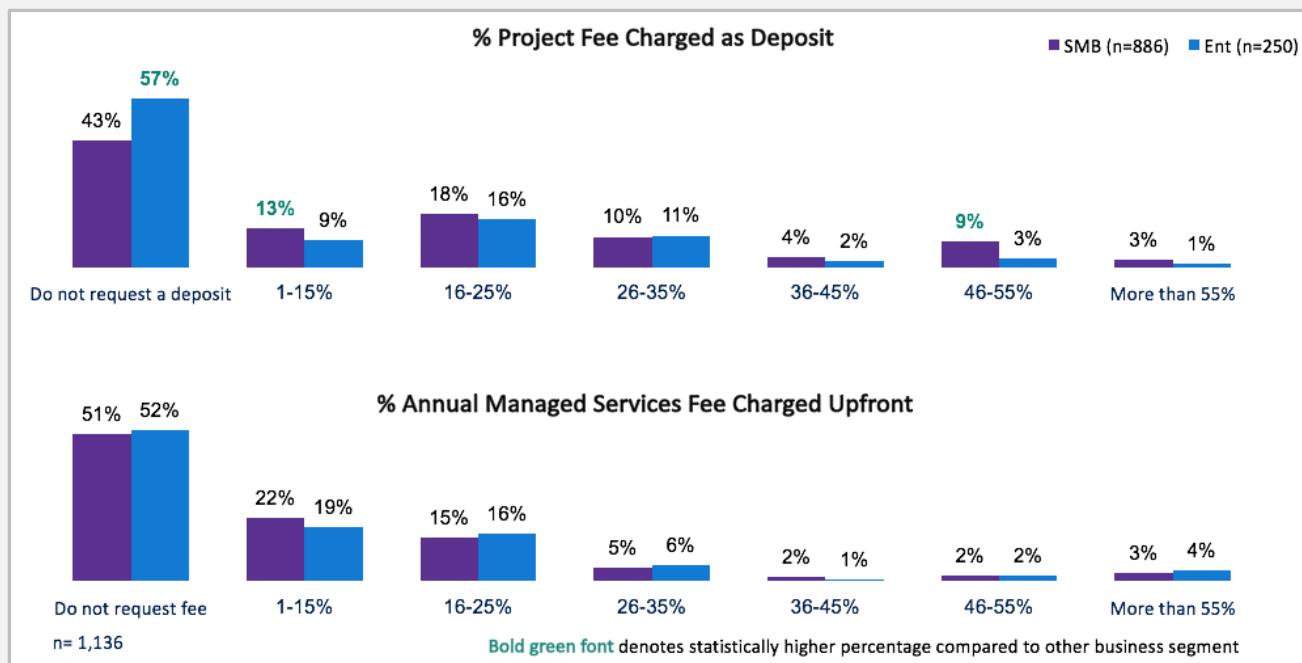
© 2016 Lemon Operations for Microsoft

UPFRONT FEES

Another consideration of your pricing strategy is whether to charge your customers an upfront fee.

Reasons for doing so, including providing some working capital to get resources going in the early days of your practice, mitigate the risk that a customer abandons a project without any payment and ensure the customer is as invested in a project as you are. It can also serve to minimize financial impact to your practice when the customer has requested longer payment terms (see next section).

In our recent survey of 1,136 Azure partners, we found that only about half charged an upfront fee for project or managed services. When an upfront fee was requested, it was typically less than 25% of the total project or managed services fee.



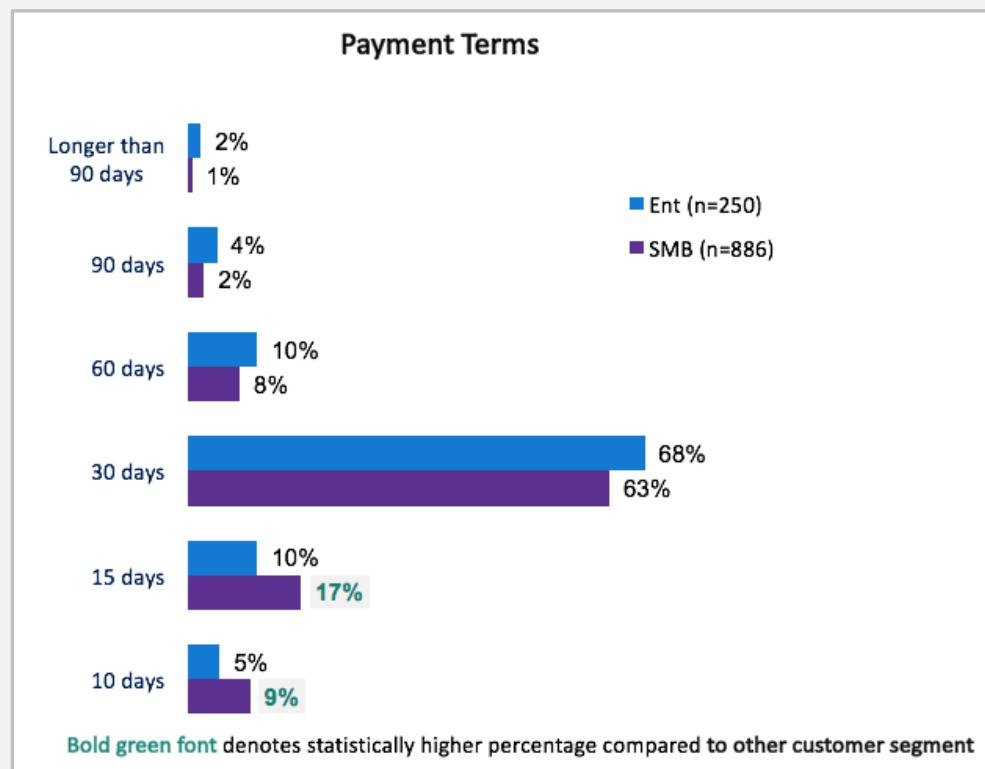
Source: Microsoft Cloud Practice Development Study, MDC Research, November 2016

PAYMENT TERMS

The final consideration for your pricing strategy is the payment terms. This is defined as the duration of time between when you invoice the customer for service rendered and when you receive payment from the customer.

Payment terms are measured in days; for example, 10 days, 15 days, 30 days or 90 days. These are usually expressed as NET 10, NET 15, NET 30 or NET 90 payment terms. In addition, you might consider offering the customer a discount for prompt payment on your shortest payment. For example, NET 2/10/30 is used to describe terms where a 2% discount is provided for payment received within 10 days of invoicing, otherwise the full invoice amount is due in 30 days.

In the Microsoft Cloud Practice Development Study, we found that the most common payment terms used was NET 30, and that for SMB customers shorter payment terms were preferred.

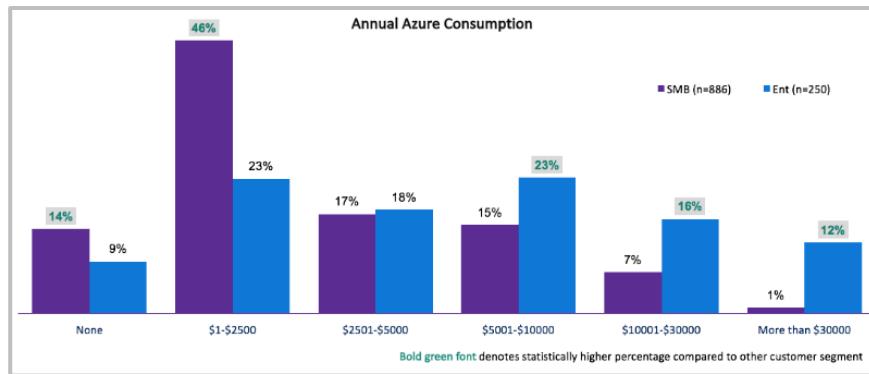


Source: Microsoft Cloud Practice Development Study, MDC Research, November 2016

Calculate Your Azure Practice Costs

Your practice relies on Azure services to deliver customer success, so understanding the Azure related expenses incurred in delivering a customer solution is critical. How do you calculate these Azure costs?

In our research of 1,136 Azure partners, we found that enterprise-focused partners spent a median of \$8,107 in Azure for research and development annually; whereas SMB-focused partners spent a median of \$1,933 annually.



Source: Microsoft Cloud

Practice Development Study, MDC Research, November 2016.

Use the [Azure Pricing Calculator](#) to estimate Azure costs and be sure to check the resources list for pricing on the various services within EMS. You can build an estimate online and export it to Excel for further refinement and analysis. This tool will give you the retail rates (also known as the Pay-As-You-Go option) for Azure services, so treat it like the "high end" of your consumption estimate.

Become familiar with the discounted pricing and Azure credits:

- **Graduated Pricing:** Services like Azure Storage have tiered pricing based upon the volume used. For example, in January 2018, if you used less than 50 TB per month it would cost \$0.0184 per GB per month, but if you used significantly more it could drop to \$0.017 per GB per month.
- **Enterprise Agreement:** By making a three-year monetary commitment, Azure services are available at a discount off retail rates. To learn more, see [Enterprise Agreements](#).
- **Azure Credits:** Microsoft Partners can receive Azure credits as a part of their benefit. For example, partners with the Silver Cloud Platform Competency receive \$500 USD per month in Azure credits; those with Gold

Cloud Platform Competency receive \$1,200 USD per month in Azure credits.

It can be helpful to identify items which are used elastically versus items that have a fixed monthly cost. Significant savings can be achieved via elastic use of resources because you can turn them off (or pause them) when they are not in use.

FOR EXAMPLE

- **Elastic:** SQL Data Warehouse is used only during month-end calculations; it can be paused the rest of the month. Another example of elastic use is to leverage auto-scale capabilities of the resource, such as auto-scaling the number of App Services instances down in the evenings and back up during the workday.
- **Fixed:** Azure App Service hosting your website in a Web App. This App Service needs to run 24x7 because your visitors will arrive at all hours.

Finally, if you don't understand how much of a given resource you will use, consider building a scaled down proof-of-concept to get a first estimate.

Understanding Managed Services

With managed services, you can help your customers on a regular basis by offering white-glove services. As a managed service provider, your offerings can span from planning and enablement to day-to-day operations and support.

Managed services is not a new business model. For more than 20 years, large enterprises have relied on service providers to manage their IT assets. Whether you call them an outsourcer, an RMM provider, or a managed IT provider, service providers have been managing their customers' workloads — either in their own data centers or those operated by their customers. Cloud, however, requires a new method of management because of its focus on scale, elasticity, and automation. For CIOs, cloud represents a paradigm shift in the way they think about embracing IT. Dev-ops has completely changed the way applications are developed and maintained. The hyper-scale nature of cloud provides a completely new meaning to scalability, elasticity and resiliency — and has redefined how applications are architected and delivered. The pay-as-you-go model provides a fail-fast, agile method of app development. Device and data proliferation mean customers want to — and can — do so much more with their IT assets, with cloud providing the computing resources to do so. Because of cloud, CIOs are demanding a new way to think about data governance and security. A cloud MSP is someone who helps their customer transition to (and embrace) this paradigm shift in technology — by guiding them in all aspects of their cloud journey. From consulting to migrations, to operations management, cloud MSPs show customers all the benefits that come with cloud adoption.



PLANNING

- Assess your customer's IT environment and determine risks and policies that are viable security opportunities.
- Deliver ongoing Security Assessments utilizing Secure Score.
- Offer customers a roadmap based on their Secure Score mitigation or recommendations.
- Provide TCO and ROI analysis for moving their security to the cloud.



ENABLEMENT

- Migrate workloads to Azure and Office 365.
- Remediate security gaps found in the Security Assessment Workshop.
- Address security needs across enterprise, including on-premises.
- Optimize security workloads for apps running across on-premises and in Azure and Office 365 cloud environments.
- Optimize advanced security workloads.



SUPPORT OPERATIONS

- Offer further support while delivering on SLAs and uptime guarantees.
- Operate and monitor your customer's Azure, Office 365, and hybrid cloud environments.
- Provide your customers with governance over their cloud strategy by managing their policies.

[Read the MSP Playbook](#)



“

Ensure you are solving a problem. Attach managed services wherever possible and make sure you have a very robust offering around it. This allows for a scalable high margin business.

NICK SONE
CEO of Ensyst



Accelerate your Managed Service Model

The [Microsoft Cloud Solution Provider \(CSP\)](#) program enables partners to directly manage their entire Microsoft cloud customer lifecycle.

Partners in the CSP program utilize in-product tools to directly provision, manage, and support their customer subscriptions. Partners can easily package their own tools, products, and services, and combine them into one monthly or annual customer bill.



CSP DIRECT

The CSP Direct model is great for partners who have the infrastructure in place to do it all. If your business meets these requirements and you are ready to go, [enroll today](#).

CSP DIRECT REQUIREMENT CHECKLIST

- Services business model
- Customer support infrastructure
- Customer billing and invoicing capabilities
- Ability to scale

KEY SERVICES FOR THIS OFFERING

- You are the first point of contact for your customers' needs.
- You own and control the billing cycle.
- You sell integrated offers and services — one sales motion to drive services, attach, and upsell.
- You receive in-product tools to directly provision, manage, and support your customers.

CSP INDIRECT

Spend more time with your customers and provide specialized service offerings. If you're not interested in building an infrastructure to provide customer support and billing, [get connected with an Indirect Provider](#).

For additional details, review the [Azure Managed Services Playbook for CSP Partners](#).

Security as a Managed Service

The current digital security landscape for businesses can accurately be described in one word: complicated. More numerous and advanced threats, more nebulous and complex compliance requirements, more difficult and intricate infrastructure to secure. Simply put, keeping data, workloads, and users secure is more than a full-time job — and organizations are having trouble keeping up. The graphic below illustrates the myriad offerings and postures taken by security companies, highlighting the fragmented nature of the market. However, this harsh environment represents a significant **opportunity for partners looking to offer security as a managed service.**



For even the most adept IT and incident response teams, effectively handling patching, malware threats, and intrusion detection can be too difficult to manage without help. MSPs can offer their services to ensure enterprise clients are secured. But in this age where we hear about security breaches almost daily, how can you help your customers stay ahead of the game, and avoid becoming a statistic?

KEY CUSTOMER CHALLENGES AND QUESTIONS

1. They lack the tools and expertise to effectively get ahead of security threats and compliance risks.
2. They are unable to identify, assess, and mitigate security risks.
3. They are able to detect threats, but are unable to correctly respond in a timely fashion.
4. They are unfamiliar with security best practices and the overall threat landscape.
5. They are confused with the myriad offerings out there.

EXAMPLE OF A SECURITY MANAGED SERVICES OFFERING

Basic	Pro	Premium
\$ per user per month with Office 365	\$\$ per user per month with Office 365 and EM+S	\$\$\$ per user per month with Office 365 Advanced Security & Compliance and EM+S
<ul style="list-style-type: none"> • Plan and deploy Office 365 capabilities • Provide end-user training • Email and data migration to cloud • Deliver end user support and incident management 	<ul style="list-style-type: none"> • Plan and deploy Enterprise Mobility Suite • Increase incident and user support roles • Create monthly services health reports and manage critical IT services dashboards • Enable Advanced Threat Analytics, device management and Identity Management services • + Basic benefits 	<ul style="list-style-type: none"> • Monitor the following services: <ul style="list-style-type: none"> • SaaS app usage • Top targeted users • Unusual signs-ins • Potential threats • Sensitive information sharing to external users • Manage customers security policies including secure score reports • Support data classification policies • +Pro and Basic benefits



SECURITY OFFERINGS	PROTECT	DETECT	RESPOND
Identity	Eliminate passwords, use multi-factor authentication, move to risk-based conditional access	Proactive notification of suspicious behavior and unusual authentications	Automatically elevate access requirements based on risks
Device	Device encryption, management of devices, consistent compliance	Auto-identify suspicious or compromised endpoints	Block, quarantine suspicious devices
Apps & Infrastructure	Identify unsanctioned apps and enforce policies on cloud resources, monitor cloud data	Detect any deviations from baseline, policies, or behavior	Deploy new controls and block risky apps
Data	Policy-based data separation, containment, classification, and encryption	Notification of any attempts for unauthorized data access	Revoke unauthorized access to documents, wipe device data

Support as a Managed Service

It should go without saying that one of the most important functions of your MSP practice is supporting your customer once their applications and data are firmly in the cloud or a hybrid deployment.

No matter how well a cloud or hybrid environment is planned, provisioned, operated or monitored, problems will arise, and those problems will need to be remediated. It's your job as an MSP to offer support to your customers to deal with outages, breaches, inefficiencies, and disaster scenarios. MSPs need to consider the level of support that makes sense for their practice — in terms of resources and revenue — as well as what makes sense to the customers they serve.

KEY CUSTOMER CHALLENGES

- They lack the expertise and resources to troubleshoot problems.
- They are unable to determine the root cause of performance issues and glitches.
- They have no knowledge of how to remediate problems when they correctly identify them.
- They do not want to spend time and resources fixing problems.

KEY SERVICES FOR THIS OFFERING

- **User Support:** Provide support for frequently asked questions, setup and usage, best practices, questions around billing and invoicing, break-fix support for developers, architecture design, and solution design support for architects.
- **System Support:** Provide customers with information on any service interruption, and relay expectations on when the system will be back online.
- **Product Support Support:** Provide support when the Microsoft product is not working as expected or the service stops working. Escalate to Microsoft when

the issue cannot be resolved with existing documentation and/or training.

- **Extended Support Support Hours:** Many customers need the ability for 24/7 support support, but cannot justify the overhead internally.
- **Account Management:** Offering an account manager that is responsible for reporting service consumption and ultimately minimizing time to resolution is a service that can be offered at a premium.
- **Dedicated Support:** The value add of a dedicated support team cannot be understated. Engineering resources that already know your customers' environment, including the business and technical reasons for how a solution was implemented can add a tremendous value over the lifetime of an agreement.

Adding managed support services to your offerings increases your value and profitability. Learn more in this article: [Four ways owning the customer life cycle makes you more profitable](#).



Cloud Monitoring Services

Back in the 2000s, Managed Services was synonymous with Remote Management & Monitoring (RMM).

In the cloud world, the tools and requirements have evolved, but the problem statement hasn't fundamentally changed. How do I monitor the health and performance of my IT infrastructure? There is no easy answer to this and customers expect their service providers to solve it for them. Most mid-market and enterprise organizations simply do not have the time, resources, or dedicated staff required to monitor every aspect of IT, and this is where MSPs add the most value. While Azure offers many monitoring capabilities built within the platform, there is still a place for partners who (a) provide additional, deeper monitoring tooling (b) triage the false positives from the real alerts (c) proactively act upon the alerts before any measurable loss in performance.

KEY CUSTOMER CHALLENGES

- I don't have the time or resources to monitor all my hosted and internal IT assets.
- I need a single pane of glass view that tells me how all my apps and VMs are performing, at any point in time.
- I find it challenging to diagnose the root cause of breakdowns or outages.
- How do I respond to so many alerts? How do I differentiate the false positives from the concerning ones?

KEY SERVICES FOR THIS OFFERING

SYSTEM HEALTH MONITORING	LOG ANALYTICS AND ALERTING	DATABASE MONITORING	APP PERFORMANCE MONITORING
Complete monitoring of VMs, CPU utilization, memory usage, storage IOPs, and OS performance. Includes monitoring of application performance and operation health, and dashboards and reports on system health.	Every client, device, and user accessing a network produces data that is logged. Analyzing those logs can offer deep insight into performance, security, resource consumption, and a number of other meaningful metrics.	A view into your customer's database that helps MSPs ensure high availability of database servers. The process involves keeping logs of size, connection time and users of databases, analyzing use trends, and leveraging data to proactively remediate issues.	End-to-end tracking of all aspects of an application (or webpage). App monitoring involves watching every part — from shopping carts to registration pages — of a customer's app(s) for performance issues in an effort to provide the best user experience possible.

RESOURCES

- ➔ [Azure Advisor](#)
- ➔ [Azure Application Insights](#)
- ➔ [Azure Diagnostics](#)
- ➔ [OMS Log Analytics](#)
- ➔ [System Center](#)
- ➔ [Log Analytics](#)
- ➔ [Automation](#)

THIRD-PARTY RESOURCES

- ➔ [App Dynamics](#)
- ➔ [Nagios](#)
- ➔ [New Relic](#)
- ➔ [Science Logic](#)
- ➔ [Splunk](#)
- ➔ [Logic Monitor](#)

Hybrid Device Management: Manage PCs, Servers and Devices

With the increasing demand to support bring-your-own-device (BYOD) scenarios, organizations are faced with the challenge of finding the right balance between allowing their employees to choose which devices they use, while making sure those devices have access to the right set of applications and meet corporate data protection and compliance requirements.

KEY CUSTOMER CHALLENGES (USER)

- Demand their own choice of devices and apps
- Expect anywhere connectivity and productivity

KEY CUSTOMER CHALLENGES (IT)

- Needs to maintain compliance and data protection
- Must avoid the complexity and cost associated with many discrete management infrastructures

KEY SERVICES FOR THIS OFFERING

	Microsoft's solution builds on market-leading client management by combining System Center Configuration Manager with Microsoft Intune to provide organizations with a comprehensive, cross-platform, and user-centric way to deploy applications and manage users' devices, whether they are corporate-connected or cloud-based.
	With Configuration Manager and Intune, organizations can enable their employees to choose devices, unify management infrastructure, and simplify IT administration. IT can deliver and manage consistent application experiences for employees based on their corporate identity, network connectivity, and device type, helping maintain productivity as employees use various devices throughout their day. Through a single infrastructure and administrative console, IT can manage PCs, servers, mobile devices, endpoint protection, and virtual machines across various platforms, including Windows, Linux/Unix, Mac OS X, iOS, and Android.
	Simplified server and client deployment, streamlined updates, and consolidated reporting enable your IT staff to easily manage your mobile, physical, and virtual client environments, reducing costs and increasing efficiency through comprehensive application and device management. Unified security, including System Center Endpoint Protection, protects your corporate information and helps you better manage risk by deploying software updates and antimalware definitions to PCs, as well as enabling selective wipe of mobile devices. New improvements — such as the support of latest Windows 10 features, Windows in-place upgrade, more frequent and easier updates, unified end-user portal, and on-premises MDM — make deploying and managing Windows easier than ever.

RESOURCES

- ➔ [Managing Corporate Devices](#)
- ➔ [Choose between Microsoft Intune Standalone and Hybrid Mobile Device Management with System Center Configuration Manager](#)

Additional Managed Services Offerings

The project services discussed earlier are all potential offerings in your managed services offering. Beyond those, as an MSP you can offer a much broader set of long-term support and consulting offerings.

In the Microsoft Cloud Practice Development Study, 866 partners that identified as having a cloud infrastructure practice were asked which managed services they offered within their practices. Consider this data when designing your managed services-based offerings.

MANAGED SERVICES OFFERINGS			
Virtual Machine Management & Upgrading	55%	PowerShell Script Automation	33%
Configuration Management	44%	Network Monitoring	33%
Microsoft support (interface between MSFT & customer)	43%	Reporting and Analytics	31%
Domain Management	43%	Critical Response Support	30%
Troubleshooting	43%	Anti-Virus Monitoring	29%
Update & Patch Management	42%	Reports and Dashboard Maintenance	28%
Hybrid Environment Support (Basic Infrastructure)	40%	Security Management & Identity Protection	26%
User Rights & Account Management	40%	Application Lifecycle Management & Support	25%
Azure Consumption Monitoring & Optimization	38%	Virtual Database Administration	25%
Reactive Help Desk Support	37%	Data Center Performance Monitoring & Optimization	25%
Disaster Recovery Monitoring & Testing	37%	Regulatory Compliance via O365 Infrastructure	18%
Performance Monitoring and Reporting	36%	Online Training and Self-Paced learning	13%
Proactive Backups & Anti-Virus Monitoring	36%	We do not offer any of these managed services	11%
Virtualization Support & Efficiency Optimization	34%		

REVENUE	
Total Median (n=118)	\$100,000
BY CUSTOMER FOCUS	
SMB (n=82)	\$75,000
Enterprise (n=36)	\$150,000

Source: Microsoft Cloud Practice Development Study, MDC Research, November 2016.

Understanding Intellectual Property

The idea of coming up with “productized” IP may sound daunting. But many partners found that they already had IP, it just wasn’t packaged that way. If you did something custom that was successful for one client, there may be more customers that would benefit from solving the same problem.

Review your most successful projects to see if there are repeatable elements that you can productize. Repeatable elements can be about your own vertical or process best practices, or else they can focus on common customer pain points. Start small. Your IP can be a simple template or just a few lines of code that automates a particular function in a way your market typically needs. Productizing IP and creating repeatable processes has been a very successful strategy for many partners. Some partners are achieving gross margins in excess of 70% by productizing IP and selling it to their customers on a recurring revenue basis. Productizing IP helps you create stickiness with customers and opens up opportunities to sell your solutions through the partner channel. If you don’t want to create your own IP, you can also look to the partner ecosystem for incremental solutions that can be bundled with Microsoft’s offerings to round out your total solution. There are multiple opportunities for building intellectual property that can be used to expedite engagements, or even as an entire engagement. With the ability to create fully automated solutions partners can challenge their creative side to offer up solutions that can save their customers money as well as add a striking differentiator amongst your peers. In the Microsoft Cloud Practice Development Study, 866 partners that identified as having a cloud infrastructure practice were asked which intellectual property offerings they provide within their practice. The results are below. Consider this data when designing your intellectual property offerings.

INTELLECTUAL PROPERTY OFFERINGS

Automated Backups & Disaster Recovery	34%	Automated Load Balancing	18%
Automated Monitoring, Alerting, & Logging	26%	Automated Consumption Monitoring & Reporting	16%
Office Connectivity & Other Plug-Ins & Add-ons	21%	Automated Disaster Recovery Testing	16%
Customer Self-Serve Portals	20%	Online Training & Self-Paced Learning	13%
Pre-Configured Dashboards	19%	Middleware for Hybrid Synchronization	12%
External Portals for End Customer Information	18%	We do not offer any of these intellectual property	40%

REVENUE

Total Median (n=67) **\$50,000**

BY CUSTOMER FOCUS

SMB (n=45) **\$40,000**

Enterprise (n=22) **\$62,500**

When designing your IP offerings, our research with partners emphasized the importance of targeting the enterprise customer to attain significantly higher managed revenues.

Leveraging Reusable IP In Your Operations Practice

Making money in the cloud usually partially requires you to retain IP to drive annuity. Annuity is a key strategic component to a cloud practice.



DELIVER HIGH-VALUE INTELLECTUAL PROPERTY THROUGH APIs

Microsoft Azure is built on a documented and well-known API that provides a common interface for interacting programmatically with Azure services. Whether through REST APIs, Azure PowerShell, the Azure CLI, or Azure Resource Manager (ARM) Templates, partners can build scripts and applications that interact with [Azure Resource Manager](#). Azure Resource Manager (ARM) enables you to deploy and manage the infrastructure for the solutions you deploy for your customers in Azure.

AZURE POWERSHELL

[Azure PowerShell](#) provides a set of cmdlets that use the [Azure Resource Manager](#) model for managing Azure resources. It can be used in the browser from [Azure Cloud Shell](#) or installed locally and used in any PowerShell session. 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.

A screenshot of the Azure Cloud Shell interface. At the top, there's a dropdown menu labeled "Select environment" with "PowerShell" selected. Below the menu, there are two options: "Cloud Shell..." (highlighted with a red box) and "terminal...". The main area shows a PowerShell session. The output includes:

```
Select environment
PowerShell
Cloud Shell... succeeded.
terminal...

Welcome to Azure Cloud Shell (Preview)
Type "dir" to see your Azure resources
Type "help" to learn about Cloud Shell

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS Azure:\> [REDACTED]
```

Microsoft offers a library of sample scripts which partners and customers can use to begin building a script repository:

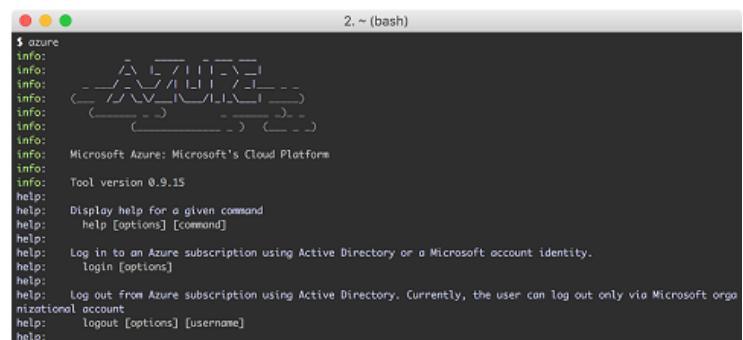
- [Azure Virtual Machine PowerShell Samples - Linux Virtual Machines](#)
- [Azure Virtual Machine PowerShell samples - Windows Virtual Machines](#)
- [Web Apps](#)
- [SQL Databases](#)
- [Cosmos DB](#)

AZURE CLI

The [Azure CLI](#) 2.0 is Azure's command-line experience for managing Azure resources. It can be used from the [Azure Cloud Shell](#) or you can install it on Linux, macOS, and Windows to run it locally. 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](#)
- [Functions](#)
- [SQL Databases](#)
- [PostgreSQL](#)
- [MySQL](#)
- [Cosmos DB](#)
- [Azure Batch](#)



A screenshot of a terminal window titled "2. ~ (bash)". The window displays the output of the Azure CLI command "az --help". The output includes the Azure logo, version information (Tool version 0.9.15), and detailed help for commands like "help", "login", and "logout".

```
$ azure
info: 
info: 
info: 
info: 
info: Microsoft Azure: Microsoft's Cloud Platform
info: 
info: Tool version 0.9.15
help: 
help: Display help for a given command
help:   help [options] [command]
help: 
help: Log in to an Azure subscription using Active Directory or a Microsoft account identity.
help:   login [options]
help: 
help: Log out from Azure subscription using Active Directory. Currently, the user can log out only via Microsoft organizational account
help:   logout [options] [username]
help: 
```

AZURE RESOURCE MANAGER TEMPLATES

Azure Quickstart Templates

Deploy Azure resources through the Azure Resource Manager with community contributed templates to get more done. Deploy, learn, fork and contribute back.



[Azure Resource Manager templates](#) (ARM templates) allow you to create templates (in JSON format) that define the infrastructure and configuration of Azure solutions. By using templates, you can repeat the deployment of customer workloads throughout their lifecycle and have confidence that deployed resources are provisioned in a consistent state.

There are hundreds of community contributed templates available on GitHub in the [Azure Resource Manager QuickStart Templates repository](#). A searchable template index is maintained on Azure.com at [Azure Quickstart Templates](#).

You can download these templates and fork the existing repository to begin to build your own re-usable intellectual property using ARM templates.

PACKAGE YOUR PROCESS

Another way in which partners are creating IP in security practices is by packaging their assessments, documents, and processes into proprietary, reusable components that only they own and can deliver. For example, package a service around security monitoring that relies on the ongoing application and review of Secure Score.

Implement IP in Your Operations and Management Offerings

Consider these tips to start productizing your IP and go to market.

DEFINE YOUR SOLUTION

When we ask partners how they determined what IP they were going to build, we often get the same answer, which is that they realized most of their customers were asking for the same thing or something very similar. And rather than continuing to do high-cost custom work for every customer, they decided to productize what their customers were asking for. Bring your sales, marketing, technical, and delivery teams together to brainstorm and define what your solution will look like.

DETERMINE WHAT WILL DIFFERENTIATE YOUR SOLUTION FROM OTHERS IN THE MARKET

It is important that you think about your differentiation strategy. What is going to make your solution better than other similar solutions in the industry?

MAINTAIN RIGHTS TO THE IP

As partners make the transition from project or custom services to packaged IP, it is critical they revise their customer agreements so the partner can maintain the IP rights to the solutions.

ESTABLISH A RECURRING REVENUE MODEL

The beauty of deploying IP in the cloud space is that you can light up the recurring revenue model, which will have a positive impact on the valuation of your business and even help your cash flows in the future.

CONSIDER YOUR CHANNEL STRATEGY

One of the advantages of productizing your IP is that it opens up a lot of doors to sell your solution through channel partners.



Azure Marketplace

Azure Marketplace is an online store that enables you to offer your solutions to enterprises and Azure customers around the world. Within a single, unified platform, customers can easily search, purchase, and deploy your solutions on Azure with just a few clicks.

[Azure Marketplace](#) is the source for thousands of software applications and services certified by Microsoft to run on Azure. Azure Marketplace supports offers that include virtual machines, developer services, and solution templates.

Azure Marketplace gives your solutions exposure through the marketplace page and the listings integrated with the Azure Portal. For example, HDInsight Applications are integrated into the steps users take to deploy an HDInsight cluster (so users could layer your application atop their HDInsight cluster), but are also available via the Marketplace blade of the Azure Portal.

The process of getting your solution listed in the Azure Marketplace is referred to as getting Microsoft Azure Certified. This comes with benefits, many of which include select benefits from the MPN Silver Cloud Competency.

CERTIFY APPLICATIONS AND SERVICES

Solutions sold in the Azure Marketplace must be [Microsoft Azure Certified](#). This provides assurance to your customers that your offers have been tested for usability, readiness, and compatibility with Azure.

- Access broad-reaching Microsoft marketing channels, and receive co-marketing assistance and promotion outside of your Azure Marketplace listing.
- Leverage technical and business planning support to help you maximize your ROI.
- Utilize a self-service portal that contains ready-to-use marketing resources to enhance your communications and messaging.
- Take advantage of resources, such as the Sales Accelerator Toolkit and credits for display, and search advertising to help drive customer adoption.

Once you identify and select the marketplace to target for promoting or selling your services, and increase your visibility. View the [Integrate into a Marketplace guide](#) for details.

“

Don't be an ostrich.
Cloud makes software
your competitive
advantage. We have
packaged repeatable
projects that are
focused around rapidly
demonstrating value
within the cloud and
identifying the big
transformational
opportunities.

Alex Brown

CEO, 10th Magnitude



Microsoft
Partner
Network

Hire & Train

Cloud Operations
& Management

aka.ms/practiceplaybooks



Executive Summary



In the previous section, you evaluated the various services your business can pursue as you set up or build your Azure Operations and Management practice. Now that you've identified some avenues of success, you may be wondering how to build and train your team.

First, we'll help you define the members of your team and the skills they should bring to the table. If you need to hire to fill gaps, we provide you with detailed job descriptions you can use, as well as ideas on where to look for resources, the factors you should look for in a candidate's skillset, and what you should expect to pay by role and region.

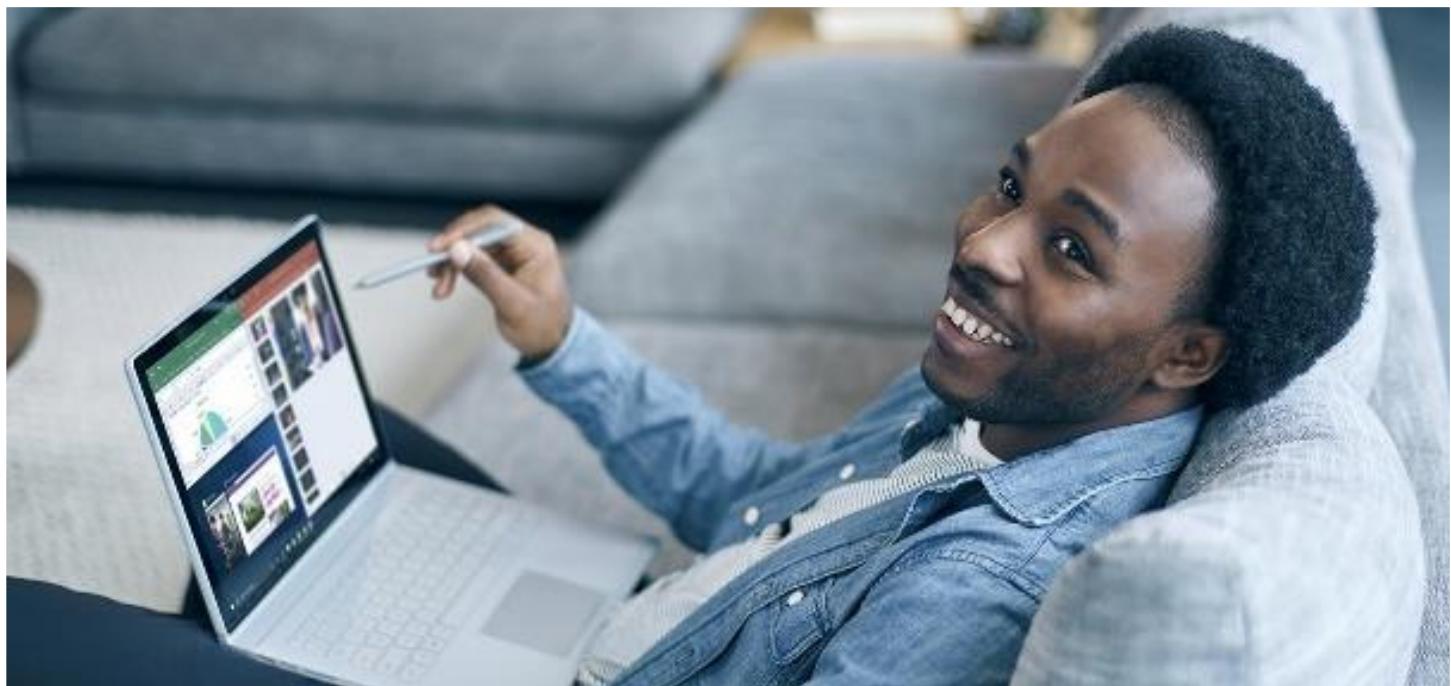
A big focus of this section is the critical piece of ensuring all of your practice resources are trained and continue to receive ongoing training. We cover not just the technical training, but also sales and marketing training.

Additionally, we'll give you details on the specific Microsoft certifications your technical resources should be working towards, both for their own professional development and to earn your organization Microsoft Partner Network competencies.

TOP 5 THINGS TO DO

You're crafting your gameplan to build your team, make sure you nail down these 5 tasks before you move to the next section.

- Define the members and roles required
- Identify capability and skills gaps
- Decide which skills to hire and train
- Hire to fill gaps in your team
- Train and certify your team



Create a Hiring Plan

Human resources are a critical asset to any services-based practice. Starting a new practice requires you to start with an evaluation of your existing team members (if any) and then make the decision of whether to hire new employees or bring your existing team up to speed.

The following sections describe the recommended resources across sales, technical and support functions that you will likely need. In many practices that are just getting started you may not be able to fill all roles with individual professionals. In this situation one person will likely be required to fulfill the duties of multiple roles.

Partner Skillsets

Referrals and LinkedIn are top sources for identifying skilled labor. Once a candidate is identified, work history, cultural fit, and years of experience become the important considerations.

Roles associated with cloud practices typically have at least 3 years of experience. Furthermore, most companies engage in at least annual ongoing staff learning efforts like conferences/events and online training. A median of 8.5% of technical resource time is spent on training.



Hire, Build, and Train Your Team



Sales Resources

You have a vision for developing the next great operations and management solution, but even the best products need a sales strategy to gain maximum market traction. Consider hiring for the following sales positions for broad reach.

The **Solution Sales Manager** (SSM) is a senior leader within the enterprise sales organization. The SSM leads, develops, and manages a team of high-performing sales and technical pre-sales/post-sales resources to drive solution opportunity revenue and market share by leveraging the Microsoft Products and Cloud offerings to meet their customers' Mission Critical Tier1 needs. Ten or more years of sales experience is required for this position. Qualifications include people management, business development, competitive selling, and the ability to thrive in complex, ambiguous, and dynamic environments.

The **Cloud Solutions Sales Manager** is a solution sales leadership role that is responsible for delivering sustainable new business growth across segments; providing thought-leadership; and driving customer acceleration to cloud and mobility across the enterprise sales and marketing teams. The Solution Sales Manager is a great sales coach and leader, has a challenger mentality,

is savvy in sales leadership practice, and contributes with vision and flawless execution of solution sales across workloads and solution areas.

The **Technical Sales Manager** (TSM) is a senior leader within the enterprise sales organization. A TSM drives revenue and market share by leading a team of technical sellers that provide customers with insights and solutions. The Technical Sales Manager will manage, coach, and lead a team of solution architects and tech sales professionals to uncover and support the business and IT goals of customers by driving the technical decision and providing business value with the Microsoft platform, thus securing long-term sustainable growth. A computer science degree or related field is required for this role. Additional qualifications include strategic insight, project management, analytical problem solving, customer/partner relationship building, and exceptional product and technical expertise.

Service Delivery (Architecture, Infrastructure, and Development)

These roles form the heart of your solution. Hiring the right people can turn your vision into reality.

A **Cloud Architect** (CA) drives customer initiatives in collaboration with customers. The CA is a technical, customer-facing role that is accountable for the end-to-end customer cloud deployment experience. CAs own the technical customer 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. A computer science or related engineering degree is required.

The **Cloud Engineer** is responsible for the design, implementation, integration, support, and monitoring of your customer deployments in Azure. This individual is responsible for setting up and configuration the Azure infrastructure, including virtual machines, virtual networks, and storage. This engineer will be a crucial component to building out reusable IP as you engage customers and work with them to onboard new workloads to Azure. For those customers who are migrating to Azure, this resource will also be responsible for assisting with the creation of migration plans.

The **Cloud Developer** is responsible for writing secure, scalable, and robust code that uses platform-as-a-service components to build new or modernize existing applications. This individual should be well versed in new capabilities to take advantage of services not available on-premises. Additionally, this individual should also be familiar with automated build tools as well as continuous integration methodologies.

The **DevOps Engineer** is a mix of infrastructure and developer. This individual will author automation artifacts such as templates and scripts along with working with software build pipelines that support Azure services and

infrastructure deployments. They may also function as reliability engineers, working with your development and infrastructure teams to help engineer scalable, resilient, and reliable systems hosted in Azure.

The **Identity Solution Engineer** is responsible for the design, implementation, integration, support, and monitoring of enterprise identity and access control solutions. The ideal candidate should have a diverse understanding of the current state of security best practices, including identity and access control, mobile technology, and best practices throughout a variety of industries. In addition, this individual must have a strong knowledge of identity standards and protocols, as well as a deep skillet with Windows Server Active Directory and industry security solutions.

Service Management Resources

Consider the following management positions if your development effort will involve eight or more technical staff.

In smaller teams, senior-level employees sometimes take on management duties along with their other responsibilities, removing the need for dedicated managers. Regardless, of the number of team members, these roles are a critical component of your service offering and delivery.

The **Reliability Manager** is accountable for the supply and demand of within the Azure fabric for your organization and your customers, including the elastic use of customer resources and shared resources. The Reliability Manager will also align customer implementations to the right security and compliance policies. These individuals will also manage relations with third parties regarding supporting and demand, including Microsoft. Finally, the Reliability Manager will also manage and monitor the thresholds regarding availability, capacity, security, and compliance.

The **Service Delivery Manager** is account for service delivery to one or more customers and is the primary contact for the customers they manage that consume resources in Azure. The Service Manager will manage and communicate your service description and service level agreements to customers as well as monitor service levels.

The Service Manager will also monitor costs across one or more clients and ensure they are clearly communicated. The Service Manager will also function as the primary contact point for non-technical or non-standard requests from customers.

The **Operations Manager** is accountable for the service operations for your customers, including being the face of the operations team for incidents and problems which customers raise. The Operations Manager is responsible for managing environmental runbooks and coordinating the testing of new runbooks, service requests, and scripts. As the owner of the operations team, the Operations Manager is also responsible for monitoring and reporting on the state of the operations team and their performance in resolving customer issues.

Support Resources

A lot of effort goes on behind the scenes, or in positions that involve post-sales customer engagement. To ensure long-term success of your projects, consider hiring some of these support roles.

A **Customer Success Manager** is passionate about engaging your customers and helping them expand their use cases. They have excellent relational skills, and can create win/win environments for all parties they work with. In their day-to-day responsibilities, they own the overall relationship with assigned clients by increasing adoption and ensuring retention and satisfaction. They make a large impact on your enterprise security business by establishing a trusted and strategic advisor relationship with each assigned client, driving continued value of your products and services. The Customer Success Manager will help drive sales by working to identify or develop upsell opportunities. Additionally, they will advocate customer needs and issues cross-departmentally and program manage account escalations. Qualifications include prior experience in customer success or equivalent history of increasing customer satisfaction, adoption, and retention.

A **Quality Assurance (QA) / Test Technician** is thorough and detail-oriented, and should work well with established processes. The primary goal of this role is to help avoid defects in your final product or solution. This

person will be involved throughout the development process and use their intuition to problem solve and identify technical, procedural, and usability concerns. They must take meticulous notes, be organized about recording process steps, and work well with others since they will be coordinating with technical and management teams to ensure that the correct measures are put into place to align the final product with the initial goal.

An **Information Security Analyst** assesses and provides security advice on cloud infrastructure, including network, service, and application components. This role conducts risk assessments and architectural reviews, provides cyber security subject matter expertise, and assists in the building and design of secure solutions. Additional duties may include network and application penetration testing, and support for cyber security investigations, as well as on-call response for cyber security incidents. A computer science or related engineering degree is required, or the equivalent combination of education, professional training, or work experience.

A **Site Reliability Engineer** is responsible for improving the reliability of your solutions across the stack. The Reliability Engineer will follow a problem from start to finish and will provide the expertise to not only identify the root cause of an issue, but also fix it. They will participate in the full incident management lifecycle, including escalation, debugging, communication of resolution, and problem management.

A **Support Specialist** assists customers who are having technical issues with the Azure solutions you deliver, or who need help realizing the full benefit of your solution to help them deliver their cloud-based workloads. They will likely be in a position to help customers navigate the operational challenges of cloud computing, so thoroughly training them on both your solution — and the infrastructure on which it is built — is paramount to their success, and ultimately, your customers' satisfaction. Qualifications include technical support experience and great communication and interpersonal skills (soft skills). Experience with cloud technologies is a major plus.

You will most likely have multiple levels of support specialists, such as Tier 1 and Tier 2 technicians with experience in varying technologies.



Job Descriptions for Your Service Delivery Team

The following tables provides detailed job descriptions you can utilize to hire the key resources. 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 customer cloud deployment experience. CAs own the Azure technical customer 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, and security solutions.
- 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	<ul style="list-style-type: none">• 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.• 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	<ul style="list-style-type: none">• MCSE Cloud Platform and Infrastructure, CompTIA Security+, CISSP, MCSA Cloud Platform Solutions Associate, MCSA Linux on Azure Solutions Associate, AWS Certified Solution Architect• Exam priorities: Architecting Azure Solutions 70-535 (retired), Microsoft Certified Azure Solutions Architect (AZ-300) and AZ-301, or AZ-302
Project Experience Types/Qualities	<ul style="list-style-type: none">• 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 consultative/complex technical sales 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	<ul style="list-style-type: none">• Azure Information Protection, Azure Active Directory, Octa, Auth0, LDAP, OAuth, SAML, Cloud App Security, Firewalls, Office 365, Windows Server Active Directory, Azure AD Connect, Active Directory Federation Services (ADFS), Mobile Iron, Airwatch, iOS, Android, Windows, Azure Virtual Machines, Virtual Networks, ExpressRoute, Operations Management Suite, Azure Site Recovery, Azure Backup, Azure App Services, Azure Storage, Azure Import/Export, Azure SQL Database, Azure Web Jobs, Azure ExpressRoute, MySQL, SQL Server, SQL Server IaaS, SharePoint on Azure, AWS EC2, S3, AWS DirectConnect

CLOUD ENGINEER

A Cloud Engineer is responsible for the design, implementation, integration, support, and monitoring of your customer deployments in Azure. This individual is responsible for setting up and configuring the Azure infrastructure, including virtual machines, virtual networks, and storage. This engineer will be a crucial component to building out reusable IP as you engage customers and work with them to onboard new workloads to Azure. For those customers who are migrating to Azure, this resource will also be responsible for assisting with the creation of migration plans.

Technical Skills	<ul style="list-style-type: none">• Develop Azure solution designs and implementation plans based on customer needs• Familiar with lift-and-shift migrations and migration methodologies for Microsoft Azure• Experience in Azure Compute, Networking, Storage, and Identity• Familiarity with containers, including Docker and Kubernetes• Proficiency in Azure Active Directory, DNS, and Azure hybrid networking
-------------------------	---

	<ul style="list-style-type: none">Working knowledge of PowerShell and shell scripting
Non-Technical Skills	<ul style="list-style-type: none">Existing experience with Azure solution design and implementationUnderstanding of cloud computing technologies (including Microsoft Windows and open source platforms), business drivers, and emerging computing trendsDemonstrated skill building technical relationships with technical resources within customer organizationsStrong communication (verbal and written) and collaboration abilities in addition to technical depthAbility to connect technology with measurable business valueDemonstrate technical thought leadership in customer-facing situations
Certifications	<ul style="list-style-type: none">Exam priorities: Implementing Infrastructure Solutions 70-533 (retired), Microsoft Certified Azure Administrator (AZ-100) and AZ-101 or AZ-102; Developing Azure Solutions 70-532 (retired), Microsoft Certified Azure Developer (AZ-203)
Project Experience Types/Qualities	<ul style="list-style-type: none">Bachelor of Science in Computer Science, Mathematics, Engineering or related degree preferredExperience with lift-and-shift IaaS migrations2+ years design, implementation and/or support of highly distributed applications demonstrating strong architectural skills to ensure availability, reliability, etc.2+ years of success in consultative/complex technical sales and deployment projects (where necessary, managing various stakeholder relationships to get consensus on solution/projects
Technologies	<ul style="list-style-type: none">Azure Information Protection, Azure Active Directory, Octa, Auth0, LDAP, OAuth, SAML, Cloud App Security, Firewalls, Office 365, Windows Server Active Directory, Azure AD Connect, Active Directory Federation Services (ADFS), Mobile Iron, Airwatch, iOS, Android, Windows, Azure Virtual Machines, Virtual Networks, ExpressRoute, Operations Management Suite, Azure Site Recovery, Azure Backup, Azure App Services, Azure Storage, Azure Import/Export, Azure SQL Database, Azure Web Jobs, Azure ExpressRoute, MySQL, SQL Server, SQL Server IaaS, SharePoint on Azure, AWS EC2, S3, AWS DirectConnect



CLOUD DEVELOPER

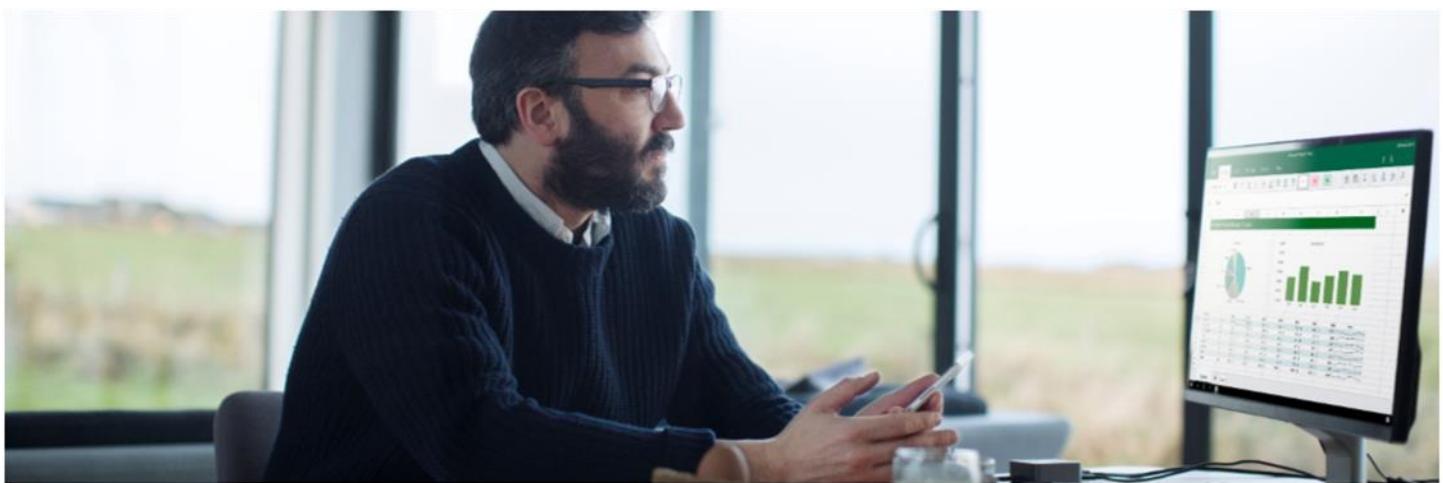
A Cloud Developer is responsible for writing secure, scalable, and robust code that uses platform as a service components to build new or modernize existing applications. This individual should be well versed in new capabilities to take advantage of services not available on-premises. Additionally, this individual should also be familiar with automated build tools as well as continuous integration methodologies.

Technical Skills	<ul style="list-style-type: none">Cloud technologies (with a focus on PaaS), leveraging the Microsoft Cloud Platform (Azure) or experience with Amazon Web ServicesKnowledge of Amazon and Google cloud technologies, third party solutions running on Azure, and the ability to create hybrid and migration scenarios for customers with the Microsoft Azure platformDesigning, architecting, developing and proving cloud based solutions with sustained availability, smart scale, and enterprise grade securityHands-on architecture and development experience with Microsoft .NET platform, Cloud and Mobile technologies, including Open Source software as well as languages (e.g., .Net, Node.js, Python, Java, Objective C/Swift, etc.); Microsoft and Open Source integration technologies and ESB/SOA architecturesDelivering cloud enabled mobile solutions across various platforms and languages (Windows, iOS, Android)Capable in understanding the data domain including Microsoft and Open Source (e.g., SQL, NoSQL, Hadoop, Document DB) to create large, scalable applications.
Non-Technical Skills	<ul style="list-style-type: none">Ability to grasp strategic customer/partner business objective quickly and to articulate solution vision that addresses these objectives
Certifications	<ul style="list-style-type: none">Exam priorities: Developing Microsoft Azure and Web Services 70-487, Developing Microsoft Azure Solutions 70-532 (retired), Microsoft Certified Azure Developer (AZ-203)
Project Experience Types/Qualities	<ul style="list-style-type: none">Bachelor's Degree in Computer Science, Information Technology, or related field or equivalent work experience
Technologies	<ul style="list-style-type: none">Entity framework, Visual Studio, Visual Studio Team Services, WCF Services, Web API, ASP.NET, C#, JavaScript, SAML and OAuth Authentication, Azure Logic Apps, Azure Web Apps, Azure Storage, Azure SQL, Azure SQL Data Warehouse, Azure Data Factory, Azure Mobile Services

DEVOPS ENGINEER

A DevOps Engineer is a mix of infrastructure and developer. This individual will author automation artifacts such as templates and scripts along with working with software build pipelines that support Azure services and infrastructure deployments. They may also function as reliability engineers, working with your development and infrastructure teams to help engineer scalable, resilient, and reliable systems hosted in Azure.

Technical Skills	<ul style="list-style-type: none">• Experience with cloud-based architecture (AWS, Azure etc.)• Strong networking knowledge• Proven knowledge and operation track record for most of these technologies: C#, Powershell, Python, bash, etc.• Familiarity with CI/CD tools such as TeamCity, Jenkins etc.• Hyper-v, VMWare, Azure, AWS, etc.• Kerberos, LDAP, NTLM, TCP/IP, SSL, DNS, HTTP etc.
Non-Technical Skills	<ul style="list-style-type: none">• Existing experience with Azure solution design and implementation• Understanding of cloud computing technologies (including Microsoft Windows and open source platforms), business drivers, and emerging computing trends• Demonstrated skill building technical relationships with technical resources within customer organizations• Strong communication (verbal and written) and collaboration abilities in addition to technical depth• Ability to connect technology with measurable business value• Demonstrate technical thought leadership in customer-facing situations
Certifications	<ul style="list-style-type: none">• DevOps Institute DevOps Foundation® Certification, AWS Certified DevOps Engineer – Professional, Microsoft Professional Program in DevOps
Project Experience Types/Qualities	<ul style="list-style-type: none">• Bachelor's Degree in Computer Science, Information Technology, or related field or equivalent work experience• 3+ years experience in scripting for CI/CD processes (test, automation, build, deployment)• Strong C# .Net development experience• Strong PowerShell scripting experience
Technologies	<ul style="list-style-type: none">• C#, PowerShell, Python, bash, etc.• TeamCity, Jenkins etc.• Hyper-v, VMWare, etc.• Azure, AWS, etc.• Kerberos, LDAP, NTLM, TCP/IP, SSL, DNS, HTTP



IDENTITY SOLUTION ENGINEER

The Identity Solution Engineer is responsible for the design, implementation, integration, support, and monitoring of enterprise identity and access control solutions. The ideal candidate should have a diverse understanding of the current state of security best practices, including identity and access control, mobile technology, and best practices throughout a variety of industries. In addition, this individual must have a strong knowledge of identity standards and protocols as well as a deep skillet with Windows Server Active Directory and industry security solutions. The candidate must have prior experience formulating, planning, and implementing an identity and access control strategy, including formulating policies for the "bring your own device" (BYOD) policy and remote access. The ideal candidate will have a strong understanding of network infrastructure, such as firewalls, proxies, and cross-site connectivity options. 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.
- Experience with Windows Server Active Directory and other LDAP-based directory services.
- Experience with Azure AD and Azure Infrastructure as a Service (Virtual Machines, Virtual Networks).
- Integration and migration experience with Skype for Business, Exchange, SharePoint, and Office 365.
- Experience with Windows, Linux, iOS, Android, Blackberry.
- Experienced troubleshooter, analyzing log files, network traffic, permissions issues, identifying problems with performance and scale.
- Developer experience with .NET, Java, HTML, CSS, JavaScript.

Non-Technical Skills	<ul style="list-style-type: none">• 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.• Basic understanding and knowledge of PCI and SOX regulatory standards.
Certifications	<ul style="list-style-type: none">• MCSE Cloud Platform and Infrastructure, MCSA Cloud Platform Solutions Associate, MCSA Linux on Azure Solutions Associate, CompTIA Security+, CISSP, AWS Certified Solution Architect.• Exam priorities: Identity with Window Server 2016 70-742, Implementing Azure Infrastructure Solutions 70-533 (retired), Microsoft Certified Azure Administrator (AZ-100) and AZ-101 or AZ-102
Project Experience Types/Qualities	<ul style="list-style-type: none">• 3–5+ years senior (tier 3) level support with identity management as part of responsibilities.• 5–8 years of experience with identity architecture and management.• 3–5 years deploying, migrating, or managing an Azure environment or equivalent Office 365 environment using Azure identity.
Technologies	<ul style="list-style-type: none">• Azure Active Directory, Office 365, Windows Server Active Directory Domain Services, ADLDS, Rights Management Server, Microsoft Identity Manager (FIM/MIM), Active Directory Federation Services (ADFS), Active Directory Certificate Services (ADCS), Web App Proxy, Site Minder, Octa, Auth0, WebSphere, Enterprise Mobility Suite, Intune, Azure Information Protection, Azure Active Directory, OAuth, SAML, Cloud App Security, Citrix XenMobile, MobileIron, Airwatch, Blackberry, Firewalls, Office 365, Windows, Linux, iOS, Android, System Center Configuration Manager, Exchange, Skype for Business, SharePoint

RELIABILITY MANAGER

The Reliability Manager is accountable for the supply and demand of within the Azure fabric for your organization and your customers, including the elastic use of customer resources and shared resources. The Reliability Manager will also align customer implementations to the right security and compliance policies. These individuals will also manage relations with third parties regarding supporting and demand, including Microsoft. Finally, the Reliability Manager will also manage and monitor the thresholds regarding availability, capacity, security, and compliance.

Technical Skills	<ul style="list-style-type: none">• Understanding of configuration management and orchestration (e.g. ARM Templates, Chef, Puppet, Terraform, Cloud Formation); container platforms (e.g. Docker, Kubernetes, Mesos, Azure Kubernetes Service, Elastic Container Service); Cloud/PaaS Environments (e.g. AWS, Azure, Google Cloud Platform)• Develops and implements predictive and preventive maintenance strategies
-------------------------	--

	<ul style="list-style-type: none">• Works with operations and support to ensure that customer environments meet required specifications• Defines the strategy for developing reusable frameworks as well as defining the telemetry and operational analytics
Non-Technical Skills	<ul style="list-style-type: none">• Owns results of the people, processes, and technologies that impact the reliability of the operation while fully utilizing the support and reliability resources• Ability to partner with multiple teams to engineer and design customer environments for resiliency
Certifications	<ul style="list-style-type: none">• MCSE Cloud Platform and Infrastructure, CompTIA Security+, CISSP, MCSA Cloud Platform Solutions Associate, MCSA Linux on Azure Solutions Associate, AWS Certified Solution Architect• Exam priorities: Architecting Azure Solutions 70-535 (retired), Microsoft Certified Azure Solutions Architect (AZ-300) and AZ-301, or AZ-302
Project Experience Types/Qualities	<ul style="list-style-type: none">• Bachelor's degree in computer science or related field• 5+ years experience in the systems or software engineering space• 5+ years experience managing engineering teams responsible for supporting and deploying systems for multiple customers or large-scale, complex single customer environments• 3+ years architecting or designing solutions hosted on a major cloud provider• Experience managing multiple hosting environments including public and private cloud solutions
Technologies	AWS, Azure, Google Cloud Platform, ARM Templates, Chef, Puppet, Terraform, Cloud Formation, Docker, Kubernetes, Mesos, Azure Kubernetes Service, Elastic Container Service

SERVICE DELIVERY MANAGER

The Service Delivery Manager is account for service delivery to one or more customers and is the primary contact for the customers they manage that consume resources in Azure. The Service Manager will manage and communicate your service description and service level agreements to customers as well as monitor service levels. The Service Manager will also monitor costs across one or more clients and ensure they are clearly communicated. The Service Manager will also function as the primary contact point for non-technical or non-standard requests from customers.

Technical Skills	<ul style="list-style-type: none">• Experience with cloud computing environments (AWS, Azure, Google Cloud Platform)• Experience in application development in the cloud (AWS, Azure, Google Cloud Platform)• Ability to drive technical teams to the resolution of customer issues• Experience with ITSM systems such as ServiceNow, System Center Service Manager, Provance, or Cherwell
-------------------------	---

Non-Technical Skills	<ul style="list-style-type: none">Ability to present to multiple audiences and levels of an organization from executive leadership to individual team membersAbility to work with multiple stakeholders, including upper management and executive leadershipExcellent customer relations skills to understand and resolve client concerns and requirementsProvides oversight on quality, cost, and schedule for customer projectsCreate and manage service level agreementsCreate and own budgets for solutions hosted for customersExperience managing multiple clients, projects, programsExperience coordinating with 3rd party providers/suppliers for client delivery
Certifications	<ul style="list-style-type: none">ITIL Practitioner or higher certification
Project Experience Types/Qualities	<ul style="list-style-type: none">Bachelor's Degree in Technical/Engineering or equivalent experience4+ years of experience with the delivery of products and/or equivalent program management experience4+ years of client facing infrastructure service delivery/consulting team management2+ years of hands on infrastructure service delivery in cloud operations, data center, networking, security and/or systems administrationExperience managing business requirements, scope, schedule, and budgetsExperience with delivering agreed work within budgetITIL certified
Technologies	Azure, AWS, Microsoft Office, ServiceNow, System Center Service Manager, Provance, Cherwell

OPERATIONS MANAGER

The Operations Manager is accountable for the service operations for your customers, including being the face of the operations team for incidents and problems which customers raise. The Operations Manager is responsible for managing environmental runbooks and coordinating the testing of new runbooks, service requests, and scripts. As the owner of the operations team, the Operations Manager is also responsible for monitoring and reporting on the state of the operations team and their performance in resolving customer issues.

Technical Skills	<ul style="list-style-type: none">Strong technical aptitude with cloud infrastructure and platforms (AWS, Azure, Google Cloud Platform)Understanding of ITIL framework, specifically Change, Incident, Configuration and Problem ManagementKnowledge and experience with Linux, Azure, AWS, Containers, Git, Source control, Splunk, CI/CD and networkingKnowledge of infrastructure monitoring and alerting tools, such as OMS/Log Analytics, System Center Operations Manager, SolarWinds, Logic Monitor, Data Dog or Nagios
-------------------------	---

	<ul style="list-style-type: none">Prior experience working with PowerShell, Perl, Bash, Python, REST APIs, and JSON
Non-Technical Skills	<ul style="list-style-type: none">Analyzes production operations and initiates corrective actions to ensure operational stability across multiple environments and customersCollaborates and coordinates with multiple internal business groups to ensure the successful delivery of service levels (<i>i.e.</i> Service Delivery Managers)Experience in managing varying sizes of projects and/or programs across multiple clientsWorking knowledge of audit and compliance requirementsLeads team innovation to revise and improve operational playbooks and procedures to increase team efficiency and effectiveness, including orchestration and self-healingManages active incidents by organizing the necessary resources to minimize service downtime while keeping leadership and key stakeholders informedFollow-up incidents with post-mortem reviews and problem management actions as required working with Site Reliability EngineersCan create and rationalize operational KPIs, cost management, and other optimization metrics.
Certifications	<ul style="list-style-type: none">ITIL Intermediate or higher certification
Project Experience Types/Qualities	<ul style="list-style-type: none">5+ years experience managing physical operations in a IT and/or other infrastructure environmentExperience leading and managing technical teams, including ongoing talent developmentExperience with and understanding of concepts within systems administration, networking, orchestration, hardware, monitoring, databases, virtualization, release management, and public/private cloud infrastructure and services
Technologies	Linux, Azure, AWS, Mesos, Kubernetes, Git, Jenkins, Ansible, SaltStack, Docker, Python, Splunk, Prometheus, Spark, CI/CD, TCP/IP, Software Defined Networking, SolarWinds, Logic Monitor, Data Dog, Nagios, OMS/Log Analytics, System Center Operations Manager

SITE RELIABILITY ENGINEER

A Site Reliability Engineer is responsible for improving the reliability of your solutions across the stack. The Reliability Engineer will follow a problem from start to finish and will provide the expertise to not only identify the root cause of an issue, but also fix it. They will participate in the full incident management lifecycle, including escalation, debugging, communication of resolution, and problem management.

Technical Skills	<ul style="list-style-type: none">Familiarity with one or more general purpose programming languages including but not limited to: Java, C/C++, C#, Python, JavaScript, PowerShellTroubleshooting skills across network, application, caching, queuing, load-balancing, storage and distributed services layers
-------------------------	--

	<ul style="list-style-type: none">Ability to analyze network and performance monitor traces, application performance problems, and windows application and crash-dump debuggingAbility to conceptualize a distributed service, its dependencies and the transactional flow when troubleshooting
Non-Technical Skills	<ul style="list-style-type: none">Experience coordinating resources across diverse teams to restore service and maintain SLA's, ITIL certification is preferred.Communication skills are a key component of this role with audiences that include customers, peers and at times executive leadershipFirm sense of accountability, ownership for end-to-end project lifecycle with solid project management and communication skills.
Certifications	<ul style="list-style-type: none">MCSE Cloud Platform and Infrastructure, MCSA Cloud Platform Solutions Associate, MCSA Linux on Azure Solutions Associate, CompTIA Security+, CISSP, AWS Certified Solution Architect.Exam priorities: Identity with Window Server 2016 70-742, Developing Microsoft Azure and Web Services 70-487, Implementing Infrastructure Solutions 70-533 (retired), Microsoft Certified Azure Administrator (AZ-100 and AZ-101 or AZ-102); Developing Azure Solutions 70-532 (retired), Microsoft Certified Azure Developer (AZ-203)
Project Experience Types/Qualities	<ul style="list-style-type: none">Minimum of 2 years of software development; automation experience in particular a plusAt least 2 years of experience designing and implementing solutions for platform and application layer telemetry and monitoringExperience in SDLC, distributed systems, networking, hardware, logistics and operations or capacity planningPractical experience running, testing, deploying and supporting large scale services on Azure, AWS or similar environments
Technologies	<ul style="list-style-type: none">Azure, AWS, Software Defined Networking, Application Insights, New Relic, Azure Storing, Windows Server, Linux, Azure Active Directory, PowerShell, Scripting, Desired State Configuration



SUPPORT SPECIALIST

A Support Specialist assists customers who are having technical issues with the Azure solutions you deliver, or who need help realizing the full benefit of your solution to help them deliver their cloud-based workloads. They will likely be in a position to help customers navigate the operational challenges of cloud computing, so thoroughly training them on both your solution and the infrastructure on which it is built is paramount to their success, and ultimately, your customers' satisfaction.

Technical Skills	<ul style="list-style-type: none">Knowledge of infrastructure monitoring and alerting tools, such as OMS/Log Analytics, System Center Operations Manager, SolarWinds, Logic Monitor, Data Dog or NagiosUnderstanding of database technologies, including Microsoft SQL ServerPreferred experience with ITSM systems such as ServiceNow, System Center Service Manager, Provance, or CherwellBasic operating systems knowledge (Windows and Linux)Working knowledge of Hyper-V & other hypervisor platformsUnderstanding of WAN/LAN/VPN and other remote technologies
Non-Technical Skills	<ul style="list-style-type: none">Understanding of incident and problem managementUnderstanding of escalation workflowsAbility to update knowledge base as requiredMaintain a high level of productivity and industry knowledge
Certifications	<ul style="list-style-type: none">Help Desk Institute (HDI) certifications in Customer Service, Support Center Analyst, Technical Support Profession, etc.Exam priorities: Implementing Azure Infrastructure Solutions 70-533 (retired), Microsoft Certified Azure Administrator (AZ-100) and AZ-101 or AZ-102
Project Experience Types/Qualities	<ul style="list-style-type: none">1+ years experience with a major public cloud platform (AWS, Azure, Google Cloud Platform)
Technologies	Azure, AWS, Google Cloud Platform, OMS/Log Analytics, System Center Operations Manager, SolarWinds, Logic Monitor, Data Dog or Nagios, Microsoft SQL Server, ServiceNow, System Center Service Manager, Provance, Cherwell, Windows Server, Linux, Hyper-V,

Reskilling Your Existing Technical Resources

The cloud offers enterprises unprecedented opportunities for agility, innovation, and cost reduction relative to traditional IT. Transforming enterprise IT to take advantage of the cloud requires deep changes to existing IT processes.

DIFFERENCES IN THE CLOUD

Building a cloud practice and keeping the right resources on your staff requires a fundamental shift in the way partners and customers have approached their existing environments. Many organizations have dedicated resources for managing their data centers and on-premises workloads, from application teams to the resources in the data center that are responsible for monitoring heating, ventilation, and cooling.

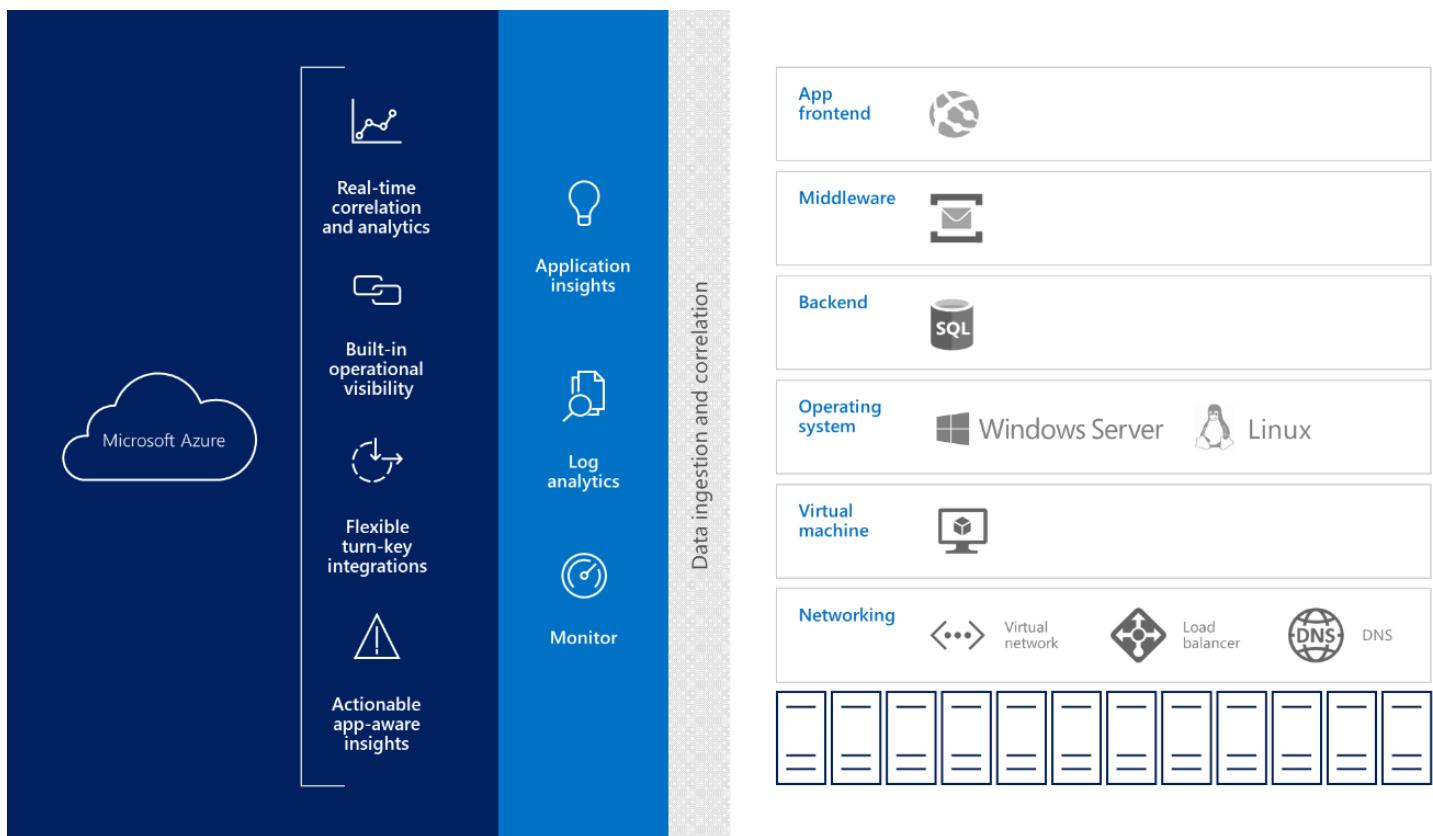


Figure 1: The Azure Difference

PLANNING CAPACITY

Planning, provisioning, and managing compute and storage capacity changes in several meaningful ways. Resources that were responsible for planning the location of racks and servers to meet data center plans no longer have to worry about where a SAN is located or if a rack is going to be close enough to an existing fibre run. In public cloud implementations such as Microsoft Azure, your resources will be managing to the boundaries and limits of Azure subscriptions. Your resources will still need to help customers understand these constraints as well as ensure application architects are designing systems that meet these constraints.

APPLICATION ARCHITECTURE AND DEVELOPMENT

Many applications are not designed for the cloud. As organizations transition to Microsoft Azure, there are opportunities with existing applications to refactor and transform either the entire application or specific components to take advantage of Azure. For instance, a traditional on-premises Microsoft SQL Server database requires not just a server to host the instance, but also the backend storage, networking, and configuration of functionality like clustering to meet customer requirements. In Azure, there are opportunities to transition these workloads over to PaaS services where appropriate, allowing your operations teams more time to focus on the issues that matter.

Through managing less servers and licensing, application architects and developers can now focus on business requirements and objectives for your customers. This brings quicker time to market with faster deployments, lower risk by leveraging platform services with defined SLAs, and the ability to make informed decisions based on the service capabilities.

NETWORKING

Your existing network engineers and networking resources will have to make a transition to the cloud as well. While there will still be a need for resources who understand existing on-premises hardware such as firewalls and routers, there will also be a need for resources who understand software-defined networking.

The networking stack in Azure is very rich, with support for hundreds of networking virtual appliances, including load balancers, next-generation firewalls, and much more. Your resources will need to understand how these virtual appliances can be integrated into your customer deployments as well as understanding the Azure networking stack and how it can be configured to secure and protect your customers.

DEPLOYMENT AND MONITORING

It is critical that your resources understand how to manage deployments in Azure as well as monitor not just deployment health, but also platform health and service availability. Your resources will need to learn new monitoring tools, including Application Insights and Log Analytics and how these tools can integrate both with each other and existing IT service management (ITSM) tools.

This is where the adoption of DevOps becomes critical. As deployments shift from "rack and stack" exercises to declarative provisioning and the creation of infrastructure as code, your resources will need to manage your templates and scripts the same way you would manage the development of an application. This includes treating your templates as source code and storing and managing them appropriately.

HIGH AVAILABILITY, DISASTER RECOVERY, AND BACKUP

Deploying applications and workloads that are highly available is easier than ever with Microsoft Azure. Azure brings unprecedented scale to the public cloud with 50+ Azure regions and availability in 140 countries. However, access to a global infrastructure does not mean that applications can take advantage of it in their current state.

Applications may need to be refactored or rearchitected to take advantage of multiple regions and your resources will need to understand the available services and platform functionality, including Azure Backup, Azure Site Recovery, and Azure Backup.



SECURITY AND COMPLIANCE

One of the best reasons to use Azure for your customer's applications and workloads is to take advantage of its wide array of security tools and capabilities. Microsoft Azure provides confidentiality, integrity, and availability of your customer's data.

Your resources will need to understand and be able to articulate to customers Microsoft's approach to Azure security as well as helping your application developers adopt the right services to make sure the applications they build and deploy are secure from the start.

This includes understanding services like Azure Security Center, Azure Monitor, Application Insights, Azure Advisor, and the networking controls that are available to secure both IaaS and PaaS services.

BUDGETING AND COST CONTROL

As a partner selling services around Microsoft Azure, your resources will need to understand the billing and cost management constructs Microsoft provides for the Azure platform. This will give your clear line of sight to not just your billing, but also downstream billing to your customers.

Up front costing can be determined with tools like the [pricing calculator](#) and the [Total Cost of Ownership \(TCO\) calculator](#). These tools can help you estimate your costs before a workload is even deployed to Azure.

After applications have been deployed, they'll need to be tracked for spend. Your resources will need to understand how to apply core platform governance features such as Azure policy to ensure resources are properly tagged for billing. There are additional tools your resources will need to learn as well, such as [Cost Management](#) (formerly Cloudyn) which are critical to managing your spend in Azure.



Recruiting Resources

Top 10 Sources to Find Skilled Labor and What to Look For

Sourcing skilled labor can be a challenge. In our recent survey with MDC of 1,136 Azure partners, we found that referrals and LinkedIn rank among the top sources for finding candidates. See the table below for the top 10 sources to identify skilled labor:

	TOTAL (n=1136)	SMB (n=886)	ENTERPRISE (n=250)
Referrals from employees or partnerships	70%	69%	73%
LinkedIn	59%	57%	66%
Posting on website	47%	45%	54%
Local Universities	38%	36%	46%
Local Technical Communities	36%	35%	43%
Recruit from competitors	30%	29%	36%
Meet ups	29%	29%	30%
GitHub	8%	8%	7%
Stack Overflow	8%	8%	7%
Other job posting sites	6%	6%	4%

Source: Microsoft Cloud Practice Development Study, MDC Research, November 2016.

Now that you have an understanding of where to look, what are the most important factors to look for in a potential hire's skillset? In the Microsoft Cloud Practice Development Study, we asked the Azure partners this question. What they told us was that the top three most important factors were work history, cultural fit, and years of experience.

	TOTAL (n=1136)	SMB (n=886)	ENTERPRISE (n=250)
Work history	69%	68%	74%
Cultural fit	43%	40%	53%
Years of experience	42%	41%	47%
Professional certifications	32%	34%	22%
Referrals	28%	29%	26%
Professional training received	20%	21%	16%
Reputation through community	16%	15%	19%
Formal education	13%	14%	11%
Contract to hire / other means to test skills "hands-on"	13%	13%	13%
Publications	3%	3%	2%
Awards received	2%	2%	2%
Attitude	0%	0%	1%
Other	4%	4%	4%

Source: Microsoft Cloud Practice Development Study, MDC Research, November 2016.



Training & Readiness

Preparing and Training IT Staff for the Cloud

For IT staff to function as change agents supporting current and emerging cloud technologies, their buy-in for the use and integration of these technologies is needed. For this, staff need three things:

- An understanding of their roles and any changes to their current position.
- Time and resources to explore the technologies.
- An understanding of the business case for the technologies.

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

[Azure Training and Certification](#) provides free online training options including online courses, learning paths, hands-on labs as well as resources to help you find learning partners who can help you achieve your skills development goals using Microsoft Azure services.

[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 Virtual Academy](#) offers training from the people who helped to build Microsoft Azure. From the basic overview to deep technical training, IT staff will learn how to leverage Microsoft Azure for their business.

[Microsoft IT Pro Cloud Essentials](#) is a free annual subscription that includes cloud services, education,

and support benefits. IT Pro Cloud Essentials provides IT implementers with hands-on experience, targeted educational opportunities, and access to experts in areas that matter most to increase knowledge and create a path to career advancement.

[The Microsoft IT Pro Career Center](#) is a free online resource to help map your cloud career path. Learn what industry experts suggest for your cloud role and the skills to get you there.

[Microsoft Learning](#) offers a wide variety of official curriculum on-demand, as well as [edX courses that are taught by Microsoft experts](#), and help you learn through hands-on experiences with a broad reach of Azure technologies.

[The Microsoft Partner Network \(MPN\) Learning Portal](#) provides a centralized interface with training opportunities and certification options organized by products, competencies, certifications, and job role.

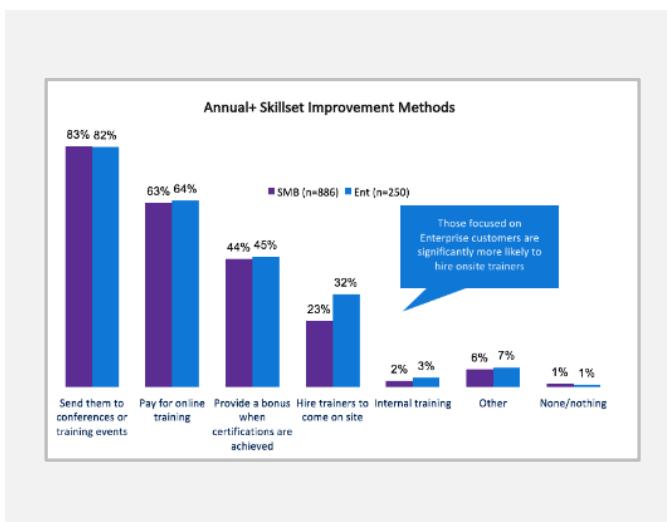
Follow a learning curriculum at your own pace to build the skills you need most to stay relevant. Suggested resources to help onboard your team for training success are available in this section.

General Technical Training

Whether you need to fill a skills gap or are looking to improve your team's skill surface area, technical training is critical to your success.



In our research, we found conferences and paid online training are the most common learning mechanisms.



Source: Microsoft Cloud Practice Development Study, MDC Research, November 2016

aka.ms/practiceplaybooks

CLOUD AND ENTERPRISE PARTNER RESOURCES

The [Cloud and Enterprise Partner Resources Portal](#) provides a source of sales and technical training for partner practices and key areas of specialization. Resources include customer success stories, sales and technical training, tools, engines, and resources available to help build your skills around selling, deploying, and architecting cloud infrastructure and management, cloud application development, data platform and analytics, and security and compliance solutions.

MPN LEARNING PORTAL

The [Microsoft Partner Network \(MPN\) Learning Portal](#) provides a centralized interface with training opportunities and certification options organized by products, competencies, certifications, and job role.

CLOUD + ENTERPRISE UNIVERSITY ONLINE

Leverage the [Cloud + Enterprise University Online](#) to build knowledge, stay sharp, and prove your expertise on selling and supporting Microsoft cloud solutions through our live and on demand webcasts and virtual, instructor-led courses—giving you the flexibility to train at your own pace.

MICROSOFT INSPIRE CONFERENCE RECORDINGS

Even if you missed the annual live event, the [Microsoft Inspire Conference](#) provides many of its sessions as on-demand recordings — no conference pass required.

PARTNER COMMUNITY EVENTS, CALLS & WEBINARS

The [Microsoft Partner Enablement Blog](#) maintains a schedule of trainings available to partners. Visit often and plan your training calendar.

SMART PARTNER MARKETING

Leverage the [Microsoft Smart Partner Marketing](#) site as your starting point for training marketing resources.

Additional Resources

[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.

- [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.
- [Opsgility](#) is a key Microsoft partner that offers Azure and Office 365 training. Find more than 70 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, dev ops, operations, sales and decision makers.
- [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.



“

#1 challenge for the cloud adoption is access to talent. Building a learning culture inside the organization is the success mantra for keeping our azure rockstars up-to-date on the ever improving azure platform.

ANIL SINGH

CEO, Hanu Software

Competencies and Certifications

There are numerous assessments and certifications your team should consider as motivation for advancing their skills, creating proof points for your practice and enabling you to achieve competencies and certifications.

MPN Competencies

One of the next steps is to ensure you align the technical team to the MPN competency for your practice. The competencies most applicable to the Operations and Management practice are:

- Cloud Platform Competency
- DevOps Competency
- Application Development

The following tables summarize the **skill requirements** needed by people in your organization to achieve either a gold or silver competency for the competencies relevant to a SaaS practice. Some competencies have alternative options your organization can elect to meet in order to achieve the competency. You only need to meet the requirements of one option in any given competency.

CLOUD PLATFORM COMPETENCY	SILVER REQUIREMENTS	GOLD REQUIREMENTS
Azure Consumption Option	1 individual must pass one of the following exams: Exam 70-532: Developing Microsoft Azure Solutions (retired) or replacement Exam AZ-203: Developing Solutions for Microsoft Azure Exam 70-533: Implementing Microsoft Azure Infrastructure Solutions (retired) or transition Exam AZ-102: Microsoft Azure Administrator Certification Transition Exam 70-535: Architecting Microsoft Azure Solutions (retired) or transition Exam AZ-302: Microsoft Azure Solution Architect Certification Transition Exam 70-473: Designing and Implementing Cloud Data Platform Solutions Exam 70-475: Designing and Implementing Big Data Analytics Solutions MCSA: Linux on Azure	2 individuals must complete one of the following exams: Exam 70-532: Developing Microsoft Azure Solutions (retired) or replacement Exam AZ-203: Developing Solutions for Microsoft Azure Exam 70-533: Implementing Microsoft Azure Infrastructure Solutions (retired) or transition Exam AZ-102: Microsoft Azure Administrator Certification Transition Exam 70-535: Architecting Microsoft Azure Solutions (retired) or transition Exam AZ-302: Microsoft Azure Solution Architect Certification Transition Exam 70-473: Designing and Implementing Cloud Data Platform Solutions Exam 70-475: Designing and Implementing Big Data Analytics Solutions MCSA: Linux on Azure

DEVOPS COMPETENCY	SILVER REQUIREMENTS	GOLD REQUIREMENTS
DevOps Partner Option	<p>Two individuals must each pass the following assessment:</p> <p>Azure DevOps Assessment</p> <p>OR</p> <p>The following exams will also continue to be accepted as an alternate path for competency qualification until December 31, 2019. However, the preferred path is the Azure DevOps Assessment.</p> <p>Exam 70-496: Visual Studio Team Foundation Server 2012, Administration</p> <p>Exam 70-498: Delivering Continuous Value with Visual Studio Application Lifecycle Management*</p> <p>And, one individual must pass one of the following:</p> <p>Exam 70-497: Software Testing with Visual Studio 2012*</p> <p>*Retiring December 31, 2018.</p>	<p>Four individuals must each pass the following assessment:</p> <p>Azure DevOps Assessment</p> <p>OR</p> <p>The following exams will also continue to be accepted as an alternate path for competency qualification until December 31, 2019. However, the preferred path is the Azure DevOps Assessment.</p> <p>Exam 70-496: Visual Studio Team Foundation Server 2012, Administration</p> <p>Exam 70-498: Delivering Continuous Value with Visual Studio Application Lifecycle Management*</p> <p>And, one individual must pass one of the following:</p> <p>Exam 70-497: Software Testing with Visual Studio 2012*</p> <p>*Retiring December 31, 2018.</p>

APPLICATION DEVELOPMENT COMPETENCY	SILVER REQUIREMENTS	GOLD REQUIREMENTS
Application Builder Option	<p>Two individuals must each pass one exam. They can choose any exam from any of the options below:</p> <p>Azure App Dev Focus</p> <p>Exam 70-532: Developing Microsoft Azure Solutions (retired) or replacement Exam AZ-203: Developing Solutions for Microsoft Azure</p> <p>Exam 70-533: Implementing Microsoft Azure Infrastructure Solutions (retired) or transition Exam AZ-102: Microsoft Azure Administrator Certification Transition</p> <p>Exam 70-487: Developing Microsoft Azure and Web Services</p>	<p>Four individuals must each hold a current version of the following certification:</p> <p>MCSD: App Builder</p>

Certifications

Increase readiness and marketability with MCSA, MCSE, and MCSD certifications.

There are numerous certifications your team should consider as motivation for advancing your skills, creating proof points for your practice, and earning [certification badges](#), and enabling you to achieve Microsoft Partner Network Competencies.

MICROSOFT CERTIFIED SOLUTIONS ASSOCIATE



MCSA RESOURCES

- [MCSA Cloud Platform](#)
- [MCSA Linux on Azure](#)
- [Microsoft Badges from Acclaim](#)

MCSA CLOUD PLATFORM (retired)



MCSA: Cloud Platform
Solutions Associate

Demonstrate your expertise in Microsoft cloud-related technologies to reduce IT costs and deliver more value for the modern business.

Requires any two of the following exams

- [70-532: Developing Microsoft Azure Solutions](#) (retired)
- [70-533: Implementing Microsoft Azure Infrastructure Solutions](#) (retired)
- [70-535: Architecting Microsoft Azure Solutions](#) (retired)
- [70-537: Configuring and Operating a Hybrid Cloud with Microsoft Azure Stack](#)

MCSA LINUX ON AZURE (retired)



MCSA: Linux on Azure
Solutions Associate

Demonstrate your ability to design, architect, implement, and maintain complex cloud-enabled Linux® solutions that leverage Microsoft Azure open source capabilities. This certification also validates your Linux system administration skills to show that you are fluent in today's cloud-native world.

Required Exams

- [70-533: Implementing Microsoft Azure Infrastructure Solutions](#) (retired)
- [Linux Foundation Certified System Administrator](#)

MICROSOFT CERTIFIED SOLUTIONS EXPERT



RESOURCES

- [MCSA Cloud Platform and Infrastructure](#)
- [MCSE Data Management and Analytics](#)

MCSE CLOUD PLATFORM AND INFRASTRUCTURE (retired)



MCSE: Cloud Platform and Infrastructure
Solutions Expert

The Microsoft Certified Solutions Expert (MCSE): Cloud Platform and Infrastructure certification validates that you have the skills needed to run a highly efficient and modern data center, with expertise in cloud technologies, identity management, systems management, virtualization, storage, and networking.

Pre-Requisites:

- [MS Certified Solutions Associate – Window Server 2016](#)
- [MS Certified Solutions Associate – Cloud Platform](#)
- [MS Certified Solutions Associate – Linux on Azure](#)
- [MS Certified Solutions Associate – Windows Server 2012](#)

Choose one of the following Azure exams:

- [70-532: Developing Microsoft Azure Solutions](#) (retired)
- [70-533: Implementing Microsoft Azure Infrastructure Solutions](#) (retired)
- [70-535: Architecting Microsoft Azure Solutions](#) (retired)
- [70-473: Designing and Implementing Cloud Data Platform Solutions](#)
- [70-475: Designing and Implementing Big Data Analytics Solutions](#)
- [70-744: Securing Windows Server 2016](#)
- [70-745: Implementing a Software-Defined Datacentre](#)
- [70-413: Designing and Implementing a Server Infrastructure](#)
- [70-414: Implementing an Advanced Server Infrastructure](#)
- [70-537: Configuring and Operating a Hybrid Cloud with Microsoft Azure Stack](#)
- [70-538: Implementing Microsoft Azure DevOps Solutions](#)
- [70-539: Managing Linux Workloads on Azure](#)

MCSE DATA MANAGEMENT AND ANALYTICS



MCSE: Data Management and Analytics
Solutions Expert

Demonstrate your broad skillset in SQL administration, building enterprise-scale data solutions and leveraging business intelligence data — both on-premises and in cloud environments.

Pre-Requisites:

- [Microsoft Certified Solutions Architect – SQL Server 2012/2014](#)
- [Microsoft Certified Solutions Architect – SQL Server 2016 Database Administration](#)
- [Microsoft Certified Solutions Architect – SQL Server 2016 Database Development](#)
- [Microsoft Certified Solutions Architect – SQL Server 2016 Business Intelligence Development](#)

- [Microsoft Certified Solutions Associate – Machine Learning](#)
- [Microsoft Certified Solutions Associate – Business Intelligence Reporting](#)
- [Microsoft Certified Solutions Associate – Data Engineering with Azure](#)

Choose one of the following Azure exams:

- [70-473: Designing & Implementing Cloud Data Platform](#)
- [70-475: Designing & Implementing Big Data Analytics Solutions](#)
- [70-464: Developing Microsoft SQL Server Databases](#)
- [70-465: Designing Database Solutions for Microsoft SQL Server](#)
- [70-466: Implementing Data Models and Reports with Microsoft SQL Server](#)
- [70-467: Designing Business Intelligence Solutions with Microsoft SQL Server](#)
- [70-762: Developing SQL Databases](#)
- [70-767: Implementing a Data Warehouse using SQL](#)
- [70-768: Developing SQL Data Models](#)
- [70-773: Analyzing Big Data with Microsoft R](#)
- [70-774: Perform Cloud Data Science with Azure Machine Learning](#)
- [70-775: Perform Data Engineering on Microsoft Azure HDInsight](#)

MICROSOFT CERTIFIED SOLUTIONS DEVELOPER



MCSD RESOURCES

→ [MCSD App Builder](#)

MCSD APP BUILDER



The Microsoft Certified Solutions Developer (MCSD): App Builder certification validates that you have the skills needed to build modern mobile and/or web applications and services.

Pre-Requisites:

- [Microsoft Certified Solutions Associate \(MCSA\) – Web applications](#)
- [Microsoft Certified Solutions Associate \(MCSA\) - Universal Applications](#)

Choose one of the following Azure exams:

- [70-357: Developing Mobile Apps](#)
- [70-486: Developing ASP.NET MVC Web Applications](#)
- [70-487: Developing Microsoft Azure and Web Services](#)

Microsoft
Partner
Network

Operationalize

Cloud Operations
& Management

aka.ms/practiceplaybooks



Executive Summary



In the previous section, we reviewed how you should hire, train, and equip your staff. In this section, we will guide you through the steps to operationalize your business plan.

We walk you through the options for leveraging your internal use benefits that provide you complimentary software licenses and subscriptions for use within your organization, as well as show you how can deepen relationships with your customer by re-selling it as an overall package along with your custom software, creating a new revenue stream for your business.

This section also provides guidance on how to operate your business, from how to build materials to support your sales and marketing efforts to the key contracts you will want to put in place.

Whether you're building products, providing managed services, or performing project work for customers, your success may be impacted by your ability to manage your customer records, your projects, and your support trouble tickets. We provide guidance on what tools and systems you should consider implementing.

We also cover how you can increase visibility for your practice by reviewing the Microsoft marketplaces and how to get listed on them as well as provide guidance on the social offerings your practice should setup.

We conclude this section with checklists and templates you can use to standardize your customer engagement process.

TOP 5 THINGS TO DO

Get your practice off ground by putting your plan into action. These are the top 5 things you should do to get the momentum going.

- Leverage your internal use benefits.
- Prepare your key contracts.
- Setup your support process and systems.
- Setup your social offerings.
- Standardize your engagements using checklists.

Azure Virtual Datacenter and the Enterprise Control Plane

Azure Virtual Datacenter (vDC) is an approach to making the most of the Azure cloud platform's capabilities while respecting the existing security and networking policies of your customers and allowing you to implement "secure-by-design" Azure deployments. When deploying enterprise workloads to the cloud, all organizations must balance governance with service delivery and agility. Azure Virtual Datacenter provides models to achieve this balance with an emphasis on governance.

ADDRESSING CUSTOMER NEEDS

Customers look to Microsoft and its partners to reduce costs in Azure while reproducing the isolation, security policies, and audit models they have today. They also want you to demonstrate you have access to mature tools for identifying workload suitability as well as the one-time deployment and ongoing operational costs of Azure. As we balance these needs, we also need to consider the needs of the end-users of the Azure platform such as developers who will need to do their work independently of a centralized IT organization while still adhering to organizational policies.

By implementing the practices and tools of the vDC, partners can deliver services on the Azure platform to even the most sophisticated enterprise customers.

The vDC delivers:

aka.ms/practiceplaybooks

- Tooling that automates Azure deployments that are isolated, secure, and policy driven
- Suggested practices, tools, and models that support Azure migration decision making
- Integration with well-known Microsoft Developer Tools to enable governed applications and CI/CD pipeline
- Integration with Azure monitoring tools, including Log Analytics, Azure Security Center, and Azure Monitor

There are four pillars that make the vDC possible: identity, encryption, software-defined networking (SDN), and compliance (including logging and reporting). As you implement operations for your customers, consider adhering to these four pillars in all of your implementations.

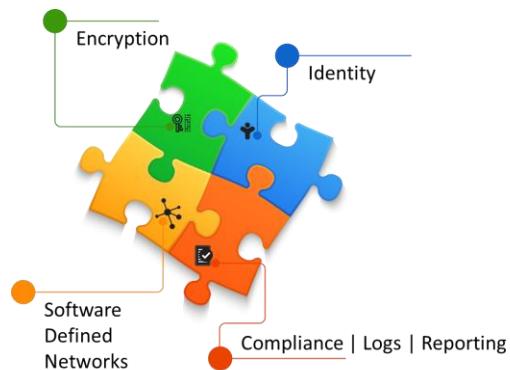


Figure 2: The Four Pillars of the Azure Virtual Datacenter

By adhering to these principles, you will enable Azure to become a natural extension of your customers' existing environments. Each of the components allows you to build a true virtual datacenter – fully isolated from other customers that supports the application of organization policies like security and compliance.

Throughout the remainder of this section, we will explore the services that you can implement as a partner to enable the vDC and the enterprise control plane for your customers. We will walk you through deploying subscriptions, implementing identity management and role-based access controls, configuring Azure to meet the compliance needs of your customers, and implementing secure deployments with encryption and software-defined networking abstractions.

Managing Azure Subscription Creation Resources



- [Licensing Azure for the Enterprise](#)
- [Enterprise Portal](#)
- [Direct Customer Onboarding Guide](#)

Subscriptions are the bedrock of the Azure Virtual Datacenter. Organizations can use subscriptions to manage costs and impose limits on the creation of resources by users, teams, projects, or using many other strategies.

Microsoft Azure Enterprise Portal

The Microsoft Azure Enterprise Portal for Enterprise Agreement customers (EA Portal) is where customers can administer the Azure subscriptions that are associated with their Enterprise Agreement, obtain billing and usage reports, and understand their current monetary commitment balance(s) and burn down. Within the portal, customers can create Account and Department Administrators. Account owners are then associated with one (or more) subscriptions where they also become the Service Administrator.

As customers setup their portal, customers divide their enrollment into Departments and Accounts, followed finally by subscriptions.

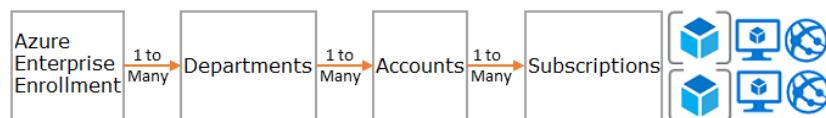
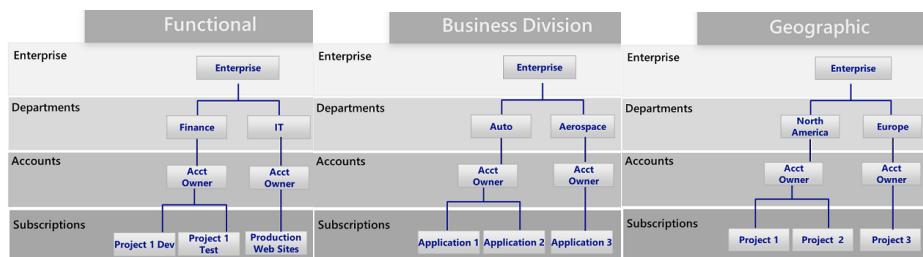


Figure 3: Enterprise Enrollment Hierarchy

While the resources created in a given subscription are the most tangible aspects to Account and Service Administrators and managed in the [Management Portal](#), Enterprise Administrators and Department Administrators perform their tasks through the [Enterprise Portal](#). Depending on the user's role associations, they could perform management tasks in any of the three portals.

Account Owners are solely responsible for the lifecycle of a subscription, including its creation and, if needed, deletion. Subscriptions are created and managed within the hierarchy defined at the Enterprise and Department levels.



Partner Center

An Azure CSP customer must be created within Partner Center before you can place orders for a customer. When a customer is created, you also create:

- An Azure Active Directory (Azure AD) tenant object for the customer.
- A relationship between the reseller and customer, which is used for delegated administrator privileges.
- A username and password for signing in as an administrator for the customer.

Customers can be provisioned through the Web UI, PowerShell, C#, or the available REST API.

The screenshot shows the Microsoft Partner Center dashboard. On the left, there's a sidebar with links like Overview, Customers, Service requests, Service health, Product analytics, Azure spending, Activity log, Billing, Pricing and offers, Promotions, and Referrals. The main area displays "Azure spending" information, including a section for "Email notifications" where a toggle switch is set to "On". Below this, it shows a "Billing period" from June 26 - July 25 and "Days remaining" as 20. A section titled "Customers with Microsoft Azure subscriptions" shows a report for 7/4/17 8:38 PM, stating the data is an estimate and may be delayed by up to 48 hours. It includes a "Monthly budget" input field, an "Apply" button, a "Remove budget" button, and a "Search" bar. A table lists four customers: SEATTLEIOT, ANDREWS CONCERT TICKETS, and DAN INC, each with their monthly budget, current estimate, and percentage used (123%, 24%, 17% respectively).

Figure 4: Microsoft Partner Center

As the customer is created, you will select the offers that will be provisioned for the customer, including Azure. Note that there are separate offers for Enterprise, Small business, and Government. The Azure CSP offer can be found under the Enterprise category.

The initial admin user account and associated password are only available when the customer is created and the offer provisioned. Make sure you note them, especially when using the Web UI.

RESOURCES

- ➔ [Create an Azure CSP customer](#)
- ➔ [Partner Dashboard](#)
- ➔ [Azure in CSP](#)

Managing Azure Subscription Access Resources



- [Add an RBAC Owner admin for a subscription in the Azure portal](#)
- [Add or change Co-administrator](#)
- [Azure CSP subscription permissions management](#)

Accessing a customer's subscription and the delegation of management of a subscription is dependent on the type of subscription and how it was created.

AZURE ENTERPRISE ENROLLMENT AND PAY-AS-YOU-GO SUBSCRIPTIONS

To access a customer's existing enterprise enrollment, your customer will need to grant you rights within their Azure subscription. There are several ways they can accomplish this.

AZURE RESOURCE MANAGER SUBSCRIPTIONS

Azure Resource Manager (ARM) subscriptions provide support for role-based access control (RBAC) and offer fine-grained access management to the resources hosted in an Azure subscription with many built-in roles, flexible scopes, and custom roles. It is recommended that all Azure subscribers use RBAC for assessment management whenever possible, even if it requires reconfiguring existing access policies to accommodate RBAC.

Customers can follow the instructions in the article at [Add an RBAC Owner admin for a subscription in the Azure portal](#) to add a partner user account to their subscription.

You may have customers which still utilize Azure Service Management (ASM) (otherwise known as Classic subscriptions). Classic subscriptions are managed through a different set of APIs and it is recommended that customers redeploy existing resources through ARM. For customers that are still managing Classic resources, you should consider offering services to assist those customers in transitioning to the modern ARM APIs and deployment model. For more resources on Classic to Resource Manager migrations, see [Migrate from classic to Resource Manager](#).

AZURE CSP SUBSCRIPTIONS

Azure CSP subscriptions that have been created on behalf of a customer by a partner will not require additional intervention for the partner to gain access. In fact, in this case, it is the partner who must grant the customer rights to access the subscription if that the customer requires it or the partner has structured the service agreement in such a manner. The article at [Assign and manage permissions within an Azure subscription](#) contains the steps that show how this is done.

Identity and Access Management (IAM)

IAM Resources

Subscriptions provide the first layer of isolation in the vDC and robust role-based access controls (RBAC) provide the next with Azure Active Directory (Azure AD). Azure AD helps you manage user identities and create intelligence-driven access policies to secure your Azure resources within an Azure subscription. The roles that you create in Azure AD are used to control management access to resources in Azure, including services, virtual machines, storage, and databases.

ROLE-BASED ACCESS CONTROL

Access to manage resources can be delegated to individual users, groups, and roles - or a combination of all three. It is important to remember that while RBAC can be used to control the access to the top-level resource, the internal configuration of a resource is not controlled through Azure AD and RBAC. For instance, access to a virtual machines' configuration in Azure can be delegated with RBAC, however the access to the underlying guest operating system is configured within the operating system.

Access to resources in Azure should always be explicitly granted to specific users, groups, or applications performing a particular function. The users and groups that are assigned to roles and resources can be created on-premises and synchronized to Azure AD with Azure AD Connect or created as cloud-only objects in Azure AD and managed exclusively in the cloud.

If a customer has existing security policies in place, including well defined security groups in an on-premises

environment, they can absolutely be repurposed in Azure. By leveraging Azure AD Connect, roles can be managed on-premises and surfaced in Azure, where they can be applied to access rules. This allows for a distributed approach to give your customers access to specific workloads without impacting the services you provide as a partner.

When you are planning your roles in Azure, it is important to note that roles are comprised of two components:

- **Role definitions** describe the set of permissions allowed within a role. For instance, a role definition may include the Contributor permission, which allows you to manage everything related to a resource except access to the resource.
- **Role assignments** allow users, groups, and service principals to be associated with role definitions at a scope. For instance, an application administrator can be granted Contributor rights to a resource group, allowing that user to manage all of the resources within the group while the delegation of access control can remain with another group.

You must also consider role-inheritance in the design of your roles. ARM provides a very granular RBAC model where management rights are assigned at a scope level. A scope is the boundary that access applies to.

There are three RBAC scopes in ARM:

- **Subscription level** which grants permissions to all resources in a subscription
- **Resource group level** which grants permissions to all resources in the resource group
- **Resource level** which grants permissions to a specific resource

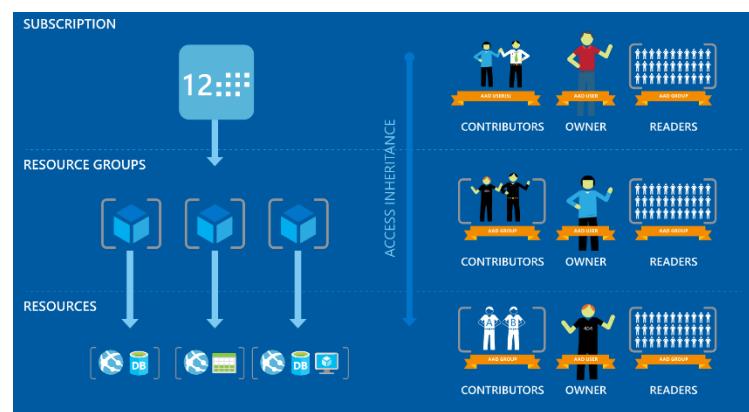


Figure 5: Role inheritance

As you plan your roles, the goal should always be to follow the principals of least access. By following this model, users will be able to do the tasks their job requires, but no more than that. For example, an IT operations manager may require access to read an activity log and view reports, but will not need access to update the permissions for a networking component. By granting them access to only the resources they need, you can ensure that resources are properly isolated and that the proper controls have been implemented.

BUILT-IN ROLES

Azure RBAC has many [built-in role definitions](#) that can be assigned to users, groups, and service principals. As a best practice, you should always try to leverage built-in roles whenever possible. There are 40+ built-in roles today, and more are added all the time.

When you are considering built-in roles, there are three primary roles:

- **Owner** can perform all management operations for a resource and its child resources including access management and granting access to others
- **Contributor** can perform all management operations for a resource including creating and deleting child resources. Contributors cannot grant access to other others.
- **Reader** has read-only access to a resource and its child resources. A reader cannot read secrets.

Beyond the primary roles, there are 40+ resource-specific roles. These roles are permissions scoped to resources and actions that are commonly required by consumers of Azure. One example of this would be the Virtual Machine Contributor role. This role lets assignees manage virtual machines, but not the access to them or the virtual network or storage account they are connected to.

CUSTOM ROLES

It is recommended that you leverage the built-in roles whenever possible. However, if the built-in roles do not meet the needs of your customers, [custom roles](#) can be created. Just as with built-in roles, custom roles can be assigned to users, groups, and service principals at the subscription, resource group, and resource scopes. Custom roles are stored in Azure AD and can be shared across subscriptions.

To create a custom role, you can start with a built-in role, edit it, and then finalized as a custom role. It is important to note that while you may use a built-in role as a template for a custom role, if that built-in role is even updated no updates will be made to your custom role. This is the primary driver behind the recommendation to use as few custom roles as possible. The more custom roles you implement, the more operational overhead you will incur to maintain them moving forward as new actions are introduced.

RESOURCE LOCKS

[Resource locks](#) allow you to create policies within your subscriptions which restrict operations on high-value resources where modifying them or deleting them could have a significant impact on your cloud infrastructure and applications.

Just as with roles, resource locks are applied at a subscription, resource group, or resource scope. Resource locks are commonly applied to resources related to your core infrastructure such as virtual networks, gateways, storage accounts, and ExpressRoute circuits (if applicable).

Resource locks can be CanNotDelete or ReadOnly locks. CanNotDelete means that a resource can be read and/or modified by users with the appropriate rights but that resource cannot be deleted. A ReadOnly lock means that authorized users cannot delete or modify a resource.

When considering resource locks, the first place you can look to them for practical application is your core networking resources. While resources like a virtual network cannot be deleted while in use, it is always helpful to have additional safeguards in place.

ACTIVITY LOGS AND AUDIT

Even with a well-planned access management strategy in place, regular audits should be performed to ensure the integrity of your subscriptions. The Azure Activity logs captures common operations related to RBAC changes and maintains the history of those operations for 90 days.

The entire lifecycle of RBAC is included in the Activity Log under the Administrative event category. This includes the creation and deletion of role assessments as well as the creation, updates, and deletion of custom role definitions.

The Activity Logs also capture all write operations performed the resources in a subscription. Read

operations are not included in the log today. Using the activity logs, you can determine:

- **Who** initiated the operation (although operations initiated by a backend service do not return a user as the caller)
- **What** operations were taken on the resources in your subscription
- **When** the operation occurred
- The **status** of the operation
- The **values** of other properties that might help you research the operation

The activity logs are a crucial resource for understanding the actions and operations that are occurring in your subscriptions, whether you are using them for audit controls or even basic troubleshooting.

AZURE POLICY

[Azure Policy](#) is a service that can be used to enforce different rules and effects over the resources in your Azure subscriptions. You can think of Azure Policy as a risk management and mitigation mechanism, keeping your users on a defined path.

At the core, policies restrict, enforce, or audit certain actions within an Azure subscription. Policies have multiple actions that allow for a fine-grained approach to governance:

- **Deny:** Blocks the resource request
- **Audit:** Allows the request but adds a line to the activity log (which can be used to provide alerts or to trigger runbooks)
- **Append:** Adds specified information to the resource. For example, if there is not a "CostCenter" tag on a resource, add that tag with a default value.

With actions such as Audit, you can combine policy with the activity log and ensure your compliance and governance needs are being enforced.

Policies can be defined to implement platform governance for many common use cases.

- **Geo-compliance/data sovereignty** by implementing policies which dictate the regions in which resources can be provisioned
- **Cost management** by restricting the types of resources that can be provisioned (e.g. do not allow

Azure SQL Data Warehouse) and even the scale of resources (e.g. only allow certain VM sizes and SKUs)

- **Required tags** to ensure resources in Azure can be tracked, inventoried, and allocated properly in billing reports or other cost management tools

As you define your policies, consider *where* resources can be created and *what* types of resources can be created. Building policies that address these key items will allow you to construct common sense policies that can be applied to your subscriptions as they are created.

MANAGEMENT GROUPS

It is quite common for customers to have more than one subscription and as a partner [Management groups](#) (currently in Preview) can be used to build a hierarchy that organizes Azure Policies and RBAC controls across multiple subscriptions. Management Groups provide a level of scope above subscriptions which allows you to apply your controls and governance conditions in a repeatable, automated fashion.

Management groups allow you to organize your subscriptions on your terms. For instance, you can create a hierarchy of customers or departments, apply policy to those groups, and then assign one or more subscriptions to each group.

While Management Groups are in preview, there are several limitations which must be considered.

- For commercial subscriptions (Pay-as-you-Go and Enterprise Enrollment) there is a limitation where you cannot view subscriptions that you have inherited access to. This limits the ability to view these inherited subscriptions in the Azure Portal and interact with these subscriptions through the ARM API.
- For CSP Partners, there is a limitation where you cannot create or manage your customer's management groups within their directory.

Both of these limitations will be resolved before Management Groups are announced as "General Availability".

IAM Tools

Now that you understand the resources that are available to you to implement identity and access management, we'll explore tools and licensing features of Azure Active Directly that will allow you to implement hybrid identity management and put additional security controls in place to better control access to the resources hosted in your Azure subscriptions.

AZURE AD CONNECT

[Azure AD Connect](#) allows you integrate an existing Active Directory with Azure Active Directory and perform hybrid identity management. This allows you to leverage your customer's existing investments in Active Directory in Azure, including the use of on-premises users and groups in RBAC assignments.

Azure AD Connect also allows your customers to use features such as single sign-on (SSO) to access resources in Azure with the same identities they use on-premises today. Azure AD Connect provides capabilities to support your identity synchronization needs and replaces older versions of identity integration tools such as DirSync and Azure AD Sync.

With Azure AD Connect, identity management and synchronization between on-premises and Azure AD is enabled through:

- **Synchronization** – This component is responsible for creating users, groups, and other objects. It is also responsible for making sure identity information for your on-premises users and groups is matching the cloud. Password write-back can also be enabled to keep on-premises directories in sync when a user updates their password in Azure AD.
- **AD FS** – Federation is an optional capability provided by Azure AD Connect that can be used to configure a hybrid environment using an on-premises AD FS infrastructure. Federation can be used by organizations to address complex deployments, such as single sign on, enforcement of AD sign-in policy, and smart card or third party MFA.
- **Health Monitoring** – [Azure AD Connect Health](#) can provide robust monitoring and provide a central location in the Azure portal to view this activity.

MULTI-FACTOR AUTHENTICATION AND CONDITIONAL ACCESS

Azure AD can also enable additional levels of validation such as [multi-factor authentication](#) and [conditional access policies](#). Monitoring suspicious activity through advanced security reporting, auditing and alerting helps mitigate potential security issues.

In the public cloud, identity is your control plane and protecting the identity of the users that consume Azure resources, especially your administrators and operators, is critical. One of the easiest steps you can take to protect these and other privileged accounts is enabling multi-factor authentication (MFA). Azure offers multiple verification options, including phone call, text message, or mobile app notification through the [Microsoft Authenticator app](#).

Conditional access policies, a feature available through Azure AD Premium licensing, give you the ability to create policy-based access rules for any Azure AD-connected application (SaaS apps, custom apps running in the cloud or on-premises web applications). Azure AD evaluates these policies in real time, and enforces them whenever a user attempts to access an application. Azure identity protection policies enable you to automatically take action if suspicious activity is discovered. These actions can include blocking access to users at high risk, enforcing multi-factor authentication, and resetting user passwords if it looks like credentials have been compromised.

PRIVILEGED IDENTITY MANAGEMENT

[Privileged Identity Management](#), included with the Azure Active Directory Premium P2 offering, allows you to discover, restrict, and monitor administrative accounts and their access to resources in your Azure Active Directory and other Microsoft online services. It also helps you administer on-demand administrative access for the exact period of time you need.

Privileged Identity Management can enforce on-demand administrator rights so that administrators can request multi-factor authenticated, temporary elevation of their privileges for pre-configured periods of time before their accounts return to a normal user state.

Security and Networking

Azure's hyperscale networking and built-in security services allow you to extend the concept of the vDC to another layer. We'll build on the foundation of our subscriptions and access controls and put configurations and services in place that bring secure and private connectivity to your Azure workloads. In addition, we'll model policy into our subscriptions that allows you to be "secure by design". Then we'll secure additional resources including virtual machines and disks to provide holistic protection of your entire Azure estate.

Networking Resources

When approaching the design of your networks in Azure, it is important to consider that Azure provides multiple layers of network security, some of which are native to the Azure platform and others which can optionally be implemented as customer needs changes.

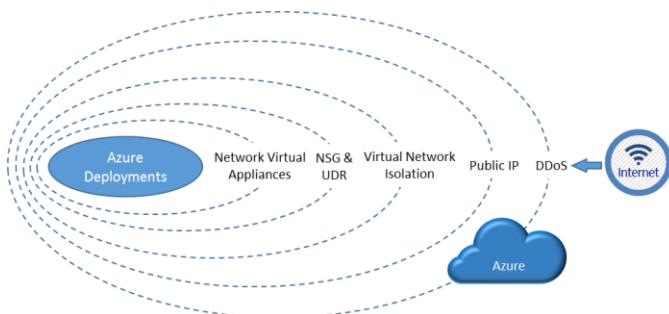


Figure 6: Azure Network Security Layers

Throughout this section, we will explore the available networking features and help you understand "when to use what".

VIRTUAL NETWORK

The core of your software-defined network in Azure is a virtual network. A [virtual network](#) is an isolated portion of the Azure public network that is dedicated to a subscription. Within a subscription, you can have one or more virtual networks which are segmented into subnets and then layered with network security groups, application security groups, and user-defined routes. As we continue to build out your vDC, consider how the design of your virtual networks will contribute to isolation and segmentation of workloads within your subscriptions.

There are many questions you will want to answer as you are designing your virtual networks such as:

- Are there existing security requirements for isolating traffic into dedicated networks?
- Do you need to isolate your networks to specific subscriptions or regions?
- How many network interfaces and private IP addresses will you require?
- Do you need to connect your virtual network to another network – either virtual or on-premises?
- Do you have administration or management requirements for resources in different networks?
- Have you accounted for services in Azure which create their own virtual network?
- Have you accounted for the [networking limits](#) within an Azure subscription?

The above questions will help you determine where your networks will be provisioned and their potential address spaces. They will also guide you in understanding where policy and RBAC will be applied to allow for administration and management of the networks.

SUBNETS

An equally important consideration for the design of your virtual networks will be how you segment them with subnets. Each subnet must have a unique address range within the address space of your virtual network and that subnet range cannot overlap with other subnets in the network.

There are some Azure service resources which may require (or even create) their own subnet and you will need to make sure there is enough allocated space for them to do so. Planning for services like Service Fabric, HDInsight, Virtual Machine scale sets, and even VPN Gateways

becomes a critical consideration. See [Services that can be deployed into a virtual network](#) for a full list of services which will consume address space within your virtual networks. If you are not planning to use these services, consider restricting the ability to provision them with Azure Policy.

NETWORK SECURITY GROUPS

[Network security groups](#) (NSGs) allow you to limit inbound and outbound traffic to resources in your virtual networks for both subnets and individual network interfaces on virtual machines. The security rules that you implement in a network security group can limit traffic based on source or destination IP address, port, and protocol. NSGs can be shared between multiple subnets and network interfaces, offering you the ability to create a single set of rules that can then be applied to multiple resources.

Consider that subnets and network interfaces can have zero, or one, associated NSG. A best practice is to ensure you have NSGs in place for your resources, even if only to deploy a minimal ruleset.

Microsoft also includes [service tags](#) which can be used when building NSGs. A service tag represents a group of IP address prefixes which can minimize the complexity of your NSGs. Consider an NSG that needs to allow inbound access from an Azure Load Balancer. With a single service tag, you can define an NSG which will automatically whitelist inbound connections from the Azure Load Balancer service when using the AzureLoadBalancer service tag. Without this tag, you would need to manually maintain a whitelist of IP addresses (or address ranges) for the service and manually update all of your NSGs that need to allow access from the Load Balancer any time the public service changes.

Service tags are available for many Azure services, including the previously mentioned Azure Load Balancer, Azure Traffic Manager, Azure Storage, Azure SQL Database, Azure Cosmos DB, and Azure Key Vault. For the full list of service tags and their values, see [Service tags](#).

APPLICATION SECURITY GROUPS

[Application security groups](#) (ASGs) allow you to group virtual machines and define network security policies based on those groups. Much like NSGs, ASGs provide a further level of abstraction for network policy, simplifying

aka.ms/practiceplaybooks

management and deepening the control plane. By defining and implementing ASGs, you can model and implement a set of rules that can be reused multiple times based on your business requirements.

For example, consider a traditional two-tier application with a web and a data tier. With ASGs, you can create a rule that defines the inbound and outbound security for your web tier (e.g. traffic is allowed inbound from the internet on port 80 and outbound to the data tier on port 1433). You can then create a similar rule for your data tier (e.g. traffic is allowed inbound on port 1433 from the web tier). The security rules defined, you can then apply them to your virtual machines, with the web rule applied to your web services and the data rule applied to your database servers. As new servers or applications come online that can make use of the same ruleset, they can have the same ASGs applied as needed.

USER-DEFINED ROUTES

By default, Azure routes network traffic between all subnets in a virtual network. You can override Azure's default routing to prevent Azure routing between subnets, or to route traffic between subnets through a network virtual appliance by implementing [user-defined routes](#) (UDRs). Implementation of UDRs allows you to implement additional security controls through network virtual appliances (NVAs) such as firewalls or other network filtering devices.

VIRTUAL NETWORK SERVICE ENDPOINTS

You can limit access to Azure resources such as an Azure storage account or Azure SQL database, to specific subnets with a [Virtual Network Service Endpoint](#). Further, you can deny access to the resources from the internet. You can even create multiple subnets, and enable a service endpoint for some subnets, but not others.

Virtual network service endpoints allow you to extend the control plan for Azure PaaS services, improving the security for your service resources by allowing traffic from only your virtual networks. Service endpoints also ensure that optimal routes are in place when you are using hybrid networking features such as forced tunneling.

Service endpoints are available for Azure Storage, Azure SQL Database, Azure SQL Data Warehouse (in Preview), and Azure Cosmos DB today.

NETWORK VIRTUAL APPLIANCES

There are hundreds of [Network Virtual Appliances](#) (NVAs) available in the [Azure Marketplace](#) which let you use industry best-of-breed network appliances that are easy to configure, scalable, and highly-available.

NVAs allow you to execute even the most advanced networking scenarios in Azure when combined with native platform features like UDRs. NVAs are available for many functions, including next-generation firewalls (NGFW), web application firewalls (WAF), gateways and routers, application delivery controllers (ADC), and WAN optimizers.

The choice to use a NVA will depend on your specific requirements and security needs. For instance, you may have a requirement to inspect all outbound internet traffic from one or more virtual networks. With NVAs, you can deploy a NVA pair (for high-availability) to a hub network and route traffic from your spoke networks through the hub. Another example would be the implementation of a third-party load balancer that has additional features beyond what Microsoft's native load-balancer or application gateway provide.

If you deploy NVAs, there are many considerations. Some are straightforward, such as the need for additional licensing, while others are less well known such as accounting for the additional operations overhead of maintain additional virtual machines and appliance specific configurations. Ask yourself the following questions prior to deploying NVAs:

- Is there an equivalent Azure service which meets my requirements?
- Do I need my NVA to be highly available? If so, what are the cost and management impacts?
- How many NVAs will I need based on my network throughput? Azure limits will once again come into play as virtual machine network interfaces have a maximum throughput.
- What type of support will you need from the NVA vendor in the event assistance is required?
- Do I need multiple NVAs in series? For example, an NVA implementing a firewall could be place in series with an NVA performing ADC.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

Distributed denial of service (DDoS) attacks are often one of the largest concerns customers surface when bringing their workloads to the cloud. DDoS attacks flood resources with network requests which exhaust an application's resources. This makes the application unavailable to legitimate users and leads to additional cost for application owners to remediate the attack.

[Azure DDoS Protection](#) is available in two tiers -Basic and Standard. Basic DDoS protection is built directly into the Azure platform and is available for no additional cost. This free coverage is included for both IPv4 and IPv5 Azure public IP addresses.

If you require additional protection, the Azure DDoS Protection Standard tier provides additional mitigation abilities for protecting Azure resources with public IP addresses such as Azure Load Balancer or Azure Application Gateway. The Standard tier provides mitigations for volumetric attacks, protocol attacks, and application layer attacks.

The Azure DDoS Protection service can be layered with other Azure services, including WAFs and NVAs providing layer 3 to layer 7 mitigation capabilities. The DDoS service also integrates with your monitoring services, including Azure Monitor, Azure Log Analytics, Azure Storage, or third-party SIEM tools like Splunk.

PENETRATION TESTING

Microsoft [performs regular penetration testing of its networks](#), including Azure. They do not however provide penetration testing for the applications and workloads that you deploy into Azure.

Customers can perform their own penetration testing as needed. You are encouraged (but not required) to inform Microsoft of such activities by filling out the [Azure Service Penetration Testing Notification form](#). Standard tests that you can perform include:

- Testing internet endpoints for any of the [OWASP top 10 vulnerabilities](#)
- Fuzz testing of your endpoints
- Port scanning of your endpoints

There are tests which cannot be performed under any circumstance such as any kind of Denial of Service (DoS) attack. All pen testing must comply with the [Microsoft Cloud Unified Penetration Testing Rules of Engagement](#).

Security for Virtual Machines

There are many considerations for securing virtual machines in Azure beyond the network layer. Now that we've explored how to secure access to the resources that make up your virtual machines and how to perform network filtering, we can add additional protections including anti-virus and antimalware solutions, disk encryption, and threat detection.

VIRTUAL MACHINE ACCESS CONTROL

There are two layers to controlling access to your virtual machines – controlling access to the Azure resource (e.g. the VM configuration) and controlling access to the VM itself (e.g. local logon via SSH). We've already discussed the former control plane with Azure RBAC, but it should be noted there are several built-in RBAC roles specifically for virtual machines:

- **Virtual Machine Contributor:** Can manage VMs, but not the virtual network or storage account to which they are connected.
- **Classic Virtual Machine Contributor:** Can manage VMs created by using the classic deployment model, but not the virtual network or storage account to which the VMs are connected.
- **Security Admin:** Can manage security components and security policies.
- **DevTest Labs User:** Can view everything and connect, start, restart, and shut down VMs.

By grouping virtual machines with the same lifecycle together in the same resource group and using the built-in roles, you can simplify the management and improve the security posture of these Azure resources.

ANTIMALWARE PROTECTION

There are antimalware and anti-virus solutions available from Microsoft and other vendors in the Azure Marketplace. Considerations for selecting an antimalware solution include understanding which operating systems you will need coverage for and any requirements for

integrating with other Azure services such as Log Analytics or Azure Storage for event collection and aggregation.

When protecting compatible Windows workloads, Microsoft [Antimalware for Azure Cloud Services and Virtual Machines](#) is available at no additional cost as a native Azure virtual machine extension. If you have Linux workloads that require antimalware protection or have relationships with other antimalware vendors, there are multiple offerings in the Azure Marketplace from vendors like Symantec, Trend Micro, and Kaspersky.

DISK ENCRYPTION

Encrypting data in your virtual machines can be considered a mandatory step, especially when considering needs for data privacy, compliance, and data sovereignty. By encrypting your disks, you reduce the threat of data theft or exposure from unauthorized access in the event a disk is moved.

By default, [Azure Storage Service Encryption](#) (SSE) is enabled for all new and existing storage accounts and cannot be disabled. This ensures that your data is encrypted at rest in all Standard and Premium storage accounts, both ARM and ASM, and for all storage services (blob, queue, table, and files).

To go a step further, [disk encryption](#) in Azure is available for both Windows and Linux operating systems, with Windows leveraging Bitlocker and Linux using DM-Crypt. This allows you to use SSE for your virtual disks and encrypt the contents of those disks as well, providing protection at the resource level as well as within the configuration of the resource itself (in this case, a VHD). Encryption can be enabled for both your operating system and data disks. Disk encryption in Azure is integrated directly with [Azure Key Vault](#) for the storage of your encryption keys, meaning you are in control of your data the entire time.

Azure Key Vault allows you store and manage the lifecycle of your encryption keys for both SSE and Azure Disk Encryption. By utilizing Azure Key Vault, you can automate the end-to-end lifecycle of your data in Azure, ensuring you are the only one with access and retaining the ability to revoke access as needed by simply invalidating an encryption key.

UPDATE MANAGEMENT

Patching and maintaining your virtual machines is critical to your security posture. Azure offers a first-party patch management service as a part of Azure Automation that allows you to discover, inventory, track changes, and update both Linux and Windows workloads hosted in Azure, on-premises environments, and even other cloud providers.

[Update management](#) will specifically allow you to quickly assess the state of patch installation, including the status of available updates, schedule required updates, and verify the installation of updates through change tracking.

To leverage update management, an Azure Automation account will need to be created to hold a watcher, the action runbooks, and a watcher task. Update management also leverages a Log Analytics workspace, where it stores the logs and metadata associated with the watcher.

Onboarding a virtual machine to Update management requires that the solution be enabled for a given virtual machine. The Update management solution can be enabled for individual machines, all current machines, all current machines and all future machines, or only on a specific set of virtual machines.

There is no additional charge for Update management in Azure Automation beyond the charges for the metadata stored in Log Analytics. By using Update management, you can ensure your customers have a patch management tool in place for their entire Azure estate.

THREAT DETECTION

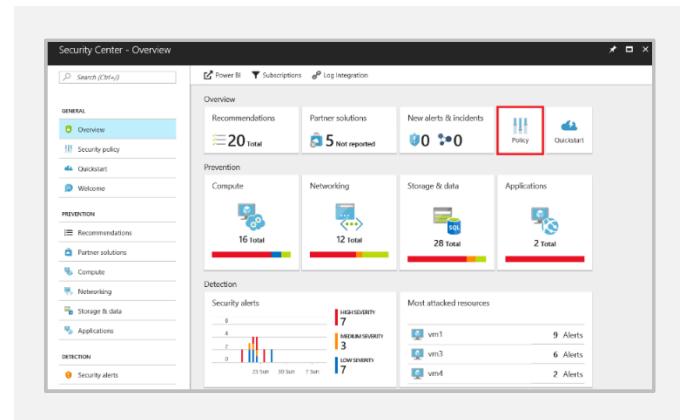
You need to consider the posture of all of your workloads and all of the security aspects of your VMs, from update management to network access. Implementing these controls is not enough, you also need to monitor your virtual machines and analyze their security posture on an ongoing basis.

[Azure Security Center](#) helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions. Azure

Security Center should be part of any Azure practice to assist with monitoring and support.

Security Center delivers effective threat prevention, detection, and response capabilities that are built in to Azure. Some of its key capabilities are:

- Monitor the security state of your Azure resources
- Defines policies for your Azure subscriptions and resource groups based on your company's security requirements, the types of applications that you use, and the sensitivity of your data
- Uses policy-driven security recommendations to guide service owners through the process of implementing needed controls
- Rapidly deploy security services and appliances from Microsoft and partners
- Automatically collect and analyze security data from your Azure resources, the network, and partner solutions like antimalware programs and firewalls
- Leverages global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds
- Apply advanced analytics, including machine learning and behavioral analysis
- Provides prioritized security incidents/alerts
- Offers insights into the source of the attack and impacted resources
- Suggests ways to stop the current attack and help prevent future attacks



Security Center is available in two tiers – Free and Standard. Every Azure customer should be using the Free tier of Security Center and it is a powerful tool to demonstrate how you can keep your customers more secure in Azure.

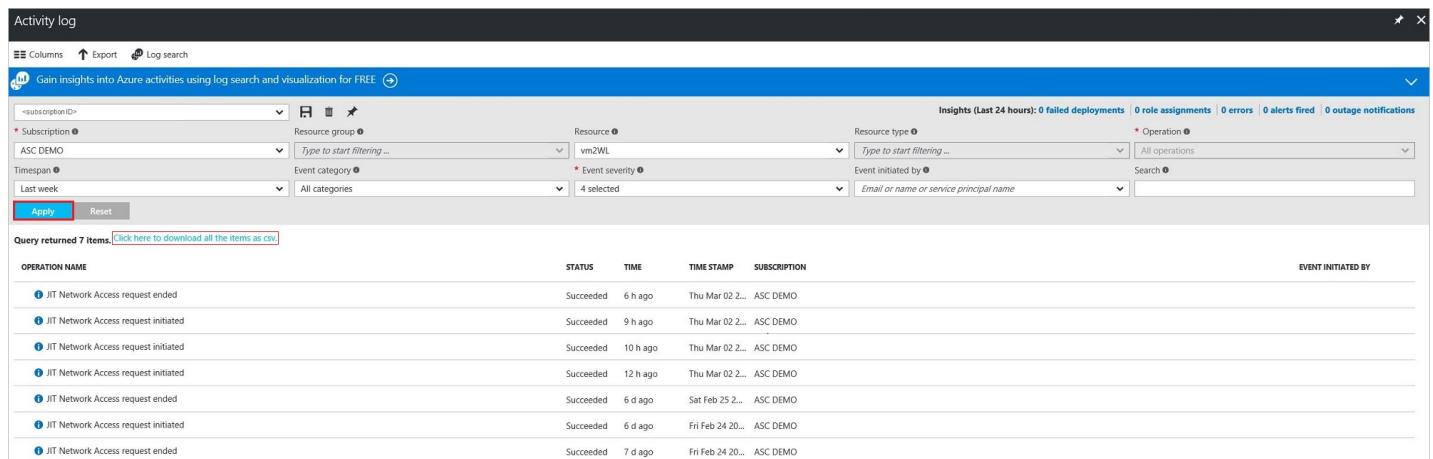
JUST IN TIME VM ACCESS

A feature of the Standard pricing tier of Azure Security Center, Just In Time VM Access (JIT) brings both a security and access management feature to your virtual machine control plane. With JIT, you can restrict inbound management traffic (e.g. RDP and SSH traffic) to your virtual machines and expose the required ports for access on an on-demand basis. JIT greatly reduces the amount of time these management ports are open which reduces the time windows for common attacks like brute force login attempts.

With JIT enabled, Azure Security Center can manage the NSG rules associated with your virtual machines.

Administrators and other operators can request access to the virtual machine through Security Center. It is at this time that RBAC is evaluated, and if the user has rights to request access the ports are opened for the specified amount of time. After the time has expired, Security Center automatically revokes access to the management ports by restoring the NSG to its previous state.

Just in time VM access can be audited and monitored through the Azure Activity Log which provides a full detail of all of the operations for the VM, including the time, date, and subscription.



The screenshot shows the Azure Activity Log interface. The top navigation bar includes 'Activity log', 'Columns', 'Export', 'Log search', and a 'Gain insights into Azure activities using log search and visualization for FREE' button. The main search area contains filters for 'Subscription' (set to 'ASC DEMO'), 'Resource group' (set to 'vm2WL'), 'Event category' (set to 'All categories'), 'Event severity' (set to '4 selected'), 'Operation' (set to 'All operations'), and 'Event initiated by' (set to 'Search'). Below the filters, a message indicates 'Insights (Last 24 hours): 0 failed deployments | 0 role assignments | 0 errors | 0 alerts fired | 0 outage notifications'. The main table lists 7 items returned, each representing a JIT Network Access request. The columns include 'OPERATION NAME', 'STATUS', 'TIME', 'TIME STAMP', 'SUBSCRIPTION', and 'EVENT INITIATED BY'. All listed operations are 'Succeeded' and occurred between 6 hours ago and 7 days ago, all under the 'ASC DEMO' subscription.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
JIT Network Access request ended	Succeeded	6 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	9 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	10 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	12 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request ended	Succeeded	6 d ago	Sat Feb 25 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	6 d ago	Fri Feb 24 20...	ASC DEMO	
JIT Network Access request ended	Succeeded	7 d ago	Fri Feb 24 20...	ASC DEMO	

Figure 7: Azure Just in time VM access Activity Log

Configuration Management

The ongoing management of your Azure deployments should be grounded in automation. Azure offers several services which can help you not only deploy your environments in a repeatable fashion, but also ensure that they are configured to your requirements from the start.

AUTOMATE THE CONFIGURATION OF VMs

There are many tools which can help you create and manage your Azure virtual machines (VMs) in a consistent manner at any scale. These solutions all contribute to the overall infrastructure management and deployment lifecycle of your Azure workloads.

ANSIBLE, CHEF, AND PUPPET

[Ansible](#) is an automation engine for configuration management, VM creation, or application deployment. Ansible uses an agent-less model, typically with SSH keys, to authenticate and manage target machines. Configuration tasks are defined in playbooks, with a number of Ansible modules available to carry out specific tasks

[Chef](#) is an automation platform that helps define how your infrastructure is configured, deployed, and managed. Additional components included Chef Habitat for application lifecycle automation rather than the infrastructure, and Chef InSpec that helps automate compliance with security and policy requirements. Chef Clients are installed on target machines, with one or more central Chef Servers that store and manage the configurations.

[Puppet](#) is an enterprise-ready automation platform that handles the application delivery and deployment process. Agents are installed on target machines to allow Puppet Master to run manifests that define the desired configuration of the Azure infrastructure and VMs. Puppet

can integrate with other solutions such as Jenkins and GitHub for an improved DevOps workflow.

CLOUD-INIT FOR LINUX VMs

[cloud-init](#) is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files, or to configure users and security. Because cloud-init is called during the initial boot process, there are no additional steps or required agents to apply your configuration.

cloud-init also works across distributions. For example, you don't use apt-get install or yum install to install a package. Instead you can define a list of packages to install. Cloud-init automatically uses the native package management tool for the distro you select.

There are even [cloud-init enabled VMs in the Azure Marketplace](#). These images make your cloud-init deployments work seamlessly with VMs and Virtual Machine Scale Sets.

PUBLISHER	CLOUD-INIT READY
Canonical	Yes
Canonical	Yes
CoreOS	Yes
OpenLogic	Preview
RedHat	Preview

Figure 8: cloud-init Ready Distributions

POWERSHELL DESIRED STATE CONFIGURATION

[PowerShell Desired State Configuration \(DSC\)](#) is a management platform to define the configuration of target machines. DSC can also be used on Linux through the [Open Management Infrastructure \(OMI\) server](#).

DSC configurations define what to install on a machine and how to configure the host. A Local Configuration Manager (LCM) engine runs on each target node that processes requested actions based on pushed configurations. A pull server is a web service that runs on a central host to store the DSC configurations and associated resources. The pull server communicates with

the LCM engine on each target host to provide the required configurations and report on compliance.

AZURE CUSTOM SCRIPT EXTENSION

The Azure Custom Script Extension for [Linux](#) or [Windows](#) downloads and executes scripts on Azure VMs. You can use the extension when you create a VM, or any time after the VM is in use.

Scripts can be downloaded from Azure storage or any public location such as a GitHub repository. With the Custom Script Extension, you can write scripts in any language that runs on the source VM. These scripts can be used to install applications or configure the VM as desired. To secure credentials, sensitive information such as passwords can be stored in a protected configuration. These credentials are only decrypted inside the VM.

AUTOMATE INFRASTRUCTURE MANAGEMENT

There are a suite of technologies and tools which can be used in Azure to perform infrastructure management and contribute to the principles of managing infrastructure as code.

PACKER

[Packer](#) automates the build process when you create a custom VM image in Azure. You use Packer to define the OS and run post-configuration scripts that customize the VM for your specific needs. Once configured, the VM is then captured as a Managed Disk image. Packer automates the process to create the source VM, network and storage resources, run configuration scripts, and then create the VM image.

TERRAFORM

[Terraform](#) is an automation tool that allows you to define and create an entire Azure infrastructure with a single template format language - the HashiCorp Configuration

Language (HCL). With Terraform, you define templates that automate the process to create network, storage, and VM resources for a given application solution. You can use your existing Terraform templates for other platforms with Azure to ensure consistency and simplify the infrastructure deployment without needing to convert to an Azure Resource Manager template.

AZURE AUTOMATION

[Azure Automation](#) uses runbooks to process a set of tasks on the VMs you target. Azure Automation is used to manage existing VMs rather than to create an infrastructure. Azure Automation can run across both Linux and Windows VMs, as well as on-premises virtual or physical machines with a hybrid runbook worker. Runbooks can be stored in a source control repository, such as GitHub. These runbooks can then run manually or on a defined schedule.

Azure Automation also provides a Desired State Configuration (DSC) service that allows you to create definitions for how a given set of VMs should be configured. DSC then ensures that the required configuration is applied and the VM stays consistent. Azure Automation DSC runs on both Windows and Linux machines.

AZURE CLOUD SHELL

[Azure Cloud Shell](#) is an interactive, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work. Linux users can opt for a Bash experience, while Windows users can opt for PowerShell.

Azure Cloud Shell even includes pre-configured tools such as Ansible and Terraform which can accelerate your adoption of infrastructure automation.

Availability and Business Continuity

Your control plane for your Azure resources needs to provide coverage for the availability of the workloads you host and the account for the business continuity and disaster recovery needs of your applications.

Virtual Machine Availability

AZURE MAINTENANCE

To protect your critical applications and workloads you will need to consider a number of factors. As you design your virtual machine availability strategy, you will need to account for both maintenance in the Azure platform and downtime. There are three scenarios which can impact virtual machine availability: unplanned hardware maintenance, unexpected downtime, and planned maintenance.

Unplanned maintenance events occur when the Azure platform detects a pending failure in a virtual machine host, storage, or any other platform component associated with the physical platform. Microsoft uses Live Migration technology for your virtual machines, allowing Microsoft to migrate virtual machines from the faulting hardware to a healthy physical host. Live Migration allows Microsoft to perform these migrations while keeping memory, files, and network connections open during the migration but there may be performance impacts to your virtual machines before, during, and after the event.

Unexpected downtime occurs when the physical host fails unexpectedly. This can be anything from a network failure, a disk failure, or even a rack-level failure. When these events are detected, your virtual machine is automatically migrated to a healthy physical host with minimal downtime. While minimal, there is downtime in these types of events, including a reboot of your virtual machine and the reset of any ephemeral storage such as a temporary drive/scratch disk.

Planned maintenance events occur as a part of regular and ongoing Azure datacenter maintenance. In the majority of cases, Microsoft attempts to use [VM Preserving Maintenance](#), where your VM is paused while the underlying host is patched and unpause without any reboot once maintenance has completed. However, there

are instances where a reboot of your VM will be needed. In these instances you can use [Planned Maintenance](#) to schedule the reboot or redeployment of your virtual machine to a new host.

IMPROVING AVAILABILITY

There are three financially-backed [service level agreements for virtual machines](#) in Azure that you can select from based on your requirements.

- **99.9%** availability is guaranteed for single-instance virtual machines that use premium storage
- **99.95%** availability is guaranteed for at least one virtual machine when two or more instances are deployed in the same Availability Set
- **99.99%** availability is guaranteed for at least one virtual machine when two or more instances are deployed across two or more Availability Zones

AVAILABILITY SETS

Availability Sets allow you to spread two or more virtual machines across up to twenty update domains (UDs) within an Azure datacenter. During planned maintenance, Microsoft guarantees that only one update domain is updated at any given time. As UDs are updated within the data center, there is a 30-minute recovery window before the next UD is updated. This guarantee is what provides you with the increased SLA of 99.95% on your virtual machines.

The adoption of availability sets also increases your availability by ensuring your virtual machines are placed into multiple fault domains (FDs). FDs ensure that your virtual machines are grouped in a way that prevents them from sharing a common power source and network switch.

AVAILABILITY ZONES

Availability Zones offer even more resiliency than Availability Sets, hence the increased SLA of 99.99%. Availability Zones allow you to physically separate your virtual machines within an Azure region, with up to three Availability Zones supported per region. Each Availability Zone comes with its own power source, network, and cooling.

This makes Availability Zones a natural choice when you need to guarantee the protection of your applications in the event of the loss of an Azure datacenter.

Backup and Recovery

Azure offers both backup and recovery services natively with Azure Backup and Azure Site Recovery. Both services can backup and restore data, but each serves a different purpose in regards to business continuity and disaster recovery.

Azure Backup allows you to backup and restore data at a very granular level, including file and folder recovery. Azure Site Recovery can be used to replicate virtual machines between datacenters, orchestrate failovers, and

even perform migrations. At their most basic level, Azure Backup protects your data wherever it resides – in the cloud or on-premises while Azure Site Recovery coordinates virtual machine and physical server replication, failover, and failback.

Both services contribute to the business continuity and disaster recovery needs of your workloads and applications by keeping your data safe (Azure Backup) and keeping your workloads available (Azure Site Recovery) when outages occur.

As you determine your needs for backup and recovery, consider the following as you select services:

- **Recovery Point Objective (RPO)** – The amount of acceptable data loss if a recovery is needed
- **Recovery Time Objective (RTO)** – The amount of time that it takes to perform a restoration or recovery
- **Retention** – The amount of time the data needs to be stored

These characteristics will drive your selection. Note that you may have workloads which require both backup and disaster recovery (e.g. local resiliency as first layer and geo-redundancy for additional protection).

	BACKUP	DISASTER RECOVERY
RPO	Workloads with variable RPO. Servers may be days while databases may be hours or even minutes.	Workloads with low RPOs where DR copies are only a few minutes behind their source.
RTO	Backup solutions typically have longer RTOs as wider RPO windows drive larger backup sets. This can lead to recovery times of hours or days.	DR solutions will have much smaller RTOs, sometimes less than a minute as data is constantly synchronized with the source.
RETENTION	Backup is suitable for workloads with both long and short term retention needs. Compliance often drives the retention window (e.g. financial records often need to be retained for years).	DR is not suitable for long term retention as it is capturing so many changes in a short period of time.

AZURE BACKUP

[Azure Backup](#) is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure.

Traditional backup solutions have evolved to treat the cloud as an endpoint, or static storage destination, similar to disks or tape. While this approach is simple, it is limited and doesn't take full advantage of an underlying cloud platform, which translates to an expensive, inefficient solution. Other solutions are expensive because you end up paying for the wrong type of storage, or storage that you don't need. Other solutions are often inefficient because they don't offer you the type or amount of storage you need, or administrative tasks require too much time. In contrast, Azure Backup delivers these key benefits:

- **Automatic storage management** that offers automatic allocation and management of backup storage all in a pay as you use model – meaning you only pay for the storage you consume.
- **Unlimited scaling** with the built-in capabilities of Azure storage, including high availability, multiple storage sizes, and multiple storage tiers.
- **Multiple storage options** with access to both locally redundant storage and geo-redundant storage. Regardless of the option you choose, your data is always protected with at least three copies in a region.
- **Unlimited data transfer** with no caps on the amount of inbound or outbound data you transfer.
- **Data encryption** allows for the secure transmission and storage of your data with you in full control of the encryption passphrase (or key)
- **Application-consistent backup** means your recovery points have all the required data to restore the backup copy with no additional fixes required – reducing the restoration time and getting you running quicker.

- **Long-term retention** means you can keep data in the Recovery Services vault as long as you need.

AZURE BACKUP COVERAGE

Azure Backup provides coverage for a wide range of workloads and applications. At a high-level, Azure Backup provides coverage for files and folders, Hyper-V virtual machines, VMware virtual machines, Azure virtual machines, and application consistent backup for Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange,

A complete matrix of the data and workloads that can be protected with Azure Backup can be found at [Which applications and workloads can be backed up?](#).

DATA RETENTION

The length of time that backups can be retained is determined by the instance being protected (protected instance) and the frequency of backup (recovery points). Each protected instance can have up to 9,999 recovery points and there is no expiration limit on a single recovery point. A protected instance is defined as a Windows computer, a service (physical or virtual), or SQL database.

The configuration of your backup policy ultimately determines how quickly you consume recovery points. For example, if you create one recovery point a day every day of the week, you will be able to retain up to 27 years of recovery points (9999 recovery points / 365 days a year). If your application only requires monthly recovery points to meet its recovery needs, you will be able to store up to 833 years of recovery points (9999 recovery points / 12 months a year)

$$\frac{9999 \text{ Recovery Points}}{\text{Backup Frequency}} = \text{Retention}$$

Figure 9: Azure Backup Retention Formula

RECOVERING FROM FAILURE

Your backups are only as good as those that you test with recovery and you *must* regularly test your backups. You should test your backups at a minimum on a monthly basis if not more often to ensure their integrity and to ensure you have a viable recovery plan in the event restoration is required.

The restoration method for your protected data in Azure Backup will differ based on the type of backup (file and

folders versus full server) and the restoration tool (Azure CLI, Azure PowerShell, or the Azure Portal).

File and folder recovery is performed by determining the desired recovery point, mounting that recovery point to your virtual machine, copying the files you need, and then unmounting the recovery point. Files and folders can be restored to the same VM they were backed up from or restored to any entirely different machine.

Virtual machines that are backed up can be restored to a whole new virtual machine or disks can be mounted as additional data disks to existing virtual machines. Just as with file and folder recovery, you must select a recovery point along with the restore configuration (new VM or disk restore).

With support for Azure CLI and Azure PowerShell, you can even execute advanced restorations which may require additional post-restore configuration such as the instantiation of multiple network interfaces or a specific mount order for data disks on a virtual machine.

Disaster Recovery

AZURE SITE RECOVERY

[Azure Site Recovery](#) (ASR) helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it. Azure Site Recovery also forms the cornerstone of a lift-and-shift migration strategy, with support for replicating virtual machines between Azure regions (Azure-to-Azure), on-premises VMs and physical servers to Azure (Site to Azure), and even on-premises VMs and physical servers to a secondary site (Site to Site).

Azure Site Recovery offers a host of features:

- **Simple BCDR solution** – Using Site Recovery, you can set up and manage replication, failover, and fallback from a single location in the Azure portal.
- **Azure VM replication** – You can set up disaster recovery of Azure VMs from a primary region to a secondary region.

- **On-premises VM replication** – You can replicate on-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter. Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter.
- **Workload replication** – Replicate any workload running on supported Azure VMs, on-premises Hyper-V and VMware VMs, and Windows/Linux physical servers.
- **Data resilience** – Site recovery orchestrates replication without intercepting application data. When you replicate to Azure, data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created, based on the replicated data.
- **RTO and RPO targets** – Keep recovery time objectives (RTO) and recovery point objectives (RPO) within organizational limits. Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V. You can reduce RTO further by integrating with [Azure Traffic Manager](#).
- **Keep apps consistent over failover** – You can replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process.
- **Testing without disruption** – You can easily run disaster recovery drills, without affecting ongoing replication.
- **Flexible failovers** – You can run planned failovers for expected outages with zero-data loss, or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters. You can easily fail back to your primary site when it's available again.
- **Customized recovery plans** – Using recovery plans, you can customize and sequence the failover and recovery of multi-tier applications running on multiple VMs. You group machines together in a recovery plan, and optionally add scripts and manual actions. Recovery plans can be integrated with Azure automation runbooks.
- **BCDR integration** – Site Recovery integrates with other BCDR technologies. For example, you can use Site Recovery to protect the SQL Server backend of corporate workloads, with native support for SQL

Server AlwaysOn, to manage the failover of availability groups.

- **Azure automation integration** – A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery.
- **Network integration** – Site Recovery integrates with Azure for simple application network management, including reserving IP addresses, configuring load-balancers, and integrating Azure Traffic Manager for efficient network switchovers.

APPLICATION REPLICATION

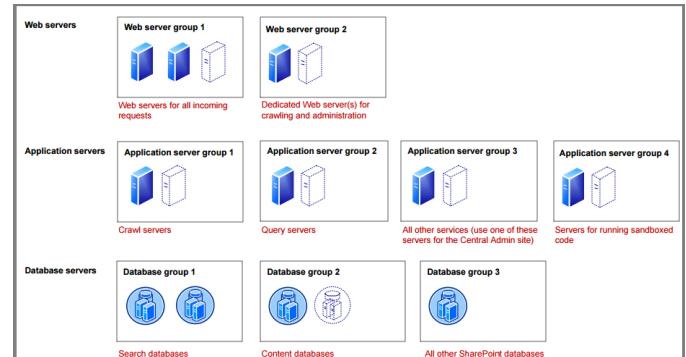
As previously mentioned, ASR allows you meet extremely low RPOs as a part of your recovery strategy. Due to its near-synchronous replication, you can execute recovery plans with RPOs as low as 30 seconds and low RTO network switchovers.

ASR is also suitable for single and multi-tier application recovery when properly configured. ASR is directly integrated with SQL AlwaysOn and supports other application level replication as well, including Active Directory replication, Exchange Database Availability Groups, and Oracle Data Guard.

To better understand ASR and its application-consistent recovery, we will show you how to [protect a multi-tier SharePoint farm with ASR and recover it to Azure](#) while calling out important considerations.

SharePoint is an interesting application, as it does not provide any out-of-the-box disaster recovery capabilities. It does have individual components that can be backed up and restored, however DR has always been a pain point. Any DR solution should have the ability to define and execute complicated recovery plans with automated and easily testable failover.

For our hypothetical SharePoint farm, we have three tiers: a web tier serving content to end users, an applicate tier providing core SharePoint functionality such as search crawlers and other application services, and a data tier made of Microsoft SQL servers.



Our first consideration after initial replication is can we improve availability and resiliency further by leveraging Azure services? With each tier performing a specific purpose, we have an opportunity to position the application with better availability in Azure. We can do this by configure the replicated VMs in each tier to be members of the same Availability Set.

Without machines replicated and configured for availability, we next need to ensure that the virtual network the farm will be hosted in is properly configured. For our SharePoint farm, we can define the target network in Azure and even set static IP addresses as needed. For applications like SharePoint which utilize fixed application and database servers, this is especially helpful.

Continuing our networking configuration, we also need to consider how users will access the SharePoint farm. With [Azure Traffic Manager](#), we can create a single endpoint which we can configure to server requests from both our on-premises SharePoint farm and a post-failover farm hosted in Azure. This leads to a streamlined end-user experience, as our users will use one URL to access SharePoint, and they do not need to be concerned with where the farm is hosted.

Finally, we will create a recovery plan. Recovery plans allow us to sequence the failover of tiers, which is critical in the case of applications like SharePoint where servers need to come online in a prescribed order. For our SharePoint farm, we will create multiple failover groups, ensuring that our database servers come online first, followed by our application servers, and finally our web servers.

Within the failover groups, we will leverage pre and post actions to execute runbooks in Azure Automation. These runbooks will provide us the flexible to execute SQL server availability group failovers in a coordinated fashion for

our data tier, and even attach a load balancer to the servers in our web tier as it comes online to service end-user requests.

TESTING FAILOVER AND DR DRILLS

Much like backup, your recovery plans are only good when they are tested and known to be valid. With ASR, you can test your failover to validate to disaster recovery and replication strategy, without any data loss or downtime. This means you can test and validate the entire recovery lifecycle without impacting production workloads.

In the case of our hypothetical SharePoint farm, we can use ASR's native failover testing capability to validate our replication and the configuration of our Azure Automation runbooks. Once validation is completed, we can use ASR's "Cleanup test failover" functionality to clean up all of the resources associated with our test failover, saving us time and money.

If there are errors that are found as a part of testing, you can update and iterate rapidly. Once you have a valid solution, you can also come back and execute your drills on a regular basis to ensure their ongoing validity.

Compliance and Monitoring

Governance and control of workloads begins with collecting data. In your virtual datacenter, we will build out a strategy for collecting and analyzing the data in your Azure estate to determine the performance, health, and availability of your workloads and the resources that they depend on.

Azure Monitoring Concepts

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.

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.

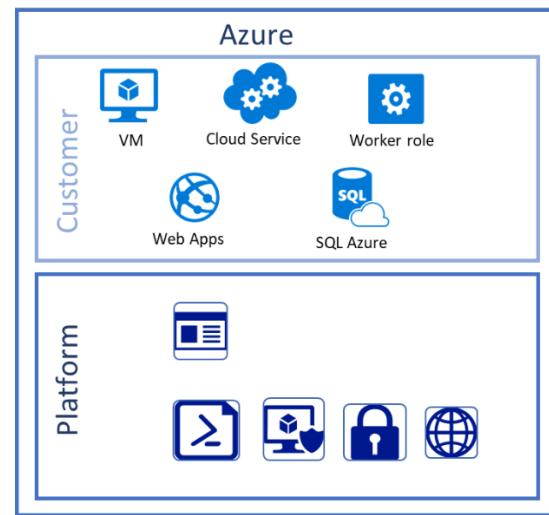


Figure 10: Azure Customer and Platform Monitoring

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 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 minute 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

[Log Analytics](#) plays 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.
- [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.

Support and Incident Management

Supporting an Azure estate for your customers includes interactions with Microsoft and with those customers to offer a best-in-class support service. As an intermediary to Microsoft, we'll show you your options for engaging Microsoft support and discuss strategies for streamlining customer support.

Engaging Support

COMMERCIAL SUPPORT

At some point, you may need to contact Microsoft to escalate an issue. Microsoft offers several options via forum support or via paid options.

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:

- **Developer:** Suitable for trial and non-production environments
- **Standard:** Suitable for non-critical production environments
- **Professional Direct:** For critical production workloads

- **Premier:** For customers who need support beyond Azure and have a substantial dependence across multiple Microsoft products

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. Developer support plans do not include a response SLA for anything above a Severity C issue.

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.

CSP SUPPORT

If you are a CSP or have sold support as part of your managed services solution you are the front-line support for your customer. As the first point of contact for your customers, your responsibilities increase.

If you are an Azure CSP direct partner, you will provide all technical and account support services for your customers. This means many things, including:

- Describing the capabilities of different Azure services.

- Providing answers to Azure pricing and usage questions.
- Providing billing and subscription support.
- Providing provisioning and deployment help.
- Resolving performance problems, service availability problems, incomplete software integration problems, or other deployment problems.

If you are an Azure CSP indirect reseller, the responsibilities noted above are shared by both you and your Azure CSP indirect provider.

As a CSP, you must provide your customers with a clear description of how they will receive support, and that description must include an SLA. Again, your SLAs can also be as good as the SLA that Microsoft provides you, so keep this in mind when you consider the [Azure CSP support plans](#).

The Azure CSP Support Plans use the same severity classification system as commercial support plans with the response SLA dictated by the support level purchased. All CSP direct partners have access to an included support plan or can optionally purchase a deeper level of support through the [Advanced Support for Partners \(ASfP\)](#) or the [Premier Support for Partners \(PSfP\)](#) plans. Your defining considerations will be your requirements around resolution priority for submitted issues and access to 24x7x365 critical situation support.

For your customers, consider that they rely on you for all of their Azure support needs. They cannot directly contact Microsoft for support nor is Microsoft able to provide them support. With this in mind, it is critical that you keep your organizational profile in the Partner Center updated. Specify the correct email and phone number for your helpdesk and if you have a ticket management system or other ITSM system, provide a link to the page where your customers can submit a support request. This information is shown to your customers if they try and submit a request through the Azure Portal.

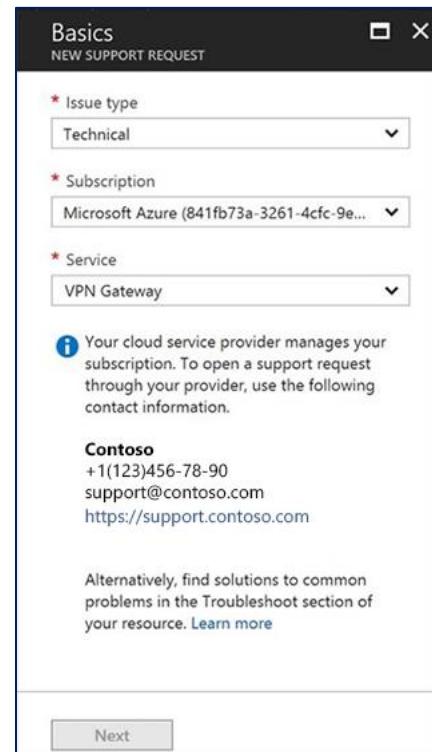


Figure 11: Azure CSP Customer Support Details

Incident Management

Now that you understand how you can interact with Microsoft support, consider how you will interact with your customers and how they will interact with you. Supporting an Azure estate and building support team are not inconsequential tasks.

STAFFING AND TECHNICAL SUPPORT

Not only will your support team need to meet your SLAs and other covenants you have with your customers, including response time, but they will also need to have the right skillset to service your customers and know who to escalate issues to when needed.

One of the best ways to ensure your customers are delighted with your service and to reduce your issue volume during known events is to proactively monitor your customer environments and notify customers in advance of pending service interruptions. This includes checking Azure service health regularly along with other daily operations.

As issues do arise, whether it is through proactive monitoring, reactive alerting, or a customer generated



issue, you must also have a defined workflow and triage process for how issues will be handled within your helpdesk. This includes escalation paths for service delivery (e.g. Tier 1 support handoff to Tier 2) and how your staffing maps to your SLAs. For instance, if you have an SLA which states you will have a dedicated engineer for all Severity A issues available 24x7, ensure you have a documented plan for how those resources will be contacted and engage with the customers throughout the triage and eventual resolution of an issue.

Regardless of the issue, your first focus should always be on resolution of the issue and not root cause analysis. There will always be time after an issue is resolved to go back and interrogate logs. In fact, you may consider offering root cause analysis as an additive offering, providing more value to the customers that require it.

KNOWLEDGE MANAGEMENT

Building a knowledge base for your support staff and engineers will be your first line of defense in addressing common customer issues and being able to fix issues quickly. A good knowledge base will integrate directly with your ITSM tooling, allowing you to quickly see relevant articles as issues are worked.

Your support, engineering, and operations team should all be encouraged to contribute to the knowledge base, and custom solutions for customers should always be documented in some fashion. By planning for support, you can mitigate many issues before they become problems for your customers.

ITSM TOOLS

There are many tools in Azure to detect, analyze, and troubleshoot issues with your Azure and non-Azure resources. However, the work items related to an issue (e.g. tickets or incidents) are often captured in another system dedicated to IT service management (ITSM).

As you are selecting your ITSM tools, consider using tools which integrate directly with Azure services such as Azure Log Analytics and Azure Monitor. Leverage compatible tools will allow you to have bi-directional connectivity between your customer's Azure environment and your ITSM tooling.

The [IT Service Management Connection \(ITSMC\)](#) allows you to integrate a Log Analytics workspace with the following ITSM tools:

- ServiceNow
- System Center Service Manager
- Provance
- Cherwell

With the ITSMC, you can create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts). Optionally, you can also synchronize your incident and change request data from your ITSM back to a Log Analytics workspace.

Another primary benefit of adopting an ITSM tool will be having the ability to offer your customers self-service tools, including dashboards, reports, and the ability to create self-service requests without having to contact you. Self-service also includes the ability to notify your customers of issue status and inform them of resolution when required.

HEALTHY SUPPORT CULTURE

Irrespective of the software you select to run your help desk and the monitoring tools you empower your staff with, your staff will always be the more important asset in your support organization. Unhappy support staff will be known to your customers and have a detrimental impact on your ability to deliver quality services to your customers.

With that in mind, be open to soliciting feedback from your staff on where improvements can be made in your processes. A helpdesk is a living thing, meant to change over time. Perform regular reviews of your workflows, escalation paths, and interaction metrics.

Also consider building post-mortems directly into your service delivery. This gives your staff an opportunity to improve over time and with a measured cadence.

Implementing these types of activities into your service delivery organization from the start will create a culture where staff are open to learning from each other and where transparency is just the way it is.

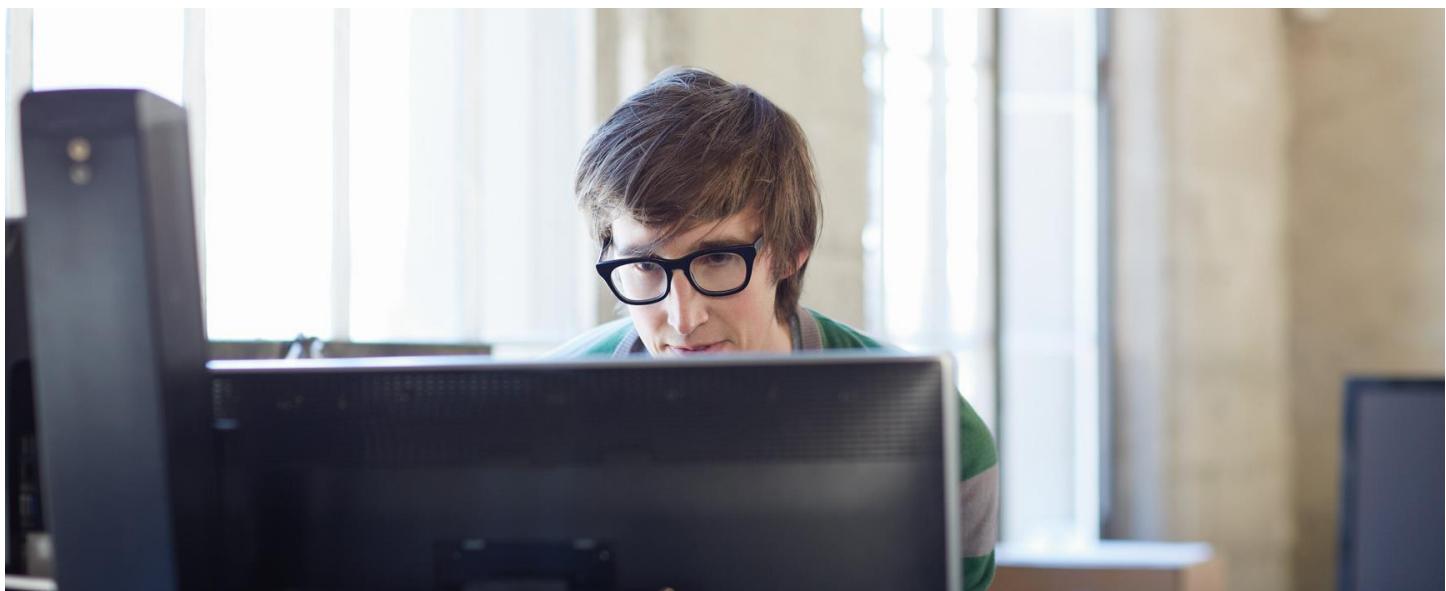
Automation and DevOps Support Resources

DevOps brings together people, processes, and technology, automating software delivery to provide continuous value to your users. With Azure DevOps solutions, you can deliver software faster and more reliably.

AUTOMATE APPLICATION DEPLOYMENT AND DELIVERY

Azure supports a rich set of tools for going beyond the configuration and management of virtual machines, with tooling that brings automated builds and deployment, continuous integration, and testing in to your DevOps lifecycle.

CONTINUOUS INTEGRATION (CI)	CONTINUOUS DEVELOPMENT (CD)	CONTINUOUS DEPLOYMENT WITH CI/CD
Take advantage of continuous integration to improve software development quality and speed. When you use Visual Studio Team Services or Jenkins to build apps in the cloud and deploy to Azure, each time you commit code, it's automatically built and tested—so bugs are detected faster.	Ensure that code and infrastructure are always in a production-deployable state, with continuous delivery. By combining continuous integration and infrastructure as code (IaC), you'll achieve identical deployments and the confidence you need to manually deploy to production at any time.	With continuous deployment, you can automate the entire process from code commit to production if your CI/CD tests are successful. Using CI/CD practices, paired with monitoring tools, you'll be able to safely deliver features to your customers as soon as they're ready.



Deployment Strategies

While deployment of code through continuous integration and deployment tools often comes to the forefront with DevOps, there is a precursor, and that is the automated deployment of your infrastructure (or infrastructure as code).

INFRASTRUCTURE AS CODE

In [Configuration Management](#), we focused on tools that can help you configure your virtual machines and infrastructure post-deployment. In this section, we will explore the methods and tools you can use to deploy your infrastructure in an automated manner and integrate that automation into a software development lifecycle.

Infrastructure as code (IaC) is the process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.

Source: https://en.wikipedia.org/wiki/Infrastructure_as_Code

The primary goals of adopting Infrastructure as Code (IaC) are:

- **Cost Reduction:** By focusing on automation, you can invest your time and the time of your staff in the development and execution of repeatable processes.
- **Faster Execution:** Through the development of repeatable processes, your time to execute builds drastically decreases and your time to provision resources becomes a known quantity
- **Risk Mitigation:** With a well-known and tested declarative provisioning model, you know your environments are going to be deployed the right way, the first time, reducing risk through manual intervention.

IaC ultimately leads us to a declarative provisioning model, where we define *what* we are going to provision. We then can use imperative provisioning to control *how* that infrastructure is configured.

Regardless of the technology you select, you should have the ability to repeatedly deploy your solution throughout its lifecycle and have confidence it is deployed in a consistent state.

AZURE RESOURCE MANAGER TEMPLATES

[Azure Resource Manager \(ARM\) templates](#) allow you to create declarative JSON files that define your Azure infrastructure and the configuration of Azure resources.

```
"resources": [
  {
    "apiVersion": "2016-01-01",
    "type": "Microsoft.Storage/storageAccounts",
    "name": "mystorageaccount",
    "location": "westus",
    "sku": {
      "name": "Standard_LRS"
    },
    "kind": "Storage",
    "properties": {}
  }
]
```

Figure 12: Sample ARM Template

When you deploy an Azure resource through the Azure Portal, a template can be generated for later re-use. This means you do not need to start from scratch. Microsoft even maintains a GitHub repository with hundreds of [QuickStart Templates](#) which can be used within your deployments.

TERRAFORM

[Hashicorp Terraform](#) is an open source tool for provisioning and managing cloud infrastructure. Much like ARM, it allows you to create text-based templates called Terraform configurations. Configurations are where you author your infrastructure and define its configuration. Configurations in Terraform follow a known syntax – the [Hashicorp Configuration Language \(HCL\)](#). Terraform can also recognize JSON files, and even supports nesting in existing ARM templates.

There are several considerations for Terraform where it may work better for you or your customers.

- Your staff have existing expertise in Terraform – if this is the case, your staff can reuse their existing skills while they get up-to-speed on Azure
- Your customers are not exclusively using Azure – Terraform has multicloud support, with resource providers for Azure and other major cloud platforms. If your customers are approaching multicloud environments, Terraform can provide a consistent deployment model for them.

```

# Configure the Azure Provider
provider "azurerm" { }

# Create a resource group
resource "azurerm_resource_group" "network" {
  name      = "production"
  location  = "West US"
}

# Create a virtual network within the resource group
resource "azurerm_virtual_network" "network" {
  name          = "production-network"
  address_space = ["10.0.0.0/16"]
  location      =
"${azurerm_resource_group.network.location}"
  resource_group_name =
"${azurerm_resource_group.name}"

  subnet {
    name      = "subnet1"
    address_prefix = "10.0.1.0/24"
  }

  subnet {
    name      = "subnet2"
    address_prefix = "10.0.2.0/24"
  }

  subnet {
    name      = "subnet3"
    address_prefix = "10.0.3.0/24"
  }
}

```

Figure 13: Sample Terraform Configuration

Microsoft has [invested deeply in the Terraform experience on Azure](#) by directly partnering with Terraform to deliver a best-in-class experience for Terraform on the Azure platform. This investment means that Microsoft is committed to bringing latest Azure resources to Terraform and ensuring Hashicorp can support them.

Microsoft has also announced a dedicated [Azure Terraform Resource Provider](#), which will allow partners and customers to provision Azure resources with native Terraform providers, deepening the integration between ARM and Terraform.

DEVOPS LIFECYCLE

Now that you know how to declaratively provision infrastructure, it is time to think about how you can integrate that code into an existing software development lifecycle (SDLC) and your DevOps lifecycle. This includes storing your templates and scripts in a source control repository, where a single version of truth can be maintained. All of your team members who need to

interact with this code should have access to the repository with appropriate roles and rights. Also consider providing staff who require it an area where they can develop and test these assets by deploying their own version of the defined infrastructure.

Another benefit of managing your code in a repository is you will have a full audit trail of your infrastructure, understanding who changed what, along with when and why they changed it. Consider integrating the commits and check-ins of these infrastructure resources into a wider continuous delivery methodology using the tools mentioned below.

Deploying Code

AZURE DEVOPS PROJECT

The [Azure DevOps Project](#) presents a simplified experience where you bring your existing code and Git repository, or choose from one of the sample applications to create a Continuous Integration (CI) and Continuous Delivery (CD) pipeline to Azure. With 5-minute Quickstarts for most programming languages, including [.NET](#), [Node.js](#), [Java](#), [Python](#), [PHP](#), [Ruby](#), and [Go](#) you can get started quickly. DevOps Projects even has step-by-step tutorials for creating Visual Studio Team Services Release pipeline with many popular Azure services.

VISUAL STUDIO TEAM SERVICES

[Visual Studio Team Services \(VSTS\)](#) is a suite of tools that help you share and track code, use automated builds, and create a complete continuous integration and development (CI/CD) pipeline. Team Services integrates with Visual Studio and other editors to simplify usage. Team Services can also create and configure Azure VMs and then deploy code to them.

JENKINS

[Jenkins](#) is a continuous integration server that helps deploy and test applications and create automated pipelines for code delivery. There are hundreds of plugins to extend the core Jenkins platform, and you can also integrate with many other products and solutions through webhooks. You can manually install Jenkins on an Azure VM, run Jenkins from within a Docker container, or use a pre-built Azure Marketplace image.

Continuous Integration / Continuous Deployment

With an understanding of how to build your infrastructure as code and some of the tools to deploy your code, we can now explore building a rich pipeline for continuous integration and continuous deployment.

For partners, this is an excellent opportunity to add value for your customers by demonstrating your ability to execute advanced deployment scenarios.

Most organizations will approach their cloud deployments as singular entities, forgetting they can integrate even on-premises environments and existing applications into these pipelines.

Consider a customer that has an Azure App Service that they want to run on-premises in Azure Stack and in the Azure public cloud. Using the principles and tools we've shown, this becomes an easy process.

Your engineers can define the entire environment declaratively in one or more ARM templates. Azure Stack

shares a common API surface with Azure, allowing you to reuse the same template across even hybrid environments. After the template is developed and tested, it is checked into Visual Studio Team Services (VSTS) where it can automatically be tested through continuous integration with application build and unit tests.

After the build passes its tests, VSTS will trigger a continuous deployment to orchestrate the deployment of the ARM template and the web app code to both environments, passing in environment specific parameters at the time of deployment.

In just a few steps, you can empower your engineers and customers to deployment to multiple environments in a repeatable, testable, and known way.

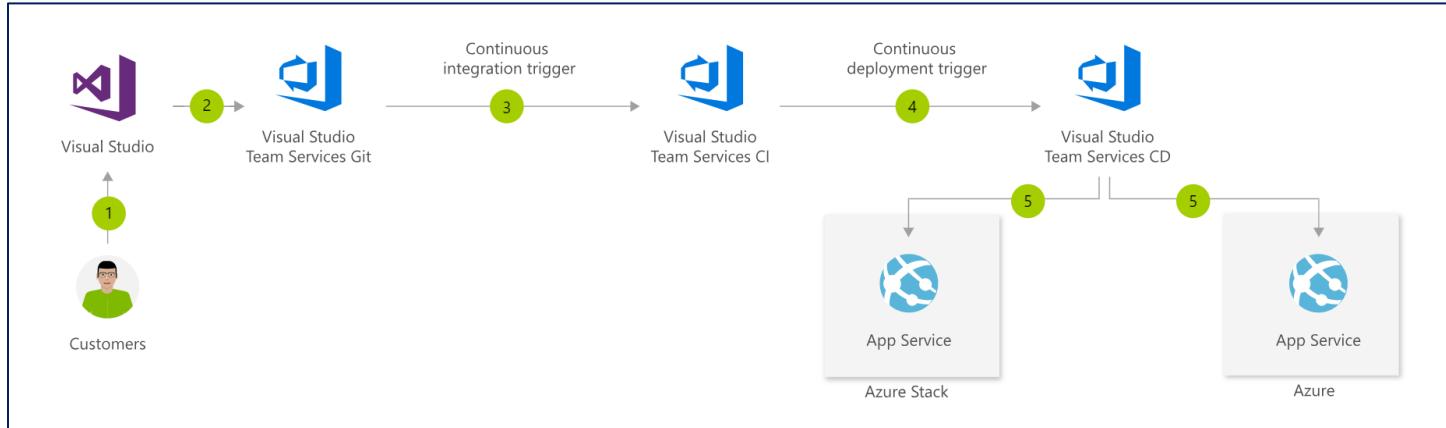


Figure 14: CI/CD with Azure

For more examples of what you can accomplish with CI/CD and Azure, visit the [Azure Solution Architecture Center](#).

Go to Market & Close Deals

Microsoft
Partner
Network

Cloud Operations & Management

aka.ms/practiceplaybooks



Executive Summary

In previous sections in the playbook, we covered topics from how to build your practice from selecting products or services to specialize in, to building and training your team to make your ideas a reality, to bringing your special offering to market and finding and keeping great customers. So, what's left to do? In this section, we'll discover strategies to compel potential customers that may be sitting on the fence to take action, from creating a good value proposition to building marketing and sales materials that tell your story.

It has been said that your current customers are your best customers. Do you know who your best customers are? What do they have in common? And how do you find more like them? We'll start by helping you build foundational marketing materials such as marketing personas, points of differentiation, value propositions, and customer business needs.

Once you've built the foundation, we'll look at how you can put these materials to work. We'll go through the different ways you can attract new customers and look at best practices. How do you put it all together? We'll discuss why integrated marketing campaigns work the best, and

the tools you need to run them, such as a CRM system and marketing automation.

But marketing is only half of the story. Your sales team is the other half. Don't forget how the two work together and what marketing can do to support sales. The job of the marketing team is to build out not only customer facing materials, but also compelling materials that can be used to train and arm your sales team.

The sales end of the bargain is to close the sale. One way to do this is by writing a winning proposal. Another way is to build a proof of concept or prototype of your product or service offering, which could help a prospect understand what it is you're offering, or solidify their vision of what you can help make possible. Microsoft is committed to helping your business grow, and provides both co-selling and co-marketing opportunities.

Finally, don't miss the Microsoft resources available in the [Go-to-Market and Close Deals guide](#), which you can leverage to help build your marketing materials and campaigns, as well as resources to help your team close the deal.

TOP 5 THINGS TO DO

Add value to your practice and turn your prospective customers into lasting ones. These are the top 5 things you should do to go to market and get deals done.

- Identify your customer's business needs
- Write a compelling value proposition
- Leverage marketing to find customers
- Build marketing and sales materials
- Collaborate with partners

Managed Services Transition

Transitioning customer support to a managed services team

This is the stage where transitioning to the service delivery management team.

Depending on what was delivered there this could be a simple as validation of expectations. However, in the transformative world of cloud there is expectations and opportunity at this stage.

EXPECTATIONS

If you delivered IP (SaaS) then there is an expectation that you will maintain and support this IP. This allows for annuity for maintenance. It is recommended your handle this stage as an upsell unless the maintenance was agreed upon prior to/or during delivery.

OPPORTUNITY

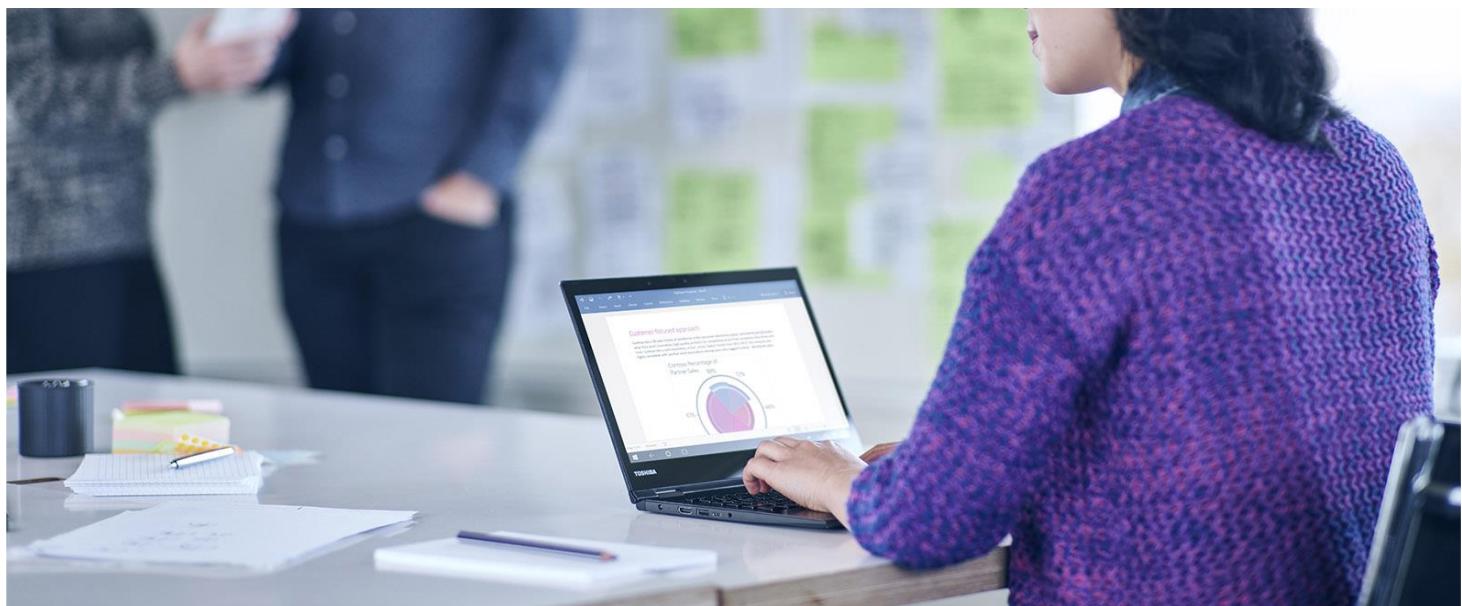
Even if you did not deliver IP to the customer there is an opportunity to make continued annuity by offering levels of support (if your company business model supports this). This is where the Digital Partner of Record (DPoR) conversation can happen for annuity, or your company can establish levels of support on your own cost structure.

DIGITAL PARTNER OF RECORD

Customers benefit from adding a Digital Partner of Record. Doing so provides the partner with access to usage and consumption data, which allows the partner to better serve the customer and help them perfect the use of Microsoft services for their desired business outcome. This partner will also be automatically contacted for any FastTrack (<https://fasttrack.microsoft.com/>) services questions or issues.

More information on Digital Partner of Record:

<https://partner.microsoft.com/en-US/membership/digital-partner-of-Record>



Marketing Your Cloud Operations Management Offerings

Plan your customer's journey to buying

The cloud changes your partner business model. Buyers buy differently than in the past. With all the information on the internet, buyers tend to research and self-educate long before they engage with sales people. By the time they do engage with sales, they've often already made some decisions.

To help illustrate this, just think about the way a buyer might go about buying a new car. Before going to the car dealership, the buyer will likely read about various car models on the internet, read reviews, and make some decisions. When the buyer is ready to visit a dealership, they already know what they want and how much they are willing to pay for that car. This poses a challenge for sellers. How can you get prospects to engage with you earlier in the process? Through marketing.

Another way partner businesses are changing is that when selling cloud-based solutions, you can gain recurring revenue streams. Recurring revenues provide business stability and confidence for business owners and managers, allowing them to make business decisions that may not be as easy when revenues are irregular and lumpy. While these recurring revenues are smaller on a per-transaction basis than buyers' large capital expenditures, you adjust for this. You'll need a higher volume of transactions. To support that, you'll need a higher volume of high-quality sales leads (through modern marketing techniques) coming in to create larger sales pipelines. Clients who are buying on a recurring basis represent great opportunities for you to upsell and cross-sell additional products and services.

Marketing is not an option anymore. Marketing helps you educate, identify, and engage with prospects earlier in the sales process. By identifying prospects who indicate interest in your products and services via their behavior (website visits, clicks, downloads, etc.), marketing can deliver high-quality leads.

Inbound marketing techniques such as search engine optimization and pay-per-click advertising make it easy for prospects to find you. Outbound marketing techniques, such as e-mail and telemarketing, enable you to tell prospects about your company's solutions.

Marketing is the toolset that addresses all these changes. Marketing today is digital and has the power to reach more people. Again, it's not to say that more traditional, non-digital marketing is ineffective. But to be found by prospective buyers that you don't have a relationship with, you need to employ digital marketing techniques. Modern marketing is focused on the prospects' and clients' views of the world.

RESOURCES

- [Planning your Cloud Business Transition: Sales Video](#)
- [Strategies for Unlocking Digital Transformation](#)
- [Smart Partner Marketing Resources](#)

Consultative Selling and Technical Pre-Sales

From the very start of your engagement with a prospect, you need to be aware of the need for technical pre-sales assistance. Many times, you are dealing with business decision makers during the buying cycle. In that case, you are less likely to have a need for technical assistance. However more than ever before, technical staff are a part of decision making with Azure practices. When the customer has one or more technical resources on the purchase committee, you need to engage technical pre-sales.

Your technical pre-sales staff should be very experienced users of your products and services. These employees need training or experience as a user of your products. Former support employees often make good technical pre-sales staff. The technical pre-sales staff is in place to explain technology, how it works, how it meets a business need and to answer any other questions. The business benefits can be left to the sales and marketing staff. This is where they shine. The technical staff should excel at the more complex issues that come from prospects. Technical staff should be dedicated to pre-sales. They should work together with sales efforts. One without the other cannot be effective. You need the sales staff to speak to business decision makers. Equally, you need pre-sales to answer all technical inquiries.

Examples of technical probing questions to ask during presales conversations supporting a cloud operations and management practice:

- Are you currently leveraging cross-platform mobile development to reach more customers?
- How do you automate your development and build process to ensure fast and efficient use of resources? Is there any bottlenecks or issues with your current setup?
- What does your Continuous Integration (CI) process look like today?
- Do you have a plan to modify your internal business apps to support a more cloud friendly and/or hybrid design?
- If your business and consequently your web application traffic was to double tomorrow, would your infrastructure be able to handle it?
- Do you feel like you would benefit from utilizing PaaS-based systems rather than maintaining your on-premises architecture, if so, what areas are you most interesting in exploring?
- What is your future proof technology plan? Have you considered a "containerized" and micro-services based approach to new and possibly your legacy applications?

RESOURCES

→ [Azure Pre-Sales Resources](#)

Guide: Go-to-Market and Close Deals

Leverage the Microsoft resources available in the [Go-to-Market and Close Deals guide](#), for details on marketing to the cloud buyer, aligning marketing goals with business goals, developing value propositions, and marketing and sales assets, resources, and best practices.



Microsoft
Partner
Network

Optimize & Grow

Cloud Operations
& Management

aka.ms/practiceplaybooks



Executive Summary

So far, we've covered strategies for building your practice, finding and keeping customers providing them with ongoing support.

In this section, we'll focus on how to optimize your practice, strengthen your relationship with customers, and evaluate your performance to help you continue to delight prospects and customers.

Are your customers delighted by your services and products? Delighted and not just satisfied? In this section, you'll learn why customer lifetime value is so important, and how to create more customers for life. We'll share how to get to know your customers better by following their journey with secret shopping and analysis. We'll also explore the use of a "land and expand" strategy and see how getting to know your customers better can lead to incremental opportunities to provide additional services.

You will also discover ways you can keep your solutions top of mind for prospects and customers through nurture marketing, and how to grow and improve your lead generation practice through a well-planned referral marketing program. We'll show you how to make the

most of your renewal process, and how to get ahead of deadlines.

We will help you learn how to grow your business by identifying the best customer personas and creating "look-alike" prospects, deepening your expertise in key verticals and marketing that expertise, and collaborating with other partners to offer your customers a more comprehensive level of service and support.

We will end by discussing how important it is to create advocates for your company. This includes turning a customer into a fan and collecting testimonials to create case studies that can be used in future marketing campaigns. Map your customer's experience and ask for feedback to ensure you are turning satisfied customers into delighted customers who can wait to tell your story!

Use the strategies we provide in this section and in the [Optimize and Grow guide](#) to optimize and grow your practice.

Top 5 things to do

Learn from your customers and experience to optimize your practice, and expand to new markets through strategic partnerships. These are the top 5 things you should do to optimize and grow your practice.

- Gather feedback from your customers
- Nurture existing customers
- Turn customers into advocates
- Generate referrals with marketing
- Nurture strategic partnerships

Guide: Optimize and Grow

Leverage the Microsoft resources available in the [Optimize and Grow guide](#), for details on building customer lifetime value, executing nurture marketing efforts, optimizing and growing from feedback, refining your customer value proposition, growing partnerships, and measuring results.



Playbook Summary

Thank you for taking the time to review this playbook. We hope you have gained new insight on how to add the cloud application development practice, and how to successfully grow your practice by taking advantage of unique offerings from Microsoft, engaging with your customers, and forming strategic partnerships.

Our goal, when creating this playbook, was to organize resources and provide insight that you can use to quickly accelerate or optimize your Azure Operations focused practice. To this end, we laid out the practice's opportunity, then provided relevant information on business strategies and technical topics to capitalize on the opportunity, within five sections that you can review in order, or individually at any time.

In the first section, **Define Your Strategy**, we helped you thoroughly define the strategy upon which your practice will be built. The key actions we prompted you to take are: Identify your unique value proposition, define and price your offer, build your business plan, leverage the Microsoft Partner Network, and plan your support options.

In the second section, **Operationalize & Get Trained**, we focused on the importance of hiring the right team, and then providing appropriate and ongoing training and certifications. We also suggested various tools and resources for building your product or service, managing your customers, and reviewing the marketplace. The top five things we suggested you do are: Hire, train, and certify your team, reskill existing resources where appropriate, and become the Digital Partner of Record on your customer's Azure subscriptions, setup your CRM, project management, collaboration, and support tools, build your sales, marketing, and legal materials, and evaluate your marketplace options.

The third section, **Go to Market**, emphasized getting your practice off the ground by finding new customers, and then nurturing and investing in them to build lasting relationships.

The key takeaways were: Define your customer's buying journey, launch a modern website and digital marketing activities, find your first customer through Microsoft's resources and nurture the relationship, build a presence in the community, and invest in marketing automation tools.

The fourth section, **Close & Execute Deals**, showed you how you can add value to your practice and turn your prospective customers into lasting ones, by working efficiently, selling Azure solutions as part of your offering, and negotiating deals. We prompted you to take action on the following: Identify opportunities to co-sell with Microsoft, write a winning proposal and be prepared to negotiate, conduct an architecture design session and build a proof of concept, provide ongoing support to your customers, and leverage Microsoft investment funds.

The final section, **Optimize & Grow your Practice**, stressed the importance of learning from your customers and your experience in providing solutions to them, to optimize your practice, and expand to new vertical markets through strategic partnerships. The top five actions we provided for you in this section were: Gather feedback from your customers, learn from your project successes and failures, create case studies and a marketing plan to expand into new vertical markets, maximize your efficiency and profit to fuel growth, and establish and nurture strategic partnerships.

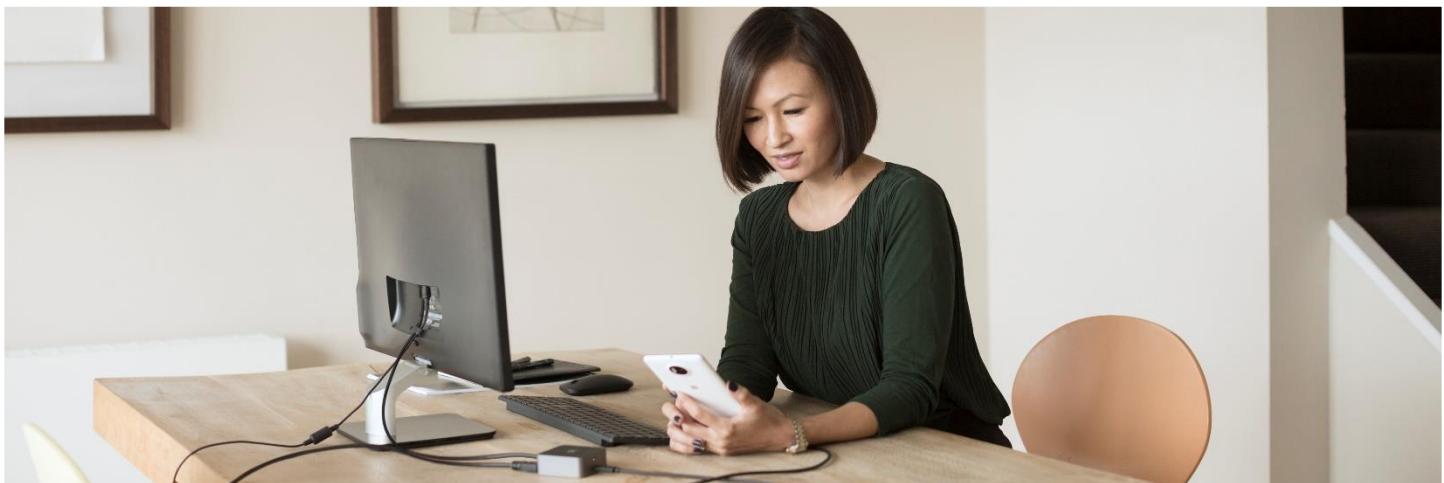
FEEDBACK

Share feedback on how we can improve this and other playbooks by emailing playbookfeedback@microsoft.com

Why Choose Microsoft?

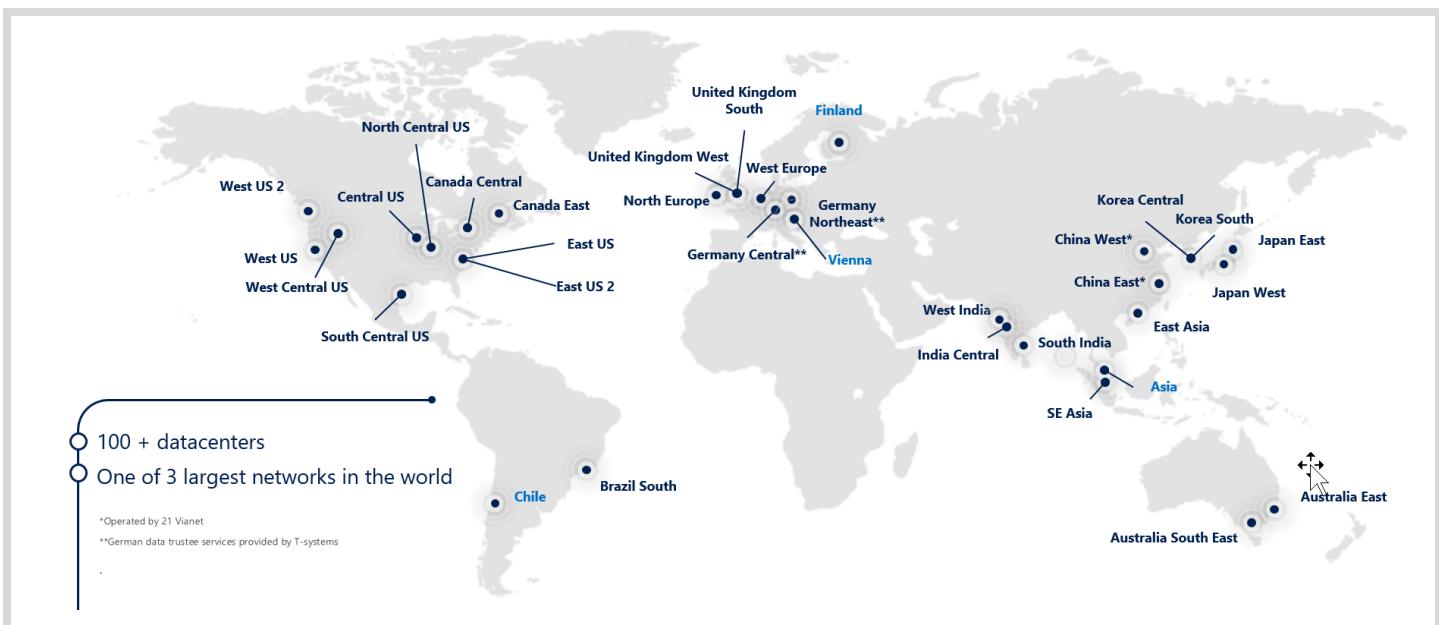
A trusted global leader, committed to partners, a leading enterprise mobility and security platform.

More than 86% of Fortune 500 companies have the Microsoft Cloud (source: Microsoft), which offers companies 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.



36 REGIONS AND COUNTING

In order to help organizations meet data residency, sovereignty and compliance requirements, Microsoft has a worldwide network of more than 30 announced Microsoft-managed datacenter regions, and continues to make significant investments in geo-expansion through our local and sovereign offerings in more than 10 unique geographic regions worldwide.



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 APIs. 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 Hyper Scale 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.

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 competitors 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.

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.

	Regulatory and Compliance Domain	Office 365	Microsoft Azure	Microsoft Dynamics CRM	Microsoft Intune
Broadly Applicable	ISO 27018:2014	✓	✓	✓	✓
	ISO 27001:2013	✓	✓	✓	✓
	SOC 1 Type 2 (SSAE 16/ISAE 3402)	✓	✓	✓	✓
	SOC 2 Type 2 (AT Section 101)	✓	✓	✓	✓
United States Government	CSA STAR 1	✓	✓	✓	No
	FedRAMP Moderate	✓	✓	✓	No
	CJIS Security Policy, Version 5.3	✓	✓	✓	No
	DISA SRG Level 2 P-ATO	✓	✓	✓	No
	FDA 21 CFR Part 11	✓	✓	✓	No
	ITAR	✓	✓	No	No
	IRS 1075	✓	✓	No	No
Industry Specific	HIPAA BAA	✓	✓	✓	✓
	PCI DSS Level 1	N/A	✓	N/A	N/A
	FERPA	✓	✓	✓	N/A
	CDSA	N/A	✓	N/A	N/A
Region/Country Specific	EU Model Clauses	✓	✓	✓	✓
	UK G-Cloud v6	✓	✓	✓	✓
	Australia Gov ASD	✓	✓	✓	No
	Singapore MTCS	✓	✓	✓	No
	Japan FISC	✓	✓	No	No
	New Zealand GCIO	✓	✓	✓	✓
	EU-US Privacy Shield	✓	✓	✓	✓
China (MLPS, TRUCS, GB 18030)		✓	No	No	No

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](#).

COMMITTED TO PARTNERS

From the diverse range of partner focused training Microsoft produces on sales, marketing and technical topics, to the business investment funds it makes available to help partners succeed in their customer engagements, to unique programs like the Cloud Solution Provider program that enable partners to own the complete customer relationship and to marketplaces and digital

show cases that highlight partners to new customers and give partners broad exposure, Microsoft is committed to enabling partner success in Data Platform and Analytics.

Research shows this commitment to partners and also appears in partner revenue. In a recent IDC study, partners reported earning \$9.64 in revenue for every \$1 of Microsoft revenue generated in 2017. This is expected to continue through 2022 and include a mix of software (45%), services (50%), and hardware (5%), that are sold in relation to Microsoft solutions.



Source: IDC eBook, sponsored by Microsoft, The Microsoft Digital Transformation Series, Part 1: The Digital Transformation Opportunity, 2018

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 Azure forums:

- ➔ [Azure Active Directory](#)
- ➔ [Azure Storage](#)
- ➔ [Azure Networking](#)
- ➔ [Azure Virtual Machines](#)
- ➔ [Azure Automation](#)
- ➔ [Azure Scripting and Command Line Tools](#)
- ➔ [Azure Log Analytics](#)
- ➔ [Azure Security Center](#)

AZURE TROUBLESHOOTING RESOURCES

TROUBLESHOOTING AZURE ACTIVE DIRECTORY

Azure AD Connectivity	Password Management
Azure AD Domain Services	Azure AD Connect Synchronization Issues
Troubleshooting Azure AD Connectivity	Troubleshooting Password Management
Troubleshooting Azure AD Domain Services	Troubleshooting Azure AD Connect Synchronization Issues

TROUBLESHOOTING AZURE INFRASTRUCTURE AS A SERVICE

Troubleshooting RDP Connections	Reset Remote Desktop Connections
Troubleshoot Creating a New VM	Troubleshooting Specific RDP Errors
Troubleshoot Restarting or Resizing a VM	Troubleshoot Application Access
Troubleshoot Allocation Failures on Windows	Troubleshooting SSH Connections
Troubleshooting Application Access on Linux	Troubleshooting Allocation Issues on Linux
Troubleshooting Resource Manager Deployment Issues with Linux	Redeploying a Virtual Machine
Troubleshooting ARM Template Deployment Errors	Troubleshooting and Monitoring Azure Storage
End-to-End Storage Troubleshooting	

TROUBLESHOOTING AZURE AUTOMATION

Authentication Errors Working with Runbooks	Common Runbook Errors
Common Errors Importing Modules	Common Errors with DSC
Common Errors Onboarding Solutions	Troubleshooting the Log Analytics VM Extension

TROUBLESHOOTING AZURE BACKUP

Troubleshooting Azure VM Backup	Troubleshooting Azure Backup Failure
Troubleshooting Azure Backup Server	Troubleshooting Slow Backup
Troubleshooting Azure Backup Agent	

TROUBLESHOOTING AZURE SITE RECOVERY

Troubleshooting Azure Site Recovery	Troubleshooting VMware to Azure Replication
Troubleshooting Failover to Azure	Troubleshooting Hyper-V Replication
Troubleshooting Azure-to-Azure Replication	Troubleshooting Azure Site Recovery Agent

Common Objections

When customers understand the cloud, they can trust it, so take the time to explain what makes Azure safe and secure.

HANDLING OBJECTIONS AROUND AZURE

OBJECTION	ANSWER
Microsoft isn't trustworthy	<p>Azure is the most trusted and compliant public cloud there is.</p> <ol style="list-style-type: none">1. All of your data is encrypted. For data in transit, Azure uses industry-standard transport protocols between user devices and Microsoft datacenters, and within the Azure datacenters themselves. For data at rest, Azure offers a wide range of encryption capabilities up to AES-256, giving your customers the flexibility to choose the solution that best meets their needs.2. The customer is always in control. A hybrid solution lets you decide what gets stored on-premises and what goes to the cloud. You can also move information back and forth between these options as you see fit. Microsoft takes strong measures to help protect customer data from inappropriate access or use by unauthorized persons, either external or internal, and to prevent customers from gaining access to one another's data.3. Azure is compliant. Microsoft solutions and services are built on a trustworthy computing foundation consisting of security, privacy, and reliability. Microsoft creates, implements, and continuously improves security-aware software development, operational, and threat mitigation practices, and shares this knowledge with government and commercial organizations. Microsoft continually collaborates with industry and governments to build trust in the cloud ecosystem.4. There are no shortcuts in physical security. Cloud datacenters have perimeter security around the building, building security, and room security. The data contained within the servers at the datacenter uses a higher level of standards than most organizations do. These security services are built into the solution and not added on later, so all that security is inherent <p>All of the compliance and regulatory data for Azure can be found in the Azure Trust Center.</p>
The cloud is the same regardless of who I choose	<p>Public clouds might look the same on the service, but once you dig a little deeper the differences are readily apparent.</p> <ol style="list-style-type: none">1. Azure offers a complete hybrid solution, so you can debunk that "all-or-nothing" customer assumption and explain how starting small - such as a virtual machine migration, or data backup and recovery – can be implemented without overhauling an existing process.

2. With Azure, you can move virtual machines “as-is” back and forth between on-premises and the cloud. Customers get a consistent experience everywhere without having to invest heavily in dismantling their existing infrastructure.
3. Azure supports the broadest selection of devices, operating systems, databases, languages, frameworks, and tools. Azure’s integrated tools, unified services, and proven solutions help you and your customers build enterprise, mobile, web, and Internet of Things (IoT) apps faster, for virtually any platform or device.
4. Using Azure’s Platform as a Service (PaaS) solution, the underlying Operating System (OS) and system management tasks are automated, enabling developers to focus on apps. This leads to faster on-boarding to the public cloud and lets customer quickly develop apps.
5. Microsoft matches AWS pricing for all commodity public cloud offerings. And, Azure brings more compute capacity than AWS in the instances they offer; so Azure beats AWS on a price-to-performance comparison

We'll have to redesign our applications

Moving an application to the cloud often involves some level of redesign or re-architecture, and in some cases, it is inevitable. With Azure’s wide support for both Windows and Linux and its expansive marketplace, your chances of needed a full re-architecture are greatly diminished.

The beauty of leveraging hybrid cloud is the same Hyper-V VMs (for example) that you are running on-premise or through another third-party cloud can easily be moved to Azure, and will run without needing to make modifications on Azure VMs. You can leverage Azure Site Recovery to migrate your on-premises physical Windows/Linux servers, on-premises Hyper-V VMs, and/or on-premises VMware VMs up into Azure with ease. If you are migrating on-premises VMWare VMs then Azure Site Recovery will convert the VM to a Hyper-V as part of the migration.

Migrating from on-premise to Azure can start out as a “lift and shift” strategy: simply moving a customer’s applications to Azure, leveraging the IaaS capabilities. And it gets better...moving to Azure provides customers with cost savings, efficiencies, and increased performance.

Case Studies

One important avenue Microsoft provides is a track record of successful partner engagements. A track record of customer success is an easy way to build confidence in the solutions your practice recommends and helps win over customers. Microsoft provides a collection of case studies highlighting how partners make their customers successful with Azure, including artifacts like case study PDFs, PowerPoint slides summarizing the key learnings and videos. The case studies available on the [Customer and Partner Success Stories](#) site highlight these Azure-specific studies. Use these case studies to help you position your offering to customers and to identify potential solution partners whose practices may complement yours.

There are hundreds of case studies available across Azure's product and solution offerings. You can find relevant studies to Azure Operations and Management under the following solutions:

- ➔ [Backup and Archive](#)
- ➔ [DevOps](#)
- ➔ [Disaster Recovery](#)
- ➔ [Hybrid Integration](#)
- ➔ [Monitoring](#)

It is recommended you check back periodically for new case studies that empower your efforts as a partner.