



Truly consistent hybrid cloud with Microsoft Azure

© 2017 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

Some information relates to pre-released product which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

Contents

- Why use a hybrid cloud? 1**
- Requirement: common identity 2**
 - Give your users single sign-on to applications anywhere.....3
 - Protect identities across on-premises and cloud environments4
- Requirement: integrated management and security 4**
 - Get common insight and analytics across your hybrid cloud6
 - Provide management automation for your hybrid cloud7
 - Get a unified view of security and compliance.....8
 - Use cloud-based services for on-premises backup and disaster recovery8
- Requirement: consistent data platform 10**
 - Take advantage of a common database on-premises and in the cloud11
 - Save money by moving your on-premises data to the cloud11
 - Use consistent data warehousing, analysis, and visualization services12
- Requirement: unified development and DevOps 14**
 - Run the same modern applications on-premises and in the cloud15
 - Provide integrated solutions across edge and cloud16
 - Create cloud applications that meet every regulation17
 - Use a common DevOps environment on-premises and in the cloud17
- Conclusion 18**

Why use a hybrid cloud?

Cloud computing gets a lot of attention, and for good reason: it's where much of IT is going. But on-premises datacenters also have an important role to play, both today and in the future. For many organizations, integrating these two to create a *hybrid cloud* is essential.

Microsoft understands this reality. To help you achieve it, we offer a broad range of cloud and on-premises technologies that work together in a coherent way. And unlike our competitors, we provide the flexibility to let you choose the path that's right for you. We're committed to providing a consistent hybrid cloud that supports the approach you pick.

But what exactly is a hybrid cloud? While getting everyone to agree on a definition isn't easy, there are some obvious requirements. For example, you need a way to connect your on-premises datacenters with the cloud, a problem Microsoft solves with Azure Virtual Networks, Azure ExpressRoute, and more. But basic connectivity isn't enough; a hybrid cloud should go beyond this, providing a complete set of consistent services.

Microsoft believes that a true hybrid cloud must provide four components, each of which brings significant benefits. They are the following:

- Common identity for on-premises and cloud applications. This improves user productivity by giving your users single sign-on to all of their applications.
- Integrated management and security across your hybrid cloud. This enables a cohesive way to monitor, manage, and help secure your environment, giving you increased visibility and control.
- A consistent data platform for your datacenter and the cloud. This gives you data portability, combined with seamless access to on-premises and cloud data services for deep insight into your data
- Unified development and DevOps across the cloud and your on-premises datacenters. This lets you move applications between the two environments as needed, and it also improves developer productivity, since both places now have the same development environment.

Taken together, these four requirements provide consistent experiences for developers, data professionals, IT managers, and users. Figure 1 summarizes this, showing example Microsoft technologies for each one.

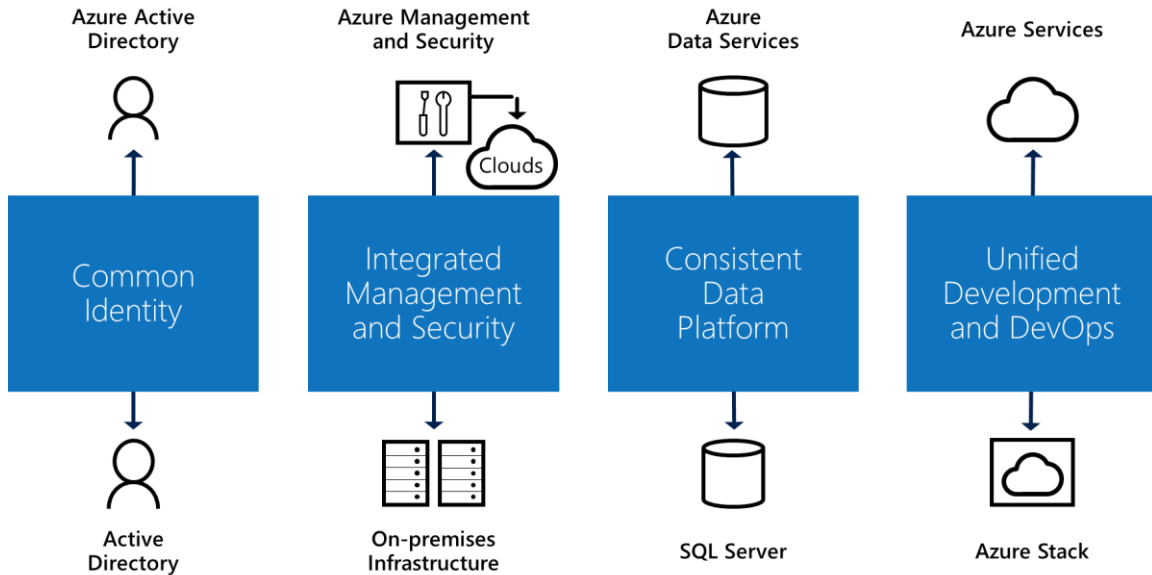


Figure 1: A hybrid cloud must provide consistent solutions in four areas: identity; management and security; data platform; and development and DevOps.

As the figure shows, Microsoft offers hybrid cloud technologies that address all four areas. Examples of these include the following:

- Azure Active Directory works with your on-premises Active Directory to provide common identity for your users.
- Azure provides integrated management and security services for both cloud and on-premises infrastructure.
- Azure data services combine with SQL Server to create a consistent data platform.
- Microsoft Azure services in the cloud combined with Microsoft Azure Stack on-premises provide unified development and DevOps.

What happens if you attempt to create a hybrid cloud without these four attributes? The short answer is pain: you'll have needless differences throughout your environment. These differences bring complexity, which in turn makes your hybrid cloud harder to use, harder to manage, and harder to secure. Your risks increase while the benefits you provide to your users shrink.

Creating a truly consistent hybrid cloud, with the advantages it brings, is a better approach. As this paper describes, Microsoft stands alone in offering these advantages.

Requirement: common identity

When users access applications, they shouldn't need to worry about whether those applications are running on-premises or in the cloud. Providing consistent identity is a core part of achieving this, which is why Microsoft created Azure Active Directory (Azure AD). This cloud service offers secure single sign-on, automated provisioning of new users, and more.

Give your users single sign-on to applications anywhere

Everyone hates having to remember different passwords. In enterprises, the problem of providing single sign-on—the ability to log in once, then access any application—was solved long ago. With the rise of Software as a Service (SaaS), however, this problem must be solved again. Rather than make users sign in separately to each application, they should be able to sign in just once, then access both on-premises and cloud (that is, SaaS) applications. Figure 2 shows how Azure AD makes this possible.

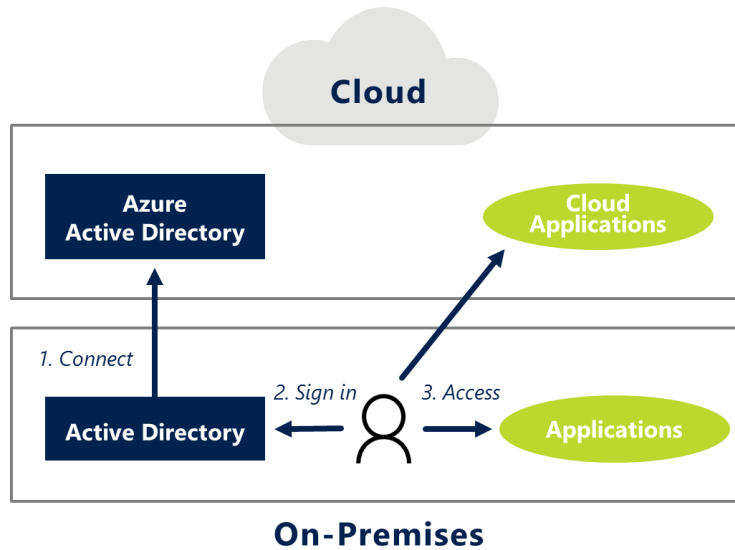


Figure 2: Azure Active Directory lets a user sign in once, then access both on-premises and cloud applications.

To use Azure AD in a hybrid cloud, an organization first connects its on-premises Active Directory to Azure AD in the cloud. Users can then sign in as usual—Azure AD is invisible to them. Those users can now access both on-premises applications and cloud applications without signing in again. They get single sign-on throughout their hybrid world.

Azure AD supports cloud applications from Microsoft, including Office 365 and Dynamics 365. It also supports many other SaaS offerings, including Google Apps, Salesforce CRM, Dropbox, Box, Slack, Service Now, Workday, and thousands more. Just as Active Directory allows single sign-on to on-premises applications from many different vendors, Azure AD provides this for cloud apps from many SaaS providers.

Using Azure AD for single sign-on also brings other benefits, including these:

- Because Azure AD provides a common account for many applications, there's less need to have multiple passwords that might get reused across different SaaS applications. This improves your security, because a breach at one site is less likely to expose a password that has been reused for another application.
- When a user leaves your organization, an administrator can end her access to multiple applications (cloud or on-premises) by simply removing her from Azure AD. If she instead had separate sign-ons to these applications, your admin would need to find and remove each one individually.

Microsoft's broad support for hybrid identity is unique among major cloud platform providers. For example, AWS Identity and Access Management focuses on managing identity for AWS itself and for resources running on AWS. Unlike Azure AD, it doesn't provide a general solution for single sign-on that works across cloud applications from many vendors.

Hybrid SaaS applications

Applications that are available as both SaaS solutions and on-premises products represent another form of hybrid cloud computing. For example, Office 365 includes several components that function this way, including Exchange and SharePoint.

In a hybrid world, hybrid SaaS applications can be quite useful. For example, SharePoint Online and SharePoint Server offer a common administrative experience, as do Exchange Online and Exchange Server. These applications also provide other hybrid benefits, such as support in SharePoint for searching across both SharePoint Online and SharePoint Server and the ability to use a common email domain across Exchange Online and Exchange Server.

Like other applications, hybrid SaaS solutions need to deal with identity. With Office 365, this challenge is addressed by Azure AD. Any organization using Office 365 is also using Azure AD, even if they don't explicitly see it. This allows things such as assigning licenses to specific Office 365 applications based on AD groups, so that everyone in a particular group is granted access. Combining hybrid identity with hybrid SaaS applications is another way that a consistent hybrid cloud provides value for your organization.

Protect identities across on-premises and cloud environments

Using a common identity to access many applications has real benefits. It also makes protecting that identity more important than ever. Microsoft offers several ways to do this.

For example, Azure AD provides Multi-Factor Authentication (MFA). With this option, logging in to Azure AD requires more than just a simple password. Users also need a second factor, such as entering a code sent to their mobile phone. With MFA, even an attacker who steals a user's password can't log in as that user. The attacker would also need access to the user's phone or another factor being used for authentication. The result is better identity protection and lower risk.

Azure AD also supports conditional access policies. These let your administrators control access to specific applications using not just the user's identity, but also based on what device she's using, her location, the groups she belongs to, and more. User identities define the perimeter of your hybrid cloud, so protecting them with MFA and conditional access is important. Along with this, Microsoft offers cross-platform APIs to integrate identity management into on-premises or cloud applications, with support for all modern protocols, including SAML 2.0, WS-Fed, OAuth 2.0, and OpenID Connect.

Requirement: integrated management and security

Using a hybrid cloud can broaden your options for delivering IT services to the organization. But there's no getting around the fact that hybrid clouds bring new hurdles for management and security. The challenges include these:

- Monitoring your combined on-premises infrastructure and cloud resources.
- Effectively automating whatever you can, such as the response to alerts raised through monitoring.
- Securing the larger surface area that a hybrid cloud brings.
- Providing effective data backup and disaster recovery for both cloud and on-premises resources.

Addressing these challenges requires an approach to management and security that's designed for hybrid clouds. To provide this, Microsoft delivers management and security services from Azure, giving you built-in capabilities across the operational lifecycle. Azure includes a cohesive set of tools for monitoring, configuring, and protecting your hybrid cloud. Figure 3 shows the big picture of Azure management and security (which you may have heard referred to as the Operations Management Suite).

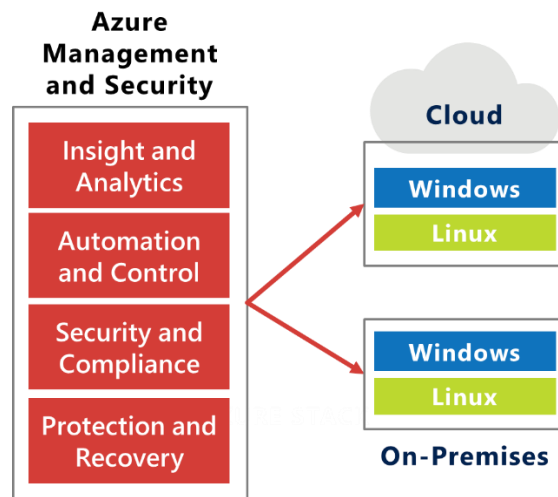


Figure 3: Azure provides integrated management and security services for a modern hybrid cloud.

Designed for a hybrid and heterogeneous world, Azure management and security services give you increased control of Windows and Linux systems running in Azure or in your on-premises datacenter. In fact, although it's not shown in the diagram, these Azure services can also extend to management of Windows and Linux systems running at hosting services or on other cloud platforms, such as AWS.

Four key services comprise the lifecycle approach to management from Azure: Insight and Analytics, Automation and Control, Protection and Recovery, and Security and Compliance. All of them are accessed through a single dashboard, an example of which is shown in Figure 4.

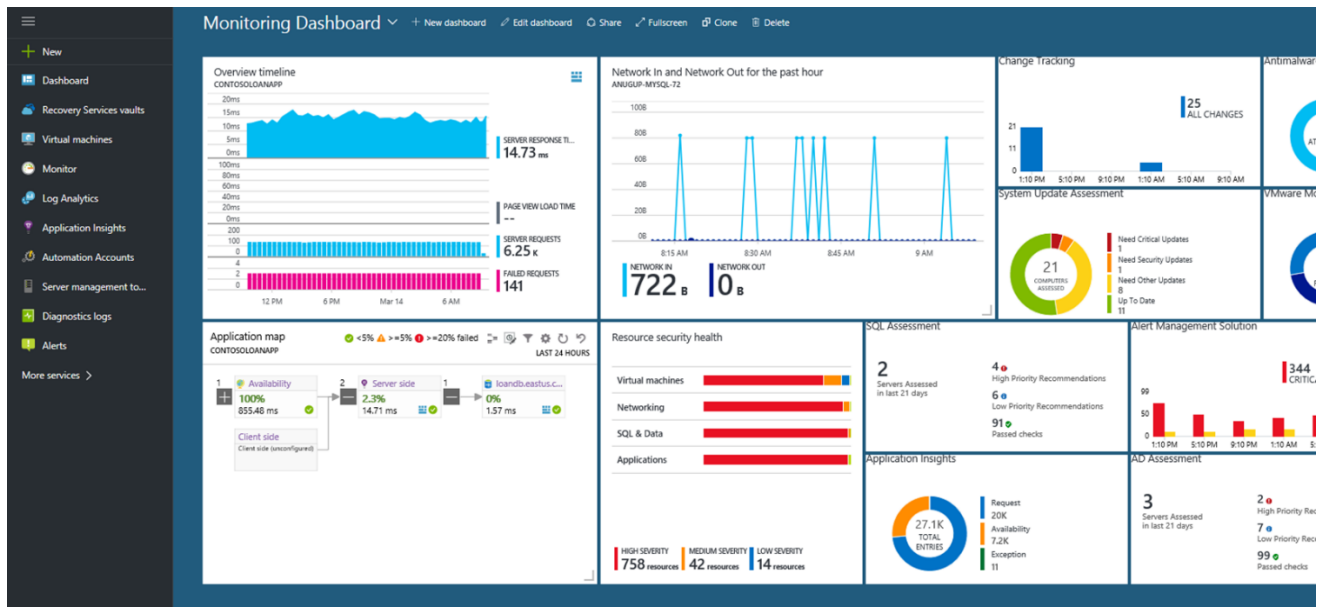


Figure 4: The Monitoring Dashboard provides a broad and customizable view of a hybrid cloud environment.

The console is built from tiles, and each user can customize what tiles appear to suit her needs. A user focused on security, for example, might choose to show the current status of antimalware software on managed systems, the number of outstanding security issues, and a map showing where threats are coming from. A user who's responsible for backup might choose to display information about the latest backups for virtual machines, email, and other data. A user who's responsible for all of these areas—Azure management and security services are designed to be effective tools for generalists—might display some combination of these things. Whatever the requirement, this customizable interface gives all users access to the information and services most relevant to their own needs. And because Azure cloud services are designed for a hybrid world, the picture the dashboard presents can span both on-premises and cloud datacenters.

Get common insight and analytics across your hybrid cloud

One of the most important aspects of management is monitoring to keep track of what's happening in your world. Doing this effectively in a hybrid cloud is especially challenging, since you need the ability to reach into both on-premises and cloud datacenters. Azure addresses this with the Insight and Analytics service.

The Insight and Analytics service collects information, such as log and performance data, about the systems it monitors. Using the dashboard, a user can then issue custom queries against this data or create queries that run regularly, then generate an alert if something is out of the ordinary. And to support common situations, Insight and Analytics includes a group of solutions that provide pre-defined queries and logic for addressing a specific area. For example, the AD Assessment solution displays the status of Active Directory, along with recommendations for improvement, while the SQL Assessment solution provides similar information for SQL Server.

This Azure monitoring service can also connect directly to System Center Operations Manager. Doing this lets Insight and Analytics receive information and alerts that Operations Manager gets from the systems it monitors. Connecting to Operations Manager provides easy access to useful information, and so it's a common way to get started with Insight and Analytics.

Insight and Analytics also provides other useful tools, including the following:

- Service Map can automatically discover distributed applications in your hybrid environment, show the dependencies among application components (such as databases and business logic), and help troubleshoot problems.
- Network Performance Monitor lets an administrator track network performance, including links between on-premises and cloud datacenters, then find and fix network problems.

To understand the value of this technology, think about a simple scenario. Suppose Insight and Analytics raises an alert about an application in your environment. An administrator might use Service Map to understand the structure of that application and then determine that the problem lies with the application's SQL Server database. The admin can use the SQL Assessment solution provided by Insight and Analytics to take a closer look at that database. Perhaps the problem is that one of the database's tables has reached its maximum size, for instance. Once the admin knows this, he can truncate that table and return the application to normal operation.

This process of finding and fixing an error is the same whether the problem database is running on-premises, at a hosting provider, or in the cloud. It's also the same for SQL Server and Azure SQL Database. Consistency is an integral feature of the Insight and Analytics service because it was designed for a hybrid world.

Compare this with other cloud vendors. AWS, for example, provides CloudWatch for monitoring a cloud environment. Yet this technology provides little information about anything else because isn't designed for a hybrid world. Service Map, by contrast, can automatically discover applications that span cloud and on-premises datacenters, and the monitoring capabilities of Insight and Analytics in Azure treat both environments equally. This Azure service is designed from the ground up to work with a hybrid cloud.

Provide management automation for your hybrid cloud

In general, it's a good idea to automate as much of your systems management as possible. To allow doing this from the cloud, Azure includes the Automation and Control offering. This service lets your administrators create PowerShell scripts called runbooks to automate common processes.

For example, think about the scenario just described, where Insight and Analytics raises an alert based on detection of a problem with an application. One way to handle this is to rely on an administrator to find and fix the problem. This might be the only option the first time a problem surfaces. If it's likely to appear again, why not create an automated solution? Using the functionality in Automation and Control, the administrator can create a runbook that takes the same steps (such as truncating the database table), then configure the runbook to execute whenever the alert appears. Doing this can make problem resolution faster, more reliable, and less expensive.

The Automation and Control offering also addresses many other scenarios. Admins might create runbooks that reset user passwords or set up virtual machines for a development environment or schedule and deploy patches for Windows and Linux. To make this easier, Microsoft and others provide a gallery of predefined scripts that address many common scenarios. Besides runbooks, this Azure service offering also provides Desired State Configuration (DSC), which is the ability to specify how a Windows or Linux server should be configured, then monitor and enforce that configuration.

Together with Insight and Analytics, Automation and Control has one overarching goal: to help you proactively find and fix problems in your hybrid cloud before they impact your business.

Get a unified view of security and compliance

No aspect of systems management is more important than security. Which of your systems are being attacked right now? Where are the attacks coming from? What's the status of antimalware software on each of those systems? In a hybrid cloud, you should be able to answer all of these questions in a common way for systems in both on-premises datacenters and the cloud.

Azure Security and Compliance addresses these concerns. By providing a unified set of tools, it lets your administrators, even those who aren't security specialists, prevent, detect and respond to threats across your hybrid cloud. Here are some examples of what this capability provides:

- Admins can see the security state of their entire hybrid cloud in a single view. This view can include antimalware status, whether systems conform to defined baseline configurations, and more. In fact, the Security and Compliance service offering relies on the repository and query mechanism used by Insight and Analytics, bringing the same breadth and power to security management.
- This broad visibility can help administrators quickly detect and respond to security threats. For example, an administrator can determine that a virtual network isn't correctly configured, then click a button in the dashboard to fix it, or she might see that a database in Azure SQL Database doesn't have encryption enabled, and then turn it on with a few more clicks. Security and Compliance even provides a prioritized list of security vulnerabilities like these, along with guidance on how to fix them.
- Because Azure Security and Compliance is continually updated by Microsoft, it learns about new threats as they appear. This helps your administrators maintain an up-to-date security posture across your hybrid cloud. And because these updates draw from Microsoft's own information about attacks on Azure, Xbox, and other cloud services, this threat intelligence is based on a very large dataset. You get the benefit of Microsoft's broad experience, along with the ongoing updates possible in a cloud-based solution.

Once again, it's worth comparing what Azure provides with what most other cloud providers offer. Because these vendors are focused solely on the cloud, their solutions don't typically address the wider needs of a hybrid environment. And since the other major cloud providers tend to lack Microsoft's long experience as a provider of enterprise management software, they might not understand what's required to manage an on-premises computing environment as well as the cloud.

Use cloud-based services for on-premises backup and disaster recovery

Wherever it's stored, data needs to be backed up. Given the massive amount of low-cost storage available in a cloud platform like Azure, using a cloud service to do this makes sense. Similarly, many applications need disaster recovery (DR) to make sure they keep running in the face of unexpected failure. The cloud is also well suited for providing this service.

To meet these needs, Microsoft provides two distinct services: Azure Backup and, for DR, Azure Site Recovery. As its name suggests, Azure Backup backs up data to Azure datacenters. This data might be from Windows or Linux virtual machines, Exchange, SharePoint, SQL Server, or Windows files. Whatever the source, Azure Backup lets you store copies of data on Azure, then restore that data as required. And you can restore just the data you need. Unlike tape backup, there's no need to fetch an entire tape from an offsite location. Azure Backup also lets you keep that data on geo-redundant storage to protect your backup in the unlikely event that an entire Azure datacenter is disabled.

Azure Site Recovery is a cloud-based disaster recovery service designed to take advantage of the scalability and resilience of Azure. Figure 5 illustrates this service.

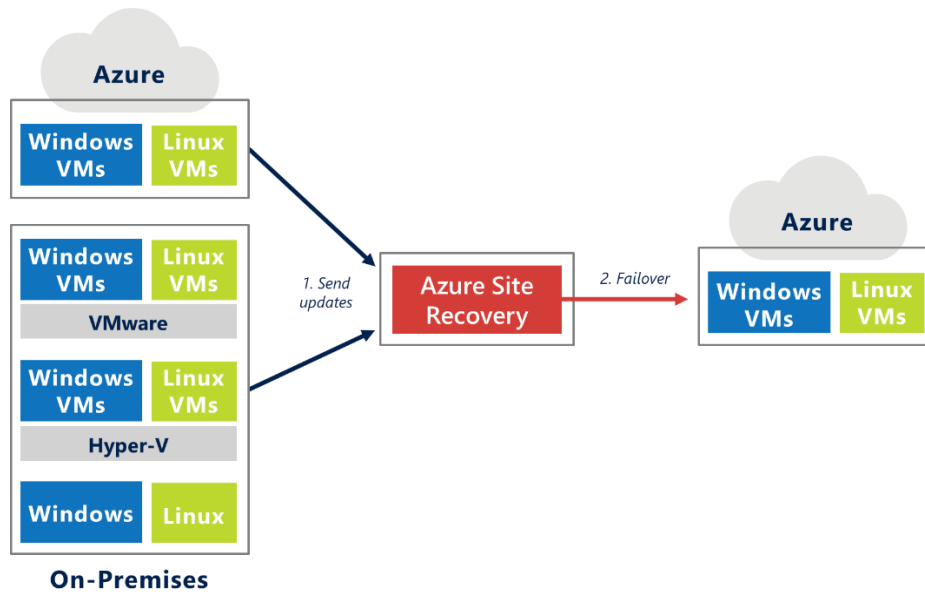


Figure 5: Azure Site Recovery provides disaster recovery for virtual machines and physical servers with failover to Azure.

Azure Site Recovery can be used with Linux and Windows virtual machines running on VMware or Hyper-V, as well as with physical servers. These can be running anywhere in your hybrid cloud: on-premises, at a hosting provider, or (for virtual machines) on Azure. Wherever they are, these systems send regular updates to Azure Site Recovery in the cloud. Should disaster strike, the service manages failover to Azure. This includes creating the necessary Azure virtual machines, initializing them with the most recent state stored in Azure Site Recovery, and configuring virtual networks. Intended to be used for even complex workloads, such as SAP, this service provides easy-to-use disaster recovery at relatively low cost.

Backup and DR are commonly available offerings, so what makes these Azure services uniquely suited for a hybrid cloud? The answer is that both Azure Backup and Azure Site Recovery are managed cloud services. Any cloud platform lets you run third-party software for backup and DR, and Azure does too. (You're free to use CommVault, Veritas, or something else with Azure Blobs, for example.) The big difference is Microsoft provides managed services for both, which means you don't have to buy, install, and run your own backup and DR solutions in the cloud. This is significantly simpler than managing your own servers in the cloud, and it's an important example of the benefits of a hybrid cloud.

Stay hybrid? Or migrate entirely to the cloud?

Some organizations plan to remain hybrid indefinitely. Others, though, view hybrid as a waystation on their journey to the cloud. In other words, they think of a hybrid cloud as part of their migration strategy.

If you're in this second category, a consistent hybrid cloud can make migration significantly easier. For example, Azure Site Recovery can help with migration as well as disaster recovery because it can create new instances of on-premises applications on Azure. Rather than manually moving applications to the cloud, you can rely on Azure Site Recovery to do this and to help you cut over to the new cloud instances. The Microsoft hybrid cloud provides other tools as well, such as the migration wizard built into SQL Server Management Studio to help move on-premises SQL Server applications to Azure IaaS virtual machines.

Microsoft also helps lower the cost of migration by enabling you to bring your on-premises licenses to Azure. You can use your existing Windows Server licenses with Software Assurance to enable up to 40 percent savings on Windows Server virtual machines in Azure by using the Azure Hybrid Use Benefit. Similarly, license mobility provides the flexibility to deploy existing SQL Server licenses with Software Assurance in the cloud without additional fees. These benefits used alone or together can unlock significant savings as you look to extend into cloud or lift and shift to cloud. You can also rely on Microsoft's extensive partner ecosystem, including firms such as Cloudamize and Moveve, to provide both migration knowledge and tools.

Whatever options you choose, Microsoft's consistent approach to hybrid cloud can make migration to a full cloud environment simpler, faster, and less expensive.

Requirement: consistent data platform

What's the best approach for working with data in a hybrid cloud? There's no single answer that's right for every organization, but one thing is clear: you'll have important information both in the cloud and on-premises. Given this, it makes sense to have a common approach to working with data in both places.

To allow this, the Microsoft hybrid cloud provides a consistent data platform. This consistency lets your organization use the same tools and the same skills throughout your environment. And because organizations use data in various ways, the Microsoft platform works with both operational data, such as orders in an online shopping application, and analytical data, such as aggregated information used for data analysis. The challenges this helps you address include:

- Using a common database across your own datacenter and the public cloud.
- Using data services in the cloud to complement your on-premises database.
- Providing consistent services on-premises and in the cloud for data warehousing, data analysis, and data visualization.

Take advantage of a common database on-premises and in the cloud

Microsoft SQL Server is a mature offering that supports mission-critical workloads in datacenters around the world. In a hybrid cloud environment, you can use this technology in a number of helpful ways.

One option is to run SQL Server in an Azure IaaS virtual machine. You might do this as part of moving an entire application to the cloud to lower your costs, for example, or perhaps to create a development environment for applications that are deployed on-premises. Whatever the reason, you can use the same database technology throughout your hybrid cloud. This makes it easier to move your data and applications as needed to respond to changing business requirements.

Another possibility is to take advantage of the cloud to provide business continuity with SQL Server AlwaysOn Availability Groups. Figure 6 shows how this looks.

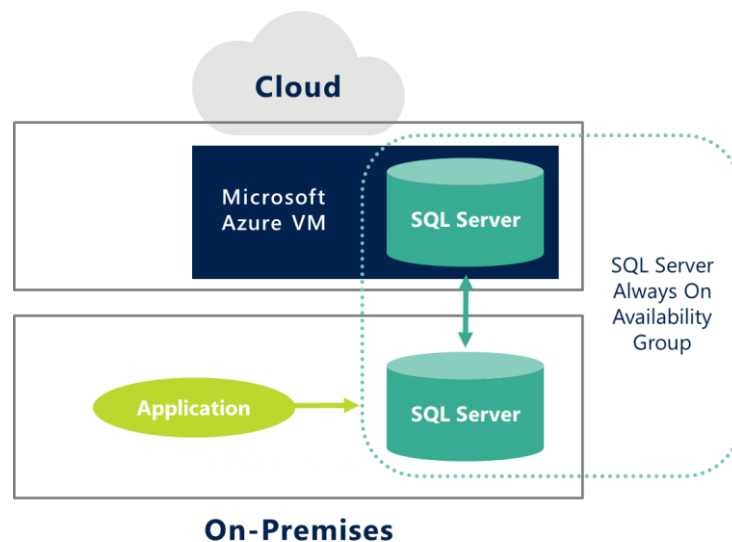


Figure 6: With SQL Server AlwaysOn, a secondary server can run in an Azure virtual machine, using the cloud to provide business continuity for an on-premises database.

As the figure shows, an availability group has two (or more) instances of SQL Server running on two different systems. The AlwaysOn technology automatically replicates changes to data across these systems. If the primary fails, the secondary can automatically take over, letting applications that use this database continue running. This kind of replication is essential for mission-critical workloads, and AlwaysOn supports scenarios with a low recovery time objective (RTO).

Running the secondary server in the cloud can save you money and time. This secondary can also be made readable to help you scale access to data. For example, a readable secondary could be located in an Azure datacenter that's closer to salespeople using a mobile business intelligence app.

Save money by moving your on-premises data to the cloud

Running a database in a cloud virtual machine is useful. But a hybrid data platform should also provide cloud database services that complement your on-premises databases. The Microsoft hybrid cloud does this in several ways.

SQL Server, for example, provides built-in support for backups to Azure Blobs. This support is simple to use—setting up scheduled backup requires just a few clicks—and it lets you take advantage of the low-cost storage provided by Blobs. It can also provide geo-replication of your backup data, making sure this

data is stored in two different Azure datacenters. Given the ever-growing amount of data that organizations need to store, having easy access to this bottomless cloud storage is useful.

Using Azure SQL Database, a PaaS data service, brings more possibilities. Because Azure SQL Database is based on SQL Server (in fact, the two share the same core database engine), applications can access data in the same way with both technologies. Azure SQL Database can also be combined with SQL Server in useful ways.

For example, the SQL Server Stretch Database feature lets an application access what looks like a single table in a SQL Server database. In fact, however, some or all rows of that table might be stored in Azure SQL Database. This technology automatically moves data that's not accessed for a defined period of time to the cloud, as Figure 7 illustrates.

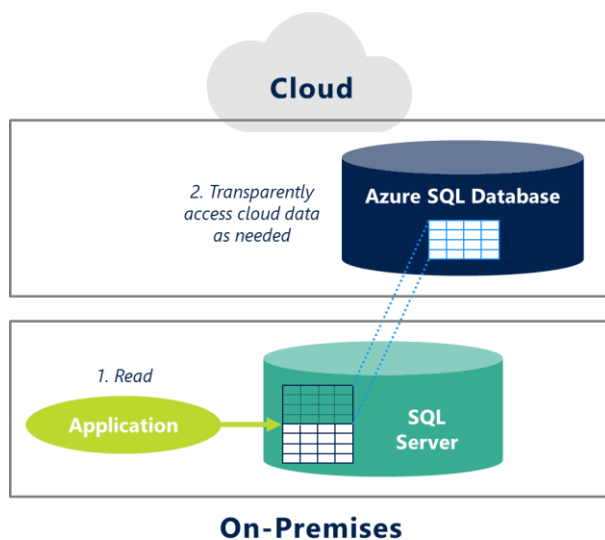


Figure 7: SQL Server Stretch Database automatically archives cold relational data in the cloud.

An application reading this data is unaware that any of it has been moved to the cloud. The application just issues SELECTs as usual. When colder data is required to satisfy a query, SQL Server Stretch Database will automatically fetch this data from Azure SQL Database. (The data is protected throughout the entire process, both at rest and in motion.) The result is automatic archiving of less-used data in the lower-cost cloud. You might use this, for instance, to store the order history of your customers. In this situation, you certainly want to retain the older data, but since older orders are accessed less frequently, storing them in Azure SQL Database can save you money while requiring no changes to your applications.

SQL Server Stretch Database offers another example of how Microsoft's hybrid cloud differs from its competitors. Because we provide both SQL Server and Azure SQL Database, we can combine the two to deliver innovative services in unique ways. AWS, for example, doesn't support this—the SQL Server Stretch Database feature is available only with the Azure cloud.

Use consistent data warehousing, analysis, and visualization services

So far, the focus has been on operational data. To see the full value of a consistent data platform, however, we need to broaden our scope. Analytical data is also an important part of the story, and it's another area where Microsoft's consistent hybrid cloud can improve how your organization works with data. Figure 8 shows one possible scenario.

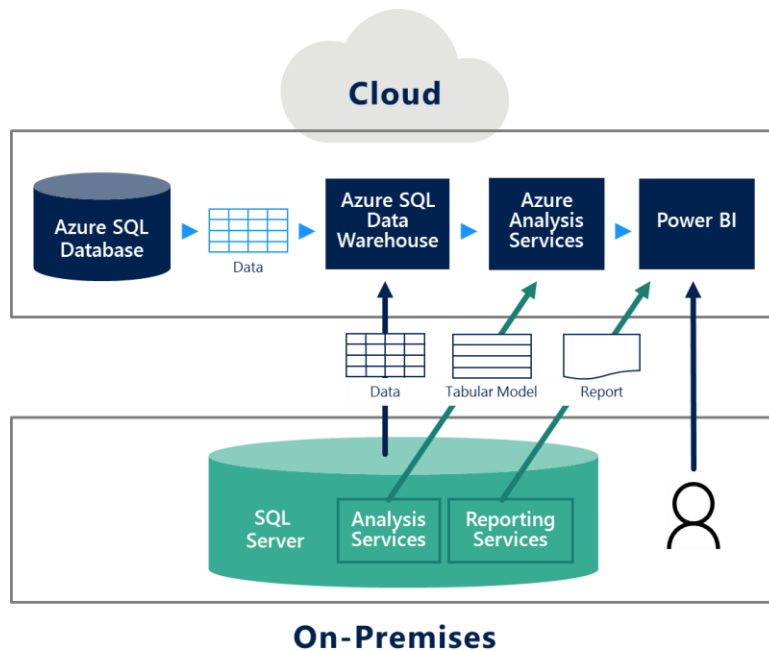


Figure 8: Microsoft's hybrid cloud data platform includes consistent services for analyzing and visualizing on-premises and cloud data.

Suppose you need to analyze operational data held in an on-premises SQL Server database and in Azure SQL Database. As Figure 8 shows, you can load data from both sources (and many others) into Azure SQL Data Warehouse. This cloud service can hold very large amounts of data, both relational and unstructured, and lets your staff set up a data warehouse in a few minutes. The service also makes scaling simpler: just move a slider to increase or decrease your warehouse capability. And to let you issue queries over both relational and unstructured data, Azure SQL Data Warehouse provides PolyBase, a technology for using any language with any data.

You can use Azure Analysis Services to analyze this data, as the figure shows. Based on the proven technology of SQL Server Analysis Services, this cloud service lets your organization make use of existing skills and familiar tools. Rather than learning something entirely new, your staff can be productive immediately. And as Figure 8 shows, you can import existing tabular models to reuse work you've already done. Data analysts can also create new models, then deploy them to either Azure Analysis Services or SQL Server Analysis Services just by changing a URL.

The last link in the analytics chain is visualizing the data. To enable this, the Microsoft data platform provides the cloud-based Power BI. This service can work with data from many different sources, including Azure Analysis Services, reports produced on-premises using SQL Server Reporting Services, and lots more. (It even has a connector to AWS Redshift, Amazon's data warehousing service.)

Power BI can display dashboards through a web browser, mobile devices, or in other ways. It can also be accessed via natural language queries spoken to a phone. For example, a salesperson might use a phone to easily call up information about last month's sales in London or to make other specialized requests.

Microsoft's consistent data platform provides other technologies for a hybrid cloud as well. For example, your organizations can gain rich insights from all your data, relational and non-relational, with fully managed big data services in the cloud, including Azure HDInsight and Azure Data Lake. The Microsoft hybrid cloud also enables analytics, deep learning, and intelligent applications across on-premises and

cloud data with common templates and reusable R language support. Azure Machine Learning, Cognitive Services, and other offerings make this possible.

Why is Microsoft's hybrid cloud data platform better than competing alternatives? There are several reasons. First, it's broad, providing software and services for working with data in many different ways. The platform also lets you move data and other artifacts, like tabular models, as needed. And just as important, the cloud components of this data platform are all PaaS services. Rather than running on-premises servers in IaaS virtual machines, with all of the management effort this implies, PaaS services take care of this for you. Creating and scaling resources in the cloud is straightforward, and Azure handles high availability. These factors can lower your costs and free your people for more valuable work.

Alternative solutions lack the breadth of Microsoft's hybrid data platform, as well as consistency across the cloud and your datacenter. They also don't offer Microsoft's commitment to providing PaaS services wherever possible. If you don't have this kind of consistent data platform, you don't really have a hybrid cloud.

Requirement: unified development and DevOps

One of the biggest challenges in using the cloud is that the cloud development platform differs from traditional on-premises platforms. Some things are the same, of course—both environments offer virtual machines running Windows Server and Linux—but others are quite distinct. These differences can create problems, including the following:

- An application built for a cloud platform might be hard to move back on-premises. If the application uses a technology that's not available in your datacenter, you might find yourself committed to the cloud.
- Providing up-to-date platform technologies in cases where a cloud solution isn't appropriate can be difficult. A primary example of this is edge-computing scenarios, where applications can't always connect to the cloud or must run close to their users for performance reasons.
- Creating applications that exploit the cloud while still complying with every applicable regulation can be challenging. If the application must run in even one geography where data sovereignty rules require an on-premises solution, your developers might need to create different versions for the cloud and an on-premises datacenter.
- Differences between a cloud platform and your on-premises environment can make it hard to create a common DevOps environment for applications deployed in both places.

Microsoft Azure Stack addresses all of these challenges. You can use this technology to provide a subset of the cloud services offered by Microsoft Azure on your own premises. Figure 9 shows how this looks.

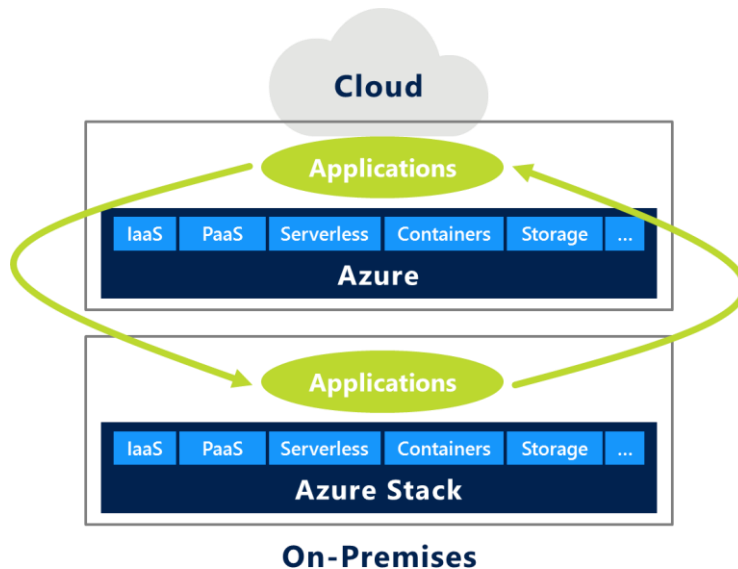


Figure 9: Azure Stack provides a subset of Azure services in your datacenter, letting the same applications run in both places.

Azure Stack lets your developers build and deploy software the same way, whether it runs on-premises or in the cloud. It also lets them implement consistent DevOps mechanisms across your hybrid cloud. To allow these things, Azure Stack provides many of the most important Azure technologies, with more to come. The technologies in Azure Stack include:

- Infrastructure as a service (IaaS), providing Windows and Linux virtual machines on demand.
- Platform as a service (PaaS), including App Service, with support for creating applications in .NET, PHP, Java, and other environments, and Service Fabric, a foundation for microservices applications. Both Azure and Azure Stack also support Cloud Foundry, a cross-platform PaaS technology.
- Serverless computing with Azure Functions.
- Container support with Azure Container Service (ACS), which provides container orchestration using Kubernetes, DC/OS, and Swarm.
- Storage, including Azure Blobs and Tables.

Rather than trying to stretch existing on-premises technologies to provide cloud services, Azure Stack brings Azure services into your datacenter. Creating this consistent hybrid cloud helps you solve the problems described earlier.

Run the same modern applications on-premises and in the cloud

Because Azure and Azure Stack offer the same technologies—the same services with the same interfaces—moving applications between the two is straightforward. This has several advantages.

First, your organization can choose where to deploy an application based on your needs. You're not committed to either the cloud or an on-premises datacenter. Instead, where an application runs in your hybrid cloud can change with your business and technical requirements.

Also, your developers can use up-to-date technologies for all of the applications they create, whether they run in the cloud or in your own datacenter. This includes externally facing applications, such as an e-commerce system used by your customers, as well as internally facing applications, such as a line-of-business solution used by your own employees. The most recent innovations, including serverless computing with Azure Functions and modern container support with ACS, are available in both places. Your on-premises development projects are no longer limited to older technologies.

Just as important, using the same technologies in both places means that your organization can exploit the same skills in both places. Rather than finding (and keeping) people with different skills for cloud and on-premises development, you can use the same people for both kinds of projects. You can also use the same processes for deploying and updating applications, as described in more detail later.

Compare this with what's required if you choose a cloud platform from a provider that's solely focused on the cloud, such as Amazon Web Services (AWS). Without an on-premises equivalent, you're forced to use different technologies, people, and processes in these two environments. This is a clear example of why a consistent hybrid cloud is so important.

Provide integrated solutions across edge and cloud

Many business requirements can be met by applications running in the cloud. This isn't true for everything, however—the edge is still important. For example, think about a situation where the latency inherent in cloud access isn't acceptable. In a manufacturing environment, for instance, a real-time control application might need to be located very close to the robots it controls. (The speed of light is a constraint that's not going away.) Or suppose a continuous connection to the cloud isn't practical. Think of a cruise ship at sea, for example, which might have only intermittent Internet access.

In all of these situations, organizations still want to create applications using modern platform technologies. They also might want to create applications that can run in the cloud if needed. Why lock these applications into an on-premises environment if it's not required? Using Azure Stack lets an organization create the best possible applications at the edge while still taking advantage of the cloud as needed. For example, a cruise ship might rely on a shipboard application built on Azure Stack to collect and aggregate data about that ship. The same application might also run on the Azure cloud to collect and aggregate data across the company's fleet of ships. Having the same development environment in both places makes this possible.

The Internet of Things as edge computing

The Internet of Things (IoT) provides another example of combining edge computing with the cloud. To support IoT applications, Microsoft Azure provides IoT Hub, a cloud service that can accept and buffer large numbers of events from many devices. These events can then be processed by applications running on Azure, perhaps using Azure Stream Analytics or another Azure streaming technology. And to help create field gateways, systems that aggregate data from multiple simple devices, Microsoft provides the IoT Gateway SDK.

This approach combines on-premises devices and the cloud, so it can be thought of as part of Microsoft's hybrid cloud. However you view it, many IoT applications clearly wouldn't be possible without harnessing the power of the cloud.

Create cloud applications that meet every regulation

For many organizations, the biggest barrier to embracing cloud computing is regulatory. Sometimes the law prohibits storing customer data outside your own datacenter, or maybe remote storage is allowed, but only within your own country. Since no cloud provider has a presence in every nation, these regulations can prevent you from using the cloud for some applications.

With Azure Stack, your developers can create an application that can be deployed without modification on either Azure or Azure Stack. If regulations allow using the cloud, running your application on Azure might be the least expensive, most scalable, and most secure choice. If you're obligated to keep your data on-premises, however, you can run the same application on Azure Stack in your own datacenter. And if you'd like to run the application externally but are required to keep it within a specific national border, you can rely on a hosting provider that runs Azure Stack in an in-country datacenter. Whatever the regulatory requirement, the combination of Azure and Azure Stack lets you meet it using the same application. And as always, these applications can be externally facing or internally facing, with web clients, mobile clients, and more.

Compare this to your options with a public-cloud-only provider, such as AWS. To address the same regulatory diversity, you'd likely need to build two different versions of your application. A true hybrid cloud doesn't require this; it provides the same modern cloud platform everywhere.

Use a common DevOps environment on-premises and in the cloud

DevOps is a combination of tools, processes, and culture that can improve how software is deployed and updated. Among the most important aspects of doing DevOps well are these:

- Automating creation of the environment an application needs. This might include creating virtual machines, setting up networks, deploying application code, and more. Automation means doing all of this with software, and so this aspect of DevOps is often referred to with the phrase "infrastructure as code."
- Automating the deployment of new software into this environment. This typically uses tools such as Jenkins or Visual Studio Team Services that allow creating pipelines to build, test, and deploy new code.

In a hybrid world, the same application might be run either on-premises or in the cloud. Accordingly, an important part of creating a hybrid cloud is setting up a DevOps process that works identically for both. With Azure and Azure Stack, the Microsoft hybrid cloud provides this, as Figure 10 shows.

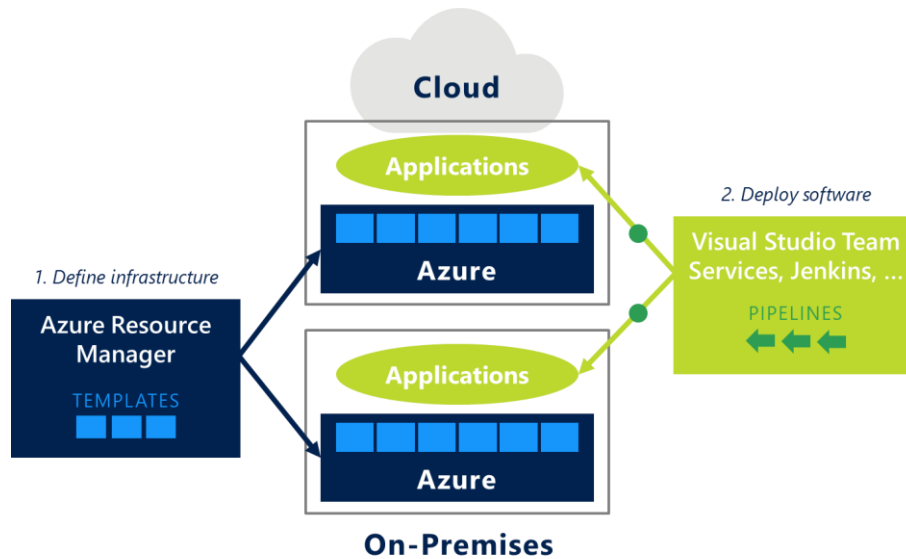


Figure 10: Azure and Azure Stack can share identical DevOps environments.

As the figure shows, a DevOps team uses Azure Resource Manager (ARM) to define the required infrastructure in both Azure and Azure Stack. By creating an ARM template, the team can fully specify whatever environment an application requires. And because Azure and Azure Stack provide completely consistent services, the same template can be used to create this environment either in the cloud or on-premises.

Once this is done, the DevOps team can use its choice of tools to create deployment pipelines for new software. Because Azure Stack is a subset of Azure, the same pipeline can target either environment. Sending software to one or the other requires changing only the URL a pipeline targets. For example, suppose you've created an application that serves most of its users from Azure in the cloud, but runs on Azure Stack in a particular country for regulatory reasons. Your development team can create an ARM template to set up an identical environment in both places, then use whatever build server they choose to deploy updates to both in the same way. This consistency lets them create applications in a common way, then easily deploy them to the right location. It also lets the team reuse ARM templates across your hybrid cloud as needed, simplifying your DevOps process.

Compare this to the situation with a provider that's focused solely on the cloud. Amazon Web Services offers CloudFormation, for example, a technology that's broadly analogous to ARM. But CloudFormation is limited to defining environments in the cloud—you need to do something different for an on-premises solution. Once again, the value of a consistent hybrid cloud is clear.

Conclusion

Hybrid cloud computing is important for many organizations, and it's not going away anytime soon. Given this, picking the right hybrid cloud vendor is fundamentally important. When you're doing this, remember that a truly consistent hybrid cloud should provide four key components, all explicitly designed for a hybrid world:

- ❑ Common identity
- ❑ Integrated management and security

- A consistent data platform
- Unified development and DevOps

The Microsoft hybrid cloud offers all four. Whether your goal is integrating your on-premises environment with the cloud, optimizing your computing across both worlds, or innovating with the new services cloud computing provides, we support you.

If you're looking for a holistic computing environment that lets on-premises resources and the cloud smoothly work together, provides a unified approach to management, and allows a single identity everywhere, you're looking for the Microsoft hybrid cloud. Our enterprise credibility and consistent hybrid capability make us the trusted vendor for your journey.