



Microsoft

Capgemini

THE BRIDGE

Hybrid Operations Management

One central control bridge for Cross Cloud, On-Premises, and Edge management of your Enterprise IT with Azure Arc.



TABLE OF CONTENTS

PAGE NO.

03

**EXECUTIVE
SUMMARY**

PAGE NO.

05-11

**INTRODUCTION
INTO AZURE ARC**

P.06

Concept

P.07

Benefits

P.07 Governance, Risk, and
Compliance Management (GRC)

P.09 Observability
Security Management

P.11 Configuration Management
Automation

PAGE NO.

12-20

**IMPLEMENTATION
INSIGHTS**

P.13

Network Connection

P.14

Governance and Conventions

P.15

Onboarding Servers

P.17

Onboarding Databases

P.18

Onboarding Containers

P.19

Onboarding of Hypervisors
and Platform Stacks

P.20

Take the Landscape under
new Control

PAGE NO.

21-26

**OPERATIONS
INSIGHTS**

P.22

GitOps across multiple
container locations

P.23

Cost implications due to
Azure Arc

P.24

Multi-tenant Management

P.25

Machine Learning

P.26

Managed Services by
Capgemini

PAGE NO.

27-30

WHAT'S NEXT?

P.28

Proof the Concept

P.29

Microsoft Azure Hybrid
Roadmap

P.30

Multi-Platform Scenarios

PAGE NO.

31-32

**ABOUT
CAPGEMINI**

PAGE NO.

33

TEAM

EXECUTIVE SUMMARY

Cloud-first strategies are on the rise, and the payload of applications as well as infrastructure services are shifting over time. This will lead to coexisting heterogeneous environments and needless complications for organizations across industries. Enterprises are moving to the cloud for increased scalability, flexibility, and cost optimization, as well as improved reliability and security of their IT infrastructure. The vast majority get stuck in complex hybrid scenarios during this transformation, where some critical application components remain on-premises and a cloud or even multi-cloud architecture must be connected. An overarching solution is needed for consistent overview and control.

This is where Azure Arc comes in: It provides the ability to manage and monitor resources from both worlds – the on-premises and various clouds from a single place. It enables a seamless integration into the Azure ecosystem and leverages many governance and configuration capabilities – such as monitoring and logging – and even integrates with cutting-edge AI/ML services, regardless of where your IT infrastructure is located.

This helps to streamline your operations, increase efficiency, and tighten security, while enabling you to embrace digital transformation at your own pace.



Cloud is not just another technology platform anymore. Agile approaches, DevOps, and the leveraging of data and AI/ML are areas that have accelerated innovation powered by cloud. Cloud, therefore, is the enabler for business innovation and business transformation and is changing not just IT departments but also whole companies and industries."

Sylvia List

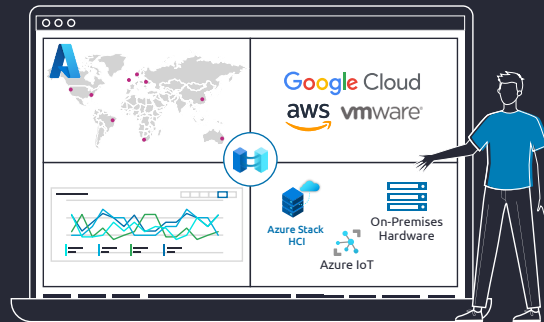
Head of Cloud Center of Excellence - Capgemini

The Bridge - Hybrid Operations Management

Capgemini observes that businesses amid cloud transformation journeys are struggling with the upkeep of multiple management frameworks in both the cloud and their own data centers. At the same time, users are demanding the ability to access innovative services both on-premises and on the edge.



Microsoft allows enterprises to innovate anywhere with Azure Arc and the most comprehensive portfolio of hybrid solutions. A centralized inventory, unified control plane, and simplification are the key benefits of Azure Arc.



Capgemini continuously evaluates the cloud market and has gained deep expertise in the implementation and run of hybrid cloud solutions. Azure Arc is seen as an innovative enabler of sustainable improvement for Capgemini's clients' landscapes.

Improve your management framework by implementing real hybrid operations management with central security and governance control across any location. Introduce new cloud services for container and data in your own data center. Enable agility and cloud native deployment capabilities in on-premises landscape.

Up to
80%

lower risk of data breach, 90+ compliance standards

Up to
30%

ITOps productivity gain

65+

Azure Regions worldwide

20+

Years as a Microsoft Partner

10,000+

Azure-certified Architects

22

Gold Competencies & Specializations

Almost all hyperscalers have revised their strategies toward hybrid cloud and edge. Microsoft, with its hybrid portfolio and services like Azure Stack HCI or Azure Stack Edge, combined with services like Azure Arc, promises a seamless experience by stretching their services and abilities across any premise, even backwards to legacy systems. You participate from the reinforced added value with the advice of Capgemini as a global service integrator (GSI). To deliver on time and satisfy customer expectations, Capgemini is in line with best practices for clients' architecture landscapes (cybersecurity, enterprise service management, and industrial expertise, among others), which are at the heart of our Group Portfolio. We provide an instrument for getting the necessary velocity to gain a coherent view of all of your assets by getting rid of the periscope perspective.

Therefore, as an early adopter, we will introduce and showcase the major advantages of Azure Arc.

With a lucid sense of the future, and excellence in innovation and application of the right tools and strategies, we are perfectly positioned to offer an end-to-end commitment to consolidating your operational hurdles into one clear path to success.



The enablement of an insight-driven business by enterprise intelligence is required to achieve business advantages in operations. This journey on the ocean starting with cross cloud and ending up in the own data center, with Azure Arc's single pane of glass approach, creates a high degree of autonomy."

Timotheus Kuckelkorn

Lead Author - Capgemini

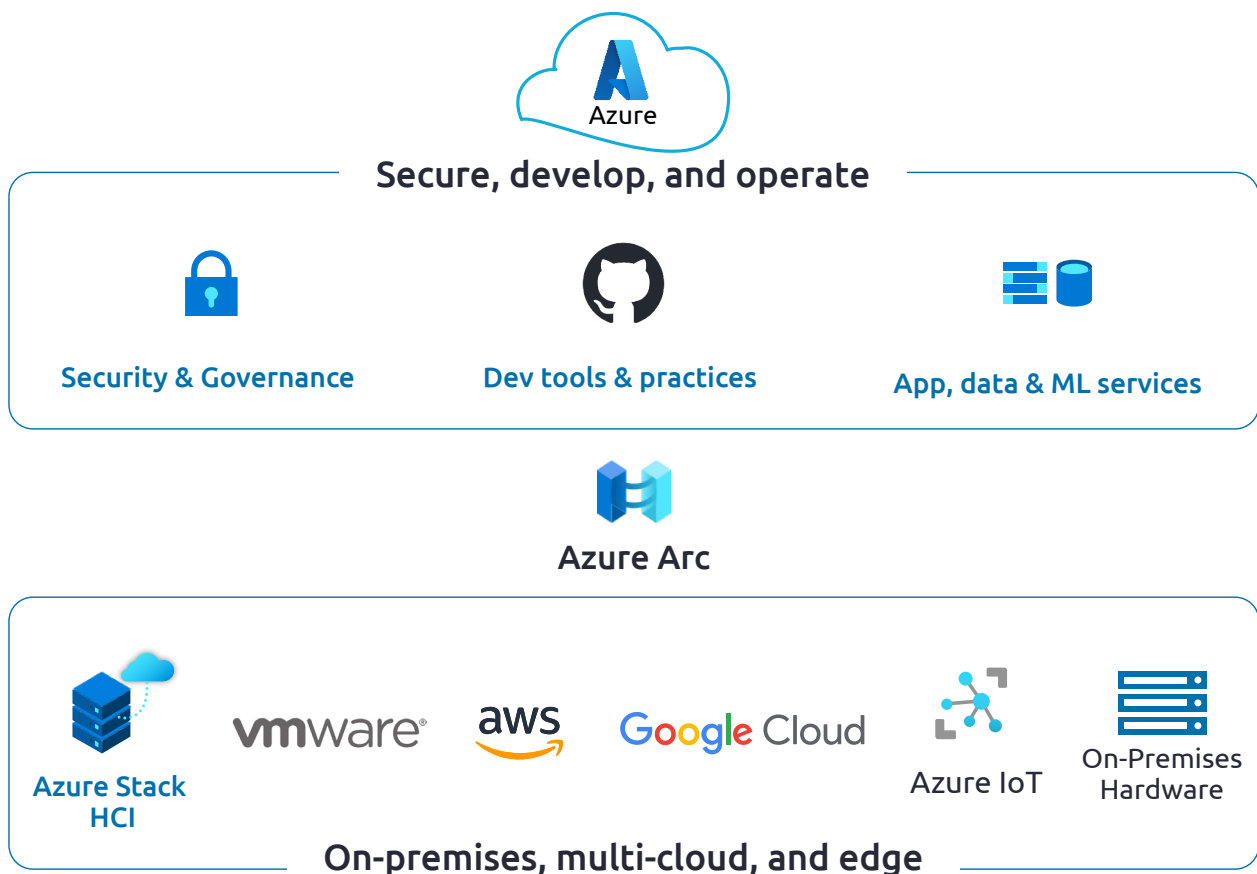


INTRODUCTION INTO AZURE ARC

CONCEPT

The core feature and concept of Azure Arc is to provide a centralized control panel in Microsoft's public cloud environment that allows for the onboarding and management of infrastructure and services in one central place. It integrates different types of deployment models and helps companies overcome the hurdles of on-premises and cloud environments.

Figure 1 Security, Development, and Operation across multiple platforms and locations



Apart from an aggregated inventory and a catalogue of basic operational tasks, Azure Arc users get the freedom to configure and apply rules to role-based access control (RBAC), security, and compliance policies – all from a central Azure Arc control plane. This includes typical capabilities of a public cloud, like monitoring.

Microsoft Defender for Cloud is another overarching feature supported by Azure Arc to assess, identify,

harden, and continuously defend security aspects of Azure Arc-enabled resources.

There are more than just servers; for instance, the following list shows the four domains that Azure Arc can operate by integrating its ecosystem with (Azure Arc-enabled) on-premises computer resources:

1. **Classic infrastructure services: Servers, virtual machines, Kubernetes clusters**
2. **Database services: MS SQL, PostgreSQL**
3. **Application deployment and management**
4. **Machine Learning (ML)**

Next to bare metal servers, VMware vSphere, and Azure Stack HCI-based platforms can be integrated into Azure Arc. Both of them provide lifecycle and extended resource management on their own, but integration with Azure Arc allows them to be managed on a common control plane.

Methodologies like CI/CD and GitOps can be easily realized when integrated with Azure Arc.

This will help companies shift their focus to their core businesses by reducing infrastructure management and application deployment efforts. Furthermore, with services like ML, a company can achieve an increased level of data competency and insight – from the edge to the public cloud core.

BENEFITS

The main benefit of using Azure Arc in hybrid scenarios or during cloud transformations is a standardized and automated operating model for infrastructure in every location – on-premises, cloud, and edge. This follows the principles of BizOps as a bridge builder between IT and business.

The ability to roll out services and configurations centrally takes infrastructure management to a completely new level (e.g., by allowing CI/CD

integration), and the implicit standardization helps reduce overheads and complexity. It also allows adaptation to changing requirements and demands, making it more flexible and letting companies exploit their full potential.

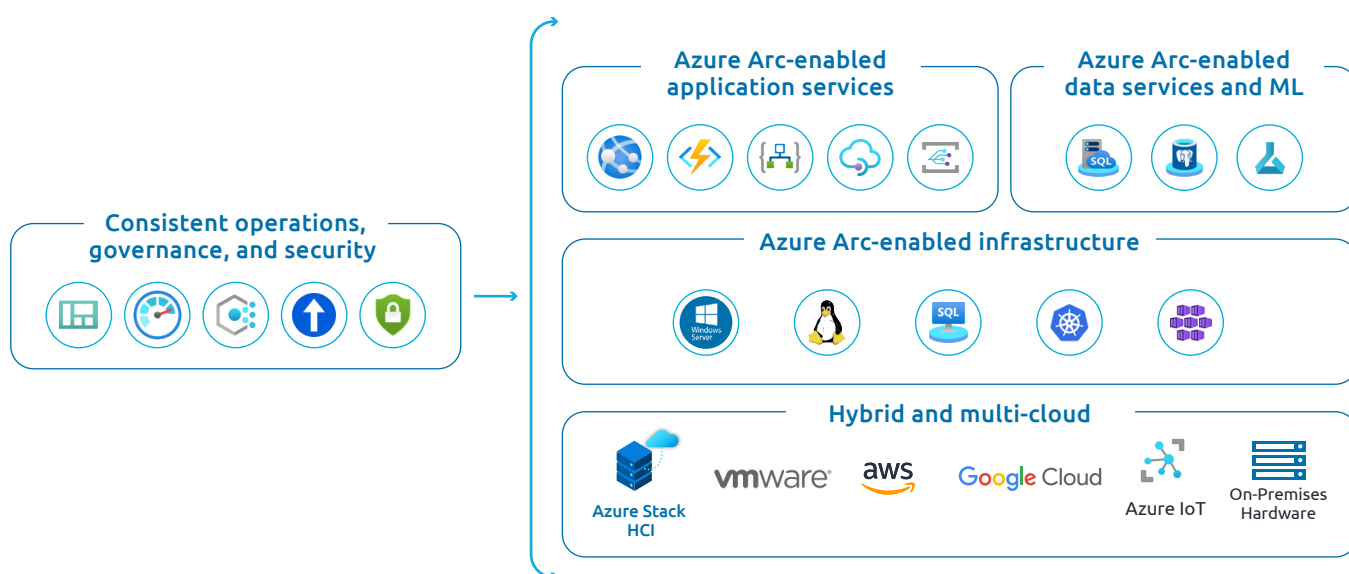
Once this operating model and automation baseline have been set up, it is even easier to deal with the almost inevitable emergence of hybrid architectures in general. Depending on the type of workload that is running on your infrastructure, you can also make use of the inbuilt service tiers like “business critical” for SQL Managed Instances to implement high availability right from the central control plane. When setting up an Azure Arc Resource Bridge, full VMware or Azure Stack HCI clusters can be onboarded and a broad set of functions transferred to the mentioned central control plane.

Operational benefits can be seen in the following dimensions:

Governance, Risk, and Compliance Management (GRC)

The GRC requirements are implemented after an Azure landing zone is configured and the Azure well-architected framework is in place. With Azure Arc, one can monitor and protect the onboarded on-premises or edge workloads by the same configurations. Existing workloads can remain unchanged until mitigation measures have been identified and decided. This can include tracked changes on the operating system, application files, and registry to identify operational and security issues on the on-premises and cloud environments.

Figure 2 Consistent Governance, Security for Platform Infrastructure and Applications Updates



As Azure Arc allows the management of infrastructure centrally across any cloud or dedicated installation or location, you can release and roll out new requirements immediately across the whole estate. The “Custom Locations” feature helps achieve a granular separation of resources and security contexts. It appears as a new region in the Azure portal and can be treated in a similar fashion with respect to the deployment capabilities of Azure Arc-enabled services. You can apply basic principles like RBAC similarly and consistently, such as applying Azure Policy, Azure Monitor, and Microsoft Defender for Cloud to provide consolidated insights into the daily work and increase the level of sovereignty. The governance of (personal) data is of utmost importance, especially for the public sector in tandem with today’s comprehensive GDPR and data privacy regulations. Implementing Azure Arc helps satisfy these requirements as data stays in the local infrastructure and is controlled with services like Azure Monitor.

When it comes to governance, you need to consider cultural aspects as well. In the recent past, working locations were across the globe, and teams from diverse cultures and professional backgrounds worked together. The uniform provision of data and its centralized presentation enable them to improve their communication level. This reaches far into the governance of non-technical areas of the company, like finance and controlling. The employees and their company gain more transparency, visibility, and insight into their data. This makes it easier to apply agile methodologies to deliver solutions to different scenarios quickly, based on a company’s trust in their own governance strategy.



Architect’s Insight:

“What is a Custom Location?”

The Custom Location is used in Azure to uniquely assign resources to the on-premises data center. It appears in the overview of the other Azure regions and can be handled and queried precisely. It is possible to configure several custom locations.



Observability

With Azure Arc's hybrid operation management, you have a variety of options for monitoring the local and cloud infrastructure. Performance monitoring solutions and log management can be utilized to include a collection of on-premises logs that are required for auditing, security, and additional insights.

Azure Arc data can be presented via Azure Monitor. The latter can graphically display various performance logs and optionally offer the possibility to display the logs of several assets cumulatively, so that it is easy to identify the bottlenecks. Predefined alerts can be used, but it is also possible to define own alerts. In the alert chain, it can be freely decided which person or group of people should be informed in which way.

With the help of Azure Monitor Insights, detailed log files from the respective assets can be analyzed and thus targeted **alerts** and **monitoring** can be carried out.

Collected security logs can be easily evaluated via Azure Monitor Insights. They are also automatically evaluated via Microsoft Defender for Cloud, which helps uncover vulnerabilities and secure the entire infrastructure. By using Azure Sentinel over Azure Arc, threats are evaluated with the help of ML and artificial intelligence (AI).

Figure 3 Unified Operation Monitoring across custom and cloud locations



Security Management

Because of regular cyberthreats, the biggest challenge one faces is enterprise security. The Azure perspective is a combination of Azure Arc-integrated services, Microsoft Defender for Cloud, and Azure Monitor, together with Azure Sentinel and, more generically, the broader Azure ecosystem, which gives you a comprehensive security package for your on-premises environment.

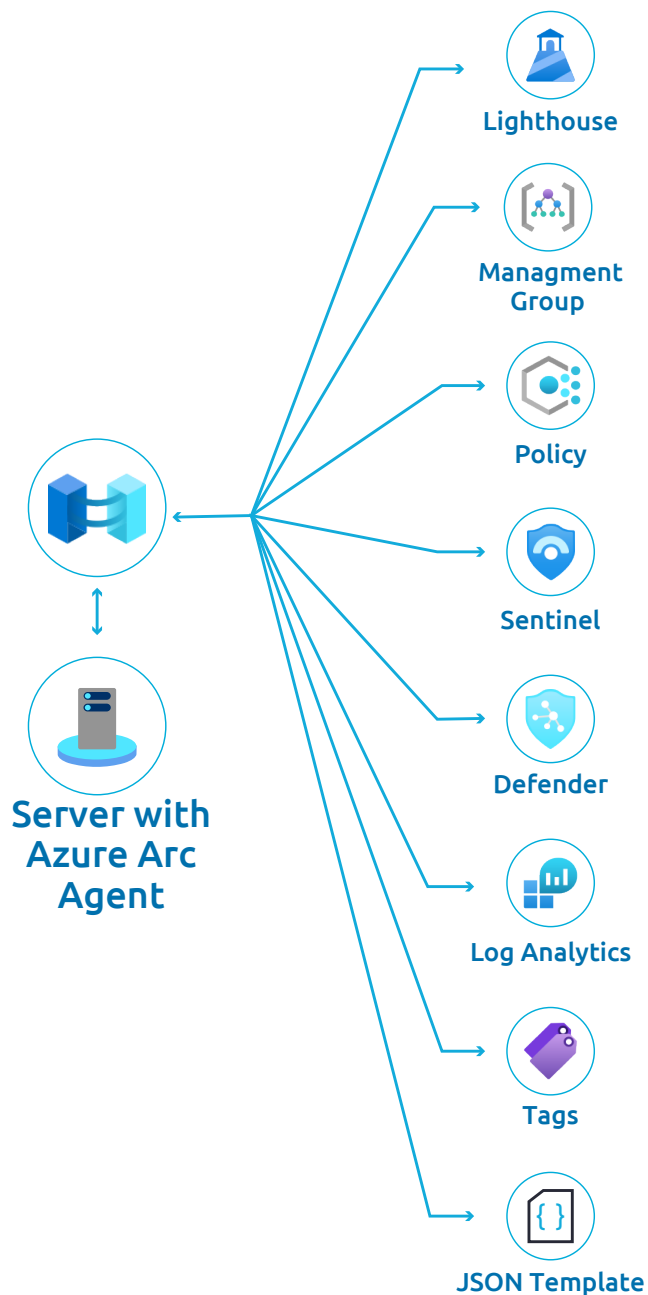
This challenge is well known to Capgemini and we provide security consulting, implementation, and operations to enable client organizations with

Capgemini's end-to-end security frameworks. The goal of a holistic cybersecurity portfolio includes preventive protection, which is more meaningful than the treatment of cyberthreats.

Azure Arc extends control mechanisms to the on-premises parts of the infrastructure and similarly with native Azure services like Microsoft Defender for Cloud or the RBAC model in Identity Services. Servers, clusters and databases are represented as their own objects or identities that can be targeted by Azure and security policies, implementing governance, and are included in compliance reports or configurations in general. They can be rolled out to specifics or all VMs.

Figure 4

Cloud Security capabilities and more managed via only one Arc Agent



The management connection between remote infrastructure and Azure is established securely and encrypted via the Connected Machine agent for servers or their respective containers on Kubernetes clusters. A Virtual Private Network (VPN), ExpressRoute, or the use of Private Link are options to further increase the security level and limit the traffic to private networks.

Besides the basic meta-data inventory and monitoring purpose, one can also configure the Connected Machine agent for servers. On each server, you can individually configure which actions the Connected Machine Agent is allowed to perform. This means that the agent can be adapted to your situation and fits into your security concept.

By enabling a **custom location**, it is integrated into the Azure resource manager and then has access to the RBAC of the cloud. This enables the use of managed identities in your environment. With change tracking, all changes to your operating systems, application files, and the registry are detected and evaluated for security vulnerabilities regardless of where they are hosted, whether in a cloud environment or in your on-premises data center.

By enabling Microsoft **Defender** across all subscriptions, Azure Arc-enabled servers are in scope too. This helps identify security vulnerabilities and track system compliance. With the help of Azure's intelligence, hybrid workloads are securely protected from threats.

An additional plus in terms of security is the advantage that Azure Arc is region specific, which means that customers can choose the Azure region to which their on-premises data center is connected. The required data is then stored exclusively in the selected region. This also applies to Azure Arc-enabled servers. With the help of Azure **Monitor** and **Log Analytics**, you can monitor the rollout process and set up alerts that automatically inform you the moment an asset does not correspond to the desired state.

All the above-mentioned capabilities and service integrations help gain broad security posture insights regarding an enterprise's complete hybrid (cloud) landscape. The ability of reporting security incidents quickly (vulnerability management, threat hunting, and security intelligence) and responding in a fast, adequate way is crucial to stay ahead of the cyber threat.

300+

sites across 34 countries are ISO 27001-certified

TOP 3%

in Cybervadis's cybersecurity and data protection assessment

500+

cybersecurity and data protection professionals

Configuration management

Azure Arc also has competencies in the area of inventory management. Tags, a well-known concept in IT offered by various cloud providers, can be assigned and extended to local resources through hybrid management. This significantly simplifies operations as it leads to a common management approach for cloud and on-premises resources. Depending on company taxonomy, standards, and conventions, an intelligent tag strategy can be used to explore resources. For instance, Azure's Resource Graph Explorer allows you to query, group, and filter resources and makes it possible to extend this service to machines connected through Azure Arc.

With the reporting and remediation options around Patch and **Update Management**, the standardized maintenance of your complete inventory is far easier. For example, the need for updates across all hybrid servers is displayed in an aggregated and categorized view and indicates any need for action at one glance.

The operation teams are dependent on a reasonable amount of data and information in order to react adequately to incidents and optimize the inventory. Combining Azure Log Analytics to gather log data, gain system insights, identify issues, and derive patterns with Azure **Policy** to define and apply resulting policies at scale allows a very convenient and efficient infrastructure operation at the same time.

Automation

Automation and targeted safeguarding of processes that form a standardized and capable solution are important prerequisites for fast and broad **business**

scaling. Today, Microsoft **Azure** and the **CNCF** (Cloud Native Computing Foundation) offer many principles and patterns to economize work.

With Azure Arc, you can use the usual infrastructure-as-code tools like Azure Resource Manager (ARM), JSON, PowerShell, or Bicep. This makes it possible to integrate infrastructure at any location into central CI/CD pipelines. If already established for public cloud, you can use the same process to trigger different sources and locations. Also, the "Custom Script Extension" of Azure can be applied to the hybrid-managed resources. If this is done in combination with policies and tags, Azure Arc-enabled resources (VMs, databases) can be automatically equipped with custom scripts. You can use the same method for automated distribution of updates and the whole patching management in Azure but also on-premises through Azure Arc.

While further automation like start and stop scripts might make more sense to save cost in the cloud, they may also apply locally to free up resources for other users in shared environments. The good news is that, once developed for the public cloud resources, they can be easily reused on-premises and on the edge without any more effort.

The comprehensive and right use of tags is a major vehicle for a high degree of automation. Via Azure Arc, tags can be assigned to any Arc-enabled resource, applying the same benefits of the Microsoft cloud. The fact that automation goes beyond the local and offers a global rollout of updates, patching, IaC, and more really opens the door to better management.

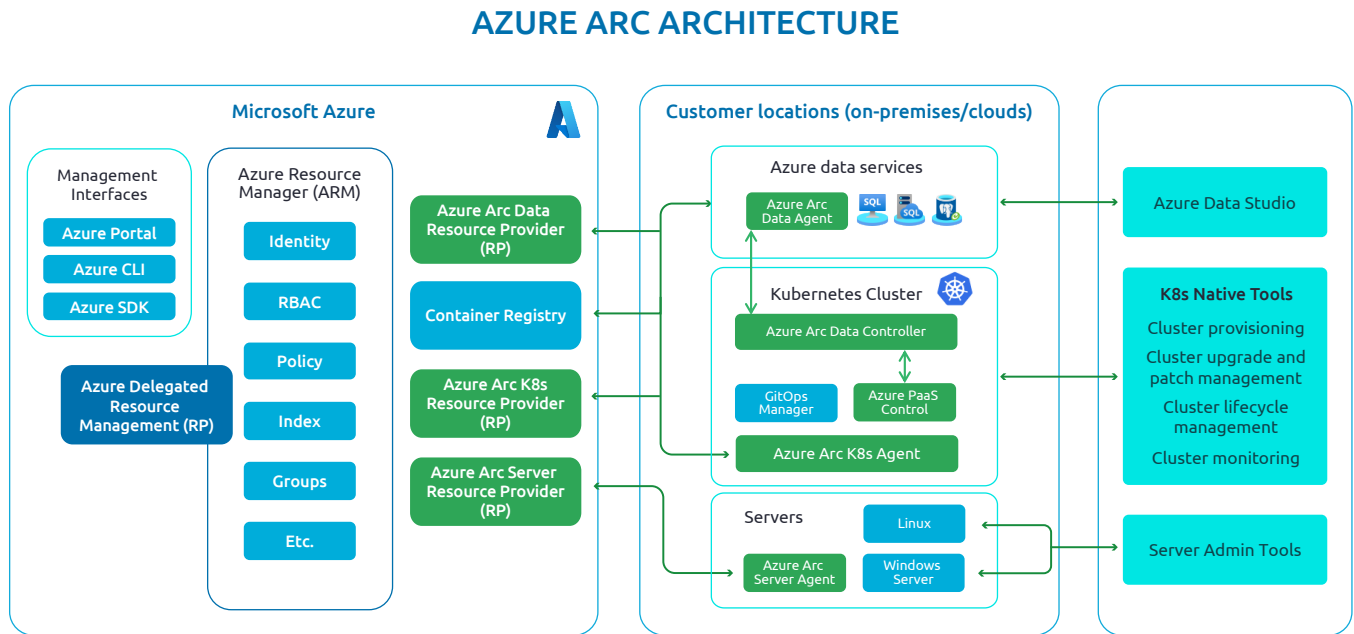
Figure 5 Azure Update Management visualizes required Updates





IMPLEMENTATION INSIGHTS

Figure 6 Azure Arc Architecture to connect custom locations



In this chapter, we describe concrete steps on how to implement the Azure Arc technology to gain the above-mentioned benefits. The following section is more technical and therefore dedicated to professionals like cloud architects.

Enable infrastructure and integrate service

NETWORK CONNECTION

There are various options for connecting Azure and on-premises data centers using Azure Arc.

1. Direct connection via internet:

You can establish a connection from the local data center directly via the public internet. Like others, this Arc connection type is encrypted as well but recommended for experimental workloads.

2. Connection via VPN:

Alternatively, you can use a site-to-site VPN connection. This adds an additional encryption layer for the traffic to run through and is recommended for dev and test workloads.

3. Connection via ExpressRoute:

ExpressRoute grants dedicated bandwidth. For example, failover options are features in it that enterprises can benefit from for any type of workload.

4. Connection via VirtualWAN:

Using Azure VirtualWAN, branches, sites, network hubs, and remote users can connect to and through Azure with optimized and automated network connectivity. It is considered an extension to options 2 and 3.

Each of these network connection methods offers advantages and disadvantages that need you need to evaluate in detail depending on the situation. If needed, service providers like Capgemini can advise you to choose the most appropriate option to connect your data center with Azure Arc and realize further cloud transformation scenarios in this context.



Architect's Insight

"How can you ensure more network security?"

Combining Azure Private Link with ExpressRoute is a great way to optimize your traffic flow. With a Private Link Scope attached to Arc resources, the respective traffic from on-premises is solely traversing the Microsoft backbone and no public networks. Similarly, you can configure other services within the Azure ecosystem, with private endpoints to be reached from Arc-enabled resources.



Architect's Insight

"What are the internal network prerequisites?"

Azure Arc only uses port 443 for communication with the cloud. It must be ensured that all assets that are to communicate with Azure are allowed to use this port. It is also possible to interpose a proxy server (without authentication only) and configure bypassing for certain Azure private endpoints depending on the network requirements.

GOVERNANCE AND CONVENTIONS

To display and manage all local assets in Microsoft Azure, you need to assign them to an Azure subscription. Depending on how the Azure Landing Zone has been set up, many aspects need to be taken into account. These include the following:

- What is the general purpose and strategy of the Landing Zone?
- Do you need a dedicated subscription for Azure Arc-connected resources?
- Should you use one subscription or multiple subscriptions for all site locations?

It is therefore not possible to make a general statement about how Azure Arc can be integrated into your Microsoft Azure environment. This can be decided based on individual situations. A good orientation is provided in the Microsoft documentation around Azure Landing Zones and the hybrid scenario (cloud-adoption-framework/scenarios/hybrid).

Furthermore, you need to consider the principle of custom locations. With this feature, it is possible to group Arc-enabled Kubernetes and hypervisor resources and target them for particular tasks. For instance, they appear as locations to deploy managed database instances and can be listed and queried precisely. Once you define a suitable governance concept, the following Azure **resource providers** must be registered in the corresponding subscription(s):

- **Microsoft.HybridCompute**
- **Microsoft.GuestConfiguration**
- **Microsoft.HybridConnectivity**

Azure resource providers are a collection of REST operations that provide functions for an Azure service.

Regarding required permissions, the responsible administrator needs at least the contributor role in the subscription(s) to configure these resource providers accordingly. As the common Azure RBAC principles apply to custom locations as well, this configuration limits the access to those respectively.

ONBOARDING SERVERS

Azure Arc supports physical servers, virtual machines on a hypervisor (like VMware vSphere or Microsoft Hyper-V), and servers from any other cloud provider. As a prerequisite, a key-based, secure connection needs to be established. A small software component, the Azure Connected Machine agent, needs to be installed to be able to list the target server as a manageable entity. Each agent also offers the option to specify which actions it can carry out. Administrator permissions are required to install it.

The agent rollout itself can happen in different ways:

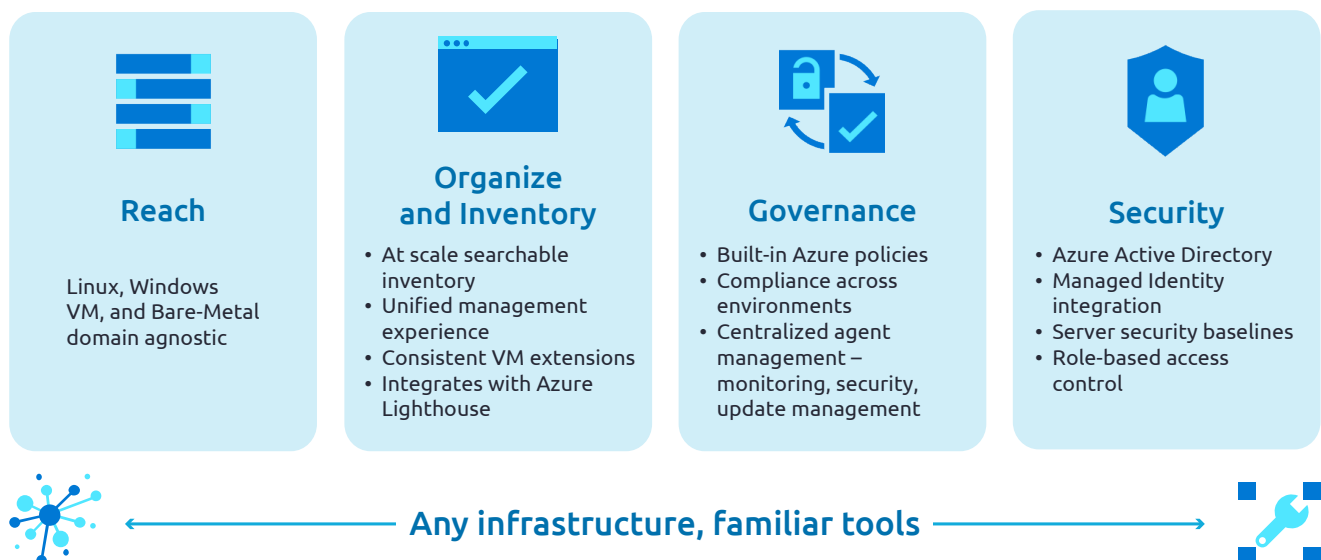
1. **Manual installation**
2. **Installation using a predefined script**
3. **Rollout via group policy (GPO)**
4. **Software distribution solutions such as System Center Configuration Manager (SCCM) or Ansible are supported as well**

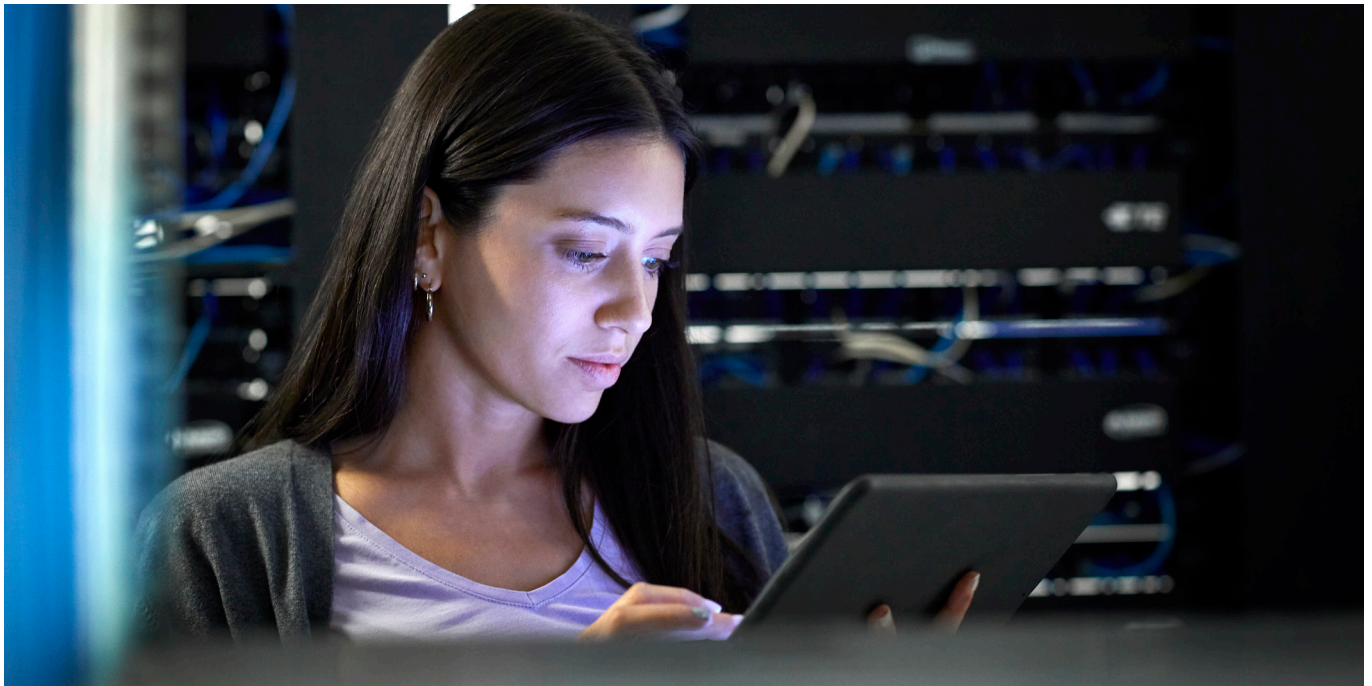
After the Connected Machine Agent is deployed successfully, it automatically connects to Azure Arc and can now be configured and customized. This is done via a command prompt on each server or using the automation solutions mentioned above.

Figure 7 Arc-enabled Servers under control of the (same) Azure Ecosystem

AZURE ARC-ENABLED SERVERS

Bring on-premises and multi-cloud servers to Azure with Azure Arc





Servers are the starting point to discover the possibilities with Arc and they lead to a convenient user experience because it is the same Azure ecosystem. As depicted in Figure 4 above, there are numerous built-in integration options for a secure and structured setup that also apply to any other Azure cloud resource that might already exist or could be created right away to start the cloud journey.



Architect's Insight "What about full Linux support?"

For many years, Microsoft has been heavily engaged in open-source projects and supported Linux similarly to how they support their own Windows products. Due to the large number of Linux distributions, not every distribution can be supported by Azure Arc at present. The most important supported distributions are CentOS, Debian, Red Hat, and Ubuntu. Microsoft is constantly working on supporting more distributions.



Architect's Insight "Which operating system versions are supported?"

A broad range of 64-bit operating systems is supported such as **Windows Server** 2008 R2 or later and Windows IoT Enterprise, as well as many common **Linux distributions**. In common customer engagements, we usually see a broad coverage of above 95% of the possible options. Besides that, Microsoft is constantly extending support, but it is in any case a good idea to work on technical debt (such as OS upgrades to supported versions) during cloud transformations. Once upgraded and put under Azure Arc control, it is far easier to achieve a later cloud migration. An overview of currently supported operating system versions can be found here:

<https://learn.microsoft.com/en-us/azure/azure-arc/servers/prerequisites#supported-operating-systems>

ONBOARDING DATABASES

To onboard an existing Microsoft SQL Server database, you need to execute a script on the server to initiate and establish the connection. Apart from the common Azure **Connected Machine agent**, this will also require registering the **resource providers** “Microsoft.AzureArcData” and “Microsoft.HybridCompute”. Once you connect the SQL Server, it offers great advantages. You can manage it directly from the Azure Portal and perform on-demand SQL assessments. In addition, **Microsoft Defender** can monitor and protect the (remote) SQL server centrally from the cloud.



Architect's Insight “Which databases are supported?”

When onboarding existing databases in on-premises environments, currently only **Microsoft SQL Server 2022** (version 16.x) installed on Windows Server 2016 or above is supported. However, with so-called Azure Arc-enabled **data services** it is possible to host PaaS databases such as PostgreSQL and Azure SQL Managed Instances with **Kubernetes**. This allows to build upon “serverless” databases quickly and easily for new applications but also for applications planned to be moved to cloud the later on.



ONBOARDING CONTAINERS

If you are connecting to an existing Kubernetes cluster, it does not matter if it is running at a hyperscaler or on-premises, for example, in Azure Stack HCI or just simply in existing infrastructure. The onboarding is achieved with the help of a script provided through the Azure Portal. To connect a Kubernetes cluster securely and permanently, multiple pods are set up in

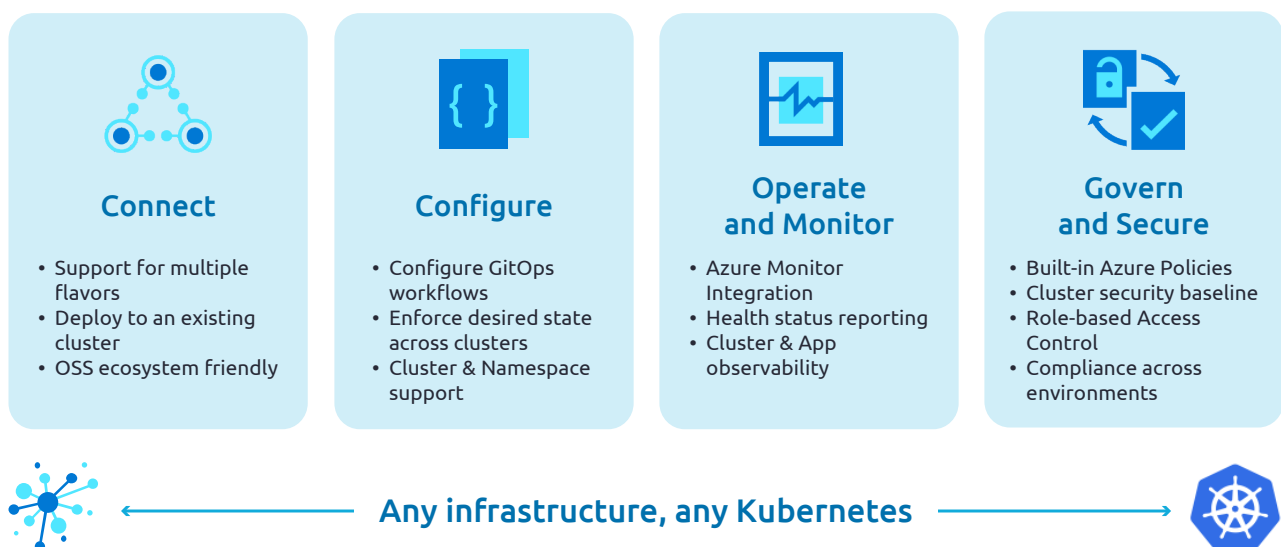
the dedicated namespace “azure-arc”. Those containers allow you to collect generic information, metrics, and monitoring data and control the cluster. Furthermore, you need a kubeconfig file and the installation of Helm 3 (version 3.7.0 or lower). With respect to compatibility and support, it supports any type of Kubernetes cluster with CNCF certification.

As with onboarded servers and databases, Kubernetes clusters benefit from the same ecosystem as shown in the graphic below.

Figure 8 Arc-enabled Kubernetes Clusters under control of the (same) Azure Ecosystem

AZURE ARC-ENABLED KUBERNETES

Connect, manage, and operate Kubernetes clusters and applications running anywhere using Azure Arc



Architect's Insight

“What are the hardware requirements of the Resource Bridge?”

16 GB of RAM and 4 vCPUs are recommended for the Resource Bridge VM per custom location. Furthermore, at least 100 GB of hard disk space should be available.

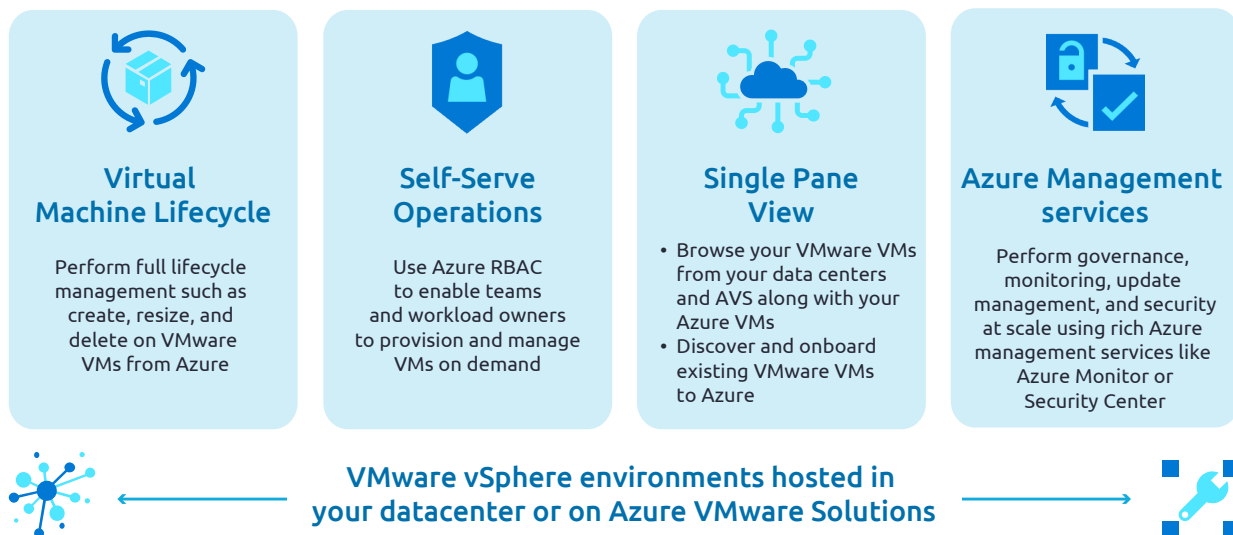
ONBOARDING HYPERVISORS AND PLATFORM STACKS

In addition to individual assets, Azure Arc can also support hypervisors and platform stacks. Once integrated, one can manage and monitor existing workloads or virtual machines and also deploy and configure new workloads in(to) these environments. Again, all this is steered from the central Azure control plane.

Figure 9 Arc-enabled Hypervisors and Platform Stacks allow the operation of virtual machine lifecycles

AZURE ARC-ENABLED VMWARE VSPHERE

Provision and Manage VMware VMs from Azure using Azure Arc



To connect with an Azure Stack HCI or a VMware vSphere cluster, it is required to establish an Azure Arc Resource Bridge. This is a lightweight VM in the cluster, which handles the encrypted communication between both the cluster and cloud.

Connecting an Azure Stack HCI Cluster to Azure requires to register it first. With this base configuration in place, the Azure Arc integration can be activated. Then you need to set up a Resource Bridge and optionally a custom location may be executed as documented. Suitable tools to perform these tasks are Windows Admin Center or PowerShell.

In order to connect a **VMware vCenter** instance to Azure Arc, you need to meet the necessary specifications and prerequisites. This includes an installation script that is prepared from the Azure portal including information about the Resource Bridge VM. Running this script locally connects to the vCenter instance, authenticates and installs the Resource Bridge VM, and connects to Azure including further metadata like the name of the custom location and network information. A permanent connection proxied through the Resource Bridge is then established to control and connect to the VMware hypervisor.



Architect's Insight "What hypervisors or platforms are supported?"

The Azure Arc Resource Bridge supports **VMware vCenter 6.7 and 7.0** as well as **Azure Stack HCI versions 22H2, 21H2, and 20H2**. A maximum of 9500 VMs can be managed with one Resource Bridge.

If the hypervisor used is not officially supported by Azure Arc, control of the guest systems is not strictly excluded or blocked. It might still be possible to connect and control the guest from Azure Arc through the Connected Machine agent.

TAKE THE LANDSCAPE UNDER NEW CONTROL

Azure Arc is the perfect enabler to introduce the cloud to any enterprise, with the various options to connect and register existing on-premises infrastructure and the described benefits. What this means is that there is no absolute need to create a lot of (expensive) resources and complex application stacks in the cloud for a business outcome right away. Instead, this is a chance to kick off a full transformation journey and familiarize oneself with the cloud as a new environment. With the central control plane in Azure Arc, it is possible to monitor health the security posture, and compliance status information of existing servers, clusters, or databases in one place. Compliance is both a very crucial obligation to prove in reporting lines and a component of every governance strategy to be designed and implemented.

To begin, key questions in the cloud governance strategy regarding network connectivity, an RBAC model, (naming) conventions, and cost control need to be answered and the various options weighed. Once a baseline that is eventually accelerated by a structured assessment or solution design has been prepared, one may start simply by onboarding the first Arc-enabled servers from on-premises and explore cloud service options in parallel.

The subsequent logical next steps could be the following

Migrate, lift, and shift application candidates to the cloud

Leverage automation opportunities like CI/CD pipelines or scaling features

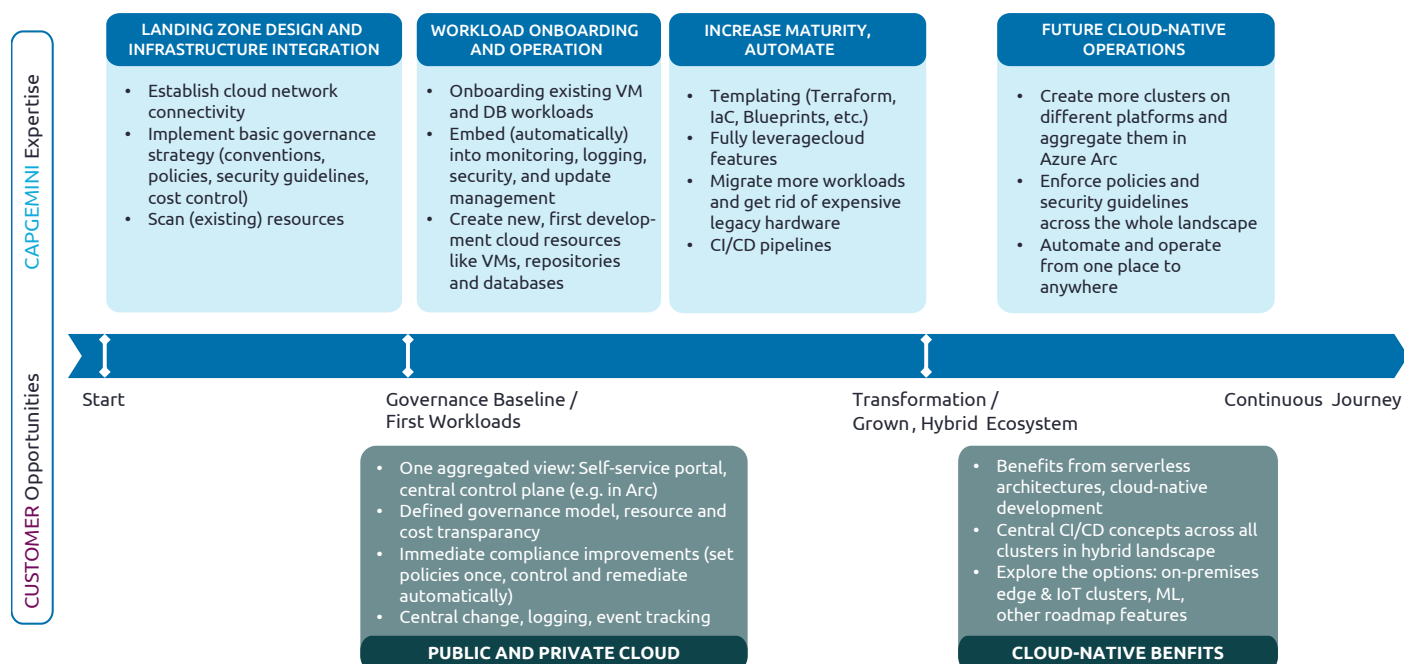
Realize template and stage concepts combined with other cloud ecosystem services for modern application architectures and faster, repeatable deployments

Gradually, the cloud footprint can be extended. Whether a particular workload is hosted on Arc-enabled on-premises infrastructure, in the cloud, or in a hybrid model depends on the individual application requirement and probably also an update/release strategy. Either way, these changes require thinking about new operating models as new technology fields, tools, and workflows will be introduced too.

Finally, one thing that you should not forget is that such a business transformation is also a transformation of employees and their mindsets. The ways of working will change and offer great opportunities at the same time.

The illustration below shows how Capgemini can help you with your cloud transformation with best practices and the 6 R's of cloud migration like application migrations or modernizations, and lists potential aspects on that continuous journey:

Figure 10 Sample Cloud Transformation Journey accelerating benefits through Capgemini



An aerial photograph of a large cable-stayed bridge with a prominent white pylon and orange stay cables. The bridge spans a wide river. In the foreground, a large container ship is loaded with colorful shipping containers (blue, red, yellow, and orange). A small boat is visible on the river near the bridge. The background shows a city skyline under a sunset sky.

OPERATIONS INSIGHTS

In the next few chapters, you can find some considerations around the run phase, details on how to extend the integrations to manage multiple container locations and tenants easily, and some information around the implications regarding costs using the Azure Arc technology.

GITOPS ACROSS MULTIPLE CONTAINER LOCATIONS

One can extend and use Azure Arc as a unified container management system across Kubernetes clusters of different kinds, even when they are located in different clouds by applying GitOps and Service Mesh principles. In the container context, you can easily manage workloads, applications, and cluster infrastructure and change them centrally using GitOps.

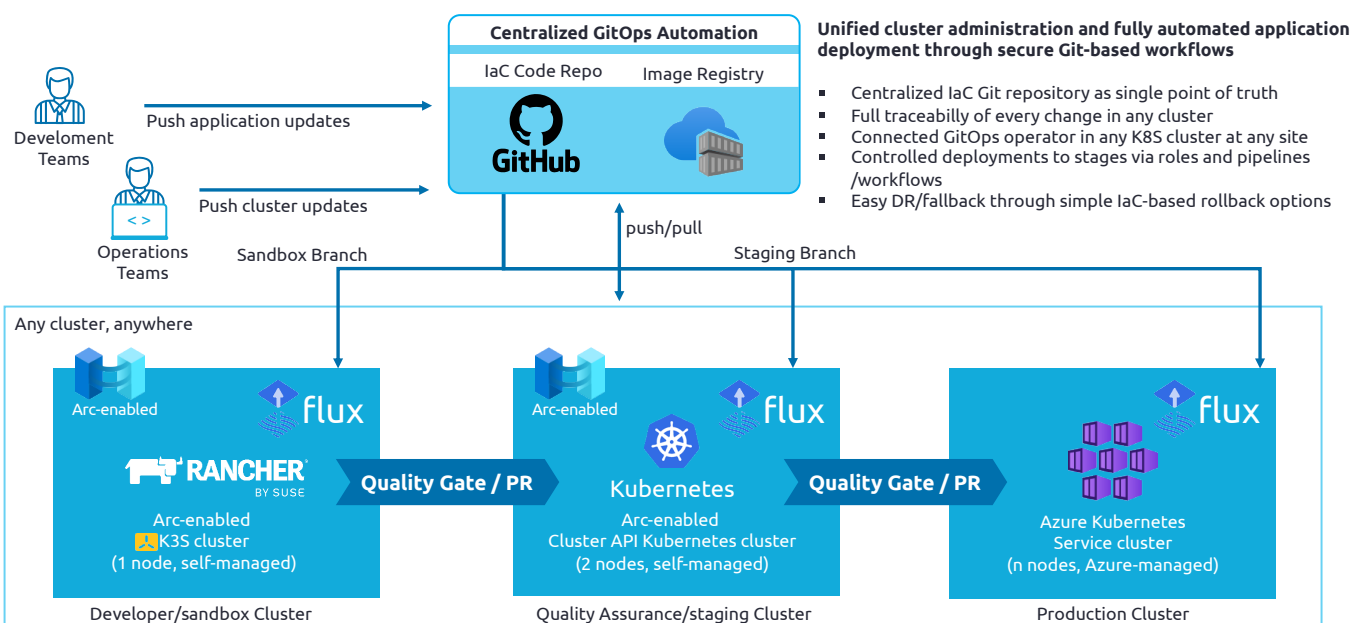
The architecture above shows a possible setup for applied GitOps in a heterogeneous Kubernetes landscape. The heart of the architecture is a centralized Git repository holding IaC, which can be deployed through CD pipelines triggered through a single code push, defining target states that are maintained and configured accordingly.

Short recap: When onboarding a Kubernetes cluster in Microsoft Azure Arc, a set of agents are deployed into the dedicated namespace “azure-arc” to establish the Azure backend connectivity, monitor the cluster, and perform general configuration changes, for instance, due to enforced policies.

To apply GitOps, you need to install an additional Flux extension in the Kubernetes cluster (called “microsoft.flux”). With the shipping Flux Config agent and controller components, it is possible to let a cluster listen for changes in the code baseline and roll them out with the help of YAML-defined state descriptions. Flux graduated from being the core component to realize GitOps on Arc-enabled Kubernetes clusters from the CNCF incubator and has seen an increase in demand.

Generally, GitOps is a methodology and strategy to bring code and operations together and to achieve shorter implementation cycles. It goes beyond the usual separated approach of the development team that delivers changes and new features in the form of artifacts that the operations team then rolls out. Meanwhile, GitOps has also become an industry standard that can be introduced in different ways and with different characteristics. With shorter change cycles and the central Git repository in combination with CI/CD pipelines and Flux picking up the changes and turning them into rolling updates in the target Kubernetes clusters, several advantages can be achieved:

Figure 11 Unified Cluster Administration - Exemplary GitOps architecture with different types of Kubernetes Clusters in stages



Versioning and automation:

The code in GIT is naturally maintained with versions, exact references, and release information that can be picked up by automation solutions – for example, respectively designed CI/CD pipelines and resulting changes pushed to different Kubernetes clusters anywhere. Rather than a general set of changes, flux and state definitions, and even applications, can be steered centrally in an automated fashion.

Improved code quality and reliability:

In combination with a staging concept and due to more frequent changes with almost immediate effect on the infrastructure or application landscape, the feedback loop from operations to the developers is shortened massively as well.

Centralized, unified control plane:

With Azure Arc, Git and the broader Azure and Kubernetes ecosystem, the required tools and user experience of dev and ops teams is simplified.

COST IMPLICATIONS DUE TO AZURE ARC

Azure Arc agents and the enablement of this service come with no cost. There are some minor infrastructure components that you need to build and enable a secure connection to the on-premises or other cloud platforms' resources, such as private link, VPN Gateways, or similar. After this, utilizing the Azure management components, for instance Azure Monitor, Azure Defender, or the Kubernetes Cluster administration, comes with the same cost and pricing models as within Azure. With that, costs are known

and predictable, and scaling effects for an efficient and similar use in hybrid- and multi-cloud scenarios apply.

On the contrary, many savings are possible:

- Any patch tool can be replaced by the Azure internal patching algorithms.
- The same applies for any third-party software deployment tool: there are no licensing, tool updates, or tool operations.
- Deployment tools can be combined into one, triggering similar APIs for provisioning resources in clouds and on-premises and running the same as-code templates and scripts for further configuration.
- A built-in user and rights management allows for more granular and deeper self-service capabilities and therefore reduces wait times and transaction times between different teams.
- Automation only needs to be built and maintained once for the whole hybrid landscape.
- Being focused on one common management model and toolset helps when it comes to training costs, common understanding, technical language, and fixing issues together.
- Working under the same policies and governance framework not only increases security and compliance but it also reduces risk and cost for risk mitigations, and helps the consumers develop easily under a commonly understandable cloud framework.

There are many potential savings and benefits possible and it would be best to experience it yourselves, maybe in a PoC installation as outlined in the next chapter.

MULTI-TENANT MANAGEMENT

An administrator can face the challenges of permanently switching identity contexts when managing multiple tenants in the public cloud. Each tenant has its own identity system. An administrator who is responsible for many of thee must jump from one identity to another to be able to log in to each customer environment and manage the resources.

To make this procedure a bit easier, Microsoft provides a solution directly from Microsoft Cloud. The service called Azure Lighthouse enables a delegation of resource management to a different tenant, which in turn enables an administrator to manage all delegated resources without logging in to the separate tenants. In this manner, the administrator can manage all delegated customer resources from within the service provider tenant. All resources will show up in the administrator's context as long as adequate access rights are granted.

Figure 12 The challenge of switching identities in operating multiple tenants

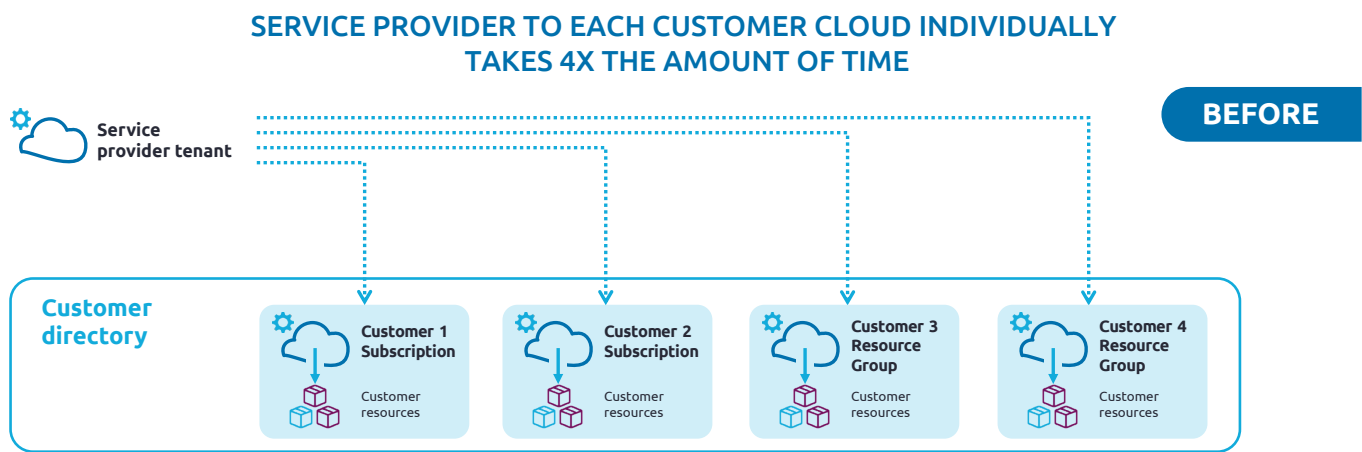
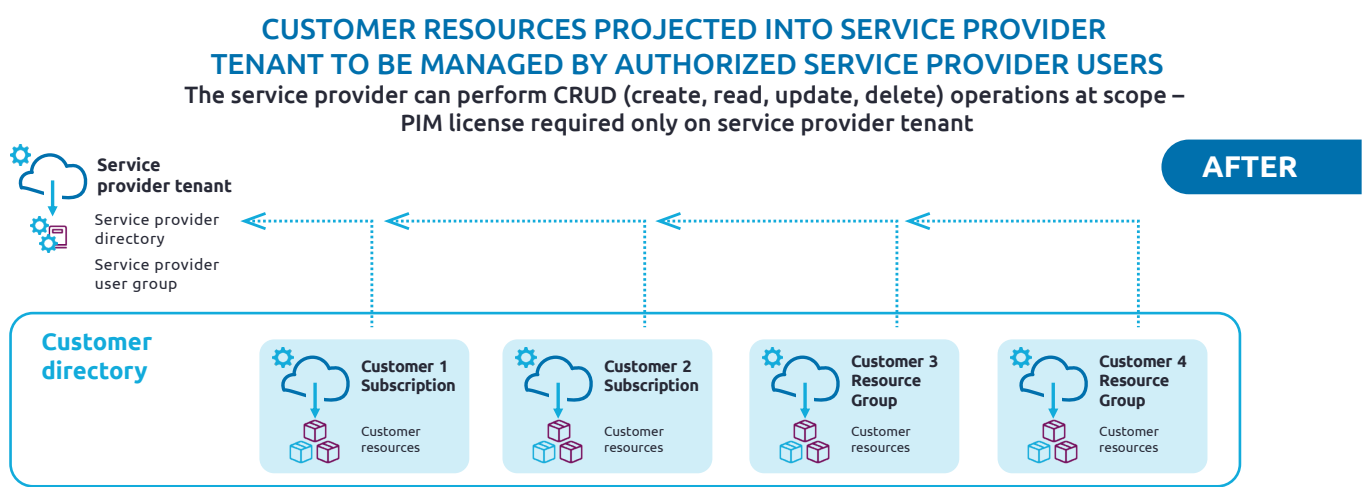


Figure 13 Azure Lighthouse allows resource delegation across multiple tenants



All actions performed by the user in the service provider tenant are logged in the Azure activity log and are visible for the customers who delegated the management. You can integrate the approval processes (like Azure AD privilege identity management (PIM)) additionally into this delegation. This means that the service provider, i.e. the user, gets read rights all the time, but as soon as there are higher privileges necessary, like an Azure contributor role, an approval process can be triggered.

By combining Azure Lighthouse's capabilities with Azure Arc it is possible to not only manage cloud resources from different customers via delegation but also all Azure Arc enabled resources like servers, Kubernetes cluster or even data services. This multi-tenant management concept is not only an option for service providers, but also for enterprises with different organizations or entities.

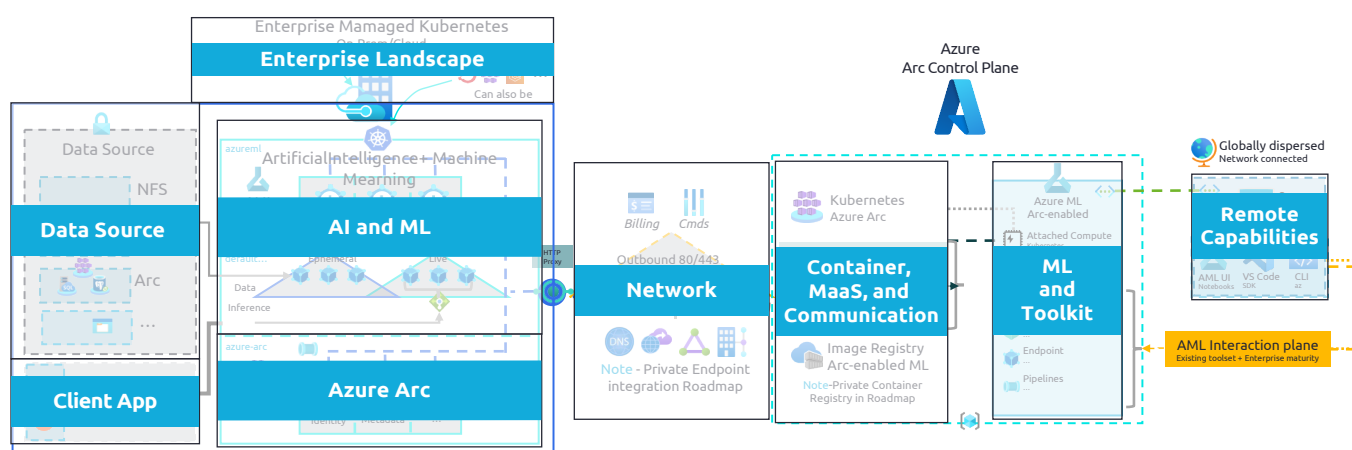
MACHINE LEARNING

By using Azure Machine Learning, data scientists and developers can deploy and manage high-quality models faster and more reliably. With Azure Machine Learning, you can deliver these benefits as a service directly from the cloud. The challenge for organizations here is to collect the underlying data and execute the ML workflows. Using Azure Arc to manage the on-premises infrastructure, other cloud providers and various Kubernetes have the advantage that it collects and evaluates data centrally in Microsoft Azure. Through the combination of Azure Arc and Azure Machine Learning, the collected resource data is used with the

same Azure Machine Learning experience found in Microsoft Azure. This provides centralized visibility, operations, and compliance. The basic principles of ML i.e. reproducibility and reusability, are thus consistently followed in the hybrid management approach and can be used for the entire ML lifecycle.

You can install the Azure Machine Learning extension by using a Kubernetes cluster. The advantage here is that you can execute Azure Machine Learning on the connected cluster without violating data protection guidelines. Furthermore, the advantages of the unified experience through the Azure Portal remain the same.

Figure 14 Comprehensive ML architecture combining remote and cloud capabilities



MANAGED SERVICES BY CAPGEMINI

Organizations are moving large portfolios of legacy applications, ITIL-based processes, and datacenters to the cloud and want a secure and efficient way to manage and govern their infrastructure and applications. They also require the ability to leverage modern hyperscaler technologies to deliver services, and thus value, faster to the business. Once they have established a new Target operating model (TOM) that fulfills all this, users want the same benefits in return – user experience and comfort in the on-premises or edge environment.

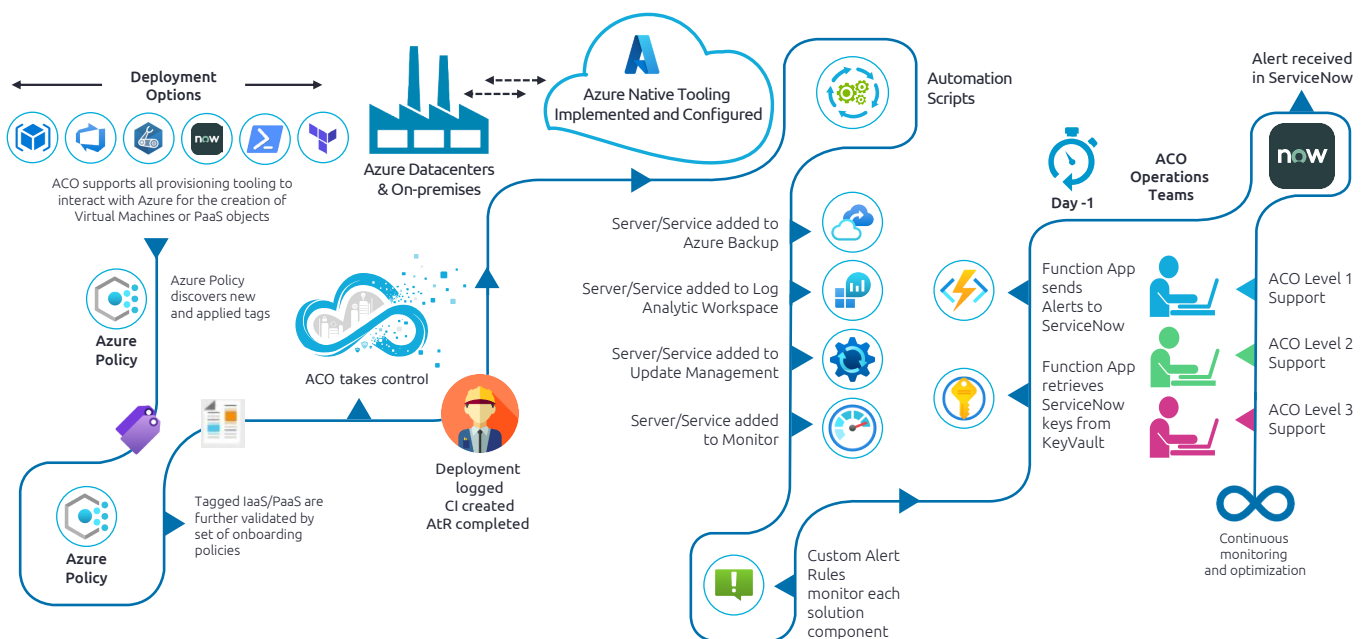
A state-of-the-art managed service can provide a reliable, secure, flexible, and efficient foundation for running applications and infrastructure across hybrid cloud environments encompassing public, private, and edge through an adaptable framework of deep cloud expertise, cloud-ready processes, modern tooling, continuous optimization, and support. For instance, Capgemini's Adaptive Cloud Operation (ACO) portfolio supports customers throughout the lifecycle of their cloud journey such as SAP transformation, datacenter

modernization, cloud transformation, and application development acceleration.

The same managed service across hybrid cloud environments brings the following key benefits:

- Security within particular cloud guardrail management and workload protection building on best practices and industry standards as well as full governance transparency
- Efficiency, such as ready-to-go cloud platforms with platforms as a product and a high degree of automation not only during deployment (desired state configuration)
- Reliability through end-to-end support building on full control via an adaptive observability across multiple regions and locations
- Adaptability to rapidly changing market needs
- End-to-end focus, such as for end-to-end applications stretching across multiple platforms and locations
- Better collaboration like monitoring provides a comprehensive overarching view, and SaaS services allow for common DevOps processes and continuous learning (e.g., by AI)

Figure 15 Lifecycle of Adaptive Cloud Operation (ACO) services



WHAT'S NEXT



PROOF THE CONCEPT



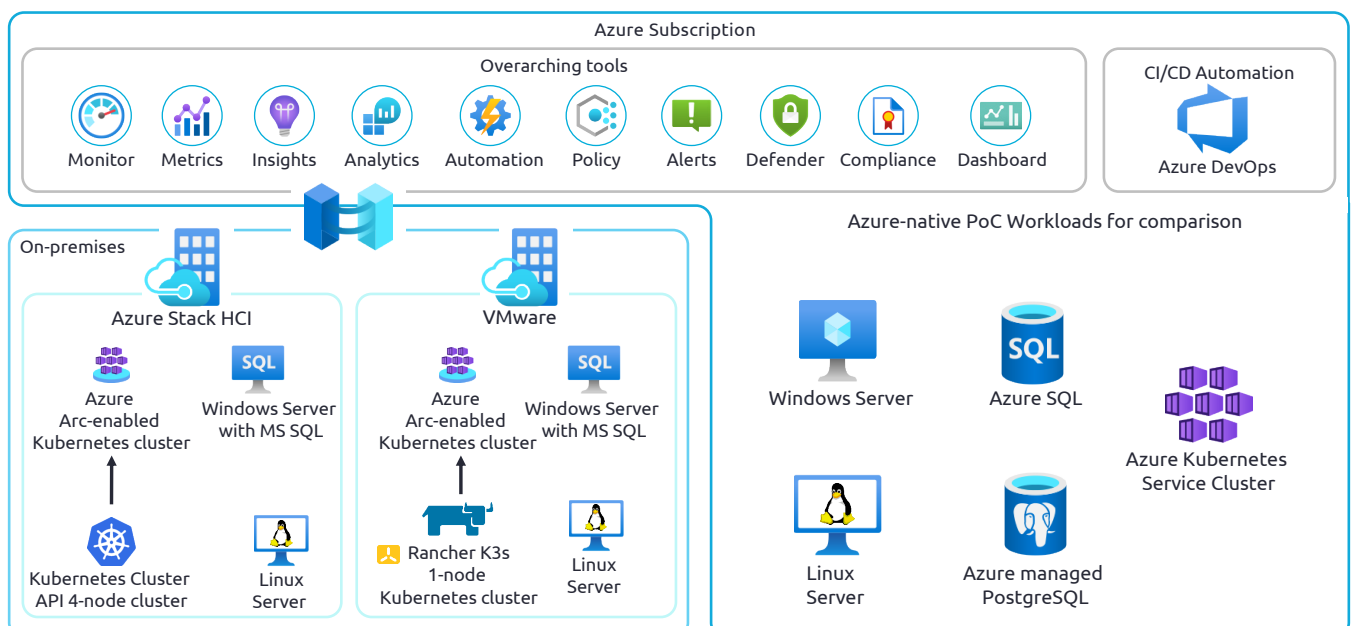
Helping customers deliver new services gives me the opportunity to act as a human enabler for new technologies. The use of proofs of concept is a compelling way to break down capabilities and gain first touch points with the identity of the solution."

Fabian Ludwig Felter
Azure Arc Expert

A good way to probe the above-described benefits and implementations is to perform a proof of concept (PoC). A central Azure subscription can be created just for this purpose. As potential targets, several options are available:

1. **Microsoft provides a couple of virtual resources within the Azure Arc Jump Box** that emulate the behavior of servers, databases, and Kubernetes in the same Azure subscription.
2. **With hardware vendors, Capgemini has built test environments in the hardware vendors, labs** and linked them via the described Resource Bridges to the Azure subscription. Possible hardware, are bare metal servers, a VMwarebased hypervisor or even Azure Stack (e.g. HCI devices). With this, complete integrational work, as well as examples under real conditions, can be tested.
3. **You can take existing workloads within enterprises, datacenters as samples.** Usually, we see some more effort here in aligning on network and security aspects before the bridge can be activated. On the benefit side, it will give the best close-to-life results, such as concrete server image compatibility or the allowed port and routing topics. And in addition, once it is established and the PoC is successful, it can be transferred into productive use.

Figure 16 Example Design of a Proof of Concept (PoC) Setup




















MICROSOFT AZURE HYBRID ROADMAP

Microsoft has made and is still investing in its hybrid capabilities. Many functions were published under “Preview” and later under “General Available” during the last few years. In this manner, Microsoft ensures that it provides high quality for its customers.

Figure 17 Azure hybrid investments beyond – 2023+

Azure hybrid investments in CY 2023+

- | | |
|--|---|
|  Leverage and build on Azure Arc as the management and control plane for hybrid and multi-cloud services |  Leverage and build on Azure Arc as the management and control plane for infrastructure, apps, and data services |
|  Evolve Kubernetes lifecycle management |  Improve efficiencies and compliance for data sovereignty /residency regulatory requirements |
|  Continue to invest in enhancing server management capabilities such as Azure Automanage | <p>Increase overall node count scalability through multi-cluster management</p> |
|  Evolve AKS capabilities to orchestrate containerized workloads with support for additional hypervisors and platforms |  Drive industry-leading security and hardening characteristics to support unique customer requirements |
|  Drive advancements in AI/ML including native integration and support | <p>Leverage software-defined hyper-converged infrastructure as the core platform architecture to run Azure Arc-enabled services</p> |
|  Enhance support for HPC workloads including hybrid mechanisms for caching |  Implement end-to-end Microsoft delivered solutions including key edge form factor hardware |
|  Enable advanced hybrid IoT implementation to light up data processing at the edge |  Evolve compute support to GPU fractional and alternative compute models (offloads) |
|  Continue to invest in improving disconnected scenarios |  Assist in best practices, performance, and governance of deployed SQL servers by connecting to Azure |
|  Run real-time analytics with Synapse link. Reintroduce PostgreSQL for business critical data | |

Request the full roadmap by contacting Capgemini.

MULTI-PLATFORM SCENARIOS

According to recent studies, the majority of medium and larger enterprises find themselves in a multi-cloud environment where multiple public or private clouds are in use. Usually, this is not by a definite strategy, but it often happens due to mergers and acquisitions (M&A) activities, certain partnerships, or specific business use cases.

There are different ways to orchestrate and control multi-cloud scenarios and that might fill another dedicated white paper. Whether you treat each of the platforms in full scope or not, it leaves you with question on compliance, security, and up-to-dateness across the whole landscape.

There are plenty of tools in the market (Gartner: Cloud Management Tooling) that promise to span a single pane of glass across whole landscapes. They often cannot fulfill all the promises, especially if services are consumed beside VMs and databases. In addition, you must deal with license management and integration efforts yourself. It may also be an issue where the governance logic is built into either the Cloud Management Portal (CMP) or directly in the supported platform. The former means that you may

only consume platform services via the CMP solution, as otherwise your workloads are not governed. This may restrict the possibilities of self-service enablement or CI/ CD pipeline integrations.

If enterprises have built a state-of-the-art controlling organization in Azure, Azure Arc can be a solution to stretch the same controls also across other platforms. This brings the benefit of a single place to go when it comes to questions like the following:

What is my degree of vulnerability?

Are all my systems up to date with new versions?

Are Cloud Infrastructure Services or any other industry security standards applied?

Azure's auto remediations and policies can help mitigate the findings on-premises. At least you have solved the burden of collecting all those compliance reports together and parsing them into a common look and feel. Other platforms are considered as secondary and do not have a mature management layer like being built for your primary Azure platform where remediations and corrections can be triggered via the native Azure capabilities. As outlined in previous chapters, this not only applies to servers but also to databases and container clusters.





Capgemini is one of the world's leading providers of IT consulting and management, strategy consulting, digital transformation support services, and software and engineering services. As a global service integrator (GSI) with 370,000 employees, we are able to provide almost any local service to our customer through Capgemini's global owned Rightshore® delivery model, like the 24x7 or follow-the-sun models.



Poly Clouds are very quickly becoming the gold standard for any sustainably successful company. Azure Arc is the unique all-purpose tool to implement it."

Dr. Marco A. Harrendorf

Guild Executive Sponsor

Within Capgemini, we run guilds for all major cloud providers. The Microsoft Guild with its several technical sub-domains and pillowed clusters for business at the moment supports 10,000+ Azure-certified consultants and project managers globally. The guild principle serves as a competence hub and platform for interdisciplinary and cross-practice-related cooperation. Partner managers and architects align on certain topics such as this white paper. This white paper is intended to add value and be freely available to our customers and anyone else whom may it concern.

Capgemini's mission is to continuously reveal and harness human potential using diverse technologies and to create a better, sustainable future. We offer in-depth industry know-how that convinces customers to let us support them in their complete enterprise IT journey, ranging from consulting through transformation to operations.

The potential that can be unleashed and leveraged through cloud and cyber security capabilities requires a competent partner. Many customers have found Capgemini as a strong and competent partner for their cloud journey while Capgemini has found a strong partner in Microsoft, with whom we have established a solid relationship over the past years.

Microsoft Partner



2022 Partner of the Year Winner
Germany

By recurringly taking a bird's eye view on various topics and by taking an agnostic perspective - we strive to gain insights and a broad overview in the market for a sustainable consultancy service. This adaptive way is a guiding principle to formulate a value proposition to our customers, finally also when using services like Azure Arc in cooperation with Microsoft and customers.

Sources:

Microsoft – Azure Arc Product

Link: <https://azure.microsoft.com/en-us/products/azure-arc/#features>

Microsoft – Azure Arc Jumpstart

Link: <https://azurearcjumpstart.io/>

Microsoft – Learn Azure Arc

Link: <https://learn.microsoft.com/en-us/azure/azure-arc/>

Explore Azure Arc enabled services

Link: <https://www.microsoftpartnercommunity.com/atvwr79957/attachments/atvwr79957/AzureHybridPartnerJourney/1/4/Explore%20Azure%20Arc%20enabled%20services.pdf>

Microsoft – Train and deploy machine learning anywhere

Link: [https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-arc-enabled-machine-learning-white-paper/MicrosoftAzureArcEnabledML-accessible%20\(1\).pdf](https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-arc-enabled-machine-learning-white-paper/MicrosoftAzureArcEnabledML-accessible%20(1).pdf)

Hybrid Dev, Compute & Management Updates with Azure Arc

Link: <https://youtu.be/J0PqDSJCV0U>

Forrester Total Economic Impact™ Of Microsoft Azure Arc for Security and Governance

Link: <https://azure.microsoft.com/en-us/resources/forrester-total-economic-impact-of-microsoft-azure-arc-for-security-and-governance/>

2022 Microsoft Partner of the Year Awards - Winner list



Microsoft's Solution Partner Microsoft Cloud - all six designations



Figure 18 Capgemini's Microsoft Partnership and Capabilities

OUR MICROSOFT PARTNERSHIP AND CAPABILITIES

THE PEOPLE



50,000+
Azure training
Consultants



10,000+
Azure certified
Architects &
Project Manager



22
Gold Competencies
& Specializations



THE PARTNERSHIP

20+ years as a Microsoft partner

Out of nearly 100,000 certified Microsoft partners, only 0.5% of the Microsoft Partner Network is actually "managed" by Microsoft. Capgemini is one of the 0.5%.



THE RECOGNITION Microsoft Awards



- Microsoft Partner of the Year Germany, Country Award (2022)
- Partner of the Year Digital Transformation, Analytics, Financial Services (2021)
- Microsoft Business Excellence Finalist Global System Integrator (GSI) (2022)
- Microsoft's Finalist for SAP on Azure Award (2022)
- Business Groups recognition through Cosmos DB (2019)
- Azure Expert, Managed Services Provider (2019)
- Inner Circle for Microsoft Business Applications (2019/2020)
- Microsoft's Winner for Powerapps (2022)
- Microsoft's Solution Partner Microsoft Cloud—all six designations (2022)



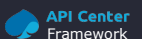
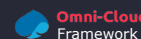
Microsoft Cloud Guild Germany

- Linked knowledge hub that connects a variety of employees across different technical and business domains
- Microsoft Azure, M365, and Dynamics
- Experts deeply linked into Microsoft organization
- Specific Domains along Microsoft Portfolio: Cloud Transformation, Cloud Native, Modern Work, AI, IoT, and Security

GOLD COMPETENCIES validated by Microsoft

- Application Development
- Application Integration
- Cloud Business Applications
- Cloud Customer Relationship Management
- Cloud Platform
- Cloud Productivity
- Collaboration and Content
- Communications
- Data Analytics
- Data Platform
- Datacenter
- DevOps
- Enterprise Mobility Management
- ERP
- Messaging
- Windows and Devices

KEY ACCELERATORS differentiated IP & Assets



THE OFFERINGS

Transforming your business at cloud scale

Application Portfolio
Modernization

Business Intelligence, AI and
Data Platform, Data Estate
Modernization

Cloud Native and API
Transformation

Risk & Cybersecurity, SIEM,
Compliance Monitoring, IDAM,
PCIDSS, and DLP

DevSecOps and Agility Solutions

Mainframe Modernization
with Azure

Modern Workplace &
Collaboration with Microsoft 365

OpenX –Banking and Insurance
Core Platform Transformation

Business Productivity –
Dynamics 365 & Power Platform

FinOps & Sustainability

Are you interested in a follow-up on the topic of hybrid cloud management, Azure Arc, or cloud in general? Is there anything we can support you with? For instance:

Would you like to share with us your actual situation or challenge?

Do you have questions or feedback on the topic above?

Do you need consulting needed regarding a target operation model for hybrid cloud?

Interested in running a PoC or requesting a demo?

AUTHORS



SYLVIA LIST

VP Cloud | Head of Cloud Center of Excellence | Executive Sponsor | Capgemini Deutschland

Sylvia.List@capgemini.com

Sylvia List has been working in the IT industry for over 25 years in various consulting and management positions. Most recently, she was a member of the Executive Board at NTT Germany, where she was responsible for Solutions & Innovation, until she took on the role of Vice President Cloud and Head of Cloud Center of Excellence at Capgemini.



DR. MARCO A. HARRENDORF

Account CTO & Microsoft Guild Migration Lead | Guild Executive Sponsor | Capgemini CIS

Marco.Harrendorf@capgemini.com

Dr. Marco A. Harrendorf has a strong focus on designing and implementing Cloud strategies and solutions for Automotive as Account CTO. Hence, he naturally has a lot of experience with migrations and knows the challenges of digital transformations. He regularly discusses and shares his expertise with the members in the Domain Migration of the Microsoft Cloud Guild.



TIMOTHEUS KUCKELKORN

Jr. Account CTO & Advisor | EA | Lead Author | Capgemini CIS

Timotheus.Kuckelkorn@capgemini.com

Tim Kuckelkorn works in a multi-directional way. To reach full synergy, he provides a connection between business, people, and technology. Besides his daily project work as an Enterprise Architect for AWS, Azure, and Google Cloud in client-facing projects, he fulfills several roles like the Sustainability Leader for CIS, which converges with his Industry Solutions domain for the Google Cloud Guild.



FABIAN LUDWIG FELTER

Senior Azure Architect | EA | Author | Capgemini CIS

Fabian-Ludwig.Felter@capgemini.com

Fabian Felter has been Azure Architect at Capgemini since 2021. His cloud experience started back in 2015 and with his growing experience. He helps Capgemini's Cloud Infrastructure Services Germany customers to make the desired adjustments for our customers in their solution, and discover more opportunities.



MICHAEL KRAH

Senior Cloud Architect | EA | Author | Capgemini CIS

Michael.Krah@capgemini.com

Michael Krah is an Enterprise Architect at Capgemini with a strong focus on private and mainly public cloud technologies. He helps enterprises in different phases of their cloud transformation journey by designing new solutions and architectures.



STEFAN KEIL

Solution Manager Multi and Hybrid Cloud | SM | Author | Capgemini CIS

Stefan.Keil@capgemini.com

Stefan Keil has a long track record in cloud technology. As a Solution Manager and Architect in Presales, he supports enterprises to transform their IT landscape into cloud and to establish state-of-the-art operations, alongside the IT and business demands.



NIELS OPHEY

Senior Cloud Solution Architect | Co-Author | Microsoft

Niels.Ophey@microsoft.com

Niels Ophey is working in the Microsoft Germany Partner organization for over 5 years as a Cloud Solution Architect covering all Azure Infrastructure topics. He supports Microsoft Partners developing Solutions for their customers as well as during delivery of customer projects.



FOR MORE INFORMATION

Stefan Baudy

Head of Presales | Cloud Infrastructure
Services Germany | Capgemini
stefan.baudy@capgemini.com

Bernd Wachter

CTO | Cloud Infrastructure
Services Germany | Capgemini
bernd.wachter@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Visit us at

www.capgemini.com

**GET THE FUTURE
YOU WANT**

Copyright © 2023 Capgemini. All rights reserved.
The information contained in this document is proprietary.