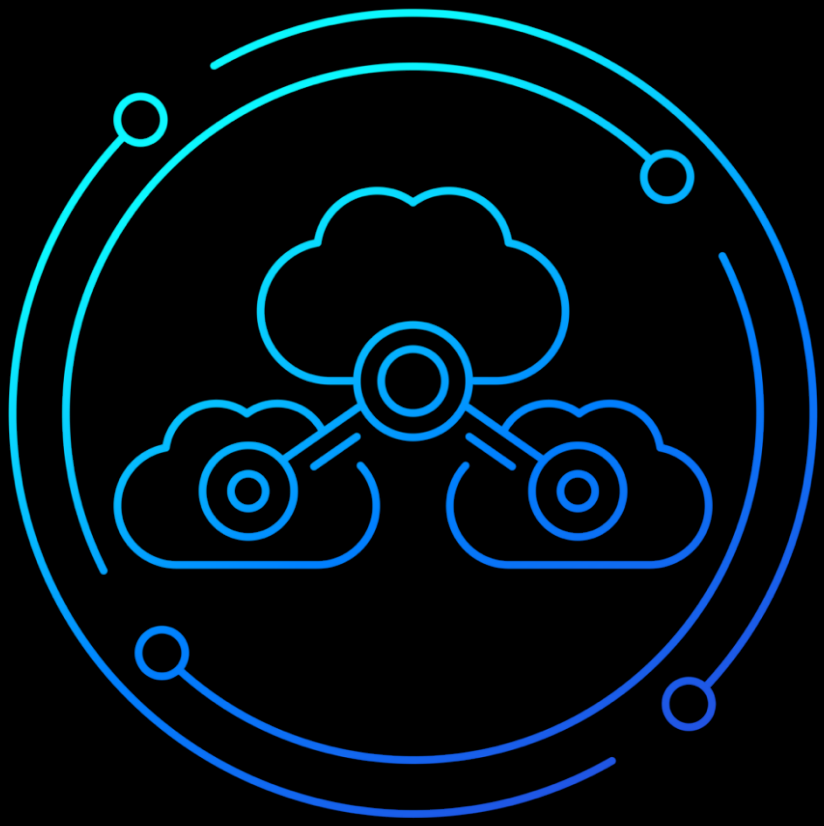
Microsoft Azure

White paper

Innovate anywhere with Azure:

Azure Arc–Enabled Data Services

Bring the flexibility of Azure data and management services to hybrid and multicloud workloads.



Contents

Introduction

Public-cloud adoption continues to be a powerful tool for IT organizations. A growing number of organizations choose to host resources in the public cloud to gain benefits such as simplified management, lower total cost of ownership (TCO), and unlimited scale. However, modern organizations also recognize that the public cloud is only one part of the optimization discussion, along with their on-premises, edge, and multicloud environments.

Although the public cloud is a powerful tool for many use cases, restrictions often prevent moving data and workloads there. For example, data-sovereignty rules, government regulations, and corporate policies often present obstacles to storing data in the public cloud. Beyond restrictions, "data gravity" naturally encourages teams to deploy applications close to where their data already resides. Internet of Things (IoT) applications also work against the overall trend toward the public cloud by creating a new center of data gravity at the intelligent edge, where latency or connectivity to the internet might be an issue.

The net result of these developments is that, even though IT organizations have benefited greatly from the level of automation, portability, consistency, and at-scale management that are available through public cloud services, the cloud still remains out of reach for many workloads. Further complicating matters, IT infrastructure is becoming less manageable than ever, dispersed not only among different locations in different clouds, datacenters, and the edge, but also diversified among different technologies, including physical infrastructure, virtual infrastructure, and—more recently—container-based infrastructure.

Organizations need the managed services and self-service administration workflows that are available through public clouds such as Microsoft Azure, and they need to be able to bring those services and workflows to any environment, including on-premises datacenters. Capabilities such as those provided with platform-as-a-service (PaaS) solutions outside of the cloud can:

- Unify management and governance of the infrastructure and data through a single control plane.
- Simplify the deployment, management, scaling, governance, and patching of databases and applications.
- Help protect workloads by easing the configuration of high availability (HA), disaster recovery (DR), and security features for these resources.

Microsoft has been a leader in recognizing and supporting businesses' needs for both hybrid infrastructure and hybrid data. Businesses might need to extend and migrate their applications while maximizing their existing investments, while also needing benefits like automation that the cloud can deliver. Or organizations might want to build new cloud-native applications as part of a larger digital transformation journey and thus require portability, real-time insights, and consistency. Azure makes these

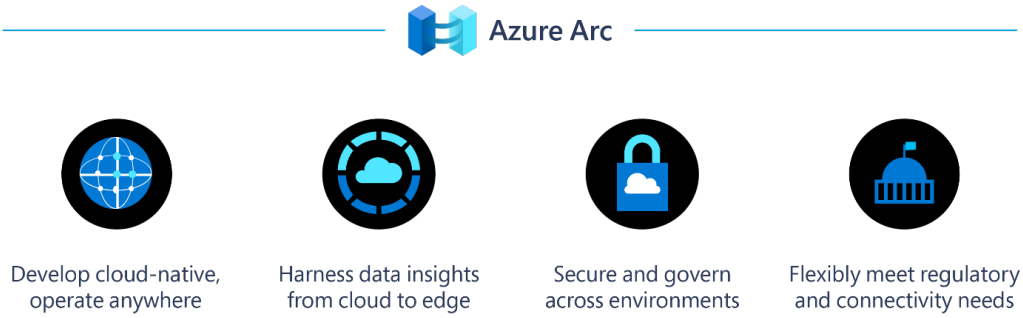
capabilities possible, and Microsoft now has a way to bring the capabilities of Azure to any customer infrastructure, whether it's on-premises, at the network edge, or in other cloud environments.

Azure Arc

Azure Arc helps bring many of the optimization benefits found in Azure to other compute services through a single control pane for workload management. That pane can run Azure management, application, and data services anywhere. These Azure Arc capabilities equip organizations like yours with the flexibility necessary to meet your regulatory and connectivity needs.

Think of Azure Arc as a bridge that extends the Azure platform to help you build applications and services that can be run across datacenters, at the edge, and in multicloud environments. With this bridge, your organization can develop cloud-native applications with a consistent development, operations, and security model. Azure Arc runs on both new and existing hardware, virtual machines (VMs), Kubernetes platforms, IoT devices, and integrated systems. Making use of your existing investments to modernize your organization with cloud-native solutions enables you to do more with less, and with no migration necessary.

Innovate anywhere with Azure



Develop cloud-native apps and operate anywhere

Azure Arc enables you to build and modernize cloud-native apps on any Kubernetes distribution. Cloud-native apps are collections of independent services packaged in self-contained, lightweight containers. Containerization enables these apps to perform consistently across different environments and to scale easily, all of which is key in driving app modernization. Your developers can also write to the same application-service APIs that can run consistently on-premises, across multiple clouds, and in edge environments using any Kubernetes distribution.

Azure Arc integrates Azure monitoring, security, and compliance into your organization's DevOps toolkit. This reduces errors and accelerates innovation with GitOps and with policy-driven deployment and configuration across all your environments. Your developers can get up and running immediately with your existing tools, including GitHub, Terraform, and Microsoft Visual Studio.

Harness insights from cloud to edge

Azure Arc can help your organization create applications faster with an end-to-end multicloud solution that uses local data collection, storage, and real-time analysis. It makes it possible for you to deploy Azure Arc–enabled SQL Managed Instance and Azure Arc–enabled PostgreSQL on any Kubernetes distribution and on any cloud. Moreover, with Azure Arc data services you can install the managed machine-learning (ML) add-on with one click and train models on any Kubernetes cluster with Azure Machine Learning.

Spanning cloud-to-edge reduces management overhead and risk exposure through integrated security and governance tools for data. And consistent data and artificial intelligence (AI) tools, services, and automations improve operational efficiency across your entire IT estate.

Secure and govern across environments

Azure Arc enables you to centrally manage a wide range of resources, including Windows Server on Azure, Linux on Azure, Microsoft SQL Server, Azure Kubernetes Service, and Azure Arc − enabled data services. You can govern your disparate environments through the Azure portal to simplify multicloud management, drive operational efficiencies, delegate access, and manage security policies for resources using role-based access control (RBAC) and Azure Lighthouse. Moreover, you can use Azure Arc to perform VM lifecycle management for your Azure Stack HCI and VMware environments from a centralized location. Finally, you can use the cloud-based threat-detection, response, and analytics features of Microsoft Defender for Cloud in all Azure Arc deployments.

Meet regulatory and connectivity needs dependably and flexibly

With Azure Arc, you can meet residency and sovereignty requirements by choosing from a variety of infrastructure options, including Azure Stack HCI. Using Azure Arc, you can bring the power of cloud-based services to sensitive data that must be retained on-premises or at edge locations, and you can do this with full, intermittent, or no internet connectivity. And because Azure Arc can run in edge scenarios, it provides simplified edge computing infrastructure for low-latency applications. Finally, with Azure Policy you can meet governance and compliance standards for apps, infrastructure, and data.

Azure Arc–enabled data services bring the hybrid capabilities of Azure Arc to your data estate. Within Azure Arc–enabled data services, Azure Arc–enabled SQL Server connects existing SQL Server runs on any physical servers or VMs to Azure so that you can modernize in place and get searchable inventory lists, enhanced security from Microsoft Defender, and can run SQL Server best-practice assessments. Azure Arc–enabled SQL Managed Instance runs on any Kubernetes deployment and has near 100% compatibility with the latest SQL Server database engine so you can lift

and shift your applications to Azure Arc–enabled data services with minimal application and database changes while maintaining data sovereignty. And Azure Arc–enabled PostgreSQL provides similar capabilities to Azure Arc–enabled SQL Managed Instance for an open-source database that can tap the power of Azure.

Business use cases for Azure Arc–enabled data services

Business use cases can help illustrate specific ways in which Azure Arc–enabled data services can help with managing infrastructure sprawl and modernizing locally bound applications and database instances.

Business use case 1: Database as a service (DBaaS) / Security and governance across on-premises and multicloud environments[1]

As Canada's largest bank—and one of the largest banks in the world—Royal Bank of Canada (RBC) sets a high standard of excellence. The bank owns and operates its own modern datacenter, and hybrid cloud gives RBC crucial control over data security and the choice of where to host the data based on compliance policies and security requirements. By offering DBaaS through Azure Arc–enabled SQL Managed Instance, RBC can provide data and application security by default. With the security and monitoring capabilities built into Azure Arc, RBC can manage, govern, and secure its apps across on-premises and multicloud environments right from the Azure portal.

"Azure Arc–enabled data services give us the ability to do a lot right out of the box—the policy enforcement, the visibility, and the health monitoring of resources. From a security standpoint, that's where we've seen the biggest value for us." — Khaled Zaky, Director of Product Management, RBC.[1]

With Azure Arc–enabled SQL Managed Instance, environments stay up to date. RBC gets the latest Azure features and capabilities, and automated updates are applied according to the bank's policies. Those capabilities reduce the operational overhead associated with managing on-premises databases at scale. In addition, by offloading the operational overhead to Azure, RBC anticipates saving millions of dollars each year in capital expenditures.

Business use case 2: Compute and real-time insights when data is created / Consistent portable databases on Kubernetes[2]

For more than a century, Swedish industrial giant SKF Group has been producing bearings, seals, and other solutions and services for global manufacturers. One of their key growth enablers was to digitalize the full value chain to enable SKF to make more intelligent decisions regarding its own operations. The solution starts at the edge, where SKF is bringing the power of the cloud to the factory. With Azure Arc, SKF can gather and analyze data on the factory floor and get a unified view

across its technology landscape, making management easier and less costly. Automation has been a game changer for SKF, as they're now able to make changes across their 100 sites—with the same amount of effort as making changes at a single site—all from the Azure portal. In addition to benefitting from the much-needed consistency that has resulted from standardizing its operations, SKF has also seen roughly 40 percent lower costs and a 30 percent reduction in machinery-related IT/OT downtime.

"With Azure hybrid cloud solutions, we can make changes at scale, while the factory keeps the application running, uninterrupted." — Sven Vollbehr, Head of Digital Manufacturing, SKF Group.[2]

Overview of Azure Arc–enabled data services

Azure Arc–enabled data services provide two types of functionalities: one to manage the existing apps on your servers and virtual machines (VMs), and one to modernize apps or build new apps with cloud-native technologies. These different types of functionalities provide two paths, or choices, for modernizing your apps. Regardless of the option you choose, Azure Arc–enabled data services provide you with centralized management that can streamline overall management and simplify DevOps and multilayer security.

Azure Arc–enabled SQL Server: manage, govern, and secure your existing SQL Server estate

You might have some legacy workloads, such as reporting or analysis, that are fully server-based and cannot be containerized. Or perhaps you run Microsoft Internet Security and Acceleration (ISA) Server applications that don't support other environments. Regardless of the underlying reason, you can keep your workloads where they are on SQL Server and modernize them in place by using Azure Arc–enabled SQL Server.

With Azure Arc–enabled SQL Server, you can start offloading the manageability and operational aspects of your on-premises data workloads and also secure your SQL Server workloads. To do so, you connect existing SQL Server running on any physical servers or VMs to Azure.

Modernizing your SQL Server workloads in place by connecting them with Azure enables you to bring modern management, governance, and security to all of your SQL Server workloads, regardless of where they run. With Azure Arc, you can manage your entire SQL Server estate using Azure and get a single view of all your SQL Server deployments in a central portal to better manage your inventory and licenses. Azure Arc–enabled SQL Server also provides the SQL Server Best Practice Analyzer to automatically evaluate characteristics of your SQL Server deployments such as security, performance, scalability, business continuity, and more, all at no additional cost.

For governing SQL Server deployments, Azure Arc–enabled SQL Server uses Microsoft Purview access policies for SQL Server through Azure Arc, so you can control and govern your entire data estate centrally and generate centralized insights. For security, Azure Arc–enabled SQL Server uses Microsoft Defender for Cloud to enhance security for SQL Server and single sign-on (SSO) with Microsoft Entra ID to secure identities. These are popular Azure security capabilities now brought on-premises.

Azure Arc–enabled SQL Server is ideal for maintaining server-based applications, reusing existing datacenter and SQL Server investments, and managing all SQL Server operations from one place.

Azure Arc–enabled SQL Managed Instance and Azure Arc–enabled PostgreSQL: cloud-native technology for app modernization

You might want to both make use of your existing infrastructure and bring a PaaS-like experience to workloads that can be containerized. In such cases, you can "lift and shift" your data workloads to Azure Arc–enabled SQL Managed Instance or Azure Arc–enabled PostgreSQL. This shift gives you consistency and manageability across on-premises and multicloud environments with a cloud-billing model.

Azure Arc–enabled SQL Managed Instance brings the best of Azure cloud data-management capabilities to any Kubernetes clusters, no matter where that infrastructure lives. It can extend to your on-premises environment, in other public clouds, and to the edge, delivering a much-needed consistent experience across your data workloads.

Azure Arc–enabled SQL Managed Instance is **always up to date** with full automation, so end of support can be a thing of the past and you can benefit from an evergreen SQL engine with the latest features using automated updates with close to zero downtime.

You also get industry-leading, multilayered protection with **built-in security** capabilities with Azure Arc–enabled SQL Managed Instance. This solution comes with comprehensive encryption including Transparent Data Encryption (TDE) and Always Encrypted, in addition to Azure RBAC and policy, so your data is protected both at the powerful database-engine-level and by Azure security capabilities from the cloud.

You can scale Azure Arc–enabled SQL Managed Instance up or down based on your application needs, with no downtime required. With **elastic scaling**, you can realize cost efficiencies by paying for only what you use, without the need to overprovision.

Azure Arc–enabled SQL Managed Instance also delivers a vastly **simplified DevOps experience** through increased automation with built-in HA/DR and rapid deployment. For example, you can setup a three-replica Azure Arc–enabled SQL Managed Instance deployment with full HA in quickly with a single command and gain a unified view into your query performance, storage capacity, and error logs using dashboards directly from the built-in monitoring.

Azure Arc–enabled PostgreSQL provides the same built-in management capabilities and on-premises cloud-billing model as Azure Arc–enabled SQL Managed Instance on any infrastructure via Kubernetes. It is a fully automated, single-server solution that provides scale-up, scale-down, scale-out, and scale-in capabilities.

Use Azure Arc–enabled SQL Managed Instance to access the latest cutting-edge technology in your SQL workloads outside of Azure, standardize your data management with agility and consistency, and reduce management costs with full automation. Table 1 provides an overview of Azure Arc–enabled data-services functionality options and use cases for the two paths.

Table 1. Current Azure Arc–enabled infrastructure and services

Azure Arc–enabled data-services functionality type	Manage existing applications	Cloud-native app modernization

Products	**Azure Arc–enabled SQL Server**
	• Connect existing SQL Server deployments running on any physical servers or VMs to Azure
	• Modernize in place and get:
	  ○ Searchable inventory lists
	  ○ Enhanced security from Microsoft Defender
	  ○ SQL Server assessment for free
		Azure Arc–enabled SQL Managed Instance
		• Is near 100-percent compatible with the latest SQL Server database engine
		  ○ Includes fully automated, evergreen SQL Server functionality
		  ○ Runs on any infrastructure via Kubernetes
		  ○ Enables you to lift and shift your SQL Server applications to Azure Arc–enabled data services with minimal application and database changes while maintaining data sovereignty
		• Includes built-in management capabilities that drastically reduce management overhead
		• Has a cloud-billing model for on-premises environments

When to use	Support existing apps	Modernize apps
Use cases	• Maintain server-based legacy applications • Reuse existing datacenter and SQL Server environments • Manage all SQL Server deployments from one place	• Gain access to the latest cutting-edge SQL Server technology • Standardize data management with agility and consistency • Reduce costs with full automation

Azure Arc–enabled SQL Server

Because Azure Arc–enabled SQL Server connects existing SQL Server deployments to Azure Arc management, you do not provision new SQL Server resources using Azure Arc–enabled SQL Server. Instead, you enroll SQL Server deployments running on bare-metal environments or VMs with Azure Arc. At a high level, the steps for doing this are as follows:

1. Onboard Azure Arc–enabled server.
2. Onboard Azure Arc–enabled SQL Server.
3. Enroll Microsoft Defender to further secure it.
4. Enroll a SQL Server Best-Practices Assessment.

Figure 1 shows how these steps fit within the broader architecture of Azure Arc–enabled SQL Server.

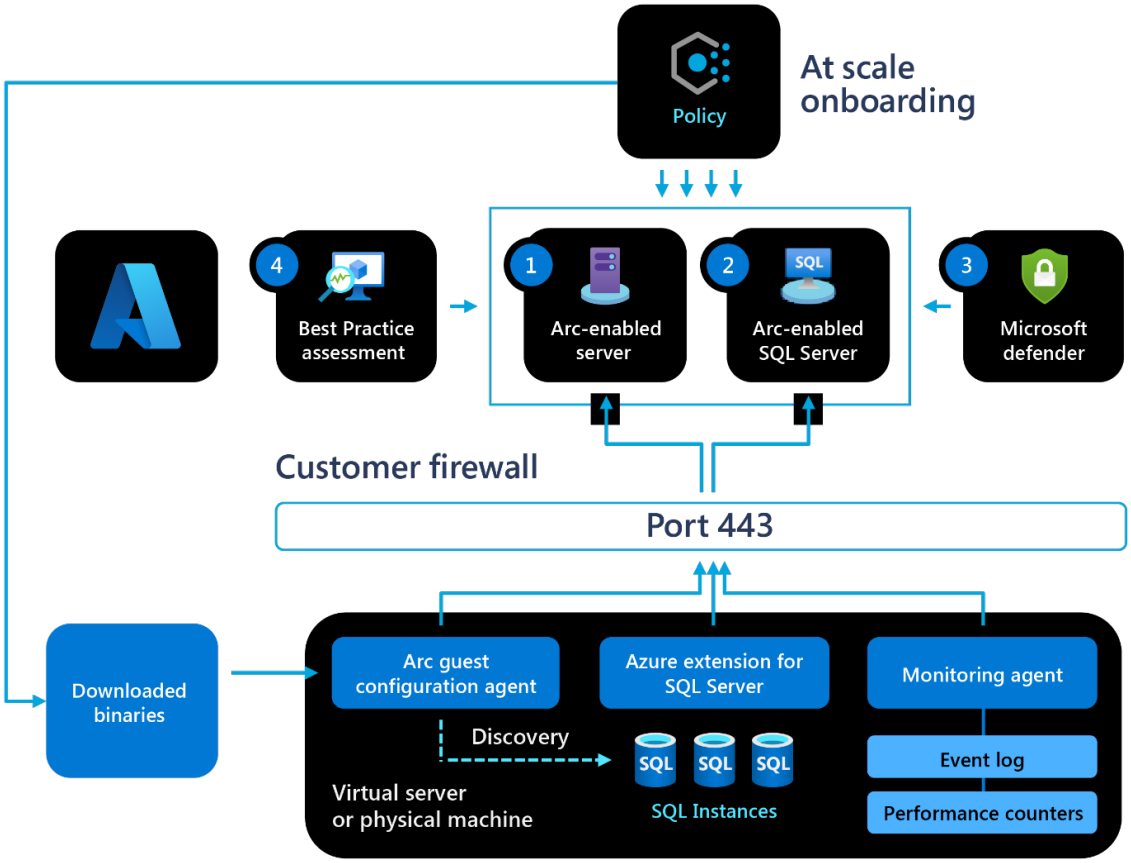


Figure 1. Azure Arc–enabled SQL Server architecture, including steps for enrollment

Working with Azure Arc–enabled SQL Server

This section provides a high-level overview of some of the features of Azure Arc–enabled SQL Server and the steps and tools used to complete common tasks in Azure Arc–enabled SQL Server. For more complete information, refer to the Azure Arc–enabled SQL Server documentation.

SQL Server pay-as-you-go licensing model

You can gain better cost efficiencies when paying only for what you use by activating the pay-as-you-go (PAYG) licensing option for your SQL Server deployments, wherever they might be. Depending on your situation, PAYG might offer a cost-effective option in these scenarios:

- You have a seasonal business with high demand for part of each year.
- You self-install SQL Server instances on any VMs on clouds outside of Azure and need a consistent behavior with SQL Server whether the VMs are deployed inside Azure or outside of Azure.
- You need a flexible licensing option and want an option other than perpetual licenses.

You can select or switch to PAYG billing through Azure to install a Standard or Enterprise edition of SQL Server
(the supported versions are SQL Server 2014 to SQL Server 2022) without providing a pre-purchased product key

Billing is calculated by the hour, and billing charges are calculated based on the SQL Server edition and the maximum size of the hosting server at any time during a given hour.

Inventory and asset management

By connecting all your servers and SQL Server deployments to Azure Arc, you can get a single, consistent view of all your SQL Server and other database deployments on-premises, at the edge, and across the multicloud. You can use the Azure Resource Graph service in Azure to query your database inventory in various dimensions in order to increase the visibility of your entire data estate. You can also receive Extended Security Updates (ESUs) for your Azure Arc–enabled SQL Server deployments. For more information about this feature, visit "What are Extended Security Updates for SQL Server?"

Viewing SQL Server databases - Azure Arc

Today, you might have to manage hundreds or even thousands of active databases. For each of these databases, it is essential to be able to create an accurate mapping of the active configurations. This could be for inventorying tasks or even for reporting

purposes. Centralizing this database inventory in Azure using Azure Arc allows you to create a unified view of all your databases in one place regardless of which infrastructure those databases might be located on—in Azure, in your datacenter, on edge sites, or even in other clouds.

To learn more about this public-preview feature and to begin surfacing all the active databases and their configurations for each of your Azure Arc–enabled SQL Servers deployments. in Azure, see "View SQL Server databases - Azure Arc."

Securing and protecting SQL Server environments with Azure

Connecting SQL Server to Azure Arc offers centralized security and data governance for all your data assets across datacenters and multicloud environments, all managed by services native to Azure, including built-in integration with Microsoft Entra ID, Microsoft Defender, Microsoft Sentinel, and Microsoft Purview.

Unified Microsoft Entra ID authentication

If you have SQL Server 2022, you can enable Microsoft Entra ID authentication, single sign-on (SSO), and unified SQL Server authentication and make use of multifactor authentication. Learn more by reading "Azure Active Directory [Microsoft Entra ID] authentication for SQL Server."

Microsoft Defender for SQL

You can better secure your Azure Arc–enabled SQL Server deployments by enabling Microsoft Defender for SQL, which includes functionality for surfacing and mitigating potential database vulnerabilities; you can also use it to detect anomalous activities that could indicate a threat to your database. Microsoft Defender for SQL provides a single go-to location for enabling and managing these security capabilities:

- SQL Advanced Threat Protection detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit your database. It continuously monitors your database for suspicious activities, and it provides immediate security alerts on potential vulnerabilities, Azure SQL injection attacks, and anomalous database access patterns. Advanced Threat Protection alerts provide details of suspicious activities and recommend actions on how to investigate and mitigate the threats.
- SQL vulnerability assessment is an easy-to-configure service that can discover, track, and help you remediate potential database vulnerabilities.

To learn more, visit "Protect Azure Arc–enabled SQL Server with Microsoft Defender for Cloud."

Microsoft Purview access policies

With new Microsoft Purview access policies for SQL Server 2022 powered by Azure

Arc–enabled SQL Server, you can gain visibility into your data assets across on-premises data centers and multicloud deployments. You can secure access to your data and safeguard sensitive data across applications deployed in multiple clouds.

This feature provides your data administrators and owners with the capability to author policies that govern access for Active Directory users directly from Azure for all of your SQL Server 2022 data sources at scale without writing T-SQL code and while also explicitly creating logins and database users. To learn more, visit "Microsoft Purview access policies for SQL Server 2022."

SQL Server Best Practice Assessments

The best practice assessment (BPA) for SQL Server feature in Azure Arc-enabled SQL Server enables you to proactively diagnose potential issues with your SQL Server environment running on-premises and in multi-cloud environments.

BPA for SQL Server performs a comprehensive evaluation of your operating system, SQL Server instances, and databases. It proactively identifies any risks that SQL Server deployments might run into, such as those involving SQL Server and database configurations, security, performance, index strategy, trace flags, disaster recovery, high availability, and many more.

Once the assessment is enabled and executed, BPA will provide a comprehensive report with a prioritized list of the risks detected, the impacted objects, and step-by-step guidance on how to mitigate the risks reported. To learn more, visit "Configure SQL best practices assessment."

Onboarding Azure Arc–enabled SQL Server

This section examines the different ways by which you can Azure Arc–enable SQL Server deployments.

SQL Server 2022 setup

The SQL Server 2022 installation wizard enables you to simplify onboarding to Azure Arc and introduces the Azure SQL extension configuration, which you can connect to Azure to start managing, securing, protecting, and governing your SQL Server 2022 deployment from Azure. To learn more, visit "Install SQL Server 2022."

When the SQL Server host server is already connected to Azure Arc

If the host server running SQL Server is already Azure Arc–enabled, you can also connect the SQL Server instances running on that server to Azure Arc by installing the SQL Server extension for Azure Arc. You can find the SQL Server extension for Azure Arc in the extension manager. To learn more, visit "Connect your SQL Server to Azure Arc."

When the host server is not connected to Azure Arc

If the server that runs your SQL Server instance is not yet connected to Azure Arc, you can initiate the connection from the target machine by using the onboarding script. This script will connect the server to Azure Arc and will install the Azure Arc extension for SQL Server. To learn more, see the "Generate an onboarding script for SQL Server" section of "Connect your SQL Server to Azure Arc."

Azure Arc–enable SQL Server deployments at scale

If the server that runs your SQL Server instance is not yet connected to Azure Arc, you can initiate the connection from the target machine using the onboarding script. This script will connect the server to Azure Arc and will install the Azure Arc extension for SQL Server. To learn more, see the "Generate an onboarding script for SQL Server" section of "Connect your SQL Server to Azure Arc."

Azure Arc–enabled SQL Managed Instance

Azure Arc–enabled SQL Managed Instance is built on a Kubernetes foundation. You can run Azure Arc–enabled SQL Managed Instance on-premises, at the edge, and in public clouds by using Kubernetes and the infrastructure of your choice. Both Azure Arc–enabled SQL Managed Instance and Azure Arc–enabled PostgreSQL run as containerized applications when they're deployed in this environment. Because Kubernetes provides a level of abstraction over the underlying hardware and virtualization engine, Azure Arc–enabled SQL Managed Instance and Azure Arc–enabled PostgreSQL are both hardware-agnostic and hypervisor-agnostic. You can use your existing hardware or purchase OEM hardware that has been certified and optimized to run Kubernetes clusters.

To set up and provision either Azure Arc–enabled SQL Managed Instance or Azure Arc–enabled PostgreSQL, use the following steps:

1. Deploy Kubernetes on the infrastructure of your choice.
2. Deploy the Azure Arc data controller.
3. Deploy Azure Arc–enabled SQL Managed Instance or Azure Arc–enabled PostgreSQL using the Azure portal or command-line interface (CLI).
4. In direct-connect mode, use Azure Arc agents; in indirect-connect mode, use CLI tools such as azdata or kubectl.
5. Connect Azure Arc–enabled SQL Managed Instance or Azure Arc–enabled PostgreSQL using an application or tool.

Figure 7 shows how these steps fit within the architecture of Azure Arc–enabled SQL Managed Instance and Azure Arc–enabled PostgreSQL.

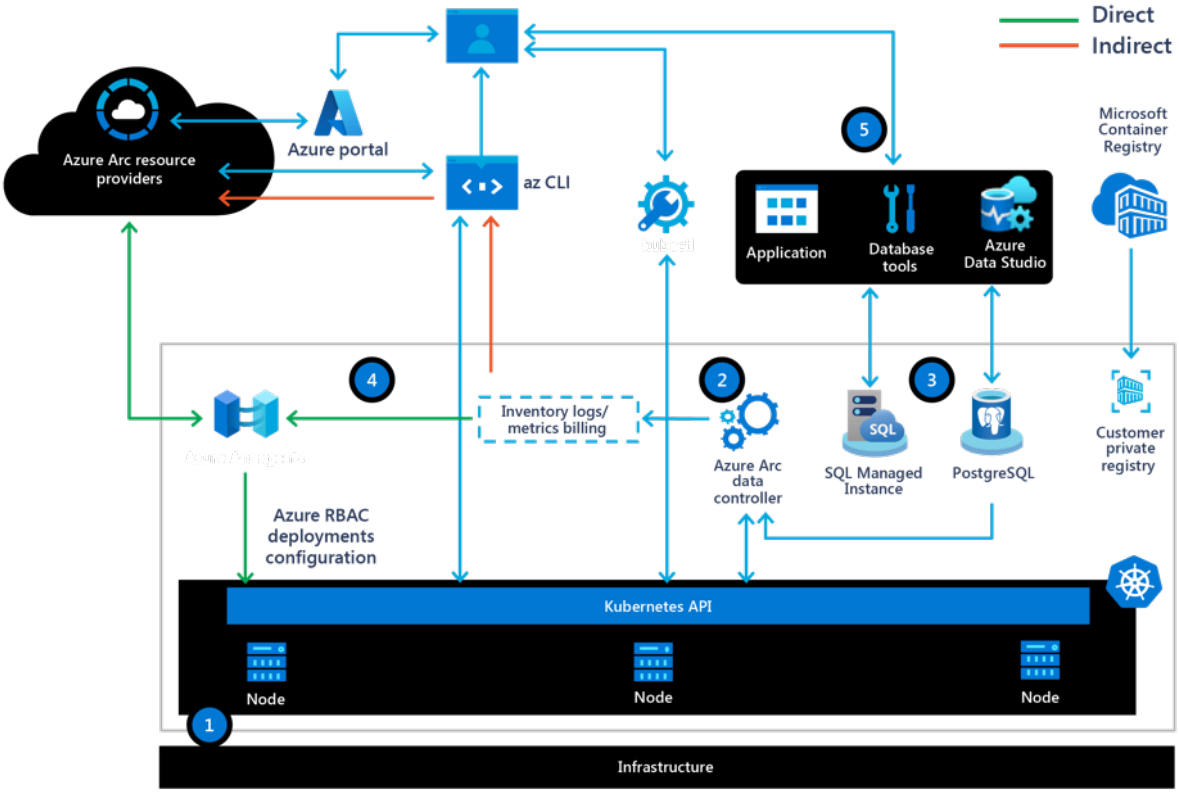


Figure 7. Azure Arc–enabled SQL Managed Instance architecture, including steps for setup and provisioning

Azure Arc data controller

The local control software for Azure Arc–enabled data services is installed as a set of containers called the Azure Arc data controller; these containers are automatically pulled down from the Azure Container Registry during installation. The Azure Arc data controller is the innovation that makes it possible for managed data services from Azure to run outside of Azure infrastructure. It delivers the same Azure Arc–enabled SQL Managed Instance or Azure Arc–enabled PostgreSQL engine in whatever location the data controller has been installed, and it provides management functionality such as monitoring, logging, patching/updating, scaling, and backup features. The Azure Arc data controller also acts as a local channel to communicate with the public Azure cloud to configure identity, role-based access control (RBAC), and Azure Policy while also sending telemetry and backup-retention information. Additionally, it gives administrators the ability to deploy resources on customer premises from within Azure when the data controller has been deployed in directly connected mode.

Azure Arc tooling

Azure Arc provides different installation options depending on customer preference and connectivity to the Internet. The Azure portal and Azure Data Studio provide familiar experiences for customers who already use these tools; for customers who

prefer scripting, Azure Arc also provides CLI options:

- Azure portal: Web-based, unified console that you can use to manage your Azure subscription using a graphical user interface (GUI). You can use this console to deploy data services to an Azure Arc–enabled Kubernetes cluster and then manage those services.
- Azure Data Studio: Cross-platform database tool for data professionals using on-premises and cloud platforms on Windows, macOS, and Linux.
- azdata: CLI tool for installing the Azure Arc data controller, in addition to deploying and managing data services in both Azure and Azure Arc.
- Kubectl: CLI tool for monitoring the underlying Kubernetes cluster.

Working with Azure Arc–enabled SQL Managed Instance

This section provides a high-level overview of some of the steps and tools used to complete common tasks in Azure Arc–enabled SQL Managed Instance. For more complete information, refer to the Azure Arc–enabled data services documentation.

Installing the Azure Arc data controller

There are four options for installing the Azure Arc data controller:

- Create a data controller with the Azure Data CLI (azdata).
- Create a data controller with Azure Data Studio.
- Create a data controller from the Azure portal via a Jupyter notebook in Azure Data Studio.
- Deploy the data controller using a Kubernetes tool such as kubectl or oc (OpenShift).

For full instructions on creating the data controller, see the respective documentation for each installation method:

- Create Azure Arc data controller using the CLI
- Create data controller in Azure Data Studio
- Create Azure Arc data controller from Azure portal – Indirect connectivity mode
- Create Azure Arc–enabled data controller using Kubernetes tools

Note
If you want to have an accelerated experience for a test deployment, you can make use of the Azure Arc Jumpstart project, which is designed to provide a "zero-to-hero" experience so that you can start working with Azure Arc right away. For more information, see "Azure Arc Jumpstart."

Deploying and managing database instances

Once the Azure Arc data controller is installed in an environment, it can provide the following services within that environment:

- Provisioning
- Scaling
- Updating and patching
- Local monitoring and logging
- Backup and restore functionality
- HA and DR
- Azure Monitor (available only when connected to Azure)

Provisioning

Typically, deploying a database instance on a VM on-premises is a lengthy process that can take hours. With Azure Arc, however, provisioning a new database in your own datacenter takes only seconds. Creating database instances in Azure Arc is actually similar to creating other data services in Azure.

There are multiple methods for provisioning a new Azure Arc–enabled data service:

- Connect to the Azure Arc data controller and provision databases.
- Provision databases from Azure Data Studio.
- Use Kubernetes tools.
- Provision databases directly from the Azure portal.

You can find Azure Arc–enabled data services to deploy from the Azure portal (such as Azure SQL Managed Instance–Azure Arc) in the Azure Marketplace. On the search results page, simply select the service you'd like to deploy, click **Create**, and then, in the page that opens, fill in the details as necessary. One new field you will see is the **Arc location** field, shown in Figure 8. Use this field to specify a location where an Azure Arc data controller has been installed and registered in Azure. This location can be in your own datacenter or in another public cloud. After you finish specifying the necessary details and creating the Azure Arc–enabled data service, the new resource will appear in the Azure portal.

Scaling

You can use either a CLI or the Azure portal for vertical and horizontal scaling of Azure Arc–enabled PostgreSQL while an application remains online, whether it's running on your own premises or in another cloud. You can use a slider in the Azure portal to adjust the number of the worker nodes assigned to the database instance. When the number of nodes is increased, rebalancing the data occurs automatically across the nodes. During this change of configuration, the data remains fully available, and the application remains online. Another slider lets you dynamically set the number virtual cores and storage assigned to each worker node.

Note
Resource requests will be validated against the resources available in the Kubernetes cluster. If there are insufficient resources available, a warning will be shown indicating the insufficient resource.

Updating and patching

Azure Arc–enabled data services include automated updating and patching for your database instances. In the Azure portal, browse to your managed database instance, and then click **Updates** in the menu on the left, beneath **Settings**. In the **Updates** section on the right, you can enable automatic updates with a simple toggle.

Local monitoring and logging

Azure Arc–enabled database instances include built-in Grafana services, an open-source analytics and monitoring solution, and built-in Kibana services, an open-source logging tool. Both of these services are available over TCP port 30777 on each database instance. Therefore, to access these monitoring and logging capabilities, you first need to create an inbound rule to allow traffic over port 30777 for the network security group (NSG) that contains the database instance, just as if the database instance were hosted in Azure. After you create this inbound rule, you can access Grafana and Kibana services through the web addresses https://[database_instance_public_ip]:30777/grafana and https://[database_instance_public_ip]:30777/kibana, respectively.

Backup and restore functionality

Azure Arc–enabled data services provide automated backups. You can restore SQL Managed Instance to a previous point in time by using the Azure portal, Windows PowerShell, or the Azure CLI. Azure Arc–enabled PostgreSQL clusters automatically create backups of each node and store them in locally redundant storage. You can restore a cluster to a previous point in time by using the **psql** command.

In addition to providing automated backups, Azure Backup can be easily connected to provide long-term, off-site backup retention and DR.

HA and DR

For Azure Arc–enabled SQL Managed Instance highly available, multiple instances are automatically deployed and wired into an Always On availability group. A Kubernetes operator can monitor the availability of the instances and perform failover functions if needed, including updating the Kubernetes service that routes the read-only and read/write traffic to the correct instance, depending on which instance is the primary one versus the secondary one. For Azure Arc enabled for PostgreSQL, there's a solution in the early stages of design and development.

Azure Monitor

You can use Azure Monitor on-premises for comprehensive operational insights across your entire data estate. Azure Monitor can even be used in a semi-connected scenario in which telemetry data is exported and uploaded to Azure. For near-continuous monitoring, an admin can choose to automate the exporting and uploading of telemetry data as a batch job on a set schedule. For example, Figure 13 shows average CPU usage from telemetry data. The dotted portions of the line in the graph reflect periods of being disconnected from Azure.

Advanced security features

The Azure portal includes an advanced data security option, which enables the following services in Azure Arc–enabled SQL Managed Instance:

- Data discovery and classification
- Vulnerability assessment
- Advanced Threat Protection

The vulnerability assessment helps your organization meet compliance and privacy requirements by monitoring a dynamic database environment 24/7/365. The periodic recurring scans option enables the system to be scanned periodically for security threats.

Advanced Threat Protection helps identify and track any malicious activity, which helps protect your data before any damage occurs. You can also set up email alerts on both the vulnerability-assessment and recurring scan features to receive threat alerts in a timely fashion.

With these advanced security settings, your databases running on-premises or in another public cloud can now get the same level of security protection as those running in Azure. Even better, you have the choice to set up these settings per instance, or to use Azure Policy to automatically enable these features at scale, applying them to many resources by default.

Security and governance capabilities

With Azure Arc, the industry-leading security and governance capabilities of Azure—provided by Microsoft Defender for Cloud, Azure Policy, and RBAC—are now made available to servers, Kubernetes clusters, and data workloads on premises.[1]

For more information about Microsoft Defender for Cloud, visit "What is Microsoft Defender for Cloud?"

For more information about Azure Policy, visit "What is Azure Policy?"

For more information about RBAC in Azure, visit "What is Azure role-based access control (Azure RBAC)?"

Disconnected operations for data services

Azure Arc delivers many management benefits through its connectivity to Azure, but it also supports continuous operation during planned or unplanned periods without connectivity. When disconnected from Azure, the Azure Arc data controller can deliver the management capabilities mentioned above, but in a more limited way. When offline, Azure Arc still supports the same elastic scalability, database task automation, and patching-and-updating features locally as it would if the datacenter were connected to Azure.

Azure Arc is even able to support the management needs for data services in scenarios involving permanently disconnected deployments, as is common in industries such as finance, healthcare, and utilities. These systems never connect directly to Azure for security reasons, but they can still benefit from offline features such as fast provisioning and elastic scaling, in addition to features that require indirect connectivity to Azure, such as patching and updating that maintains an evergreen version of the SQL engine.

Some actions that are otherwise automatic, such as downloading updates or uploading data, become semi-automated in a disconnected environment. However, the bulk of data services remain available in a disconnected system.

What's different in a disconnected system?

- Unified management of servers and clusters across hybrid and multicloud infrastructures is not available. Only local resources can be managed.
- System updates are semi-automated rather than fully automatic. Manual steps are required, but even these manual steps can be automated with some scripting.
- Planned Azure add-on services, such as Advanced Threat Protection, might not be available when disconnected, and some services provided with Azure will require manual uploading and downloading of data.
- Functionality that requires data transfers will rely on manually exporting and uploading that data when the system is disconnected.
- Changes to RBAC are not enforced when the Azure Arc data controller is offline, but RBAC will work for a period of time with a cached configuration.

The best option for hybrid and multicloud data management

IT leaders like you are charged with managing your sprawling infrastructure while also modernizing your locally bound applications and database instances through more efficient workflows. Azure Arc helps you achieve these goals by providing a single control plane to manage resources wherever they reside and by enabling Azure data services to run outside of Azure.

Azure Arc–enabled data services deliver a cloud-inspired data platform that uses proven, at-scale management workflows from Azure to help you manage your own datacenter efficiently. At the same time, Azure Arc–enabled data services also modernize your data estate through an infrastructure based on containers and Kubernetes or on-premises deployments. This management model provides many benefits, such as database instance deployment in seconds (as opposed to minutes through a VM), simple and elastic scaling, automated updates by using containers, an evergreen database engine, unified management and governance through Azure, and built-in HA thanks to failover features in Kubernetes. What's more, Azure Arc–enabled data services provide a local control plane to support the operation and management of these data services in permanently disconnected scenarios.

Azure Arc will continue to expand its feature set and capabilities as it approaches its release.

Learn more and get started with Azure Arc

- **Visit Azure Arc**
- **Review Azure Arc documentation**

1 Microsoft. October 2021. "Royal Bank of Canada speeds innovation on-premises with DBaaS based on Azure Arc-enabled data services." https://aka.ms/customerstory/RBC
2 Microsoft. August 2021. "Longtime innovator SKF unveils the factory of the future on Azure hybrid cloud." https://aka.ms/customerstory/SKF