devoteam

Azure Arc enabled server offering

Project engagement.

Creative tech for Better Change

December 2021

devoteam

Table of Contents

1. Why use Azure Arc?

In the past few years, the adoption of the cloud and modern technologies like Kubernetes to modernize applications, increase redundancy, virtualize workloads, … led to the increase of consoles to manage and tools to monitor the infrastructure resulting in overall increase of the administration charge on IT (Information Technology) teams.

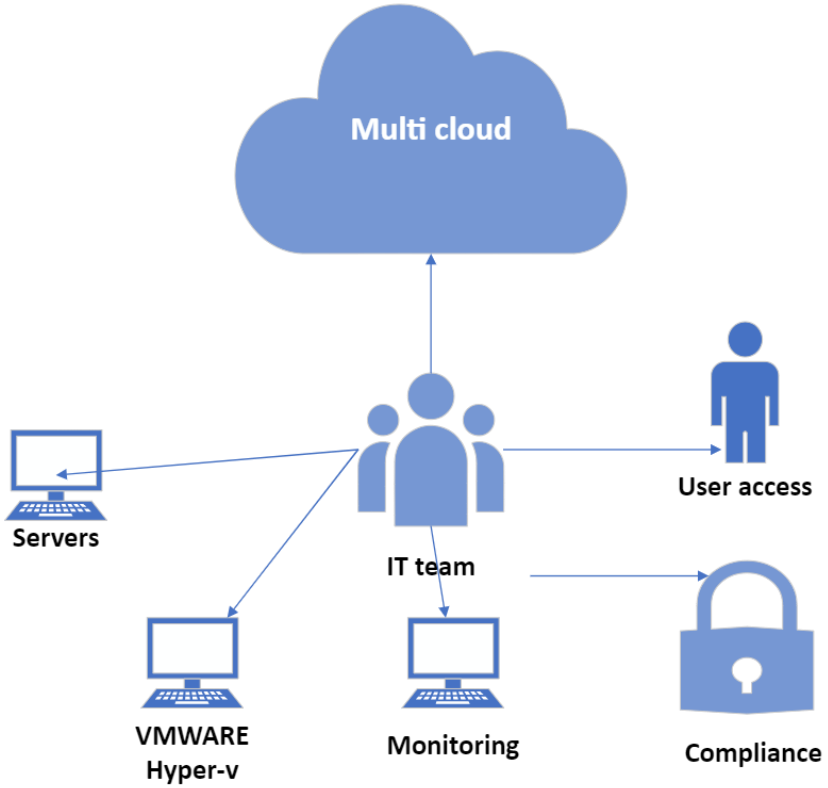

Figure 1 - IT team management responsibilities

Due to the many technologies and tools to maintain, finding or training competent IT personnel is expensive, time consuming and the attack surface becomes wider.

Azure Arc is the solution to these problems. By giving a unified console for on-premises or multi cloud servers and VM (virtual machines) and bringing Azure services to them such as Azure Monitor, you can remove the many different redundant tools from your infrastructure and manage everything in a single console.

2. Azure Arc services available

Azure Arc is available in 6 different services:

1. **Azure Arc enabled Servers**

   Focus on onboarding servers on Azure and bringing Azure Policy, Monitoring and Automation to your out of Azure servers.

2. **Azure Arc enabled Kubernetes**

   Onboard your Kubernetes clusters in Azure and allows you to easily manage and deploy apps with GitOps.

3. **Azure Arc enabled Services**

   Brings Azure PaaS (Platform as a Service) services to your own infrastructure. By using it, you can run Azure services on Kubernetes clusters that you can manage while still getting the Azure PaaS benefits from the Azure portal. Currently, these services contain: SQL managed instances, PostgreSQL hyperscale, App service, Logic apps, Event Hub, Functions and API Management.

4. **Azure Arc enabled Machine Learning**

   This service allows you to run Azure Machine Learning on your own infrastructure.

5. **Azure Arc enabled SQL Server**

   This second to last service onboard your existing SQL server instances into Azure and can provide you service assessments directly accessible from the Azure portal.

6. **Azure Arc for Azure Stack HCI**

   The ending service is the integration of Azure Stack HCI into the Azure Arc sphere. This service allows you to onboard your Azure stack HCI into Azure Arc as you register them on Azure and to manage them like any other Arc resource.

In this document, we will be presenting you how you can implement Azure Arc enabled Servers with Devoteam.

3. Azure Arc enabled Servers features

3.1 Microsoft connected agent

The agent allows you to onboard your machines on Azure Arc. By installing it, you can connect your server to Azure and start to apply Azure features on your server.

This agent has several installation methods to fit your current situation:

- Single server onboarding

By going in the “Azure Arc – Servers” blade in Azure, you can fill up information about your server and generate a script to run on your machine to onboard it to Azure. This installation method is fitting for small infrastructures of less than 10 servers and is not recommended for more.

It is also possible to use a DSC module (to first install) to onboard your servers or use the Windows Admin Center.

- Multiple servers onboarding

  Just like the single server onboard, you will generate a script in Azure. However, this script will use a service principal that you will have to create to onboard the server automatically.

  This script can then be deployed on your servers through several methods:

  - On Linux
    Ansible, Chef and other IaC (Infrastructure as Code) tools can be used to push the scripts on your servers.
  - On Windows
    The most fitting option depends on your current infrastructure.
    If you use SCCM/MECM, you can create a new application to push the script on your servers and update it by delegating the update to WSUS (Windows Server Update Services).
    If your server is not using MECM, you can also use GPOs to push the script in a comparable manner to onboard your servers.
    Also, if both use case do not fit your situation, IaC tools still work if compatible with Windows.
- Azure Update Management

  If your servers are already onboarded on Azure Update Management, you can simply add your servers on Azure by selecting them in the portal.

- Azure Migration

  This option is only available for vSphere servers through an assessment tool

Once you have chosen your best onboarding method, all you must do is to open in outbound communications to the Azure Arc URLs and you are ready to benefit from Azure features on your multi cloud or on-premises infrastructure.

Commented [GNB1]: URLs Overview of the Azure Connected Machine agent - Azure Arc | Microsoft Docs

3.2 Azure policies

Once your servers are onboarded, the first thing you can do is apply Azure policies to them.

Because your onboarded servers appear like normal Azure resources on the portal, you can apply to them the usual resources policy (tag requirements, log analytics, …) but also some arc enabled policies such as mandatory install of the Azure Dependency agent extension.

These policies are not limited to the usual Azure resource policies but can also be extended to Microsoft Defender for Cloud security policies to enforce legal compliance on your infrastructure.

Finally, Guest Configurations are also supported. Those are specific Azure policies that are automatically assigned to machines with the possibility to assign them manually. Once they are assigned, instead of verifying if the machine is compliant (it should be x), they will enforce a specific configuration to the machine (it must be x).

Onboarded Azure Arc Server can automatically make use of this feature to install agents and your own custom configurations.

3.3 Azure Monitor

Just like we mentioned before, it is possible to add monitoring extensions to your Azure Arc server with little administration load and start monitoring your servers. The monitoring dashboard can then be viewed inside the Azure portal as well, and you can create alerts for those too.

This means that if you already have some presence on Azure, you can easily reproduce your alerts on your Azure Arc servers.

If you do not have any Azure infrastructure, you still benefit of the advantages of Azure Monitor through the unified monitoring console for your multi cloud and on-premises server. You also can create alerts for these machines.

Log analytics and the dependency graph are available too. You can then query logs, create dashboards, … inside Azure to further increase visibility across all your environments.

3.4 Networking

Another interesting feature of Azure arc is the ability to use private links for your arc enabled servers.

Private links are resources that binds to a virtual network and define a resource that can be contacted using a private IP. This means that machines without a public IP or access to the internet can use the Azure network to communicate with Azure services.

This feature can be extended to your Azure Arc machine by allowing them to only contact Azure services or onboard through a VPN/ER connection to an Azure virtual network. The benefit is that you have full control of what specific resources your Arc servers can contact and allow them to do it securely without using the Internet and public IPs.

3.5 Microsoft Defender for Cloud and Microsoft Sentinel

The Microsoft Defender solution on Azure allows you to assure compliance, security, and visibility on the risks your cloud infrastructure is subject to.

With Azure Arc, these capabilities are extended to your on premise and multi cloud servers.

Each Azure Arc server with the log analytics extension is immediately onboarded for recommendations on Microsoft Defender for Cloud and can be assessed for the secure score. You can also activate Microsoft Defender Cloud for servers on your Arc resources just like you would for any Azure VM (virtual machines).

On Microsoft Sentinel side, you have access to the full power of workbooks, threat management, notebooks, … across your whole physical, virtualized and cloud infrastructure.

3.6 Azure Update Management

Similarly, to non-onboarded servers, it is possible to implement for free Azure update management on Azure Arc servers. The main difference is that just like for Azure VM (virtual machines), you can easily onboard those machines through the portal or define a strategy to automatically onboard future servers to automatically add your Arc machines.

3.7 Azure Inventory and change tracking

The last two features of Azure Automation are inventory and change tracking.

Change tracking allows you to monitor change to specific paths in the file system or Windows registry to detect potential unauthorized access or malicious changes. It also includes differential comparison for text files to be able to verify inside the Azure portal how the latest version differs from the previous ones.

Inventory allows you to inventory your server applications/packages, registry keys or even services/daemons.

Nonetheless, note that there is a limit to the amount of tracked files, packages, … These limits can be found in the following documentation.

Combined, these two tools allow you to have a near real-time view of what is happening on your servers' files. This can also be combined with Microsoft Defender for cloud's file integrity to increase your insights on file and registry changes.

Finally, these features can be combined with Azure Monitor alerts using queries to customize your monitoring experience and security baseline. On top of that, once the Log Analytics agent extension is installed on your Azure Arc servers, all these features can easily be enabled through the portal without more configurations on your side.

3.8 Azure Auto-manage

Finally, the last features that Azure Arc for servers provide is Azure auto-manage.

As you have seen above, there are many tools that can be installed or configurated on Azure Arc enabled Servers. To reduce further the workload on IT teams, it is possible to configure Azure Automanage to automatically assign to your newly onboarded servers on log analytics, change tracking, update management, …

You have several options to do so:

- Azure best practice profile for production or dev/test servers. This will configure all or most of the features that we described above
- Custom profiles. A wizard will propose you the features that you can configure, and you will choose which you want to use and save the configuration into a profile.

3.9 Limitations

Before starting with explaining the advantages that Azure Arc enabled Servers can provide you, it is important to know the limitations of the service to best determine how your current infrastructure stand compared to the requirements.

First, we have specific OS requirements. To onboard your servers into Azure Arc, you need to install an agent with the following supported OSes.

- Windows Server 2008 R2+ to Windows Server 2022 (x64) (edition core included)
- Ubuntu 16.04, 18.04 and 20.04 (x64)
- Centos 7 and 8 (x64)
- SUSE Linux Enterprise Server 12 and 15 (x64)
- RHEL 7 and 8 (x64)
- Amazon Linux 2 (x64)
- Oracle Linux 7

Commented [GN2]: Source Overview of the Azure Connected Machine agent - Azure Arc | Microsoft Docs

Note that other OSes may be able to onboard on Azure Arc. However, if doing so, Microsoft will not be able to provide support as these are not officially supported.

Secondly, ARM (aarch32 and aarch64) is not supported. If your servers run on a processor using this architecture, it will not be able to install the agent and as such onboard on Arc.

Finally, you can only onboard a maximum of 5000 machines in a single resource group. If you plan to add more machines than this, it will be necessary to use several resource groups.

Commented [GN3]: Source Azure Arc-enabled servers Overview - Azure Arc | Microsoft Docs

4. How Devoteam can help to implement Azure Arc enabled Servers in your infrastructure

4.1 What can we deliver to you?

Commented [GNB4]: Lighthouse no longer considered

Devoteam can offer you an end-to-end implementation of Azure Arc enabled servers from the onboarding to the implementation of the various Azure services like Microsoft Defender for Cloud. The process to determine how we will handle your infrastructure works as follows:

1. We will assess your current infrastructure and cloud readiness (if not already done through our Cloud Assessment offering).
2. Once we have a clear understanding of your current standing, we will discuss more in detail what are the objectives, acceptance criteria, responsibilities, etc.

3. After clearing all our and your questions, we will prepare a pilot of our migration plan following Microsoft best practices. This pilot should take at the very least 1 month unless your plan is to onboard very few servers and contains:
    a. The creation of the resource groups and tagging strategy
    b. The designing and deployment of a basic Azure Monitor and Azure Policy plan
    c. Configuration of the role-based access control (RBAC)
    d. The conversion of Log Analytics agent to extension-managed agent
    e. Onboarding of your servers at scale
    f. Creation of service health and Azure Advisor alerts
    g. Assigning of policies
    h. Implementation of Update Management
    i. Training of your IT personnel and creation of a rollback plan
4. Once the pilot plan convinces you, progressive onboarding of your servers in batches to assure an easy rollback and as little downtime as possible if any issue arises.

Commented [GNB5]: Microsoft deployment guide How to plan and deploy Azure Arc-enabled servers - Azure Arc | Microsoft Docs

4.2 Expected cost

Devoteam can offer a basic service that can be extended depending on your needs. This basic offer contains:

- The onboarding of your servers to Azure Arc. (Limited to 200 compatible servers)
- The implementation of basic Azure monitor alerts and service health for your Arc enabled servers
- The implementation of basic Azure Policy initiatives for your Arc enabled servers
- Azure RBAC configuration
- Enabling Azure update management for your Arc enabled servers

For this basic service, the resulting cost is € 5.000, with an add-on for additional servers.

To extend this offer, we can also provide you **additional** services:

- In-depth Azure monitor design and implementation;
- In-depth Azure Policy implementation;
- In-depth planification, design and implementation of Microsoft Defender Cloud for servers;
- Enabling and designing a strategy for Azure Inventory and change tracking;
- Configuring Azure Hybrid private links;
- Configuring an Azure Automanage plan.

devoteam

4.3 Task Overview

Based on the assumption that we have an infrastructure of **200** servers for the basic service:

TASK	INCLUDED / ADD-ON
OPENING WORKSHOP	Included
DOCUMENTATION AND INFRASTRUCTURE ASSESSMENT	Included (+ Add-on per additional 100 servers)
FOUNDATION BUILDING	
RBAC PLANNING	Included
TAGGING STRATEGY	Included
BASIC AZURE MONITOR PLANIFICATION	Included
ADVANCED AZURE MONITOR PLANIFICATION	Add-on
BASIC AZURE POLICY PLANIFICATION	Included
ADVANCED AZURE POLICY PLANIFICATION	Add-on
UPDATE MANAGEEMENT PLANIFICATION	Included
MICROSOFT DEFENDER CLOUD PLANIFICATION	Add-on
DESIGNING INVENTORY AND CHANGE TRACKING	Add-on
PREPARING HYBRID PRIVATE LINKS	Add-on
CREATING AUTOMANAGE PROFILES	Add-on
REVIEW WORKSHOP	Included
ONBOARDING OF THE PILOT SERVERS	Included
DEPLOYMENT OF THE FOUNDATION	Included (Add-on for additional services)
ACCEPTANCE REVIEW	Included
DEPLOYMENT OF THE PLAN TO THE REMAINING SERVERS	Included
CLOSING WORKSHOP	Included

devoteam

5. Summary

To finish, by implementing Azure Arc enabled Servers with Devoteam. You will now be able to manage, monitor and ensure compliance across all your environments on a single console inside Azure. On top of that, these environments can run anywhere, on IoT (Internet of Things) devices, any public cloud providers, private cloud, or on premises, as long as the device meets the requirements to install the agent and connect to Azure publicly or privately.

Thanks to the experience of our hundreds of Microsoft experts at Devoteam, you will also be assured that your onboarding process will be smooth, secure, and following Microsoft best practices from start to finish.

Finally, this will also open to you the door to adopt other Azure Arc services in the future such as Azure Arc enabled SQL Server or the PaaS 2.0 that is Azure Arc enabled Services.