**Zero to hero with Azure Arc enabled servers**

**Engagement guide for first-time Azure Arc customers with hybrid servers**

Azure Arc simplifies complex and distributed environments across on-premises, edge, and cloud. Azure Arc helps you extend Azure management to any infrastructure and enables deployment of Azure data services anywhere. See [Azure Arc case studies](https://customers.microsoft.com/en-us/search?sq=%22Azure%20Arc%22&ff=&p=0&so=story_publish_date%20desc).

This document aims to give step-by-step deployment guidance for customers who are getting started with Azure Arc enabled servers, based on learnings from successful enterprise-scale deployments.

# **Proof of concept with 1-5 servers**

**Estimated duration: 90 minutes**

Onboard a few servers to Arc and showcase Tagging, Application insights, Update management and Azure Security Center

**Goals:**

* Connect a few servers to an Azure subscription using the Azure Portal
* Use tags on the servers to organize your resources
* Deploy the monitoring agent and start analyzing log data from Azure
* Configure Azure Update Management for the server
* Enable Azure Defender to get security recommendations for the server

**Prerequisites:**

* 1-5 servers to use for the proof of concept:
  + Supported operating systems ([full list](https://docs.microsoft.com/azure/azure-arc/servers/agent-overview#prerequisites)) include Windows Server, Ubuntu, RHEL, CentOS, SLES and Amazon Linux 2
  + The servers must have Internet access (direct or through a proxy server)
  + The servers can be physical or virtual, running on-premises or in another cloud
* An account with administrator privileges on the server(s) to install and configure the Arc agent
* Contributor access to an Azure subscription where you’ll create the Azure Arc resources. Need an Azure subscription? [Start a free trial today](https://azure.microsoft.com/free/)

**Azure Arc Jumpstart:**

For easy, scenario-led instructions for a POC, you can use the [Azure Arc Jumpstart GitHub repository](https://github.com/microsoft/azure_arc#azure-arc-enabled-servers). The repo includes a collection of comprehensive Azure Arc automated scenarios which guide you from bootstrapping an Azure Arc environment based on your platform of choice (i.e., AWS, GCP, VMware, Vagrant, etc.) all the way to implement and test day-2 scenarios mentioned in the “Goals” section of this document and more.

Note that you can also take advantage of the Azure VM-based scenarios with [these guides](https://github.com/microsoft/azure_arc#microsoft-azure), using an Azure VM as the targeted Azure Arc server. Please note that these are designed **for demo and testing purposes ONLY and are not supported for production deployments.**

**Tasks needed for the POC:**

|  |  |  |
| --- | --- | --- |
| Task | Details | Duration |
| Generate an installation script and run it on your server configure Azure Arc | [Connect hybrid machine with Azure Arc enabled servers - Azure Arc | Microsoft Docs](https://docs.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm) | 15 mins |
| Go to your server in the Azure Portal and review, add, or modify the tags associated with it. | | 5 mins |
| Create a Log Analytics workspace to store your log data. | [Create a Log Analytics workspace in the Azure portal - Azure Monitor | Microsoft Docs](https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-create-workspace) | 5 mins |
| Enable Azure Monitor on your Arc enabled servers in the Portal to start collecting log and performance data. | [Tutorial - Monitor a hybrid machine with Azure Monitor for VMs - Azure Arc | Microsoft Docs](https://docs.microsoft.com/en-us/azure/azure-arc/servers/learn/tutorial-enable-vm-insights) | 30 mins |
| Go to the **Insights** blade and review the performance data and network connections for your machine. | | 5 mins |
| Open the **Logs** blade on your Azure Arc server and run the query in the next column to see when the latest heartbeat from the Log Analytics agent was sent. As you add more logs to monitor, you’ll be able to query for them using the same view. | Heartbeat  | where TimeGenerated > ago(24h)  | order by TimeGenerated desc | 5 mins |
| Create an Azure Automation account | [Azure Quickstart - Create an Azure Automation account | Microsoft Docs](https://docs.microsoft.com/en-us/azure/automation/automation-quickstart-create-account) | 5 mins |
| Enable Update Management on the Automation account | [Enable Azure Automation Update Management from Automation account | Microsoft Docs](https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-automation-account) | 15 mins |
| Once provisioned, use the “Manage Machines” button in the Update Management solution to enable Update Management for your Arc enabled server. | [Enable machines in the workspace | Microsoft Docs](https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-automation-account#enable-machines-in-the-workspace) | 5 mins |
| It may take up to 12 hours for update data to appear for your machine. Once it does, you will be able to see it both in the Arc server resource and in the Automation account. |  |  |
| Go back to the Arc server resource and click the **Security** blade. If you don’t already have Azure Defender enabled on your subscription, click “Try it free for 30 days” and enable it. |  | 5 mins |
| Deploy a vulnerability assessment solution to your server by clicking “A vulnerability assessment solution should be enabled on your virtual machines” in the Security blade. In the window that pops up, review the details and click “Remediate” to deploy the agent. Security insights will become available within a day. |  | 5 mins |

# **Production trial with 10s of servers**

**Estimated duration: 3-6 hours**

Onboard 10s of servers and use Azure policy to audit compliance and automate deployment of Azure services such as monitoring as well as try out Azure Resource Graph for at scale queries.

**Goals:**

* Assign a policy to automatically install the monitoring agents on new Arc enabled servers
* Assign a guest configuration policy to audit password policies on your servers
* Configure Update Management to automatically start monitoring new servers
* Create an onboarding script and credential that can be used to onboard several servers to Azure Arc
* Use Azure Resource Graph to find and analyze your resources

**Prerequisites:**

* 10-100 servers to use for the production trial:
  + Supported operating systems ([full list](https://docs.microsoft.com/azure/azure-arc/servers/agent-overview#prerequisites)) include Windows Server, Ubuntu, RHEL, CentOS, SLES and Amazon Linux 2. It’s recommended to pick a heterogeneous group of servers reflective of your production environment for the trial.
  + The servers must have Internet access (direct or through a proxy server)
  + The servers can be physical or virtual, running on-premises or in another cloud
* An account with administrator privileges on the server(s) to install and configure the Arc agent. You can also use automated tools to push out the installation script to your machines.
* Contributor access to an Azure subscription where you’ll create the Azure Arc resources.

**Tasks:**

|  |  |  |
| --- | --- | --- |
| Task | Details | Duration |
| Create a resource group where you’ll onboard your Arc enabled servers. We’ll scope our policies to this resource group so other resources in Azure aren’t affected by the trial. | [Manage resource groups - Azure portal - Azure Resource Manager | Microsoft Docs](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal#create-resource-groups) | 5 mins |
| Decide if you want to use your production Log Analytics workspace or a separate one for testing. You can re-use the one from the proof of concept if you want. |  |  |
| Assign the **Enable Azure Monitor for VMs** policy to your resource group to automatically install the Azure monitoring agents (Log Analytics and Dependency agents) on new Arc enabled servers.  Use the resource group and log analytics workspaces created in previous steps to configure the policy assignment. | [Enable Azure Monitor for VMs by using Azure Policy - Azure Monitor | Microsoft Docs](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-policy) | 10 mins |
| Assign the **Audit machines with insecure password security settings** guest configuration policy to your resource group to audit operating system settings on each of your servers. | Navigate to Policy > Definitions in the Azure Portal  Filter the list for “Audit machines with insecure password security settings” and click the initiative definition  Click “Assign” and set the scope to your resource group (use the […] button to search for resource groups)  On the “Parameters” tab, set “Include Arc connected servers” to **True**, then finish creating the assignment. By default, guest configuration policies do not apply to Arc enabled servers, so always check the parameters tab to see if you need to opt in.  You’ll be able to see compliance results for this policy within an hour. | 5 mins |
| To configure Update Management to automatically monitor new servers added to your Log Analytics workspace, you need to disable scope configuration for Update Management. | [Enable machines in the workspace | Microsoft Docs](https://docs.microsoft.com/en-us/azure/automation/update-management/enable-from-automation-account#enable-machines-in-the-workspace)  Select the “Enable on all available and future machines” option | 5 mins |
| Now that your Azure services are ready to automatically be deployed to your Arc servers, it’s time to create an onboarding script that can be used on multiple machines. Unlike with the POC, you’ll use a Service Principal to allow the script to run unattended. | [Connect hybrid machines to Azure at scale - Azure Arc | Microsoft Docs](https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal) | 10 mins |
| Run the script to install the Arc agent on the servers. You can automate this with your favorite automation tooling. | Sample at-scale onboarding resources:   * [Scaled Onboarding VMware vSphere Windows Server VMs to Azure Arc](https://github.com/microsoft/azure_arc/blob/master/azure_arc_servers_jumpstart/docs/vmware_scaled_powercli_win.md) * [Scaled Onboarding VMware vSphere Linux VMs to Azure Arc](https://github.com/microsoft/azure_arc/blob/master/azure_arc_servers_jumpstart/docs/vmware_scaled_powercli_linux.md) * [Scaled Onboarding AWS EC2 instances to Azure Arc using Ansible](https://github.com/microsoft/azure_arc/blob/master/azure_arc_servers_jumpstart/docs/aws_scale_ansible.md) * [PowerShell remoting at-scale deployment (Windows only)](https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-powershell) | 1+ hour  (depends on your automation tool and maintenance window) |
| Once your servers are connected to Azure, you can start using Azure Resource Graph to query across your hybrid resources. In the Azure Portal, go to Resource Graph Explorer and try some of the queries to the right. | See the operating system distribution across your servers:  Resources  | where type =~ "microsoft.hybridcompute/machines"  | summarize count = count() by osName = tostring(properties["osName"])  Find Arc servers that haven’t sent a heartbeat in the last hour: Resources  | where type =~ "microsoft.hybridcompute/machines"  | where todatetime(properties["lastStatusChange"]) < ago(1d)  [Use tags to organize and find resources](https://github.com/microsoft/azure_arc/blob/master/azure_arc_servers_jumpstart/docs/arc_inventory_tagging.md) | 15 mins |

# **Production deployment**

**Estimated duration: 1 week**

**Goals:**

* Ensure corporate policy allows the Azure Arc agent to be installed and security controls permit the agents to run.
* Set up a Resource Health alert to know when an Arc agent has stopped sending heartbeats to Azure
* Set up an Azure Monitor alert to identify machines running outdated versions of the Arc agent.
* Identify servers that are compatible with Azure Arc and determine if there may be any naming conflicts
* Determine approach for organizing servers into resource groups and tagging
* Assign policies at the subscription or resource group scope
* Replace standalone agents with Arc extensions for simplified management and centralized reporting.
* Develop a migration plan for any servers that may move to Azure in the future.

**Prerequisites:**

* List of all servers ready to be connected to Azure:
  + Supported operating systems ([full list](https://docs.microsoft.com/azure/azure-arc/servers/agent-overview#prerequisites)) include Windows Server, Ubuntu, RHEL, CentOS, SLES and Amazon Linux 2
  + The servers must have Internet access (direct or through a proxy server)
  + The servers can be physical or virtual, running on-premises or in another cloud
* Automation tooling to deploy and configure the Arc agent on each server.
* Contributor access to an Azure subscription where you’ll create the Azure Arc resources.

**Tasks:**

|  |  |  |
| --- | --- | --- |
| Task | Details | Duration |
| Consult with your IT security team to ensure the Azure Arc agent will not be blocked on production servers and that network firewalls allow access to Azure Arc service endpoints (and any other services you use like Monitor, Security Center, etc.) | Update any policies that would prevent successful installation and connection of the Azure Arc agent.  While reviewing these policies, also consider if Azure Arc should be included in your security controls as part of your enterprise-wide monitoring and security story. | 1d |
| Create a Resource Health alert to be notified or trigger an action if a server stops sending heartbeats to Azure | If a server stops sending heartbeats to Azure for longer than 15 minutes, it can mean that it is offline, the network connection has been blocked, or the agent is not running. Develop a plan for how you’ll respond and investigate these incidents and use Resource Health alerts to get notified when they start:  [Create Resource Health Alerts Using Azure Portal - Azure Service Health | Microsoft Docs](https://docs.microsoft.com/en-us/azure/service-health/resource-health-alert-monitor-guide)  Resource type = Azure Arc enabled servers  Current resource status = Unavailable  Previous resource status = Available | 1h |
| Create an Azure Advisor alert to be notified when Azure Arc servers are running outdated versions of the Arc agent. | For the best experience and most recent security and bug fixes, we recommend keeping the Azure Arc agent up to date. Out of date agents will be identified with an Azure Advisor alert.  [Create Azure Advisor alerts for new recommendations using Azure portal - Azure Advisor | Microsoft Docs](https://docs.microsoft.com/en-us/azure/advisor/advisor-alerts-portal)  Recommendation type = Upgrade to the latest version of the Azure Connected Machine Agent | 1h |
| Identify which servers will have Azure Arc installed on them. | Gather inventory of your servers and verify they meet the network connectivity and operating system requirements. Note the following information to help you decide where the server will be represented in Azure:   * Department/group * Application/service hosted on the server * Who should have access to manage the server? * Geographic location of the server (datacenter, cloud, etc.) * Hostname | 1d |
| Identify the target resource group for each server in Azure. The resource group is the easiest way to configure role-based access control for the server, so consider both function and access when you organize them. | Consider the roles, locations, departments/groups, and access rules for each server and start organizing them into resource groups in a spreadsheet. An Azure resource group can have at most 800 Arc enabled servers in it, so you may need to break larger environments into several resource groups. The resource group you select for a server is used at initial onboarding, but a server can be moved to another resource group at a later time. | 1d |
| Check for any naming collisions | Once you’ve sorted the resources, check to ensure there are no duplicate hostnames in a single resource group. The hostname is used by default to name the Azure resource, so if two servers share the same name, one of them will need to be manually registered and have its name overridden to ensure uniqueness. | 4h |
| Determine a tagging strategy for the servers | [Resource naming and tagging decision guide - Cloud Adoption Framework | Microsoft Docs](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging/) | 4h |
| Generate installation scripts for your unique resource group, tag, and Azure data residency combinations. | Consider the tooling you will use to deploy the script across all your servers. Does it have an easy way to customize scripts when they’re deployed? If not, create separate scripts and deployment tasks for each unique configuration. | 4h |
| Deploy the scripts to your existing servers. Ensure your new server images and deployments also include Azure Arc. | Use your automation tool of choice to deploy the scripts to your servers and connect them to Azure. | Varies |
| Assign Azure Policies to your subscription or resource group scopes | The policies you assigned during the production trial were scoped to that trial resource group. Consider assigning the “Enable Azure Monitor for VMs” policy and others that meet your needs to the subscription scope, to ensure all your Arc enabled servers are automatically configured for monitoring. | 1h |
| Create a plan to convert existing monitoring agent deployments to extension-managed agents so they can be monitored and managed from Azure. | If you were already using the Microsoft Monitoring Agent (or OMS Agent) on-premises, consider switching to the Azure Arc extension based agent so it can be managed declaratively from the cloud. This enables you to audit installed versions from Azure and use a consistent approach to managing the extensions across Azure and non-Azure servers. Simple deployments with only one Log Analytics workspace and no on-premises Log Analytics Gateway can be converted by uninstalling the old agent and letting Azure Policy push down the latest version. More complex configurations may need additional configuration to support extension management. | Varies |
| Develop a migration plan for Azure Arc servers that may be migrated to Azure in the future. | Azure Arc is a great pre-migration tool because it lets your on-premises admins, and your cloud admins use the same tools no matter what kind of machine they’re managing. If you choose to migrate your server to Azure in the future, you can use the current tags, extensions, RBAC configuration, etc. to make planning your migration even easier. | Varies |