# **Managed identities for Azure resources:**

A common challenge for developers is the management of secrets and credentials to secure communication between different services. On Azure, managed identities eliminate the need for developers having to manage credentials by providing an identity for the Azure resource in Azure AD and using it to obtain Azure Active Directory (Azure AD) tokens. This also helps accessing [Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/general/overview) where developers can store credentials in a secure manner. Managed identities for Azure resources solves this problem by providing Azure services with an automatically managed identity in Azure AD.

Here are some of the benefits of using Managed identities:

* You don't need to manage credentials. Credentials are not even accessible to you.
* You can use managed identities to authenticate to any Azure service that supports Azure AD authentication including Azure Key Vault.
* Managed identities can be used without any additional cost.

Note: Managed identities for Azure resources is the new name for the service formerly known as Managed Service Identity (MSI).

## **Managed identity types**

There are two types of managed identities:

* **System-assigned** Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity an identity is created in Azure AD that is tied to the lifecycle of that service instance. So when the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Azure AD

How we can assign this through azure portal:

Step1: Open the azure resource, select system assigned identity and create an Identity and Enable it.(source)

Step2: Go to the target resource and click on access control and add a role which grant the Identity access to the azure resource

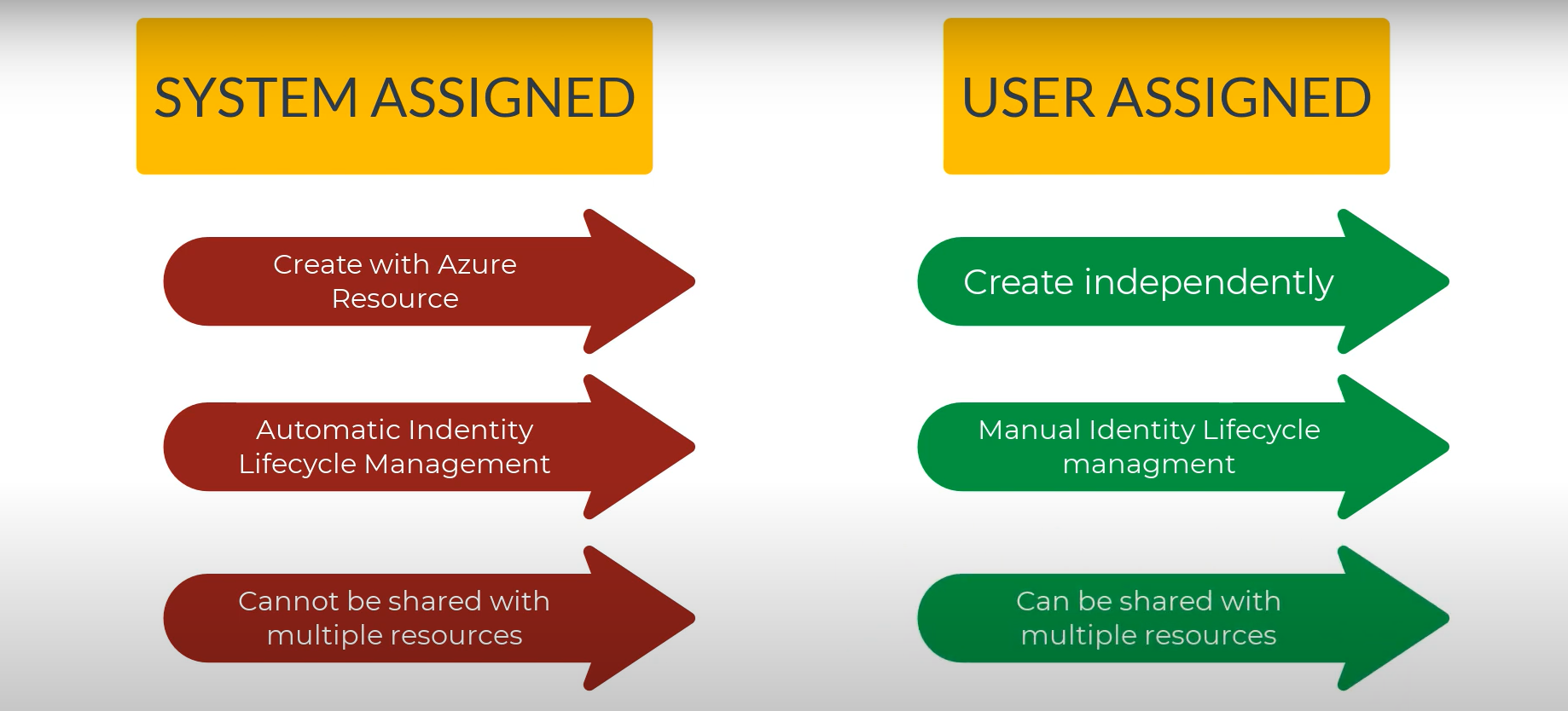
* **User-assigned** You may also create a managed identity as a standalone Azure resource. You can [create a user-assigned managed identity](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-manage-ua-identity-portal) and assign it to one or more instances of an Azure service. In the case of user-assigned managed identities, the identity is managed separately from the resources that use it.

How we can assign this through azure portal:

Step1: Search for managed identity and create a User Managed Identity

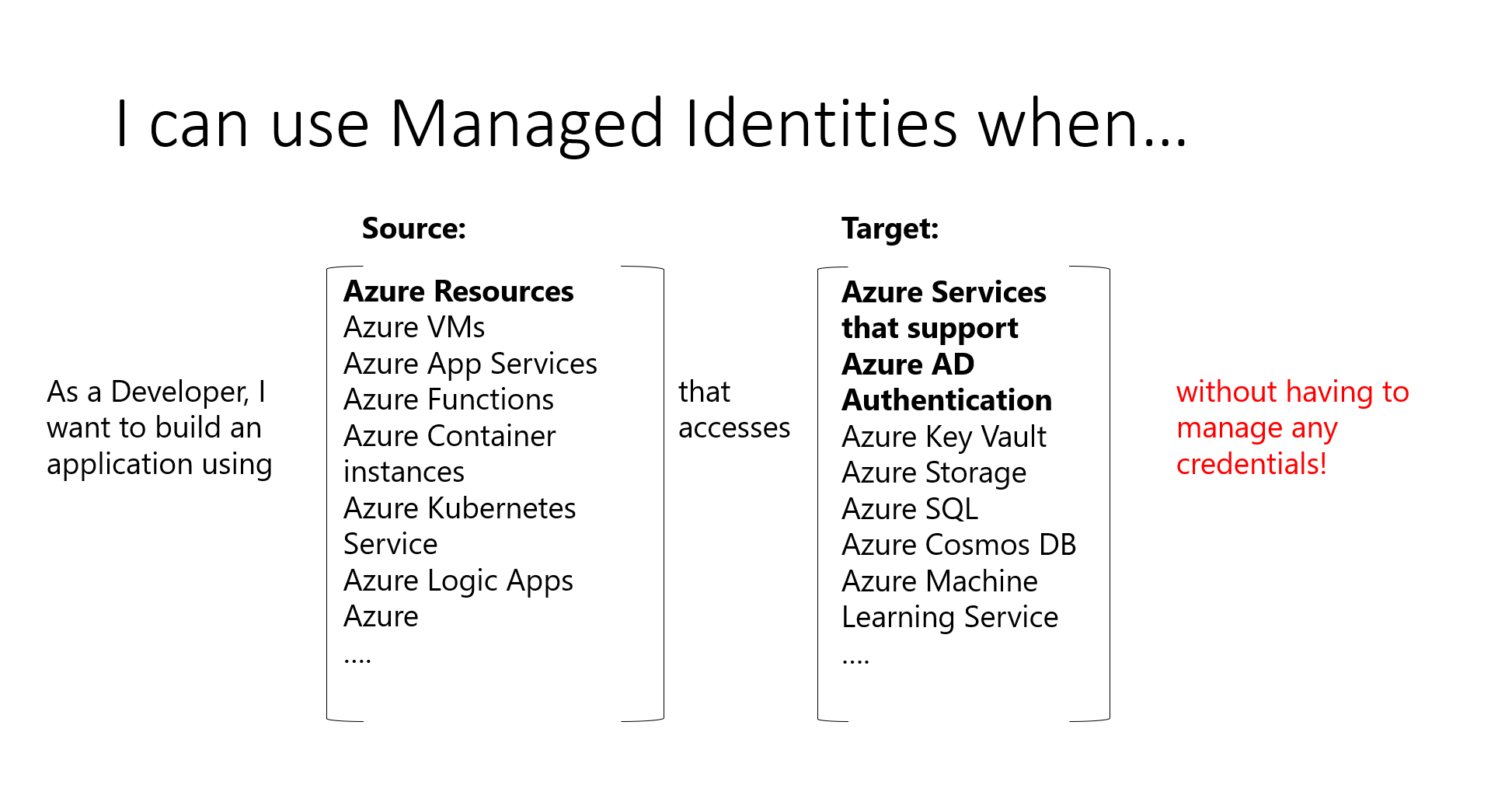
Step2: Open the azure resource, select User assigned identity and we chose the created user managed identity

Step3: Go to the target resource and click on access control and add a role which grant the Identity access to the azure resource



**Important**

Regardless of the type of identity chosen, a managed identity is a service principal of a special type that may only be used with Azure resources. When the managed identity is deleted, the corresponding service principal is automatically removed.



## **What Azure services support the feature?**

Managed identities for Azure resources can be used to authenticate to services that support Azure AD authentication.