

**Managed Azure Cloud Ops**

- Managed Azure Cloud Operations, Made Easy -

***Date: 25thth April, 2025***

***Version No: 01***

***Written By: Ian Hanley, Lead Security Architect, KMicro Tech, Inc.***

***For: Deena Naidoo, Director of Managed IT Servicse, KMicro Tech, Inc.***

Contents

[🔍 Overview: What This Template Does 3](#_Toc196723619)

[✅ Customer-Side Pre-Requisites for Running the Deployment 3](#_Toc196723620)

[📋 Quick Client Checklist: 4](#_Toc196723621)

[🚩 Notes: 4](#_Toc196723622)

[📦 Key Components of This Deployment 5](#_Toc196723623)

[📧 Suggested Client Correspondence 6](#_Toc196723624)

[Step-by-Step Deployment Guide 7](#_Toc196723625)

[✅ Confirmation 8](#_Toc196723626)

## 🔍 Overview: What This Template Does

This Azure Resource Manager (ARM) template enables your organization to **onboard our services via Azure Lighthouse**. Lighthouse is Microsoft’s delegated resource management solution, allowing us (your MSSP partner) to manage your Azure subscriptions securely, without needing to create accounts in your tenant.

## ✅ Customer-Side Pre-Requisites for Running the Deployment

| **Requirement** | **Details** |
| --- | --- |
| **Azure Tenant Access** | They must have access to their **Azure Active Directory (AAD) tenant** where the subscription resides. |
| **Azure Subscription Owner Role** | The user running the deployment must have **Owner** permissions on the **target subscription**. (**Contributor** is not enough because this deployment registers management delegation at the subscription level.) |
| **Resource Provider Registration** | The **Microsoft.ManagedServices** resource provider must be **registered** in the subscription. (We can help them check this.) |
| **Azure CLI / Portal Access** | They should either be able to: <ul><li>Login to the **Azure Portal**</li><li>Or have **Azure CLI** installed and authenticated (if running via command line)</li></ul> |
| **Permissions to Consent to Delegations** | They must be able to approve registration definitions and grant delegated access. This usually comes with **Owner** or **User Access Administrator** roles. |
| **Tenant Not Locked Down by Conditional Access** (sometimes) | If their Conditional Access policies restrict role assignments or privileged operations (like device compliance requirements), we may need a temporary exclusion. (This is rare.) |
| **Subscription Not Under a Management Group With Policy Blocks** | If their subscription inherits policies that block 'Microsoft.ManagedServices/registrationDefinitions' deployments, we’ll need a policy exemption created first. (Again, rare but possible.) |

## 📋 Quick Client Checklist:

* I have **Owner** access to the subscription.
* I can log into the **Azure Portal** or use **Azure CLI**.
* My subscription has the **Microsoft.ManagedServices** provider registered.
* No Conditional Access or Policy blocks will prevent delegation.

## 🚩 Notes:

* **Resource Provider Check**:  
  They can quickly check if **Microsoft.ManagedServices** is registered by running in Azure CLI:

bash

CopyEdit

az provider show -n Microsoft.ManagedServices --query "registrationState"

It should return **"Registered"**.  
If it’s not registered, they can run:

bash

CopyEdit

az provider register --namespace Microsoft.ManagedServices

* **Multiple Subscriptions**:  
  If they have multiple subscriptions, they must specify **which one** during deployment.

### 📦 Key Components of This Deployment

| **Parameter** | **Purpose** |
| --- | --- |
| name | Unique identifier for the registration (GUID). |
| definitionName | Friendly name: “KMicro's Managed Azure Cloud Ops”. This is what shows in your Azure Portal. |
| definitionDescription | Describes the service offering. |
| managedByTenantId | Our tenant ID (KMicro). Azure uses this to link your environment with our managed services. |
| authorizations | Assigns specific **Azure RBAC roles** to groups in our tenant (like "CLOUD OPS1", "CLOUD OPS2") so we can provide support. |
| eligibleAuthorizations | Currently empty, but can be used later for Just-In-Time access via Privileged Identity Management. |
| apiVersion | Uses 2019-06-01 – Microsoft’s stable API for Lighthouse. |

Each role assignment maps one of our support teams (identified by GUID) to Azure roles such as:

* **Reader**
* **Contributor**
* **Monitoring Reader**
* **Security Reader**
* **Virtual Machine Contributor**
* And more, per least privilege best practice.

## 📧 Suggested Client Correspondence

**Subject:** Schedule a Quick Session to Enable Managed Services in Your Azure Environment

Hi [Client Name],

We’re excited to begin delivering managed Azure operations through our Microsoft-verified Lighthouse integration.

To securely delegate access, we use an ARM deployment that:

* Grants limited, role-based access to our support groups,
* Enables full visibility into assigned roles,
* Does not require user creation in your tenant.

Here’s what we need from you:

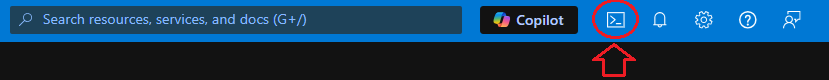
Please reply with a convenient time to schedule a brief screen share (15–20 mins). We’ll walk you through deploying this secure onboarding template from your Azure Portal or CLI.

Let us know your availability, and we’ll send over a calendar invite with join details.

Thanks,  
[Your Name]

## 🔧 Step-by-Step Deployment Guide

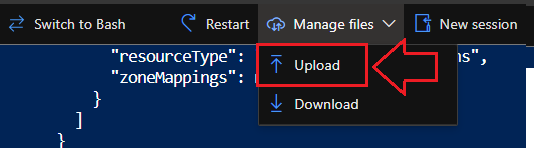
1. Login to <https://www.portal.azure.com> with a sufficiently privileged account (see pre-requisites).
2. Load the Azure CLI:



**Note**: *your* ***session*** *can be* ***ephemeral****, you can run* ***ARM deployments*** *from an* ***ephemeral CLI session.***

****

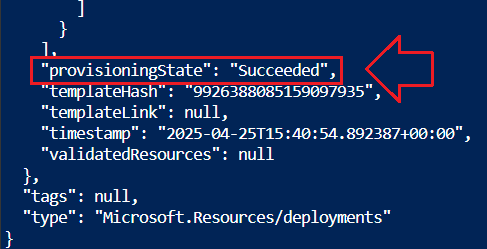
1. Upload the .json files for this deployment:



1. Run the following command in the Azure PowerShell CLI terminal:

az deployment sub create --name lighouseRegistration --location eastus --template-file /home/ian/template.json --parameters /home/ian/parameters.json

Look for “Provisioning State” in the results: "provisioningState": "Succeeded",



## ✅ Confirmation

In the client’s Azure portal, navigate to:

**Azure Lighthouse 🡪 Service Providers** and select **KMicro’s Managed Azure Cloud Ops.**

