Policy Definition and Assignment template.

There are some prerequisites that need to be checked before you can continue with the document.  
  
Verify that you have access to the Management Group that you want to deploy these templates to.   
This can easily be done by navigating to the “Management groups” service in the Azure portal.   
If you can click in the name of the management group you can skip until the deployment portion of this document.  
  
Prerequisites

If you were unable to click on the management group that you want to deploy this template to you need to follow some additional steps before you can continue.

Permissions

1. First, make sure that you have the necessary permissions to grant yourself permissions to manage access for all Azure subscriptions and management groups for the tenant that you are using.   
   Azure AD Global Administrators are the only users that can elevate themselves to gain this access.
2. The first step to grant yourself the necessary permissions to make these changes go to the Entra ID service. On the left-hand side, under “Manage” navigate to “Properties”.
3. Once you are here you should be able to see something named “Access management for Azure resources”.
4. Ensure that this setting is set to “Yes”.  
   If you for whatever reason are unable to change it from “no” to “yes” you do not have sufficient permissions to make these necessary changes in the AD and won’t be able to continue until this is changed.

A screenshot of a computer

Description automatically generated

Now that you can click on the management group you are ready to add some much-needed permissions for the user that’s going to perform these deployments. (These permissions will also be inherited down to the subscriptions under this management group as well).  
Our testing has concluded that the permissions needed for these templates are “Contributor” on the management group.

After adding the “Contributor” role you do not need to do anything else in the management group for now.

A screenshot of a computer

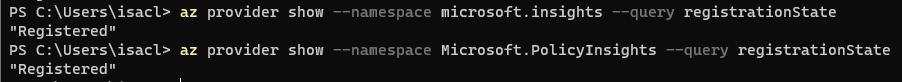
Description automatically generated

Providers

Now might also be a good time to verify that the correct “Providers” are registered on each subscription. This can be done either by using Azure CLI or by navigating in the portal.  
The following providers are needed for each subscription.  
Microsoft.OperationalInsights,  
microsoft.insight,  
Microsoft.PolicyInsights.

If you are using the Azure CLI you should follow these instructions.

1. To first verify the status of the providers run the following command
   1. Az provider show –namespace Microsoft.PolicyInsights –query registrationState
   2. If it shows up as registered do the same thing for the others.
2. If they are not registered run the following command
   1. Az provider register –namespace Microsoft.PolicyInsights
   2. After a few minutes you should run the first command again to verify that the registration was successful.



If you prefer to do these things directly in the GUI these are the steps to follow.

1. Navigate to the Subscription service and select the subscription for which you want to add the provider for.
2. When you have selected a subscription, you can start registering the providers.
3. On the left-hand side, you should once again have multiple things.
   1. Under Settings navigate to “Resource providers”.
   2. From here, either search for the provider using the search field or find it manually.
   3. After you have found the provider in question you should now click somewhere on that row.
   4. Now on the top of the page you should be able to see something like this. A screenshot of a computer

      Description automatically generated
   5. Click on “Register” and wait a few minutes.

Deployment

Now that the necessary permissions have been added to the management group and subscriptions, we are ready to start deploying the templates to Azure.

Before deploying the templates, you should make a note of the management group ID which can be found on the overview page of the management group page. The same thing should be done with your subscription that your Log analytics Workspace (LAW) is in.

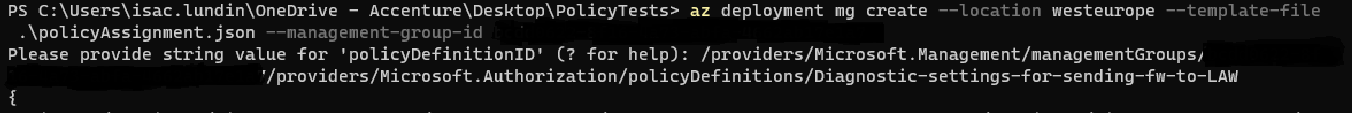
Now the deployment can finally begin.

1. If you followed the prerequisite steps its recommended to restart your PowerShell to reduce the risk of sessions being out of sync.
2. After logging in with Azure CLI by running “az login” and signing in on the website you are redirected to you can begin.
3. The command to deploy the templates are the following.
4. Az deployment mg create –location westeurope –template-file .\policyDefinition –management-group-id {MG\_group\_id}
   1. When you are prompted to supply your WorkspaceId it should be supplied in the following format.
      1. /subscriptions/{SubscriptionID}/resourceGroups/{ResourceGroup}/providers/Microsoft.OperationalInsights/workspaces/{WorkspaceName}
      2. All information that is needed for the above-mentioned command can all be found within the LAW resource in the GUI
   2. After supplying the WorkspaceID and selecting either “AllLogs” or “Audit” you should hopefully be faced with a big json blob of data which will indicate that the deployment was successful.
   3. You now need to either scroll through the giant json blob to locate the policyDefinitionID which is needed for the policyAssignment template or get the ID from the GUI.
      1. The ID should look something like this: “/providers/Microsoft.Management/managementGroups/{MG\_group\_id}/providers/Microsoft.Authorization/policyDefinitions/{name\_of\_the\_policy\_definition}”

A screen shot of a computer

Description automatically generated

1. Az deployment mg create –location westeurope –template-file .\policyAssignment –management-group-id {MG\_group\_id}
   1. When you are prompted with the question regarding policyDefinitionID you should supply the ID that you saved from the policyDefinition deployment.
   2. After supplying the necessary ID the template should start deploying.
   3. Also, this time a successful deployment is indicated when you see a big json blob.
   4. We are now done with the deployment portion of the templates.



Readding permissions to the policyAssignment (mandatory)

Now that the templates are deployed successfully, we need to re-add some permissions that are specified in the policyDefinition file.   
This is done to add the permissions to the System assigned Identity which is created on the assignment.

A screenshot of a computer

Description automatically generated

1. Navigate to the “Policy” service and on the left-hand side under “Authoring” click on “Assignment”
2. Navigate to the newly created policyAssignment. (Should be named something like this: “Assignment Deploy Diagnostic Settings for xxx to Log Analytics Workspace”).
3. Click “Edit Assignment”
4. Go to “Review + Save” directly and press “Save”
5. After saving the policy assignment you should be put right back to the policy assignment.

After reapplying the permissions it’s recommended to double check the Management group and underlying subscriptions to verify that the permissions have been successfully added and are inherited down to the subscriptions correctly.

For example see image number 2

Now the following step is only necessary if you already have existing resources that were created before these templates were deployed. This is because the assignment only does this automatically for newly created once.

1. Now still inside the policy assignment you should click on “Create remediation task”.
2. Here you have a few different settings you can mess with but if the “Scope” is your management group ID you do not need to change anything else.
3. Click on “Remediate”.
4. After creating a remediation task, you can follow it by navigating back to the policy assignment and go to “Remediation”.
5. If the “Remediation State” is “Completed” the remediation task was successful and the resource is now streaming logs to your LAW.
   1. You can also verify that the assignment was successful by browsing to any of the resources that had their diagnostic settings modified.
6. If the “Remediation State” is “Failed” the remediation task was unsuccessful, to check why it failed click on the three horizontal dots and select “View remediation task”.
7. Now on the far lower right you also need to click on these horizontal dots and select “View deployment”.
   1. This should give you a good overview of why the remediation failed.

A screenshot of a computer

Description automatically generated