Problem 2 :

DevOps team is asked to set up a security feature to the beta product k8s cluster which is planned to get released to all over world to face the load testing. As part of security concern,

DevOps team is planning to enable IP masking to the product deployed under the ingress in the cluster. So that end user will not know the actual IPs of the product which will avoid bot attacks

Ingress: nginx

DNS: Can be any provider

sub domain: can be any test domains

SSL: lets encrypt / any other

Back end: Any sample java/ hello world application

1. While creating a Kubernetes Cluster enable the Advanced option and then create the cluster.

2. Then Go your Application Insights resource, and then select Automation > Export Template.
3. Select Deploy.
4. Select Edit Template.
5. Select the Edit button highlighted in red.
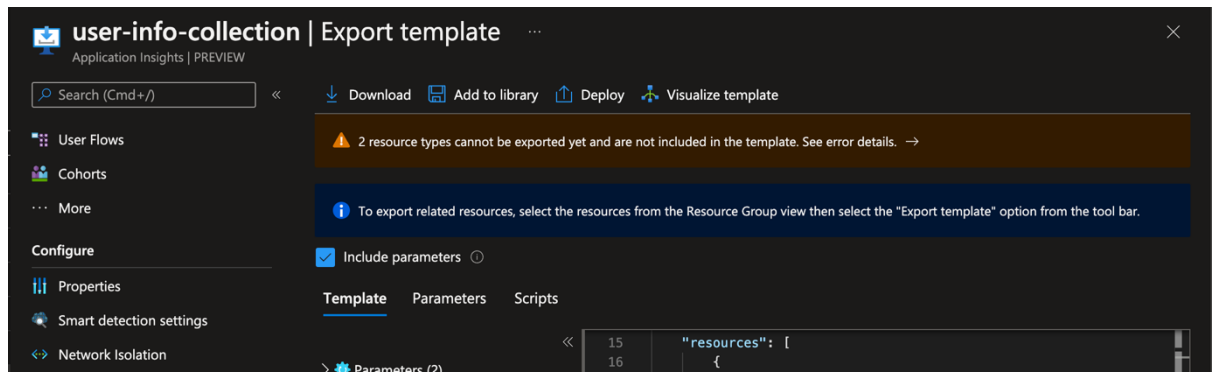
6. In the JSON template locate properties inside resources, add a comma to the last JSON field, and then add the following new line: "DisableIpMasking": true. Then select Save.
7. Select Review + create > Create.

For example,
After exporting the template,

```
{
    "id": "/subscriptions/<subscription-id>/resourceGroups/<resource-group-
name>/providers/microsoft.insights/components/<resource-name>",
    "name": "<resource-name>",
    "type": "microsoft.insights/components",
    "location": "westcentralus",
    "tags": {

    },
    "kind": "web",
    "properties": {
        "Application_Type": "web",
        "Flow_Type": "Redfield",
        "Request_Source": "IbizaAIExtension",
        // ...
        "DisableIpMasking": true
    }
}
```