

## 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

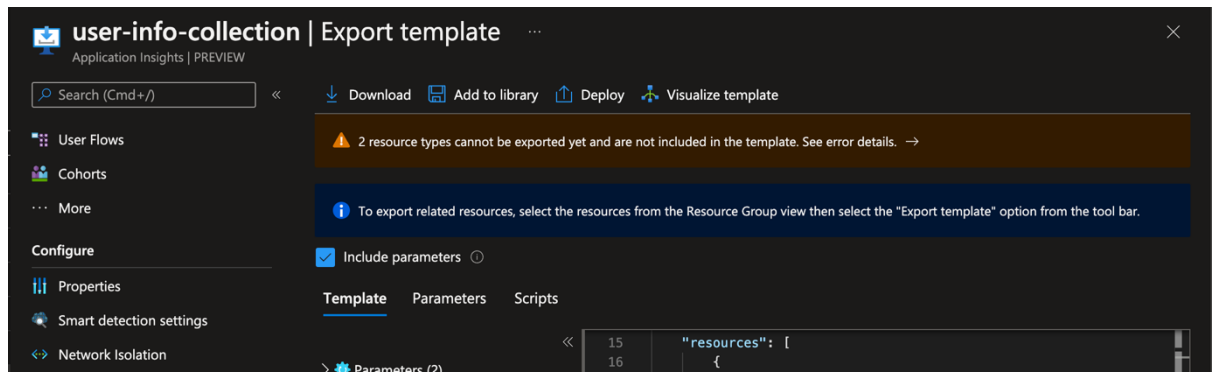
SSL: lets encrypt / any other

Back end: Any sample java/ hello world application

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

The screenshot shows the 'Create Kubernetes cluster' page in the Azure portal, specifically the 'Networking' tab. The breadcrumb navigation at the top reads: Home > New > Marketplace > Everything > Azure Kubernetes Service (preview) > Create Kubernetes cluster. The page title is 'Create Kubernetes cluster'. Below the title are tabs for 'Basics', 'Networking' (selected), 'Monitoring', 'Tags', and 'Review + create'. A message states: 'You can enable Http ingress routing and choose between two networking options for Azure Kubernetes Services - "Basic" and "Advanced".' Two bullet points describe the options: 'Basic' sets up a simple default config with a VNet and internal IP addresses, while 'Advanced' allows configuring your own VNet for automatic connectivity and full integration. A link 'Learn more about networking in Azure Kubernetes Service' is provided. The configuration section includes: 'Http application routing' with 'No' selected; 'Network configuration' with 'Advanced' selected (highlighted by a red box); 'Virtual network' set to 'aks-vnet-16033614' with a 'Create new' link; 'Subnet' set to 'aks-subnet' with a 'Create new' link; 'Kubernetes service address range' set to '10.0.0.0/16' with a green checkmark; 'Kubernetes DNS service IP address' set to '10.0.0.10'; and 'Docker Bridge address' set to '172.17.0.1/16' with a green checkmark.

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
  }
}
```