Production Deployment guideline

The requirements for deploying WSO2 products can vary based on the deployment scenario and pattern. The recommendations in this topic are intended for general production use.

WSO2 APK can be configured through `values.yaml` file. Please refer to Customize Configurations for information on how to use a customized values file for APK deployment. When deploying WSO2 APK in a production environment, we strongly recommend following these guidelines.

Change the hostnames and vhosts

By default, APK uses wso2.com for its hostnames and vhosts for the gateway. You need to change these values to your own domain, which you plan to use for production. The following values.yaml values should be modified:

- wso2.apk.listener.hostname
- wso2.apk.dp.gateway.listener.hostname
- wso2.apk.dp.configdeployer.vhosts

For further clarification on the keys, please refer to the description and default values here

Change the gateway certificates

The default APK deployment uses a self-signed certificate for the gateway. You need to update it with your domain-validated certificate through the `values.yaml` file.

Prerequisites

1. TLS certificate verified by a Ceriticate Authority (tls.crt)
2. Private key associated with the TLS certificate(tls.key)
3. Certificate Authority's (CA) root certificate(ca.crt)

Create a secret in the same namespace as APK is deployed with the following key-value pairs:

- tls.crt - Base64 encoded value of tls.crt file
- tls.key - Base64 encoded value of tls.key file

- ca.crt - Base64 encoded value of ca.crt file

Update the `wso2.apk.dp.gatewayRuntime.deployment.router.configs` of values.yaml with the following values

```
configs:
 tls:
  secretName: "<Name of the created secret>"
  certKeyFilename: "tls.key"
  certFilename: "tls.crt"
  certCAFilename: "ca.crt"
```

Remove default IDP

APK comes with a default IDP which is not production-ready. Disable the default IDP and use a production-ready IDP solution. Please follow these guidelines to setup the production ready IDP

Disable the default idp by changing the following value to `false` in values.yaml `idp.enabled` = `false`

Use a managed redis service

APK uses a built-in standalone Redis service which is not suitable for production usage. Please use a managed, production-ready Redis. You can update the following values to configure the Redis configuration in APK:

- wso2.apk.dp.redis.type
- wso2.apk.dp.redis.url
- wso2.apk.dp.redis.tls
- wso2.apk.dp.redis.auth.certificatesSecret
- wso2.apk.dp.redis.auth.secretKey
- wso2.apk.dp.redis.poolSize

Protect gateway admin port

APK uses EnvoyProxy in the router implementation. EnvoyProxy offers an administrator interface that can be used to query and modify different aspects of the server. In the production environment, we should disable or restrict access to this port. By default, APK exposes this

interface through port `9000`. To disable external access to the port, you can set the following Helm value to `false`: `wso2.apk.dp.gatewayRuntime.deployment.router.adminInterfaceEnabled`

If admin port is enabled, it is critical that access to the administration interface is only allowed via a secure network. It is also critical that hosts that access the administration interface are only attached to the secure network (i.e., to avoid CSRF attacks). This involves setting up an appropriate firewall.