Controller App Security Beta - Deployment Workflow Overview

Doc version: v12

Prerequisites:

- Trial license or paid license for NGINX Controller

Assumptions of Usage of NGINX Controller App Security Beta:

1. Beta will not be using an existing instance of Controller that is in a production environment
2. NGINX Plus and NGINX App Protect data plane instances to be used with this Beta can be removed and then re-deployed if necessary. Original NGINX configuration does not need to be restored.
3. Upgrades may require removing and installing new Controller and the data plane instances

Versions supported in the Beta:

- NGINX Controller v3.7+
- Data plane: CentOS 7.4+ on linux virtual machine(s)

Known Issues specific to Controller App Security are available here:
https://nginx-ctlr-appsec-beta-docs.netlify.app/services/apps/security/app-sec-release-notes/
(password: **NGINXapp*sec072020**)

BETA SETUP INSTRUCTIONS:

Part 1: Get and Deploy the Data Plane Components for Controller App Security Beta

1. Go to https://f5beta.centercode.com
2. Select "**NGINX Controller App Security"** under My Projects
3. Go to "**Download Area:** (menu on left)
4. Select the "**NGINX Controller App Security Build**" folder
5. Download **cas-centos7-beta-0.tar.gz** (or the one that matches the OS distribution that you are looking for. This package includes the script that will install and deploy Controller App Security data plane instances including NGINX Plus, NGINX App Protect, and components for retrieving WAF violation events
6. Download **postinst** file. This is a script to be run on the linux machines in Part 2)
7. **Copy the cas-centos7-beta-0.tar.gz and postinst files to the linux virtual machines** you are planning to use as data planes for Controller App Security beta. Copy using a utility such as secure copy (scp).
8. **SSH into the linux virtual machines** and **extract the tar file** with the following command: **tar -xvzf cas-centos7-beta-0.tar.gz.**
9. Run the deploy script using**: *sudo ./deploy_cas.sh***
10. Start the NGINX and NGINX App Protect on each instance you have installed it on
    - ***i.*** If using SELinux and setting of SELinux to 'permissive' mode is needed, run: ***sudo setenforce 0***
    - ii. run: ***sudo systemctl enable nginx***
    - iii. run: ***sudo systemctl start nginx***

Part 2: Get and Deploy NGINX Controller

1. If using trial license for Controller, please **get access to the Controller package files and trial license keys** from the F5/NGINX Sales team member you are working with.
2. **Install the Controller v3.7 (or later versions)**. See instructions to Install NGINX Controller here.
3. Enable Controller UI so show Security Events and Analytics
    a. run: /***opt/nginx-controller/helper.sh setfeature AppSec true***
4. **License your Controller**:
    a. Go to https://<FQDN>/platform/license, where <FQDN> is the fully qualified domain name for your NGINX Controller server.
    b. In the **Upload** a license section of the page, select Choose a file.
    c. Locate and select your license file in the file explorer
    d. Select **Save** license

Part 3: Register the Data Plane Instances with Controller, Then Add App Security To Your App

1. **Register the data plane instances with Controller**

Note: the data plane instances are the linux virtual machines you've deployed NGINX Plus and NGINX App Protect on as a part of Part 1 (above)

- Install the Controller Agent on each NGINX Plus Instance that you want to manage and monitor.
- Open the NGINX Controller user interface and log in.
- Select the NGINX Controller menu icon, then select **Infrastructure**.
- On **Infrastructure** menu, select Instances.
- On the **Instances Overview** page, select Create to add an Instance.
- On the **Add Instance** page, provide a name for the Instance. If you don't provide a name, the hostname of the Instance is used by default.
- To add the Instance to an existing Location, select a **Location** from the list. Or select **Create New** to create a Location.
- **Select** "Add an existing instance"

Note: Once set, the Location for an Instance cannot be changed. If you need to change or remove the Location for an Instance, you must remove the Instance from NGINX Controller, and then add it back.

- **Select** "Allow insecure server connections to NGINX Controller using TLS"
- Use SSH to connect and log in to the NGINX Instance that you want to connect to NGINX Controller.
- Run the curl or wget command that's shown in the **Installation Instructions** section on the NGINX Instance to download and install the Controller Agent package. The -i and -l options for the install.sh script specify the Instance name and Location, respectively.
- Reload NGINX Plus you just installed Controller Agent on
    run: ***sudo systemctl reload nginx***

Note: Make sure you enter the commands to download and run the install.sh script on the NGINX Instance system, and not on the NGINX Controller server.

After a few minutes, the NGINX Instance will appear on the Instances Overview page.

2. Enable seeing WAF related security violation events in Controller
   run: **chmod +x ./postinst** on the data plane instances
   run: **sudo ./postinst** on the data plane instances

3. **Add App Security (WAF) To Your App**

   Get directions from Controller App Security Beta Product Documentation site:
   https://nginx-ctlr-appsec-beta-docs.netlify.app/services/apps/security/tutorials/
   (password: **NGINXapp*sec072020**)

   On the Product Documentation site:
   a. go to section ***"Add App Security to Your Apps"***
   b. start with "***Add a Gateway***" and follow directions to also **"*Add an Environment*"**, **"*Add an App*"**, and "***Enable WAF for a Component***"

   If you want to use an example **Postman collection to call APIs of Controller to enable App Security**, please use the NGINX Controller App Security.postman_collection.json file in the Downloads Area of the Beta's centercode area. Please **edit the variables** for 'controller-fqdn' and 'instance_name'.

   Now, you should have WAF in front of a URI (component) of your app!

4. **To Verify WAF Has Been Enabled For A Component**

   To verify that WAF has been enabled by NGINX Controller App Security to protect your app component, send a GET request to the app component, simulating a request an end user would send to access the app component but with the URL parameter and value of **"?a=<script>"** appended to the end.

   Example: GET: http or https://[gateway FQDN]/<app component path>/?a=<script>

   The request should be blocked. The response would contain "Support ID".

   Note: [gateway FQDN] is the URI specified in the ingress block of the gateway referenced when creating the app component
   <app component path> is the URI (path) specified in the ingress block when creating an app component

--End of Beta Instructions--

Controller Beta Product Documentation site also contains information that will be useful after setup including: View App Security Analytics, Configure Monitor Mode for App Security, etc.