appviewX

Install and Upgrade Patch Deployment Guide 2020.3.0 FP9

Version: 2020.3.0

Patch Deployment Guide FP9

The purpose of this document is to guide the users for applying patches on AppViewX v2020.3.0 FP9.

Copyright AppViewX, Inc.

Trademarks

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
v1.0	Patch deployment for Appviewx 2020.3.0 FP9	March, 2020

About this Guide

The purpose of this document is to guide the users for applying patches on AppViewX v2020.3.0 FP9.

Audience

This document is intended for internal users and customers of Appviewx to support patch deployment activities.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Prerequisites

The existing AWS account data present in AppViewX should be deleted before applying the patch for migration. For more details, refer to the Prerequisites for Migration Guide

Chapter 2: Expectations and Recommendations

Expectations

This patch deployment process involves below steps. All the changes should be updated in the **appviewx.conf** file.

> **Note:** A considerable amount of time will be taken for the complete FP10 patch deployment process.

This patch deployment process involves two parts:

1. Part 1 - Plugins and addons upgrade
2. Part 2 - Kubernetes infra upgrade

> **Note:** FP6 patch is mandatory before applying FP9.

3. Patching of the Logstash Insight is handled as part of the FP9 patch.

> **Note:** This is applicable if insight is enabled.

Recommendations

1. The new option included from FP7 patch to enable/disable support for managing legacy endpoints works only with the deprecated TLS v1.0 or v1.1.
2. Make the decision on choosing the option ENABLE_LOWER_TLS OPTION as **Yes** or **No** before you apply any new patch on top of existing patch.
3. To disable support for TLS v1.0 and TLS v1.1 as security standards, provide the response as **NO**.
4. If a customer wants to change **ENABLE_LOWER_TLS** to **YES** or **NO** after completion of the existing patch. Follow the steps mentioned in the Frequently Asked Questions (FAQ) section.
5. In case load balancer is used for ingress gateway service, provide the URL of the Load Balancer service and port
   a. INGRESS_LB_URL=<Input the LB Service URL>

      Example: abc.123xyz.com

   b. INGRESS_LB_PORT=<Input the LB PORT NUMBER>

Note: If the above-mentioned changes are being applied during the FP8 patch, proceed with the Part 1 - Plugins and Addons Upgrade section.

If the mentioned changes are being applied explicitly, run the script `add_ingress_var.sh` available at location <INSTALLER_PATH>/appviewx_kubernetes/scripts in the **appviewx.conf** file.

Chapter 3: Part 1 - Plugins and Addons Upgrade

Follow the steps below to add the plugins and addons.

1. Log in to the release portal and download the FP10 patch files
   - **appViewX_2020.3.FP9.tar.gz**
   - **appviewx_addons_2020.3.FP9.tar.gz**
   - Download the latest dated script file **(tar.gz)** from release portal, for example - **scripts_FP9_(latest date).tar.gz**
2. Move all the downloaded files to the node where the installation is initiated.
3. Open the terminal window with valid credentials and validate the “md5sum” value of the downloaded files.
4. To know the status of the pods, execute the command,

   ```
   kubectl get pods –A
   ```

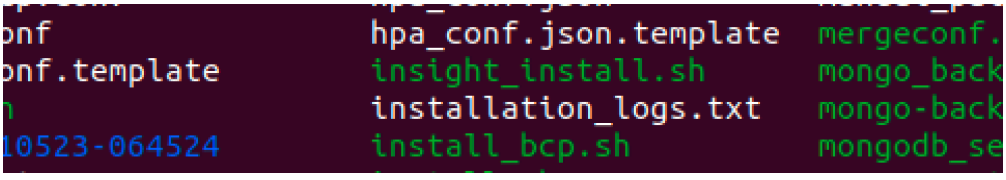
   If a pod is in a state other than *“Running”* or the two containers associated with the pod (0/2 or 1/2) are not up and running, take note of it.
5. Take a backup of the **plugins_install.sh**file in <INSTALLER_PATH>/appviewx_kubernetes/scripts using the command

   ```
   cd <INSTALLER_PATH>/appviewx_kubernetes/scripts mv plugins_install.sh plugins_install.sh.bak
   ```
6. Untar the scripts using the command

   ```
   tar -xvf scripts.tar.gz
   ```
7. Copy the files from the downloaded scripts directory to the <INSTALLER_PATH>/appviewx_kubernetes/scripts directory
   - Command to replace files (confirmations required)

     ```
     cp -r <Download_Directory>/scripts/* <INSTALLER_PATH>/appviewx_kubernetes/scripts/.
     ```
   - Command to replace files (confirmations ignored)

     ```
     rsync -av <Download_Directory>/scripts/* <INSTALLER_PATH>/appviewx_kubernetes/scripts/.
     ```
8. Check and replace the **hpa_conf.json.template** file that is present in the scripts directory.

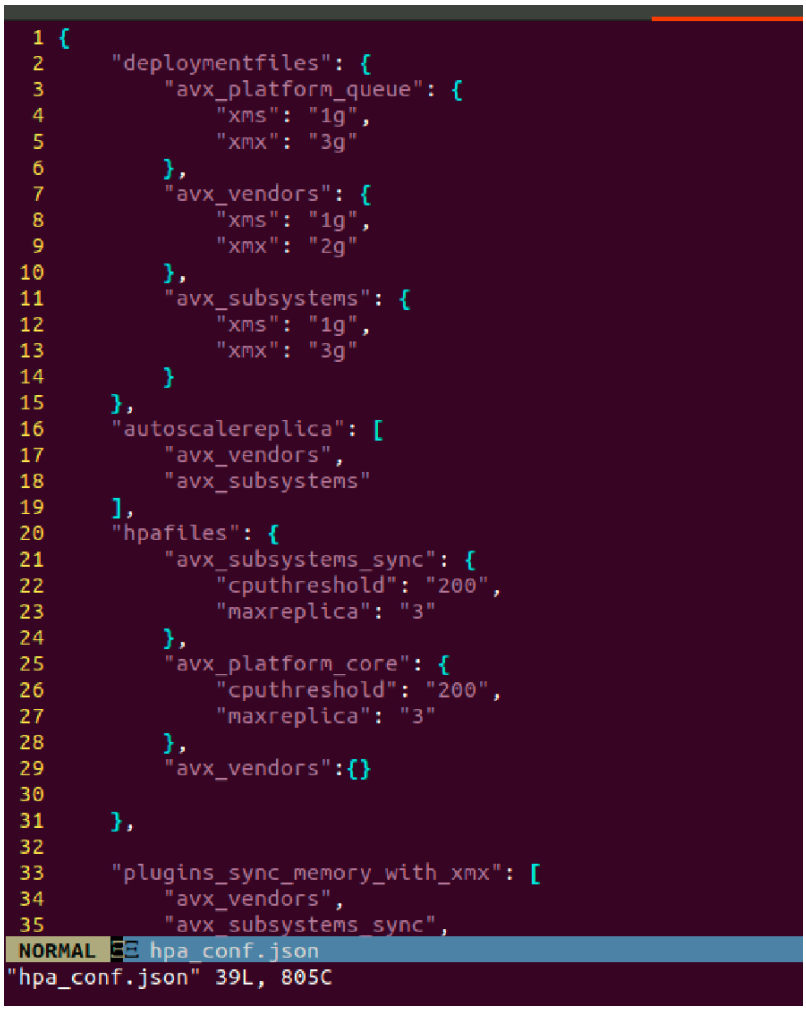


Note: If you have a **hpa_conf.json** file in the scripts directory ignore the below steps and move on to Step 9.

a. Copy the content from **hpa_conf.json.template** file to **hpa_conf.json** by executing the command:

```
cp hpa_conf.json.template hpa_conf.json
```

b. If there are customized values that need to be set for the keys in the **hpa_conf.json** file, configure them accordingly.



c. By default, if the customer does not create the **hpa_conf.json** file before patch, the file will be created using the **hpa_conf.json.template** file.

9. Configurable routing strategy for gateway

> **Note:** Data centers (greater than 60ms). If not applicable, move on to Step 14. This step is applicable only for deployment with high latency between datacenters.

The **OPTIMISE_ROUTING_FOR_LATENCY=TRUE** and **PREFERRED_DEFAULT_DC=<preferred datacenter>** option can be added to the appviewx.conf file (this needs to be added manually before the patch) and can be set to true for deployments/setups where there is a high latency (>50ms) between the data centers/nodes. This will switch the ATI-gateway routing strategy to optimize for latency. The default value for this is *false* unless specified as *true*.

10. The absolute path of the downloaded patch files should be kept ready and a decision on TLS version support should be made, before executing the command `apply_patch.sh`
    - Make a note of the downloaded absolute file path for plugins and add-on tar files
    - Enable TLSv1.0 and TLSv1.1 (Yes/No)
      - It is recommended to select “NO.”
      - Select “YES” only if it is required for the customer.

    > **Note:**
    > - Transport Layer Security (TLS) such as Secure Sockets Layer (SSL), is an encryption protocol intended to keep data secure when being transferred over a network. As of today, only TLS 1.2 and TLS 1.3 are recommended, whereas all other protocol versions have been formally deprecated in 2018 by Apple, Google, Microsoft and Mozilla
    > - AppViewX recommends to choose "NO" to defaults hardened. This will enable TLS 1.2 and above as per global security standards
    > - Reference links:
    >
    >   https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
    >
    >   https://www.sec.gov/oit/announcement/tls1_and_tls1_1_to_be_disabled
    > - Who can opt for "Enable TLSv1.0 and TLSv1.1=YES"?
    >
    >   Customers who use legacy version endpoints to support deprecated TLS version and in the process of migration.

11. Navigate to the <INSTALLER_PATH>/appviewx_kubernetes/scripts directory and execute the command

    ```
    ./apply_patch.sh
    ```

    By default, the patch script works at interactive mode and the following questions will be asked during the process:

a. Verify the list of enabled plugins and their respective data center. After the verification, provide the appropriate input to continue the deployment or exit the process.

```
-bash-4.2$ ./apply_patch.sh
Enable TLSv1.0 and TLSv1.1 (yes/no): no
```

```
Enter the absolute path of Addon tar package downloaded from the AppViewX Release Portal (Press enter to leave it blank): /home/appviewx/new/a
ppviewx_addons_2020.3.FP7.tar.gz
Enter the absolute path of Plugins tar package downloaded from the AppViewX Release Portal (Press enter to leave it blank): /home/appviewx/new
/AppViewX_2020.3.FP7.tar.gz
```

```
Extracting the package..
Successfully extracted package to: /home/appviewx/new/appviewx_kubernetes/scripts/patch/AppViewX_2020.3.0_Latest_Plugins
```

```
ENABLED_PLUGINS
--------------------------------
appviewx_dependencies
avx_commons
avx_crontab
avx_config_server
avx_platform_core
avx_platform_amc
avx_platform_queue
avx_platform_gateway
avx_platform_web
avx_subsystems
avx_vendors
avx_subsystems_sync
avx_platform_report_generator
avx_visual_page_builder
avx_platform_logforwarding
avx_vendor_cert_network_discovery
--------------------------------
ENABLED_PLUGINS AND NAMESPACES
--------------------------------
avx_commons - absecon
avx_crontab - avx
avx_config_server - absecon
avx_platform_core - absecon
avx_platform_amc - absecon
avx_platform_queue - absecon
avx_platform_gateway - absecon
avx_platform_web - absecon
avx_subsystems - absecon
avx_vendors - absecon
avx_subsystems_sync - absecon
avx_platform_report_generator - absecon
avx_visual_page_builder - absecon
avx_platform_logforwarding - absecon
avx_vendor_cert_network_discovery - absecon
--------------------------------

Do you wish to continue (Yes/No)? yes
```

b. MongoDB and Vault backup can be taken before deploying the newer version for rollback, when prompted.

```
Do you wish to take DB backup (Yes/No)?yes
```

c. Old Existing DB Backups can be cleaned.

```
Do you wish to remove Existing DB backup (Yes/No) - Default (No): ?No
```

d. Old Existing plugin backup can be cleaned up.

```
Do you wish to remove Existing plugin backup (Yes/No) - Default (No): ?no
```

12. After successful deployment, the following message will be displayed along with the manual restore commands for rollback. **Kindly wait for a few minutes for the backend process to complete**

```
Patch Process Completed and Plugins are Upgraded.
```

13. In case of any failure during the patch deployment, an automated rollback can be initiated by executing the below commands shown in the image below.

```
Please use following commands to restore:

Restore Plugins:

        1. rm -rf ../yaml//appviewx_plugins && mv /home/appviewx/new/appviewx_kubernetes/scripts/backup_20211108-132805/appviewx_plugins ../y
aml/

Restore Database:

        1. ./mongo_restore.sh /home/appviewx/appviewx/ /home/appviewx/new/appviewx_kubernetes/scripts/../../ config-server /home/appviewx/app
viewx/logs/mongo_backup_Mon_Nov_8_08_10_59_UTC_2021.tar.gz
        2. ./vault_restore.sh -p /home/appviewx/appviewx/logs/vault_backup_Mon_Nov_8_08_11_18_UTC_2021
```

Note: Edit the backup files as required.

14. Trigger the Gateway restart once all plugins have been patched. Step “a” is required and step “b” is applicable only if **avx_platform_gateway_external** plugin is enabled/ up & running

a. Once the patch process is completed execute the command below:

```
kubectl delete pods -n avx $(kubectl get pods -n avx | grep "gateway" | awk '{print $1}') --force
```

b. If external gateway plugin is enabled, the following commands can be executed:

- To verify if the external gateway is running:

```
kubectl get pods -A | grep avx_platform_gateway_external
```

- If Yes (running), execute the below command. If No, ignore the command below.

```
kubectl delete pods -n external-system $(kubectl get pods -n external-system | grep "gateway" | awk '{print $1}') –force
```

Note: At least one input for Plugins and Addons upgrade must be given to proceed with the patch process. Both inputs can be given at the same time as well.

Customers, who have implemented the ACME use case, kindly follow the steps given in the **ACME Workaround Guide** after applying the FP7 or the upcoming FPs.

15. Perform additional validations post the patching process as mentioned below:

- To check pod status and wait until all the pods are in running state, execute the command

```
kubectl get pods –A
```

Chapter 4: Part 2 - Kubernetes Infra Upgrade

1. Check whether all the pods are up and running. All the pods must be in 2/2 running state. Verify by executing the command:

```
kubectl get pods –A
```

2. Navigate to <INSTALLER_PATH>/appviewx_kubernetes/scripts/infra_upgrade directory.
3. Execute the command below

```
./upgrade.sh
```

   During execution of the above command, users will be prompted to enter certain input values, follow the instructions below:

   a. Confirm if some pods are not in running state.
      i. If it is a Prometheus pod, type “yes” to ignore and continue with the upgrade.
      ii. If some other pods are not in running state, fix those issues before continuing the upgrade.
   b. Enter valid Appviewx Sudo user password of all the nodes when prompted.
   c. If ELK is enabled, enter the elastic user password, if requested.
4. After the patch upgrade is done, execute the command:

```
kubectl get pods –A
```

   a. If the upgrade is successful, all the pods in the custom data centers should be up and running.
   b. If a pod is not in the running state but its predecessor (derived from the age of the pod) is up and running, then the latest plugin has failed to deploy. Reach out to AppViewX's support team.
5. To ensure that the Kubernetes upgraded to v1.22.6 successfully, execute the command,

```
kubectl get nodes
```

Chapter 5: Frequently Asked Questions (FAQ)

1. **How is FP9 different from our previous FP's?**

   In FP9, we plan to upgrade our infra, which means we upgrade each and every K8s and third party components to a latest stable version. Whereas in our previous patches, we only patch the avx related components.

2. **How to disable/enable TLS configuration?**

   A configuration parameter **ENABLE_LOWER_TLS** is added in **appviewx.conf**as part of the apply patch from FP7. This provides options to either enable or disable TLS (v1.0 or v1.1) communication between AppViewX and devices after the Java upgrade in FP7.

   • To enable: **ENABLE_LOWER_TLS = TRUE** (when we choose **YES** in the interactive session).

   • To disable: **ENABLE_LOWER_TLS = FALSE**(when we choose **NO** in the interactive session).

   • If a customer wants to change **ENABLE_LOWER_TLS** to **YES** or **NO** after completion of the patch.

   a. Change the option to True or False in **appviewx.conf** file as per the requirement.

   b. Perform the `./plugins_install.sh`

Note: Execute the above commands only after the replicaset has been completely deployed i.e. if it has reached the desired number of replicas and the previous replicaset has been completely terminated. It would generally take 10 minutes after the patch for this to complete. To confirm the same please execute command

```
kubectl get rs -n <datacenter>
```

The command needs to be executed for every datacenter. Verify from the output that the desired number of replicas, current number of replicas, and ready number of replicas are all equal for the latest deployed replicasets.

Chapter 6: Debugging Information

Information on debugging details are mentioned below

1. The **patch_logs.txt** file can be located at <INSTALLER_PATH>/appviewx_kubernetes/scripts
2. If deployment fails with the message: *"scp failed: Upload failed"*, run the commands below:

```
chown -R appviewx:appviewx <installation_path>/plugins
```

```
chown -R appviewx:appviewx <installation_path>/logs
```

> **Note:** The **<installation_path>** is mentioned in the **/appview_kubernetes/scripts/appviewx.conf**file as the parameter INSTALLATION_PATH.

3. The config server pod must be in "Running" state to deploy the plugin. If the config server pod is not in *"Running"* state, the script will terminate with the following error message.
   "Please ensure that config server pod is in running state before applying the patch."
4. To check the status of pods use the command below. If the plugin upgrade is successful, all the pods will be in the running state.

```
kubectl get pods -n <namespace>
```

5. If the helm install is triggered instead of helm upgrade, the following error message is displayed:*"cannot re-use a name that is still in use"*. This is due to a timeout issue while helm chart check is in progress. Fix the issue by re-triggering the following command:

```
scripts/plugins_install.sh
```

```
(and 20 more similar warnings elsewhere)


Error: Error running command 'helm install  --set-string timestamp=2021-08-17T14:59:21Z \
   --set-string appviewx.multi=true  \
   --set common.namespace="{avx}"  \
   --set appviewx.replicas="2"  \
   --set appviewx.nodeAffinity="{us,eu}"  \
   --set appviewx.installation_user=appviewx  \
   --set appviewx.installation_user_id=1000  \
   --set appviewx.appviewx_path=/home/appviewx/appviewx_cluster/  \
   avx-platform-web /home/appviewx/appviewx_binaries/appviewx_kubernetes/yaml/appviewx_plugins/avx_platform_web/chart;
: exit status 1. Output: Error: cannot re-use a name that is still in use
```

Chapter 7: More Information

For the latest, most complete information about known and fixed issues with the AppViewX modules, see the latest revision of the release notes.

To access Software Release Notifications for AppViewX Releases, visit our Help center at https://help.appviewx.com/home. You need to log in to your AppViewX account. From the Help center, search by the specific release number or navigate to Release Portal and choose the release, for example, v20.3.0.

Documentation Feedback

We request you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to *tech-documentation@appviewx.com*

If you are preferred to send feedback through e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable).

Requesting Technical Support

Technical product support is available through AppViewX help support center, request to send an email to *help@appviewx.com*

Self-Help Online Tools and Resources

For quick and easy problem resolution, AppViewX is designed an online self-service portal called the help support center that provides you with the following features:

- Find help support center: https://help.appviewx.com/home
- Find product technical documentation: https://helpcenter.appviewx.com/techdoc/
- Find solutions and answer questions using our Knowledge Base: https://internalkb.appviewx.com/knowledge-base
- Download the latest versions of software: https://release.appviewx.com