appviewX

Install and Upgrade Patch Deployment Guide 2020.3.0 FP10

Version: 2020.3.0

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 guide for Appviewx 2020.3.0 FP10	August, 2022
v1.1	Updated screenshots in the patch deployment guide for Appviewx 2020.3.0 FP10	August, 2022

About this Guide

The purpose of this document is to guide the users for applying patches on AppViewX v2020.3.0 FP10.

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 prerequisites are as follows:

1. Stop all the components and take a VM snapshot of all the nodes using the commands below.

```
cd <appviewx_installer_location>/appviewx_kubernetes/scripts
```

```
./appviewx.sh --stop –all
```

2. Start all the components once the VM snapshots are taken for all the nodes using the commands below.

```
cd <appviewx_installer_location>/appviewx_kubernetes/scripts
```

```
./appviewx.sh --start –all
```

> **Note:** Execution of steps 1 and 2 results in a downtime; ensure to inform customer in advance.

3. Ensure that the node password do not contain special characters such as single quote (‘), double quote (“), and back slash (\).
4. (Recommended step) Proceed with the NTP or Chrony setup during the plugin upgrade. This setup is included in the plugin upgrade. Ensure to get the NTP server details prior to the upgrade. Ignore if already in place.
5. Keep the existing “mtu” value by executing the command:

```
kubectl edit cm calico-config -n kube-system
```

6. Note the CA certificate path if ENABLE_CUSTOM_CERTS=TRUE.
7. Get details of the user id and user group (enter the command `id` to get the details).

```
[appviewx@pe-apvx-31-19 ~]$ id
uid=1000(appviewx) gid=1001(appviewx) groups=1001(appviewx),10(wheel),994(docker) context=unconfined_u:unconfined_r:unconf
ined_t:s0-s0:c0.c1023
```

8. Check details regarding the time synchronization enablement (NTP/Chrony).
9. If the external backup server is enabled to push backups of Mongo and Vault, keep the details of external backup server’s IP address, port, user, and path. Ignore if not enabled.
10. Keep the CLI node password ready.
11. If ELK is enabled, keep the elastic user password ready.

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 FP10.

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: AppViewX Conf File

The following parameters must be configured in the **appviewx.conf** file for the FP10 installation process:

Parameter	Description
API_ADDRESS	Specifies the hostname or IP address of the API server. **For SINGLE NODE:** The value should be empty. **For MULTINODE:** The default should be FQDN OR MASTER IP; If the cluster has a single master, use the IP of that master as the api_address. If the cluster has 3 masters, the api_address var needs to point to the IP of the TCP load balancer(Layer4)
INGRESS_LB_URL INGRESS_LB_PORT	Provide the URL of the load balancer service and port if an external load balancer(VIP) is used for the ingress gateway service.
SSH_PORT	This parameter is used to update the custom SSH port. Change the default port '22' to a custom port before installing the application.
ENABLE_LOWER_TLS	Set ENABLE_LOWER_TLS=True to enable TLSv1.0, TLSv1.1 in the application to manage devices with lower TLS versions.
OPTIMISE_ROUTING_FOR_LATENCY=FALSE PREFERRED_DEFAULT_DC=absecon	This parameter is used mainly if the application is installed across multiple DCs and the latency between the DCs is high. The local routing between the pods can be enabled by setting OPTIMISE_ROUTING_FOR_LATENCY=True and specifying the preferred DC name in PREFERRED_DEFAULT_DC to increase the application performance. *Example:* `OPTIMISE_ROUTING_FOR_LATENCY=True`

Parameter	Description
	`PREFERRED_DEFAULT_DC=absecon`
MTU_VALUE=1350	This option is used to change the MTU value for the calico during the appviewx installation. **Note:** This value should be changed before the application installation.

IPV4POOL_IPIP
 	
IPV4POOL_VXLAN
	This option is used to enable the IPinIP/VXLAN tunneling for calico.
	
	Note:
	• 'Always' should be for any one of the protocols (IPIP or VXLAN), it should not be added for both.
	• This value should be changed before the application installation.
	
	Example:
	
	`IPV4POOL_IPIP=Always`
	
	`IPV4POOL_VXLAN=Never`

SERVICE_SUBNET POD_SUBNET	This option is used to configure the pod and service default IP subnet ranges. **Note:** • The IP range should not conflict with any of the internal IP ranges. • This value should be changed before the application installation.

Parameter	Description

	Example:
	
	`SERVICE_SUBNET=10.96.0.0/12`
	
	`POD_SUBNET=10.244.0.0/16`

CALICO_PORT	This option is used to configure the default calico port. **Note:** This value should be changed before the application installation. *Example:* `CALICO_PORT=179`
SFTP_TRANSFER REMOTE_BACKUP_SERVER REMOTE_BACKUP_SERVER_SSH_PORT REMOTE_BACKUP_SERVER_USER MONGO_BACKUP_PATH VAULT_BACKUP_PATH	This option is used to configure the external SFTP Transfer for Mongo and Vault backup. It enables Passwordless communication between the remote backup server and the appviewx nodes. **Pre-installation:** Set SFTP_TRANSFER to true and configure the below listed variables **Post-installation:** Set SFTP_TRANSFER to true and configure the below listed variables and execute `./sftp_transfer.sh` script from the <appviewx-installer-location>/appviewx_kubernetes/scripts directory. The parameter description is as follows: • SFTP_TRANSFER – Enable/Disable the SFTP transfer. • REMOTE_BACKUP_SERVER – Update the SFTP server IP to store the vault and mongo backups. • REMOTE_BACKUP_SERVER_SSH_PORT – Update the External SFTP server's SSH port in case of a custom SSH port.

Parameter	Description

	• REMOTE_BACKUP_SERVER_USER – Username of the remote backup server.
	• MONGO_BACKUP_PATH – Update the External SFTP location to store the mongodb backup.
	• VAULT_BACKUP_PATH – Update the External SFTP location to store the vault backup.
	
	Example:
	
	`SFTP_TRANSFER=FALSE`
	
	`REMOTE_BACKUP_SERVER=`
	
	`REMOTE_BACKUP_SERVER_SSH_PORT=22`
	
	`REMOTE_BACKUP_SERVER_USER=appviewx`
	
	`MONGO_BACKUP_PATH=/home/appviewx/`
	
	`VAULT_BACKUP_PATH=/home/appviewx/`

ENABLE_CUSTOM_CA_CERTS=FALSE CERTIFICATE_PATHS=/home/appviewx/appviewx/ca-bundle.crt	This option is used to enable custom certs for outbound site communication. Enter the absolute path of the certificate to add to java truststore in the comma delimited format. **Note:** • It is recommended to use CA-signed certificates for better security. • If you still want to go ahead and add any internal CA's or Self-signed ones, do so at your own risk. *Example:* `ENABLE_CUSTOM_CA_CERTS=FALSE`

Parameter	Description
	CERTIFICATE_PATHS=/home/appviewx/appviewx/ca-bundle.crt

Chapter 4: 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.FP10.tar.gz**
   - **appviewx_addons_2020.3.FP10.tar.gz**
   - Download the latest dated script file **(tar.gz)** from release portal, for example - **scripts_FP10_(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

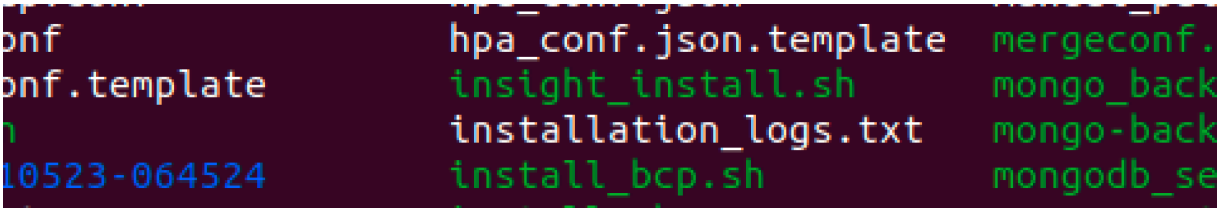
   ```
   kubectl get pods –A
   ```

   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. Untar the scripts using the command

   ```
   tar -xvf scripts.tar.gz
   ```
6. Copy the files from 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/.
     ```
7. Check and replace the **hpa_conf.json.template** file that is present in the scripts directory.

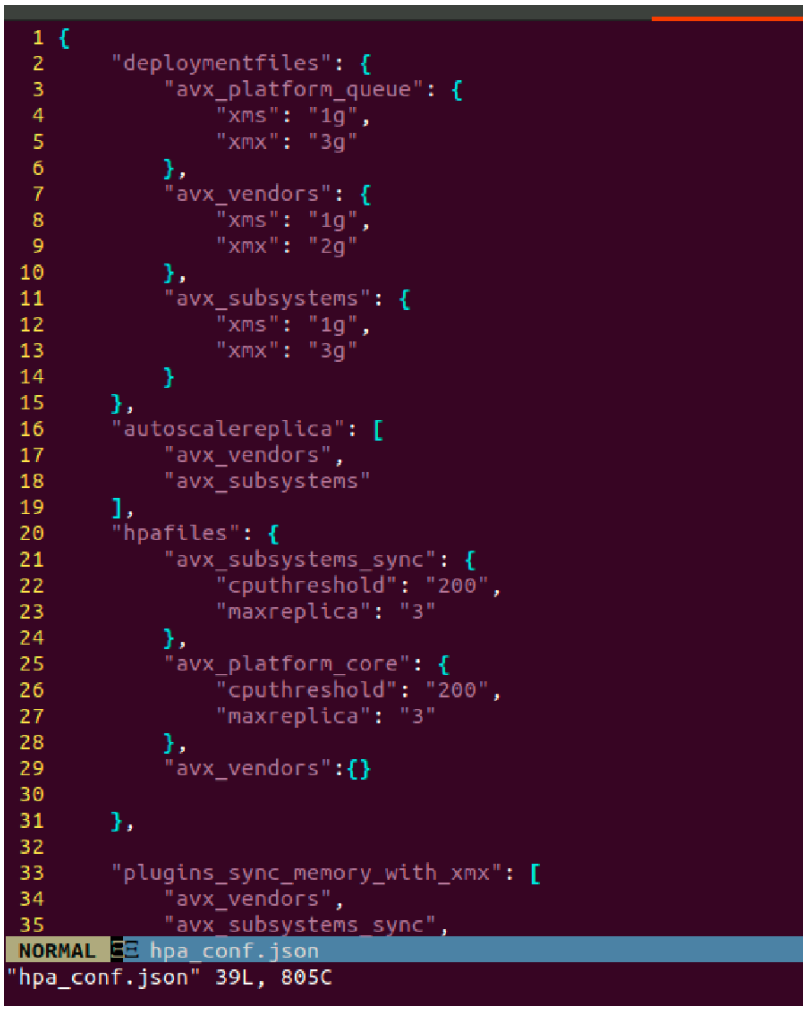


> **Note:** If you have a **hpa_conf.json** file in scripts directory ignore the below steps and move on to Step 9.

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.

8. Configure the datacenter latency optimization

> **Note:** Data centers (greater than 50ms). 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*.

The option to enable routing strategy of the gateway and other components where there is high latency(>50ms) is shown below.

```
# Option to enable local routing incase the latency between the DCs are high
OPTIMISE_ROUTING_FOR_LATENCY=FALSE
PREFERRED_DEFAULT_DC=absecon
```

9. 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.

10. 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:

- **Do you wish to cleanup the existing scripts backup ("yes"/"no"):**

  For pre-FP10 to FP10 patch answer “No”, since there will be no scripts backup. Answer “Yes/No” to remove/keep the existing scripts backups (applicable for hotfixes on top of FP10 and future FPs)

- **Do you wish to backup of the scripts ("yes"(recommended)/"no"):**

  It is recommend to answer “Yes” (the process will take a few minutes depending on the size of the scripts directory).

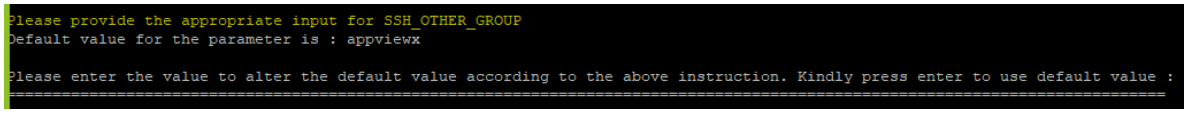
- **Enter the absolute path of the scripts tar package downloaded from the Appviewx Release Portal (Press Enter to leave it blank):**

  In case of a manual sync, press Enter without any answer.

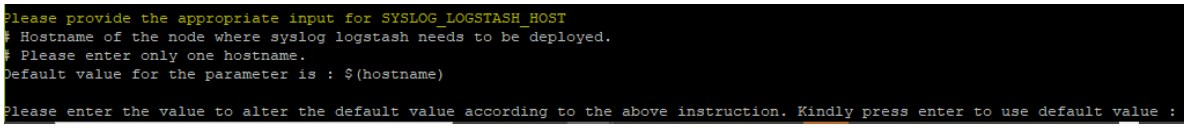
11. Change the default values of newly added **appviewx.conf** parameters, provide the valid input as per the instructions or keep them as default values.
    a. Open a duplicate terminal window and verify the SSH_OTHER_GROUP by executing the command

    ```
    id
    ```

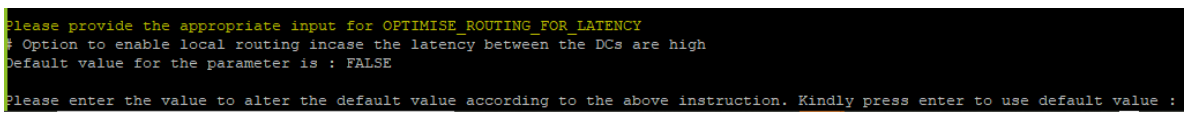
    , leave it blank and press Enter if it is “appviewx”

    b. A new FLAG “SYSLOG_LOGSTASH_HOST” has been introduced in FP10. If SYSLOG=FALSE in existing *appviewx.conf*, press Enter without supplying any answer. If the SYSLOG=TRUE in the existing *appviewx.conf,* enter a valid worker node hostname for SYSLOG_LOGSTASH_HOST.

    c. For the parameter OPTIMISE_ROUTING_FOR_LATENCY if the default value is FALSE, press Enter without supplying any answer. If required, it can be changed by entering the value as TRUE. Read through *datacenter latency optimization* in the earlier section.

d. For the PREFERRED_DEFAULT_DC parameter, it is recommended to enter any primary DC. The default value **absecon** is called out from the FP10 *appviewx.conf.template* file. However, this parameter is applicable only if the previous parameter OPTIMISE_ROUTING_FOR_LATENCY is set to TRUE.

```
Please provide the appropriate input for PREFERRED_DEFAULT_DC
Default value for the parameter is : absecon

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value : montreal
```

e. To know the MTU_VALUE, launch a duplicate CLI/terminal window and check the existing **mtu** value by executing the command:

```
kubectl edit cm calico-config -n kube-system
```

input the same value and press Enter.

```
Please provide the appropriate input for MTU_VALUE
# Configure the mtu, ipip and vxlan values
Default value for the parameter is : 1350

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value : 1440
```

f. For IPV4POOL_IPIP, if the default value is **Always**, press Enter without supplying any answer (**Note**: For Azure deployment the value should be **Never**).

```
Please provide the appropriate input for IPV4POOL_IPIP
Default value for the parameter is : Always

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

g. For IPV4POOL_VXLAN keep the default value as **Never** and press Enter without supplying any answer (**Note**: Azure deployment it should be **Always**).

```
Please provide the appropriate input for IPV4POOL_VXLAN
Default value for the parameter is : Never

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

h. For SERVICE_SUBNET and POD_SUBNET, obtain the existing kube service subnet range from <Installer_path>/appviewx_kubernetes/configs/kube using the command below:

```
vi kubeadm-config.yaml.tpl
```

Service Subnet Range

```
Please provide the appropriate input for SERVICE_SUBNET
# Configure the pod and service subnet range
Default value for the parameter is : 10.96.0.0/12

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value : 10.198.0.0/16
```

POD Subnet Range

```
Please provide the appropriate input for POD_SUBNET
Default value for the parameter is : 10.244.0.0/16

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value : 10.199.0.0/16
```

i. The default value for CALICO BGP port is 179, press Enter without supplying any answer. It is recommended to leave it as the default unless a custom port is used in the initial deployment/ installation.

```
Please provide the appropriate input for CALICO_PORT
# Configure the calico port
Default value for the parameter is : 179

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

12. The next set of questions is applicable if an external backup server is already available to store a copy of the Mongo & Vault backups. If not, ignore it for now and setup it up later with an Appviewx support engineer. Press Enter for all the values listed below without supplying any answer.

a. SFTP_TRANSFER

```
Please provide the appropriate input for SFTP_TRANSFER
# Configure the SFTP Transfer for Mongo and Vault backup
Default value for the parameter is : FALSE

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

b. REMOTE_BACKUP_SERVER

```
Please provide the appropriate input for REMOTE_BACKUP_SERVER
Default value for the parameter is :

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

c. REMOTE_BACKUP_SERVER_SSH_PORT

```
Please provide the appropriate input for REMOTE_BACKUP_SERVER_SSH_PORT
Default value for the parameter is : 22

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

d. REMOTE_BACKUP_SERVER_USER

```
Please provide the appropriate input for REMOTE_BACKUP_SERVER_USER
Default value for the parameter is : appviewx

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

e. MONGO_BACKUP_PATH

```
Please provide the appropriate input for MONGO_BACKUP_PATH
Default value for the parameter is : /home/appviewx/

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

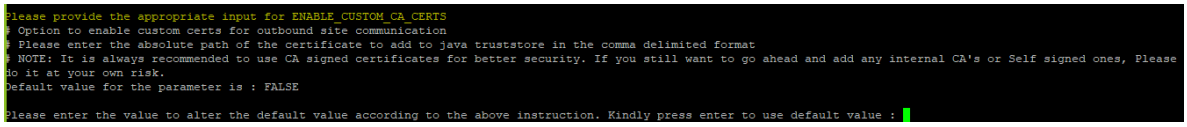
f. VAULT_BACKUP_PATH

```
Please provide the appropriate input for VAULT_BACKUP_PATH
Default value for the parameter is : /home/appviewx/

Please enter the value to alter the default value according to the above instruction. Kindly press enter to use default value :
```

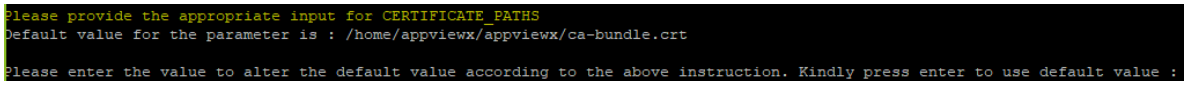
Note: The path mentioned in the Mongo and Vault parameters is the location of the remote backup server where the backup is stored.

g. ENABLE_CUSTOM_CA_CERTS

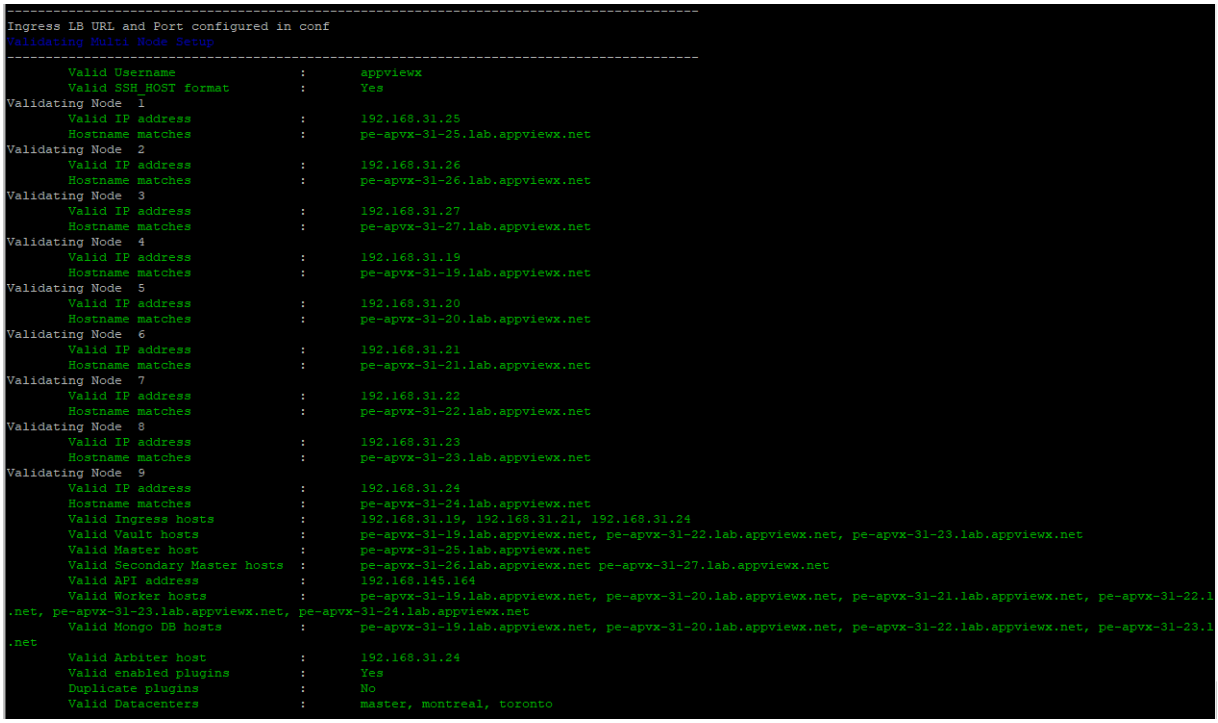


Note: The following security feature is introduced to meet input validations when an external certificate is used for authentication (Example: Client certificate used to authenticate a CA connection settings). In this case, a public key material is needed with the Appviewx java keystore to validate the trust chain of the authentication certificate.

h. CERTIFICATE_PATHS



13. Press Enter to continue with the patching process.



```
--------------------------------------------------------------------------------
secret/insight-syslog-cred created
Error from server (AlreadyExists): secrets "insight-syslog-cred" already exists
Error from server (AlreadyExists): secrets "insight-syslog-cred" already exists
secret/insight-syslog-cred created
Error from server (AlreadyExists): secrets "insight-syslog-cred" already exists
Error from server (AlreadyExists): secrets "insight-syslog-cred" already exists
/home/appviewx/appviewx//temp/avx-jobs_common_config.yaml
configmap/avx-common-config configured
/home/appviewx/appviewx//temp/avx_common_config.yaml
configmap/avx-common-config configured
/home/appviewx/appviewx//temp/external-system_common_config.yaml
configmap/avx-common-config configured
/home/appviewx/appviewx//temp/kube-system_common_config.yaml
configmap/avx-common-config configured
/home/appviewx/appviewx//temp/master_common_config.yaml
configmap/avx-common-config configured
/home/appviewx/appviewx//temp/montreal_common_config.yaml
configmap/avx-common-config configured
/home/appviewx/appviewx//temp/toronto_common_config.yaml
configmap/avx-common-config configured
Enter the absolute path of Addon tar package downloaded from the AppViewX Release Portal (Press enter to leave it blank):
```

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. (Supply the answer for the below question as applicable – This question may not be displayed if already answered in a previous fix pack patching)

```
-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/avx_binaries/FP10/appviewx_addo
ns_2020.3.FP10.tar.gz
Enter the absolute path of Plugins tar package downloaded from the AppViewX Release Portal (Press enter to leave it blank): /home/appviewx/avx_binaries/FP10/AppViewX_20
20.3.FP10.tar.gz
```

```
Successfully extracted package to: /home/appviewx/avx_binaries/dossier_installation/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_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
avx_vendor_cert_acme_agent
avx_vendor_cert_intune_agent
--------------------------------
ENABLED_PLUGINS AND NAMESPACES
--------------------------------
avx_commons - montreal,toronto
avx_crontab - avx
avx_config_server - montreal,toronto
avx_platform_core - montreal,toronto
avx_platform_queue - montreal,toronto
avx_platform_gateway - montreal,toronto
avx_platform_web - montreal,toronto
avx_subsystems - montreal,toronto
avx_vendors - montreal,toronto
avx_subsystems_sync - montreal,toronto
avx_platform_report_generator - montreal,toronto
avx_visual_page_builder - montreal,toronto
avx_platform_logforwarding - montreal,toronto
avx_vendor_cert_network_discovery - montreal,toronto
avx_vendor_cert_acme_agent - montreal,toronto
avx_vendor_cert_intune_agent - montreal,toronto
--------------------------------

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

```
Do you wish to continue to install the security updates ? (Yes(recommended)/No)?yes
```

b. The MongoDB and Vault backups can be taken before deploying the newer version for rollback.

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

c. Old existing DB backup 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.

```
Reading the package for plugins in: /home/appviewx/avx_binaries/dossier_installation/appviewx_kubernetes/scripts/patch/AppViewX_2020.3.0_Latest_Plugins

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

```
Enabling custom keystores detected

*********************************************************************************************
*  It is always recommended to use CA signed certificates for better security.    *
*  If you still want to go ahead and add any internal CA's or Self signed ones,   *
*  Please do it at your own risk.                                                 *
*********************************************************************************************
Do you want to continue? (Yes/No) :
```

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

Custom keys added to the keystore for montreal!

Custom keys added to the keystore for toronto!
```

14. 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.**

```
Apply complete! Resources: 783 added, 0 changed, 0 destroyed.
deployment.apps/avx-crontab patched (no change)
deployment.apps/avx-crontab scaled
warning: Immediate deletion does not wait for confirmation that the running resource has been terminated. The resource may continue to run on the cluster indefinitely.
pod "avx-crontab-57fc6f597b-6cbxr" force deleted
deployment.apps/avx-crontab scaled
mongo-routerdb-0                                  2/2     Terminating       0          63m
mongo-routerdb-1                                  2/2     Terminating       0          63m
mongo-routerdb-2                                  2/2     Terminating       0          63m
statefulset.apps/vault patched (no change)
pe-apvx-31-25.lab.appviewx.net master
pe-apvx-31-26.lab.appviewx.net master
pe-apvx-31-27.lab.appviewx.net master
pe-apvx-31-19.lab.appviewx.net montreal
pe-apvx-31-20.lab.appviewx.net montreal
pe-apvx-31-21.lab.appviewx.net montreal
pe-apvx-31-22.lab.appviewx.net toronto
pe-apvx-31-23.lab.appviewx.net toronto
pe-apvx-31-24.lab.appviewx.net toronto
OPTIMISE_ROUTING_FOR_LATENCY is not enabled in the appviewx.conf(Note: applicable only for the high latency environments)..ignoring..

Patch Process Completed and Plugins are Upgraded.

cmd to execute ./syncconf.sh /home/appviewx/appviewx/ /home/appviewx/avx_binaries/FP10/AppViewX_2020.3.FP10.tar.gz
```

15. To setup NTP or Chrony sever, provide the appropriate input. Enter “no” if the NTP/Chrony is already configured. This will retain the existing NTP/Chrony configurations.

```
Do you want to configure the NTP/Chrony?[Yes|No](Recommended 'Yes' and ignore if already configured): no
Exiting!
```

```
Do you want to configure the NTP/Chrony?[Yes|No](Recommended 'Yes' and ignore if already configured): yes
Enter the time sync type[ntp/chrony](default chrony): ntp
```

16. 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/installer/appviewx_kubernetes/scripts/../backups/backup_20220726-154931/appviewx_plugins ../yaml/

Restore Database:

        1. ./mongo_restore.sh /home/appviewx/installer/appviewx_kubernetes/scripts/../..//appviewx_kubernetes/mongo_backup/mongo_backup_Tue_Jul_26_15_52_10_IST_2022.tar.gz
        2. ./vault_restore.sh -p /home/appviewx/installer/appviewx_kubernetes/scripts/../..//appviewx_kubernetes/vault_backup/vault_backup_Tue_Jul_26_15_52_24_IST_2022
```

> **Note:** Edit the backup files as required.

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

18. Perform additional validations post the patching process as mentioned below:
    a. To check pod status and wait until all the pods are in running state, execute the command

```
kubectl get pods –A
```

    b. To check whether the date and time of the nodes are in sync, execute the command below from the **scripts directory**.

```
./appviewx.sh --run-on-all "timedatectl"
```

19. The patching logs are saved in <Installer_path>appviewx_kubernetes/logs

Chapter 5: 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.
d. If INSIGHT is enabled, provide the input as yes/no to take a backup of the statistical data.

4. After the patch upgrade is done, execute the command:

```
kubectl get pods –A
```

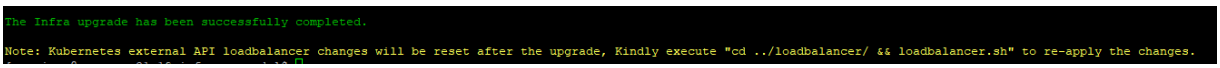
a. If the upgrade is successful, all the pods in the custom data centers should be up and running.
b. If a pod is not in the running state but its predecessor (derived from the age of the pod) is up and running, then the latest plugin has failed to deploy. Reach out to AppViewX's support team.

5. In case the upgrade stops involuntarily, execute command

```
./resume_upgrade.sh
```

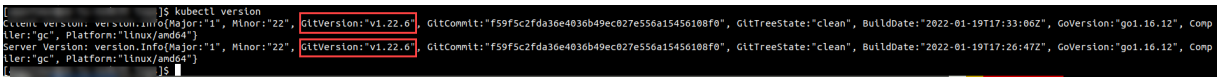
6. If the Kube API (Kube master Load balancer) has been configured, execute the command as prompted below. Ensure to keep the node CLI password ready.

```
cd ../loadbalancer/ &&loadbalancer.sh
```



7. To ensure that the Kubernetes is upgraded to v1.22.6 successfully, execute the command:

```
kubectl version
```



8. The infra upgrade logs are available under in <Installer_path /appviewx_kubernetes/scripts/infra_upgrade and the logs file is a hidden file.

Chapter 6: Frequently Asked Questions (FAQ)

1. **How is FP10 different from our previous FP's?**

   In FP10, we plan to upgrade our infra, which means we upgrade each and every K8s and third party components to a latest stable version which is similar to FP6. Whereas in our applications patches, we only patch the avx related components.

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

   In FP10, we plan to upgrade our infra, which means we upgrade each and every K8s and third party components to a latest stable version which is similar to FP6. Whereas in our applications patches, we only patch the avx related components.

   - 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 7: 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. To check the status of pods use the command below.

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

   If the plugin upgrade is successful, all the pods will be in the *"Running"* state.

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

```
scripts/plugins_install.sh
```

Chapter 8: 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