Avaya Analytics for Oceana - Release 4.1.0.1

Avaya_Analytics_4.1.0.1_078_004 ReadMe

Issue Date (DD/MM/YYYY): 24/05/2021

Patch ID: Avaya_Analytics_4.1.0.1_078_004
Patch Type: Bug Fix

Application Name: Avaya Analytics for Oceana
Product version: 4.1.0.1
Component versions:

Analytics	**Orca chart**	5.1.078*
	MSTR chart	0.1.266
Required CSP	**CSP Version**	1.1.0.2.116001
	CCM Version	1.1.0.2.116001

NOTE: This is a mandatory patch.
The main reason for this patch is to allow for the rotation of internal certificates that will expire a certain number of days after initial deployment of the cluster rendering the system unusable and requiring a reinstall.

Note:
The build number (e.g. 5.1.xxx below) that shows up in version checks on the server is an internal build number.

Product	Version	InstanceId	Health
Analytics	5.1.xxx	orca	–

The patch version is not displayed, it must be deduced from orca chart version and release notes.
e.g. Orca chart = 5.1.xxx
Release = 4.1.0.1
Patch number = 999
Patch Name = Avaya_Analytics_4.1.0.1_xxx_999

Patch Install Steps

This table describes the steps required for each of the supported deployment paths. Links to the appropriate section describing the steps are included.

Install Path	Steps Required
Fresh Install	Fresh Installs
Upgrade 4.0.0.1 Patch 6+ to 4.1.0.1 Patch	4.0.0.1 -> 4.1.0.1 Upgrades
Upgrade 4.1 Patch 1+ to 4.1.0.1 Patch	4.1.0.0 -> 4.1.0.1 Upgrades
Upgrade 4.1.0.1 GA or 4.1.0.1 GA + patch to 4.1.0.1 Patch	Upgrade Cluster Control Manager Upgrade Avaya Analytics Cluster Upgrade Avaya Analytics Services Post Installation Instructions

Fresh Installs

This patch may be used to perform a fresh install.

1. Review the Deploying Avaya Analytics for Oceana guide and follow steps in "Upgrading Avaya Analytics chapter.
2. Do not use install steps from this readme.
3. **Use the Deployment spreadsheet available with this patch instead of the GA version.**
4. Use the ova delivered with this patch for fresh installs only.
5. This will result in GA software and all software delivered in patches up to current patch being installed.

4.0.0.1 -> 4.1.0.1 Upgrades

This patch may be used to perform an upgrade from a 4.0.0.1 patch 6+ install to the latest 4.1.0.1 patch level.

1. Review the Deploying Avaya Analytics for Oceana guide and follow all install steps from there.
2. Before installing this patch ensure the Monitoring Scripts outlined in PSN005742u are installed. Use the ***checkInfra*** script to check vCenter credentials, configuration and network connectivity.
3. Do not use install steps from this readme.
4. Do run the Post Installation Instructions where relevant.
5. **Use the Deployment spreadsheet available with this patch instead of the GA version.**
6. This will result in GA software and all software delivered in patches up to current patch being installed.

4.1.0.0 -> 4.1.0.1 Upgrades

This patch may be used to perform an upgrade from a 4.1.0.0 patch 1+ install to the latest 4.1.0.1 patch level.

1. Review the Deploying Avaya Analytics for Oceana guide and follow all install steps from there.
2. Before installing this patch ensure the Monitoring Scripts outlined in PSN005742u are installed. Use the ***checkInfra*** script to check vCenter credentials, configuration and network connectivity.
3. Do not use install steps from this readme.
4. Do run the Post Installation Instructions where relevant.
5. **Use the Deployment spreadsheet available with this patch instead of the GA version.**
6. This will result in GA software and all software delivered in patches up to current patch being installed.

Installation Instructions

General

The main reason for this patch is to allow for the rotation of internal certificates that will expire a certain number of days after initial deployment of the cluster rendering the system unusable and requiring a reinstall.

This patch includes:

- A utility is provided to give the ability to rotate platform certificates during a maintenance window. The Common Services cluster contains internal platform certificates. These certificates expire anywhere from 365-825 days after the initial deployment of the cluster. After the certificates are rotated, the certificates have a lifespan of 825 days. If the certificates expire, the cluster becomes unusable and will need to be reinstalled.
- Alarms indicating that rotation is required for the certificates. The alarm type depends on when the certificates expire.
    - Warning alarm displays every 5 days if the certificates expire in 31 to 60 days.
    - Major alarm displays every 5 days if the certificates expire in 15 to 30 days.
    - Critical alarm displays every day if the certificates expire in 10 days or less.
- Script to rotate internal service certificates manually. CSP also contains internal service certificates. Services using certificates installed during solution deployment will expire 2 years after initial installation. These certificates must be manually renewed, and services restarted prior to their expiration.
- Script to check expiration of internal service certificates.
- Agent configuration report handling of unassigned channel types.
- Reduce retention period on Kafka Open Interface's dynamic topic.

Current Active Line-up

Analytics 4.1.0.1 follows a cumulative patch line-up. Unless otherwise stated this patch rolls up all previous patches.

Patch Install Timings

A maintenance window is required to perform a patch update. Rolling updates are not currently supported. No contact center activity can occur during this window.

The following timings are indicative and approximate timings to help better plan the maintenance window. These timings may vary based network bandwidth, hardware capacity, etc.

Install Step	Approximate Timing		
	4.0.0.1 -> 4.1.0.1	4.1.0.0 -> 4.1.0.1	4.1.0.1 -> 4.1.0.1

Upgrade Cluster Control Manager	0.5-1 hour	0.5-1 hour	0.5-1 hour
Upgrade Avaya Analytics Cluster	1-2 hours	1-2 hours	1-2 hours
Upgrade Avaya Analytics Services	3-4 hours	15-30 minutes	15-30 minutes
rotate-cluster-certificates	2 hours	2 hours	2 hours

A similar amount of time is required to rollback a patch if that is deemed necessary.

Pre-installation instructions

1. Before installing this patch ensure you take a database backup.
   - Take full DB backup using the Analytics control script.
     - See section Configuring database backups in Chapter: Avaya Analytics Maintenance of the Maintaining and Troubleshooting Avaya Analytics for Oceana guide.
   - Once completed, logon to the DB pod using:
     - `kubectl exec -it crunchy-primary-service-orca-dbmgr-0 -- //bin/bash`
     - Now logged into the Database Pod
   - Change directory to the backup folder using:
     - `cd pgdata/full_backup/`
   - Compress the backup file using:
     - `tar -czvf <your backup file name>.tar.gz <your backup file name>.bkp`
   - Transfer the compressed backup file to the CCM using:
     - `scp <your backup file name>.tar.gz cust@<CCM IP>:<Desired Directory>/<your backup file name>.tar.gz`
   - Enter the customer account user password when prompted
   - Log off the pod using:
     - `exit`
   - Copy the backup to secure location.

2. Before installing this patch ensure all custom reports have been archived.
   - 4.0.0.1 Method
     - Run ccm release orca analytics
     - Select 4. Historical Reporting
     - Select 7. Backup Metadata
     - Wait for the backup to finish
     - Press b for back
     - Select 4. Historical Reporting
     - Select 8. Export Backups
     - Wait for export to finish
     - Press q to quit
     - Verify that the backup is now located in the /home/<customer_account_login>/historical_md_backups/ directory on CCM.
   - 4.1.0.0 / 4.1.0.1 Method
     - Refer to Using Avaya Analytics Reports for Avaya Oceana guide, section “Exporting web objects”

3. Before installing this patch ensure the following credentials are still valid.
   - Harbor
   - vCenter

4. Before installing this patch ensure the Monitoring Scripts outlined in PSN005742u are installed.
   Use the ***checkInfra*** script to check vCenter credentials, configuration and network connectivity.

5. Preparing the deployment spreadsheet
   a. Use spreadsheet delivered with this patch as primary spreadsheet.
   b. Enable the macros before you start editing the worksheets.

c. If latest spreadsheet used for earlier deployment and/or patches is available retrieve that and copy to a location that you can access from your desktop.
d. Open current patch spreadsheet.
e. Click the Deployment Properties tab.
f. To copy your configuration from the previous version of the deployment spreadsheet click Load Previous Configuration Values.
g. To import the file from your local machine, browse for the file and click Open.
h. After the spreadsheet is updated, review the all the configurable fields and update any value that is incorrect or missing.

NOTE: The key configurable fields are marked in orange in the spreadsheet. The corresponding rows describe the information that you must enter in the respective fields. If required review Chapter 5: "Planning and preconfiguration", of the Deploying Avaya Analytics for Oceana guide, section "Avaya Analytics™ deployment spreadsheet overview" for instruction on how to complete the spreadsheet.

6. Take VM Snapshot of CCM
   - Login to vCenter managing the Analytics Cluster and take a virtual machine snapshot of the Cluster Control Manager.
     NOTE: The recommendation is to avoid using a snapshot for more than 72 hours to avoid risking performance degradation of the virtual machine as well as the ESXi host.

7. Remove previous version of Async

NOTE: Only Required if Async is installed. `ccm status` command can be used to check.
   - Refer to "Removing the previous version of Async Messaging" section of Deploying Avaya Oceana guide for instructions.

8. Manage services' certificates **before** performing an upgrade
   1. Deploy services' certificate management script.
      i. Download the CSPPatch_renewServiceCertificates.bin from PLDS and transfer this file to the Cluster Control Manager using the customer account and place it in the home directory (eg. /home/<customer account>)
      ii. Patch install instructions

          As the root user, grant execute permissions to the downloaded binary file and run it from the home directory to install the patch.
          - `chmod +x CSPPatch_renewServiceCertificates.bin`
          - `./CSPPatch_renewServiceCertificates.bin`

      iii. The script will display information related to the patch and will wait for user input to continue. If user response is to continue, Avaya EULA is displayed. Once EULA is accepted the patch is deployed.
      iv. Patch installation logs located in /var/log/avaya/ccm/patch.log.

          Deployment of the patch does not affect any of the services running in the cluster.

          This patch will install one command renewClusterCertificates on the CCM. Once the patch is installed as root, a non-root user can log in to CCM and execute the command. Command logs located in /var/log/avaya/ccm/ccm-main.log.

   2. Check the expiration of services' certificates
      - Command

        - `renewServiceCertificates --checkExpiration`
    - Purpose
        - Determine when the services' certificates will expire causing loss of service functionality.

3. Renew services' certificates **before** performing an upgrade
    - Command
        - `renewServiceCertificates`
    - Purpose
        - Renew services' certificates managed by the Certificate Manger service.
        - These renewed certificates will begin being utilised by the services after the cluster has been upgraded.
        - **NOTE:** The user is prompted to confirm that an upgrade will take place after running this command. Confirmation is needed to continue with the command. The command will take approximately 5 minutes to run.

Upgrade Cluster Control Manager

Before You Begin

Ensure the correct installation method is chosen. This will most likely be the method used at the original installation time.

Online Procedure:

1. Connect to the Cluster Control Manager (CCM) using the customer account login.
2. Create upgrade-config.yaml file

   ```
   vi /home/<customer account login>/upgrade-config.yaml
   ```

   `<customer account login>` should be replaced by correct login, which has been used to connect to CCM at the step 1).
   For example, if customer account login is cust then

   ```
   vi /home/cust/upgrade-config.yaml
   ```

   Add the following strings:

   ```
   system: <CCM-version>
   common_services_product_version: <CSP-version>
   ```

   Save the file.
   Note: CCM-version and CSP-version are in table on first page of this document

3. From the directory on CCM that contains the upgrade-config.yaml file, enter the following command:
   `screen`
   The screen utility allows the upgrade to run in the background.
   Important**:** You must perform this procedure
4. Begin the upgrade of the CCM by running the following command:

   ```
   ccm upgrade system upgrade-config.yaml
   ```

5. If you are upgrading from Release 1.1 to a later version, when prompted to perform a backup, enter y or n.
   If you enter y, then a backup runs after the upgrade is complete. You will be prompted for a password, which you will need for the restore operation. The backup takes approximately 5 to 10 minutes to complete. The backup file is located at /var/avaya/artifactCache/.

6. When prompted
   a. Enter your Avaya SSO credentials
   b. Accept the EULA
   c. Confirm the warning regarding the recommendation of a snapshot for reversion as well as acknowledgement that the CCM will be rebooted after the upgrade is applied.
   The reboot takes place approximately two minutes after the upgrade completes.

IMPORTANT: if a snapshot has not been taken, enter “no” and return to the section “Before you Begin” to confirm all steps have been completed before continuing.

d. The CCM upgrade will continue and takes about 15-20 minutes to complete. Progress may be monitored on the screen session or by viewing /var/log/avaya/ccm/upgrade.log. Once complete, the upgrade utility will exit and the CCM will be automatically rebooted.

   IMPORTANT: if the ccm upgrade command fails, resolve the issue causing the failure and restart the upgrade. Contact Avaya Support if the failure condition cannot be corrected.

7. Once the CCM is reachable, login using the customer account.
8. Verify the software version of the CCM has been updated by running:
   `swversion`

   The Cluster Control Manager will report as outlined in table on first page of this Readme.

9. The CCM upgrade is now complete. Proceed with the “Upgrade of the Analytics Cluster”

Offline Procedure

To upgrade Cluster Control Manager (CCM), you must download the CCM upgrade Docker image to your laptop or PC and then upload the image on CCM. Use the ccm-agn-ctl container for the downloading and uploading process.

Downloading the Cluster Control Manager upgrade Docker image

Before you begin you must have:

- Valid Avaya SSO credentials.
- A functional ccm-agn-ctl container on your laptop.

1. On the command line of the ccm-agn-ctl container, change the directories to the download directory at `cd /root/downloads`.
2. Create an image directory - `mkdir images`.
3. Change to the images directory - `cd images`.
4. To log in to harbor.avaya.com, run the following command:
   `docker login harbor.avaya.com`
5. Run the following command:
   `docker pull harbor.avaya.com/flex/ccmupgrade:<ccm-upgrade-version>`, where the ccm upgrade version is the version of the ccmupgrade package.
   For example: docker pull harbor.avaya.com/flex/ccmupgrade:1.1.0.1.95007.
6. To log out from harbor.avaya.com, run the following command:
   `docker logout harbor.avaya.com`

Uploading the Cluster Control Manager upgrade Docker image

Before you begin you must download the CCM upgrade Docker image.

1. To tag the CCM upgrade Docker image for the CCM registry, do the following:
    a. To obtain the name of the ccm upgrade Avaya Harbor tagged image for re-tagging, run the following command:
    `docker images --format '{{.Repository}}:{{.Tag}}' | grep ccmupgrade`
    b. To apply the new tag, run the following command:
    `docker tag <harbor-tag> <ccm-tag>`
    Note:
    - The tag is in the following format: <RegistryFQDN:PORT>/flex/image:version. If the port is 443, you can omit typing the port number.
    - The <harbor-tag> tag is part of the Avaya Harbor Docker Registry, which is harbor.avaya.com/flex/<image:version>
      This tag is the name you obtained in the previous step.
    - The <ccm-tag> tag is part of the local CCM Docker Registry, which is <CCM26FQDN>:5010/flex/<image:version>
2. To obtain the CCM tagged images to push to the CCM registry, run the following command:
   `docker images --format '{{.Repository}}:{{.Tag}}' | grep :5010 |grep ccmupgrade`
3. To get a Docker login for the CCM local Docker registry, run the following command:
   docker login <CCM-FQDN>:5010, where CCM-FQDN is the FQDN of CCM.
4. To push the CCM tagged images to the CCM registry, run the following command:
   `docker push <image-tag-name>`
5. When prompted, enter the username and password of the agn-ctl setup.
6. Log out from Docker using the following command:
   `docker logout <CCM-FQDN>:5010`, where CCM-FQDN is the FQDN of CCM.
7. **(Optional)** To remove the Avaya Harbor tagged images, run the following command:
   `docker rmi <harbor-tag>`
   The <harbor-tag> tag is part of the Avaya Harbor Docker Registry, which is harbor.avaya.com/flex/<image:version>

   The CCM local Docker registry is ready for a CCM upgrade.

Upgrading Cluster Control Manager

Before you begin

- Download the CCM upgrade Docker image to your laptop or PC and
- Upload the CCM upgrade Docker image to CCM

1. On the CCM console, create the CCM upgrade file named upgrade-config.yaml and add the following strings:

```
system: <CCM-version>
common_services_product_version: <CSP-version>
```

Save the file.

Note: CCM-version and CSP-version are in table on first page of this document.

2. From the directory on CCM that contains the upgrade-config.yaml file, run the following command:

   `screen`

   The screen utility allows the upgrade to run in the background.

3. To start the upgrade, run the following command:

   ```
   ccm upgrade system upgrade.yaml
   ```

4. If you are upgrading from Release 1.1 to a later version, when prompted to perform a backup, enter y or n.

   If you enter y, then a backup runs after the upgrade is complete. You will be prompted for a password, which you will need for the restore operation. The backup takes approximately 5 to 10 minutes to complete. The backup file is located at /var/avaya/artifactCache/.

5. When prompted
   a. Enter the credentials, type the CCM local registry username and password.
   b. Accept the EULA
   c. Confirm the warning regarding the recommendation of a snapshot for reversion as well as acknowledgement that the CCM will be rebooted after the upgrade is applied.
      The reboot takes place approximately two minutes after the upgrade completes.

Upgrade Avaya Analytics Cluster

Before you begin:

1. If required ensure the upgrade of the Cluster Control Manager has completed successfully.
2. Verify the operational state of the Avaya Analytics Cluster. Refer to **Chapter 15: Post-installation verification** from *Deploying Avaya Analytics for Avaya Oceana*
3. Once the cluster has been confirmed to be in a healthy and operational state continue with the upgrade procedure below

Ensure the correct installation method is chosen. This will most likely be the method used at the original installation time.

Online Procedure:

1. Connect to the Cluster Control Manager, as the customer account login.

2. From the directory on CCM that contains the updated Analytics Excel Spreadsheet file, enter the following command:
   `screen`
   The screen utility allows the upgrade to run in the background.

3. Run the following command to begin the upgrade of the Avaya Analytics cluster
   - `ccm upgrade spec <solution spreadsheet name>.xlsm --infra`

   If the Prometheus pod is not starting or an Async pods in a 0/1 Ready state and either of these cause the upgrade to not complete, then the validation checks on these pods can be skipped by adding the `--force` option to the end of the command

4. When prompted:
   a. Enter vCenter credentials
   b. Enter Avaya SSO credentials
   c. Confirm the cluster upgrade to the new version specified in the solution spreadsheet
   d. Accept the EULA.
   e. Confirm Upgrade

5. Run the following command to monitor the progress of the upgrade: `tail -f /var/log/avaya/ccm/patch-<timestamp>.log`

6. Once the upgrade is complete. Verify the software version of the Analytics cluster by running: `swversion`
   The cluster version should be updated and match what is defined in the solution spreadsheet.

7. Confirm the operational state of the Analytics cluster. Run the following commands:
   - `ccm smoke-test`
   - `ccm status --pod-details`

   The pods might not be operational immediately after the upgrade. Continue running these

commands periodically at 10 minute intervals until all pods are running. If these tests continue to fail after 30 minutes, contact Avaya support personnel for assistance.

8. The upgrade of the Avaya Analytics cluster is complete. Proceed with the "Upgrade of the Avaya Analytics Services"

Offline Procedure:

Downloading Avaya Analytics chart and images

Before you begin you must have:

- Valid Avaya SSO credentials.
- A functional ccm-agn-ctl container on your laptop.

1. On your Windows PC or client computer, save the Analytics Excel Spreadsheet in c:\avaya\downloads.
   Note: Windows and the CCM Controller container share a mount point, which are c:\avaya\downloads and /root/downloads respectively.
2. In the ccm-agn-ctl container, run `cd/root/downloads`.
3. To download the Avaya Analytics™ charts and images from the Avaya repository, run the following command:
   `agn download <solution spreadsheet name>.xlsm`
4. When requested enter credentials.
   The agn script processes the excel spreadsheet and the Avaya Analytics™ charts and docker images start downloading. The ccm-agn-ctl container displays an Image Pull Report when the download is complete.
5. To view a list of the downloaded images, run the following command:
   `docker image ls`
6. To view a list of the downloaded charts, run the following command:
   `ls /root/downloads/*.tgz`
7. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-agn-ctl container at `/var/log/avaya/ccm/ccm-main.log`.
   For more information on possible issues and the respective troubleshooting solutions, see the Maintaining and Troubleshooting Avaya Analytics for Oceana doc.

Uploading Avaya Analytics chart and images

Before you begin:

- Ensure air-gap running
  - `agn-ctl status`
  - If not running, then run the following:
    - `agn-ctl setup`
    - `agn-ctl startup`

1. Connect to your air gap network using your Windows PC or laptop.
2. Start the ccm-agn-ctl container by using the following `ccm-agn-ctl.bat` file in the Windows PowerShell console: C:\avaya\ccm-agn-ctl.bat
3. Using the ccm agn deployed container, run the following command: `agn upload <CCM FQDN>`, where <CCM FQDN> is the FQDN of your CCM.
4. To access the CCM docker registry and ChartMuseum, enter the username when prompted.
5. Enter the password.
6. Re-enter the password.
   The agn command starts the following in a sequence:
   a. Processes the available chart and image data on the Windows PC or laptop.
   b. Starts uploading the charts and images to CCM. When the upload is complete, the console displays an image push report.
7. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-agn-ctl container at `/var/log/avaya/ccm/ccm-main.log`.
   For more information on possible issues and the respective troubleshooting solutions, see the Maintaining and Troubleshooting Avaya Analytics for Oceana document.
8. To copy the <solution spreadsheet name>.xlsm file, run the following command in the ccm-agn-ctl container:`scp /root/downloads/`
   <solution spreadsheet name>.xlsm <ccmUser>@<CCM FQDN>:,
   where <ccmUser> is the CCM customer login account and <CCM FQDN> is the FQDN of your CCM.
   Note: Do not skip the colon at the end of the command.
9. In the **Are you sure you want to continue connecting** field, type `yes` and press **Enter**.
10. At the prompt, enter the CCM user password.
    The ccm-agn-ctl container uploads the images and charts, which you earlier downloaded on the Windows PC or client laptop, into the local CCM docker registry and chartmuseum.

Upgrading Avaya Analytics Cluster

1. Log in to the Cluster Control Manager (CCM) console as the customer user.

2. To switch to the root user, type `su` and press **Enter**.

3. To confirm that the local CCM Docker registry and ChartMuseum are running, run the following command:
   `agn-ctl status`

4. From the directory on CCM that contains the excel file, enter the following command:
   `screen`
5. Run the following command to begin the upgrade of the Avaya Analytics cluster
   - `ccm upgrade spec <solution spreadsheet name>.xlsm --infra`

If the Prometheus pod is not starting or an Async pods in a 0/1 Ready state and either of these cause the upgrade to not complete, then the validation checks on these pods can be skipped by adding the `--force` option to the end of the command

6. When prompted:
    a. Enter vCenter credentials
    b. Enter Avaya SSO credentials
    c. Confirm the cluster upgrade to the new version specified in the solution spreadsheet
    d. Accept the EULA.
    e. Confirm Upgrade

7. Run the following command to monitor the progress of the upgrade: `tail -f /var/log/avaya/ccm/patch-<timestamp>.log`

8. Once the upgrade is complete. Verify the software version of the Analytics cluster by running: `swversion`
   The cluster version should be updated and match what is defined in the solution spreadsheet.

9. Confirm the operational state of the Analytics cluster. Run the following commands:
    - `ccm smoke-test`
    - `ccm status --pod-details`

   The pods might not be operational immediately after the upgrade. Continue running these commands periodically at 10 minute intervals until all pods are running. If these tests continue to fail after 30 minutes, contact Avaya support personnel for assistance.

10. The upgrade of the Avaya Analytics cluster is complete. Proceed with the “Upgrade of the Avaya Analytics Services”

Upgrade Avaya Analytics Services

Before You Begin

Ensure the correct installation method is chosen. This will most likely be the method used at the original installation time. Review the following chapters of the Deploying Avaya Analytics for Oceana guide if unsure:

- Chapter 8: Deploying Avaya Analytics online
- Chapter 9: Deploying Avaya Analytics offline

Important:

Manual Config. Map changes are ***not supported***. Patches will overwrite these.

Verify DB Pods in standard state

Check the status of the crunchy pods using commands below:

1. Connect to the CCM server using the customer account log in.
2. Check the status of the crunchy pods
   - `k describe pod crunchy-primary-service-orca-dbmgr-0 | grep name=`
   - `k describe pod crunchy-replica-service-orca-dbmgr-0 | grep name=`

```
[root@ccml12 cust]# k describe pod crunchy-primary-service-orca-dbmgr-0 | grep name=
             name=crunchy-replica-service-orca-dbmgr
             statefulset.kubernetes.io/pod-name=crunchy-primary-service-orca-dbmgr-0
[root@ccml12 cust]# k describe pod crunchy-replica-service-orca-dbmgr-0 | grep name=
             name=crunchy-primary-service-orca-dbmgr
             statefulset.kubernetes.io/pod-name=crunchy-replica-service-orca-dbmgr-0
[root@ccml12 cust]#
```

3. If output similar to above is observed, then DB pods are in Rainy Day/non-standard state. Primary definition is pointing at replica pod as end point while replica is pointing at primary pod. If in this state follow the steps below otherwise proceed with appropriate upgrade procedure.
4. Delete the replica db pod
   - `k delete pod crunchy-replica-service-orca-dbmgr-0`

```
[root@ccml12 cust]# k delete pod crunchy-replica-service-orca-dbmgr-0
pod "crunchy-replica-service-orca-dbmgr-0" deleted
```

5. Wait for all the pods to be in running state

```
[root@ccml12 cust]# k get pods | grep crunc
crunchy-pgpool-orca-0                                 1/1     Running     0          4h57m
crunchy-primary-service-orca-dbmgr-0                  1/1     Running     0          28m
crunchy-replica-service-orca-dbmgr-0                  1/1     Running     0          28m
crunchy-watch-orca-56fdc58f94-24p7t                   1/1     Running     0          28m
[root@ccml12 cust]#
```

6. Check the status of the crunchy pod. Pod status should be the same as below. This is Sunny Day state in terms of primary/replica roles. If so, continue with upgrade.

```
[root@ccml12 cust]# k describe pod crunchy-primary-service-orca-dbmgr-0 | grep name=
             name=crunchy-primary-service-orca-dbmgr
             statefulset.kubernetes.io/pod-name=crunchy-primary-service-orca-dbmgr-0
[root@ccml12 cust]# k describe pod crunchy-replica-service-orca-dbmgr-0 | grep name=
             name=crunchy-replica-service-orca-dbmgr
             statefulset.kubernetes.io/pod-name=crunchy-replica-service-orca-dbmgr-0
[root@ccml12 cust]#
```

Online Procedure

1. Connect to the CCM server using the customer account log in.

2. Copy `<solution spreadsheet name>.xlsm` to a location on the CCM server.

3. Execute the following command as root to remove crunchy watch before starting upgrade
   - `k scale deployment crunchy-watch-orca --replicas=0`

4. From the directory on CCM that contains the excel file, enter the following command:
   - `screen`

5. Run the following command:
   - `ccm upgrade spec <solution spreadsheet name>.xlsm --products`

   If the Prometheus pod is not starting or an Async pods in a 0/1 Ready state and either of these cause the upgrade to not complete, then the validation checks on these pods can be skipped by adding the `--force` option to the end of the command

6. When prompted:
   a. Enter vCenter credentials
   b. Enter credentials
   c. Accept the EULA.
   d. Confirm Upgrade

7. The installation starts downloading and installing.

8. Run the following command to monitor the progress of the install:
   - `tail -f /var/log/ avaya/ccm/ccm-main.log`

9. The upgrade command will exit when complete.

10. Execute the following command as root to set the replica count for crunchy watcher back to 1.
    - `k scale deployment crunchy-watch-orca --replicas=1`

11. Confirm the operational state of the Analytics cluster. Run the following command:

- `ccm status --pod-details`

All pods should report running with n/n reporting ready before continuing to the next step. Refer to **Post-installation verification** chapter of *Deploying Avaya Analytics for Avaya Oceana* for further details on confirming the status of Analytics.

Important:
If the `ccm upgrade spec` command fails, resolve the issue causing the failure and restart the upgrade by running: `ccm upgrade resume` command. For more information about troubleshooting installation failures, see Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana.

Offline Procedure

Downloading Avaya Analytics chart and images

Before you begin you must have:

- Valid Avaya SSO credentials.
- A functional ccm-agn-ctl container on your laptop.

1. On your Windows PC or client computer, save the Analytics Excel Spreadsheet in c:\avaya\downloads.
   Note: Windows and the CCM Controller container share a mount point, which are c:\avaya\downloads and /root/downloads respectively.
2. In the ccm-agn-ctl container, run `cd/root/downloads`.
3. To download the Avaya Analytics™ charts and images from the Avaya repository, run the following command:
   - `agn download <solution spreadsheet name>.xlsm`
4. When requested enter credentials.
   The agn script processes the excel spreadsheet and the Avaya Analytics™ charts and docker images start downloading. The ccm-agn-ctl container displays an Image Pull Report when the download is complete.
5. To view a list of the downloaded images, run the following command:
   - `docker image ls`
6. To view a list of the downloaded charts, run the following command:
   - `ls /root/downloads/*.tgz`
7. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-agn-ctl container at `/var/log/avaya/ccm/ccm-main.log`.
   For more information on possible issues and the respective troubleshooting solutions, see the Maintaining and Troubleshooting Avaya Analytics for Oceana guide.

Uploading Avaya Analytics chart and images

Before you begin:

- Ensure air-gap running
  - `agn-ctl status`
  - If not running, then run the following:
    - `agn-ctl setup`
    - `agn-ctl startup`

1. Connect to your air gap network using your Windows PC or laptop.
2. Start the ccm-agn-ctl container by using the following `ccm-agn-ctl.bat` file in the Windows PowerShell console: C:\avaya\ccm-agn-ctl.bat
3. Using the ccm agn deployed container, run the following command: `agn upload <CCM FQDN>`, where <CCM FQDN> is the FQDN of your CCM.
4. To access the CCM docker registry and ChartMuseum, enter the username when prompted.
5. Enter the password.
6. Re-enter the password.
   The agn command starts the following in a sequence:
   a. Processes the available chart and image data on the Windows PC or laptop.
   b. Starts uploading the charts and images to CCM. When the upload is complete, the console displays an image push report.
7. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-agn-ctl container at `/var/log/avaya/ccm/ccm-main.log`.
   For more information on possible issues and the respective troubleshooting solutions, see the Maintaining and Troubleshooting Avaya Analytics for Oceana guide.
8. To copy the <solution spreadsheet name>.xlsm file, run the following command in the ccm-agn-ctl container:`scp /root/downloads/`
   <solution spreadsheet name>.xlsm <ccmUser>@<CCM FQDN>:,
   where <ccmUser> is the CCM customer login account and <CCM FQDN> is the FQDN of your CCM.
   Note: Do not skip the colon at the end of the command.
9. In the **Are you sure you want to continue connecting** field, type `yes` and press **Enter**.
10. At the prompt, enter the CCM user password.
    The ccm-agn-ctl container uploads the images and charts, which you earlier downloaded on the Windows PC or client laptop, into the local CCM docker registry and chartmuseum.

Upgrading Avaya Analytics services

1. Log in to the Cluster Control Manager (CCM) console as the customer account user.
2. To switch to the root user, enter su.
3. To confirm that the local CCM docker registry and chartmuseum is running, run the following command:
   - `agn-ctl status`

4. Copy `<solution spreadsheet name>.xlsm` to a location on the CCM server.
5. From the directory on CCM that contains the excel file, enter the following command:
    - `screen`
6. Run the following command:
    - `ccm upgrade spec <solution spreadsheet name>.xlsm --products`

    If the Prometheus pod is not starting or an Async pods in a 0/1 Ready state and either of these cause the upgrade to not complete, then the validation checks on these pods can be skipped by adding the `--force` option to the end of the command
7. When prompted:
    a. Enter your Avaya SSO credentials.
    b. Accept the EULA.
    c. Enter the vCenter user ID and password.
    d. Re-confirm the password.
8. The installation starts downloading and installing the following:
    - The Avaya Analytics™ software
9. Run the following command to monitor the progress of the install:
    - `tail -f /var/log/ avaya/ccm/ccm-main.log`
12. The upgrade command will exit when complete
13. Confirm the operational state of the Analytics cluster. Run the following command:
    - `ccm status --pod-details`

    All pods should report running with n/n reporting ready before continuing to the next step. Refer to the **Post-installation verification** chapter of *Deploying Avaya Analytics for Avaya Oceana for further details on verification.*

Important:

If the `ccm upgrade spec` command fails, resolve the issue causing the failure and restart the upgrade by running: `ccm upgrade resume` command. For more information about troubleshooting installation failures, see Maintaining and Troubleshooting Avaya Analytics™.

Post Installation Instructions

Manage Internal Certificates

Rotate Platform Certificates

1. (Optional) To check when the cluster platform certificates expire, run
   - `ccm cluster-certificates-expiration`
2. (Required) To manually rotate the platform certificates before they expire, run:
   - **`screen`** *(The screen utility allows the upgrade to run in the background.)*
   - `ccm rotate-cluster-certificates`

   This process can take up to two hours to complete. Progress can be monitored via /var/log/ccm/ccm-main.log

   If the certificates have already expired, a cluster reinstallation is required.

Install Service Certificates Script

Patch installation will overwrite the `renewServiceCertificates` script. If it is required later then it should be reinstalled.

1. Download the CSPPatch_renewServiceCertificates.bin from PLDS and transfer this file to the Cluster Control Manager using the customer account and place it in the home directory (e.g. /home/<customer account>)
2. Patch install instructions
   a. As the root user, grant execute permissions to the downloaded binary file and run it from the home directory to install the patch.
      - `chmod +x CSPPatch_renewServiceCertificates.bin`
      - `./CSPPatch_renewServiceCertificates.bin`
3. The script will display information related to the patch and will wait for user input to continue. If user response is to continue, Avaya EULA is displayed. Once EULA is accepted the patch is deployed.
4. Patch installation logs located in /var/log/avaya/ccm/patch.log.

   Deployment of the patch does not affect any of the services running in the cluster.
   This patch will install one command renewClusterCertificates on the CCM. Once the patch is installed as root, a non-root user can log in to CCM and execute the command. Command logs located in /var/log/avaya/ccm/ccm-main.log.

Verify Running Solution

To verify the solution is back running fully:

1. Follow the instructions in the chapter: Post-installation verification of Deploying Avaya Analytics for Oceana guide.
2. Verify Historical Reporting.
   a. Login to Historical reporting.
   b. Run one or more reports.
3. Verify Real Time reporting.

a. Initiate voice or multimedia contact.
b. Login into Workspace and verify the real-time reports are updating.

4. Remove the CCM Virtual Machine snapshot taken at the beginning of the upgrade procedure. Failure to do so can result in performance degradation of the CCM virtual machine as well as the ESXi host.

Async Services

Install Async Messaging = TRUE

If "Install Async Messaging" parameter was set to TRUE in the deployment spreadsheet and Oceana does not have Async Messaging do the following:

1. Log in to the Cluster Control Manager (CCM) console as the cust user.
2. To switch to the root user, enter su.
3. kubectl edit cm orca-ref-input-adaptor
4. Run the following vi command:
5. %s/SEND_NOTIFICATION/FORWARD_NOTIFICATION/g
6. Save and exit
7. Find the pod ids of the input adapter pods:
8. kubectl get pods | grep input
9. kubectl delete pod <input-adapter-primary-pod-id> <input-adapter-secondary-pod-id>

Kafka Open Interface

If using the Kafka Open Interface for Analytics, ensure the version number is correct. See instruction in PSN "PSN005625u.

Re-import 3rd Party Kafka Certs

In a system where 3rd party certs have been applied and if upgrading from a lineup pre Analytics 4.1.0.1, 1.1.0.2.116001 or pre CSP version 1.1.0.2.116001 3rd party certificates for eventing-kafka product are not retained. Therefore, there is a need to add a 3rd party CA certificate and import 3rd party identity certificates for eventing-kafka product immediately after upgrade.

Before you begin

Obtain the PEM file of the third-party CA.

Procedure to add 3rd party CA certificate

1. Log in to CCM
2. Transfer the third-party CA PEM file to the /home/<customer_account>/ directory on CCM using a file transfer utility, such as WinSCP

3. Create a file called **kafka-truststore-serviceids** on CCM with service IDs below at /home/<customer_account>/ .

```
eventing-kafka-cp-kafka-kafkatruststore
eventing-kafka-cp-kafka-connect-kafkaconnecttruststore
eventing-kafka-cp-schema-registry-kafkaconnecttruststore
eventing-kafka-eventing-operator-eventingoperatortruststore
eventing-kafka-topic-operator-kafkaconnecttruststore
eventing-kafka-cp-zookeeper-kafkaconnecttruststore
```

4. Run the following command

```
ccm release cert-manager third-party-certs --add-trustcert --list-file
/home/<customer_account>/kafka-truststore-serviceids --ca-cert-file
/home/<customer_account>/<third-party-CA_PEM>
```

5. Run ccm smoke-test and ensure that all tests pass.
6. Run ccm status --pod-details and ensure that the status of all pods is Running or Completed.

Procedure to Create and import the Kafka 3rd party identity certificate

- If third party identity certificate was imported only for **kafka** (service id eventing-kafka-cp-kafka-kafkaexternalidcert) then after upgrade re-import the third party identity certificate as explained below (refer : *Procedure to import a third party identity certificate for service id eventing-kafka-cp-kafka-kafkaexternalidcert*)

- If third party identity certificate were imported for both **kafka** (service id eventing-kafka-cp-kafka-kafkaexternalidcert) and **zookeeper** (service id eventing-kafka-cp-zookeeper-kafkaconnectidcert) then after upgrade re-import third party identity certificates for these serviceids as explained below (refer : *Procedure to import a third party identity certificate for service id eventing-kafka-cp-kafka-kafkaexternalidcert and eventing-kafka-cp-zookeeper-kafkaconnectidcert*)

Procedure to import a third party identity certificate for service id eventing-kafka-cp-kafka-kafkaexternalidcert

Before you begin

Import the third-party CA certificate for the eventing-kafka service.

Procedure

1. Log in to CCM
2. Create a file called **kafka-idcert-serviceId** in the /home/<customer_account>/ directory on CCM.

Ensure that the file contains the following service ID:

```
eventing-kafka-cp-kafka-kafkaexternalidcert
```

3. Run following command to generate CSR.

```
ccm release cert-manager third-party-certs --generate-service-csr --list-file
/home/<customer_account>/kafka-idcert-serviceId --output-dir
/home/<customer_account>/kafka-csr
```

The CSR is generated in the /home/<customer_account>/kafka-csr directory with the file name '**eventing-kafka-cp-kafka-kafkaexternalidcert.csr**'

4. Use the CSR file to obtain the identity certificate PEM file signed by the third-party CA.
5. Rename the PEM file to '**eventing-kafka-cp-kafka-kafkaexternalidcert.pem**'.
6. Create a directory called **kafka-idcert-dir** under /home/<customer account>.
7. Transfer the PEM file to **kafka-idcert-dir** using a file transfer utility, such as WinSCP
8. Run following command to import the third party identity certificate.

```
ccm release cert-manager third-party-certs --import-identity-cert-pem --id-cert-
dir /home/<customer_account>/kafka-idcert-dir
```

9. Run **ccm smoke-test** and ensure that all tests pass.
10. Run **ccm status --pod-details** and ensure that the status of all pods is Running or Completed.

Procedure to import a third party identity certificate for service id eventing-kafka-cp-kafka-kafkaexternalidcert and eventing-kafka-cp-zookeeper-kafkaconnectidcert

Before you begin

Import the third-party CA certificate for the eventing-kafka service.

Procedure

1. Log in to CCM
2. Create a file called **kafka-idcert-serviceId** in the /home/<customer_account>/ directory on CCM.

Ensure that the file contains the following service ID:

```
eventing-kafka-cp-kafka-kafkaexternalidcert
eventing-kafka-cp-zookeeper-kafkaconnectidcert
```

3. Run following command to generate CSRs.

```
ccm release cert-manager third-party-certs --generate-service-csr --list-file
/home/<customer_account>/kafka-idcert-serviceId --output-dir
/home/<customer_account>/kafka-csr
```

The CSRs are generated in the /home/<customer_account>/kafka-csr directory with the file names '**eventing-kafka-cp-kafka-kafkaexternalidcert.csr**' and '**eventing-kafka-cp-zookeeper-kafkaconnectidcert.csr**'

4. Use these CSR files to obtain the identity certificate PEM files signed by the third-party CA.
5. Rename the PEM files to '**eventing-kafka-cp-kafka-kafkaexternalidcert.pem**' and **'eventing-kafka-cp-zookeeper-kafkaconnectidcert.pem**' respectively.
6. Create a directory called **kafka-idcert-dir** under /home/<customer account>.
7. Transfer these PEM files to **kafka-idcert-dir** using a file transfer utility, such as WinSCP
8. Run following command to import the third party identity certificates.

```
ccm release cert-manager third-party-certs --import-identity-cert-pem --id-cert-dir /home/<customer_account>/kafka-idcert-dir
```

9. Run **ccm smoke-test** and ensure that all tests pass.
10. Run **ccm status --pod-details** and ensure that the status of all pods is Running or Completed.

Note:

1. **Procedure to add 3rd party CA certificate** must be done immediately post upgrade.
2. **Procedure to import a 3rd party identity certificate** can be done any time post upgrade as per requirement to import third-party certificate

Rollback Procedure

In the event a patch install cannot be completed, and it is required to rollback to the prior release use the following procedure.

1. Rollback to previous version of software:
   - Connect to the CCM server using the customer account log in.
   - Copy excel sheet backed up during Pre-installation instructions to a location on the CCM server.
   - From the directory on CCM that contains the excel file, enter the following command:
     - `screen`
   - Run the following command:
     - `ccm upgrade spec <solution spreadsheet name>.xlsm`
   - When prompted:
     - Accept the EULA.
     - Confirm Upgrade
   - The installation starts downloading and installing.
   - Run the following command to monitor the progress of the install:
     - `tail -f /var/log/ avaya/ccm/ccm-main.log`
   - To check if the installation is successful, run the following command on the CCM console:
     - `ccm status`

2. Rollback to previous version of custom reports:
   i. Bash onto mstr-md pod
      - `kubectl exec -it <mstr-md-hashed-number> --namespace=mstr -- /bin/bash`
   ii. Create directory to save backup to:
      - `mkdir -p  /opt/app-root/src/md_full_backup/`
   iii. Type 'exit' to exit the pod
   iv. On ccm change directory to where backup was exported
      - `cd /home/cust/historical_md_backups`
   v. Copy the full MicroStrategy backup file onto the pod
      - `kubectl cp <full_backup_Date-Time.bkp> --namespace=mstr <mstr-md-hashed-number>:/opt/app-root/src/md_full_backup/<full_backup_Date-Time.bkp>`
   vi. Bash onto mstr-md pod
      - `kubectl exec -it <mstr-md-hashed-number> --namespace=mstr -- /bin/bash`
   vii. Run the command to restore full backup
      - `psql -U postgres -f /opt/app-root/src/md_full_backup/<full_backup_Date-Time.bkp> postgres`
   viii. The output on the console can have to Errors pertaining to the postgres user. These can be ignored.

- *psql:/opt/app-root/src/md_full_backup/full_backup_2020_05_27_16_20_23.bkp:23: ERROR: current user cannot be dropped*
- *psql:/opt/app-root/src/md_full_backup/full_backup_2020_05_27_16_20_23.bkp:31: ERROR: role "postgres" already exists*

ix. Connect to postgres database
- `psql`

x. List available databases with \l command. Confirm the avaya_analytics_md db.
- `postgres=> \l`

xi. Quit databases with \q command.
- `postgres=> \q`

xii. Type 'exit' to exit the pod

xiii. Verify that the custom reports have been restored

3. Rollback to previous version of database

Important

A database backup taken at an earlier S/W level (i.e. patch level) should not be restored to the current one.

i. Connect to the CCM server using the customer account log in.

ii. Copy the backup taken during the pre-patch installation steps above onto the CCM.

iii. Revoke access for the postgres user to the DB
- As the root user, exec to the crunchy primary pod:
  - `kubectl exec -it crunchy-primary-service-orca-dbmgr-0 -- //bin/bash`
- Start psql with:
  - `psql`
- Then revoke access with:
  - `REVOKE CONNECT ON DATABASE analytics_db FROM PUBLIC, postgres;`

iv. End DB connections
- If not already connected to crunchy primary pod then as the root user, exec to the crunchy primary pod:
  - `kubectl exec -it crunchy-primary-service-orca-dbmgr-0 -- //bin/bash`
- Start psql with:
  - `psql`
- Then kill connections to the postgres DB with:
  -
```
SELECT pg_terminate_backend(pg_stat_activity.pid)
FROM pg_stat_activity
WHERE pg_stat_activity.datname = 'analytics_db'
AND pid <> pg_backend_pid()
```

v. Drop the DB
    - As the root user, exec to the crunchy primary pod
        - `kubectl exec -it crunchy-primary-service-orca-dbmgr-0 -- //bin/bash`
    - Start psql with:
        - `psql`
    - Then drop the database with:
        - `DROP DATABASE "analytics_db";`

vi. Run the CCM control script command to restore the database.

vii. Run through the Post Patch install steps to verify that the system is restored to its previous state.

viii. Take a full backup of the database using the CCM control script.

DR Installation

If installing this patch into a solution with a disaster recovery site the following is the recommended order:

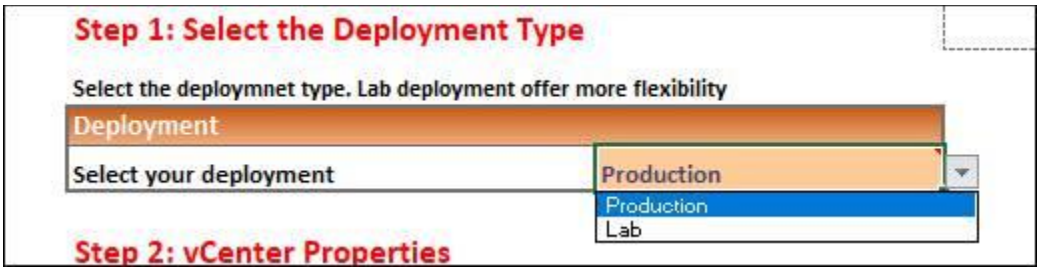
1. Apply patch to primary side.
2. When complete, apply patch to DR site.

Note: Data from the database will be replicated between the primary site and the DR site in the normal way. See Deploying Avaya Analytics for Oceana guide for details.

Deployment Excel Deployment Options

The deployment excel now supports two deployment options , **Production** and **Lab**

- The “Lab” option is for **lab only** installations adding support for Async as part of a Non-HA deployment.
- The “Production” option **must** be selected for all production based deployments as lab based deployment will not be supported in production.



Staggered Solution Upgrade Script

If you are doing a staggered Solution upgrade, please note the following new option in ‘ccm release orca analytics’

- Deployment -> Oceana Notification Types

This option should only be used for staggered solution upgrades when the following criteria are met:

- Analytics was upgraded first to 4.1.x.x and was then connecting to Oceana 3.7.0.1.
- Oceana has now been upgraded to 3.8.x.

This option will update the Oceana Notification Type from 'FORWARD_NOTIFICATION' to 'SEND_NOTIFICATION' to be compatible with Oceana 3.8.x.

WARNING: This option will restart the Input Adaptor pod

Known Issues

Issue 1

The following message may be reported during install.
WARNING: Service release "orca" did not become ready in the allotted time. Processing will continue.
This usually can be ignored as the it is just a warning that a pod is slower than others to start-up. If after the rest of the install completes all orca pods look healthy, then there is no issue here.

Issue 2 – Historical Reporting

Report Import/export

Basic and Advanced reporting users can export reports under the ***Custom Reports & My Reports*** folders. They do **not** have permissions to import/export from the ***Shared Reports*** or ***Standard Historical Reports*** folders.

Note: The following table describes the functionality supported by the various reporting users.

	Fresh Install	Upgrade from 4.0.0.1
Basic User	Export Only *	Export Only *
Advanced User	Export Only *	Export Only *
Administrator	Import & Export	Import & Export

Advanced or Basic reporting users that need to import reports on a system will need to provide a copy of the report export MMP file to an administrator user who can import the reports on their behalf.

Reports that are exported to an MMP file should be confirmed to be working before export otherwise the import of the MMP file may fail.

* Import functionality for all user types will be provided in a future release.

Import of Cloned Canned Reports

Advanced and Basic users can clone Standard historical Reports by copying a report to the 'Custom Report folder or MyReports folder'

Advanced and Basic users can export this cloned report from their 'Custom Report' folder or 'MyReports' folder to their desktop.

The Administrator user is required to import exported cloned canned reports.

Issue 3

An issue may occur after an upgrade that may manifest in a number of ways.

- All HTTPs requests failed and eventing-kafka-connect containers failed to come up after infra upgrade.

- Unable to access historical reporting URL
- Unable to access real time reports

Symptom

After upgraded CSP infrastructure the cluster fqdn/IP is pingable but all the ingress HTTPs requests failed with timeout error.

Workaround

There are 2 options for a workaround. Only one approach needs to be used.

Script:

On CCM, execute the `restartKaPods.sh` script with root privilege. restartKaPods.sh available as part of this patch.

Manual:

Locate the node where the cluster IP was assigned by running the command

- `cbosh -d cfcr ssh master ip addr show eth0`

ping <cluster IP> to verify it is pingable
Locate the IPs of the ingressgateway endpoints by running the command "kubectl describe service -n istio-system istio-ingressgateway"
Verify the IPVS routing rules defined on each node by running

- `kubectl exec -it <kube-keepalived-vip pod> – ipvsadm -L`

Make sure the IP addresses of the istio-ingressgateway endpoints are defined for https routing in the ipvsadm output from every kube-keepalived-vip pod. The IPVS routing table should be defined identically by kube-keepalived-vip pod running on each node.
Restart the kube-keepalived-vip pod on the node that has cluster IP assigned or invalid IPVS routing table by running to recover the issue

- `kubectl delete pod <kube-keepalived-vip pod>`

Compatibility with Existing Data

This Analytics patch does not retrospectively fix data already stored in the database before this patch is applied.

Appendix

Solutions provided in Avaya_Analytics_4.1.0.1_078_004

JIRA ID	Title	Impact
FLEX-20507	CSP Services fail to consume updated certificates generated by Certificate Manager CA	CSP Services will now consume updated certs so expiration is extended and system continues to operate.
FLEX-8997	CCM/Deployment - Platform Credential Management: General Serviceability - BOSH Fix and Alarm for Certificate Rotation of BOSH CLI Generated Certificates	CSP Platform certs will be rotated and expiration extended. This will allow system to continue to operate.
WAVE-17314	eventing-kafka-cp-kafka-2 pod in crash loop state	Reduce retention period on Kafka Open Interface's dynamic topic so it will not over consume disk space.
WAVE-14590	HT - Agent Configuration report - The Channel measure is not updated when we unassign channel out of agent on ACM	A new column (is_unknown) was added to the table fact.dim_accounts. This is used to now handle removed accounts and they no longer appear in report.

Solutions provided in Avaya_Analytics_4.1.0.1_071_003

JIRA ID	Title	Impact
WAVE-17505	French characters missing after R4.1.0.1 patch 002	Systems having patch 2 installed and then upgraded to patch 3 will stop experiencing issues with incorrectly displayed/not shown characters in historical reporting when setting non English language in preferences.
WAVE-17308	Dossiers feature fails for Advanced User after Patch 002	Systems having patch 2 installed and then upgraded to patch 3 will stop experiencing issues with Advanced users not being able to edit dossier reports.
WAVE-17320	AnalyticsServerAdmin page not accessible after Patch 002	Not resolved but see workaround in **Error! Reference source not found.** section.

Solutions provided in Avaya_Analytics_4.1.0.1_071_002

JIRA ID	Title	Impact
WAVE-16848	Email distribution not using the SMTP server configured - no IP or Hostname in Generic Email device	Configured e-mail server not overwritten now so email distribution will use it.
WAVE-16215	Unable to export dossier report - PDF export engine not running	Dossier reports can now be output to PDF.

WAVE-15162	mstr-srv service fails to start after configuring email distribution services - Transmitter 'Email' was not found	Configured transmitter not overwritten now so mstr-srv service will start.
WAVE-16093	Change canned reports to not use flash mstr components	Canned reports now use a non-Flash component but still look the same.

Enhancements provided in Avaya_Analytics_4.1.0.1_071_002

JIRA ID	Title	Impact
WAVE-16999	E-mail Device set "Always use Smart Host" option to checked	Historical reporting distribution service uses specified exchange server rather than using the target email address to attempt to find a publicly accessible SMTP server according to the standard workflow.

Solutions provided in Avaya_Analytics_4.1.0.1_071_001

JIRA ID	Title	Impact
WAVE-15556	Additional Time pegged but not Not Ready when agent initiates a transfer to service while in Not Ready Pending	Additional Time duration measure will work correctly in transfer to service scenario
WAVE-15112	Issue with measure Additional Work Duration when Call Alerting and setting Additional Work occur simultaneously	Additional Time duration measure will work correctly when call arrives at the same time when agents sets Not Ready
WAVE-14978	Issue with change of PushRateDuration for orca-itd-routing-service-measure-proc	Routing Service measure processor will correctly pick changes to PushRateDuration parameter set in config map
WAVE-14740	Completed measure count in Agent report is not getting updated after pod restart	Input Adaptor will correctly initiate pumpup requests after failover
WAVE-14646	Routing Service Reports show large numbers of rows with "UKNOWN_CHANNEL"	Channel ID measure will be correctly set in defer email scenario

Further Support Assistance

For further assistance please contact your Avaya Support representative for any queries on this patch or readme.