# Oracle® Communications

# Policy Management ATS Guide

Release 15.0.0.3.0
G29678-01
April 2025

Oracle Communications Policy Management ATS Guide, Release 15.0.0.3.0

G29678-01

# Contents

# What's New in This Guide

This section introduces the documentation updates for release 15.0.0.3.0.

**Release 15.0.0.3.0- G29678-01, April 2025**

Updated the following sections with the details of ATS 15.0.0.3.0:

- Added the Abort Build feature in the ATS Features section:

vPCRF ATS Release

- The following changes are made to Jenkins in ATS 15.0.0.3.0:
  - Abort build functionality is added
- Previous Release Test Cases (vPCRF): Provides a total of 26 feature files and 36 scenarios of Regression pipeline.
- Added details of vPCRF ATS feature for aborting running builds.

# 1 Introduction

The Automated Test Script (ATS) is a software that is used on the system under test to check if the system is functioning as expected. This software performs testing of the features offered by Policy Charging Rules Function (PCRF) through automation decreasing the manual test effort.

## Limitations

Only a single Multiprotocol Routing Agent (MRA) and Multimedia Policy Engine (MPE) cluster can be used in the test environment.

## Acronyms

This section lists the acronyms used in the document.

**Table 1-1 Acronyms**

| Term | Definition |
|---|---|
| API | Application Programming Interface |
| ATS | Automated Test Suite |
| CA | Certificate Authority |
| CSR | Certificate Signing Request |
| DN | Distinguished Name |
| DNS | Domain Name System |
| GUI | Graphical User Interface |
| JKS | Java KeyStore |
| KVM | Kernel-based Virtual Machine |
| MPE | Multimedia Policy Engine |
| MRA | Multi Protocol Routing Agent |
| NTP | Network Time Protocol |
| OS | Operating System |
| PCRF | Policy Charging Rules Function |
| SUT | System Under Test |
| TLS | Transport Layer Security |
| VM | Virtual Machine |

## Compatibility Matrix

This section lists the releases of OCPM PCRF compatible with vPCRF ATS.

**Table 1-2 Compatibility Matrix**

| ATS Software Release | Compatible OCPM PCRF Releases |
|---|---|
| 15.0.0.3 | 15.0.0.3 or higher |
| 15.0.0.2 | 15.0.0.2 or higher |
| 15.0.0.0 | 15.0.0.0 |

# How to use this document

Read the following instructions before performing any procedure documented in this guide:

1. Read the instructional text and all associated procedural Warnings or Notes.
2. If a procedural step fails to execute, contact Oracle's Customer Service for assistance before attempting to continue. My Oracle Support for information on contacting Oracle Customer Support.

# Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

**Table 1-3 Admonishments**

| Icon | Description |
|---|---|
|  | Danger:<br>(This icon and text indicate the possibility of personal injury.) |
|  | Warning:<br>(This icon and text indicate the possibility of equipment damage.) |
|  | Caution:<br>(This icon and text indicate the possibility of service interruption.) |

# Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training at http://education.oracle.com/communication.

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site at www.oracle.com/education/contacts.

# My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - For Technical issues such as creating a new Service Request (SR), select **1**.
    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

# Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of system ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

# 2
# ATS Server Deployment Overview

The ATS server is deployed as a Virtual Machine (VM) using any hypervisors like, KVM. It has features for Rx, Gx, and Sy cases.

## Downloading ATS Package

- Download the ATS Image from Oracle Software Delivery Cloud (OSDC).
  Example of an ATS image: `vPCRF-ATS-15.0.0.0.0_3.1.0-x86_64.tgz`.
- Extract the tgz file to get the qcow2 image.

## Deploying ATS VM on OpenStack

This section describes the procedure to deploy ATS VM on OpenStack.

To deploy ATS VM using qcow2:

1. Copy the ATS qcow2 image to the OpenStack server.
2. Launch Instance from the OpenStack Menu.
3. Enter an Instance Name.
4. Select **Flavor** as per recommendation. For reference, see Appendix A- Resource Requirements.
5. Select the **networks** as per your cloud deployment. The **networks** selected should be compatible with your PCRF setup. For reference, see Appendix B- VM Networking Layout.
6. Select the key pair to access the ATS VM.
7. Proceed further and launch the instance.
8. After the launch of the ATS instance, the ATS server can be accessed using IP and keypair.
9. If keypair is not used, access ATS VM with cloud-user/NextGen123@.

> **Note:**
>
> PCRF ATS supports both IPv4 and IPv6 deployments.

## Deploying ATS VM on KVM host using virt-install

This section describes the procedure to deploy ATS VM on KVM host using *virt-install*.

To deploy ATS VM on KVM host using *virt-install*:

1. Extract the qcow2 image from tgz package and upload to KVM host.
2. Ensure appropriate networks or bridges are present on KVM host.

3. Run the following command:

```
virt-install --name=atsbuild --ram 16384 --vcpus 8 --network
bridge:bridge1,model=virtio
      --graphics none --connect qemu:///system
      --disk=/mnt/data/ATS-15.0.0.0.0_3.1.0-
x86_64.qcow2,format=qcow2,bus=virtio --console
      pty,target_type=virtio --import
```

   Change network parameter as per customer's environment.

4. Wait for VM creation, it should prompt for login. Log in with cloud-user/NextGen123@.
5. Assign IP address to VM node with following command:
   `ip addr add <Ip address/subnet> dev <oam-interface-name>`

   `ip route add default via <gateway_ip> dev <oam-interface-name>`

   For example:

   `ip addr add 10.75.204.158/24 dev eth0`

   `ip route add default via 10.75.204.129 dev eth0`
6. (optional) Set hostname as needed with `hostnamectl set-hostname <name>`.
   Add routes on PCRF to ensure all PCRF IPs are reachable from ATS.

# Deploying ATS VM on KVM Host using cockpit GUI

This section describes the procedure to deploy ATS VM on KVM host using cockpit GUI.

To deploy ATS VM on KVM host using cockpit GUI:

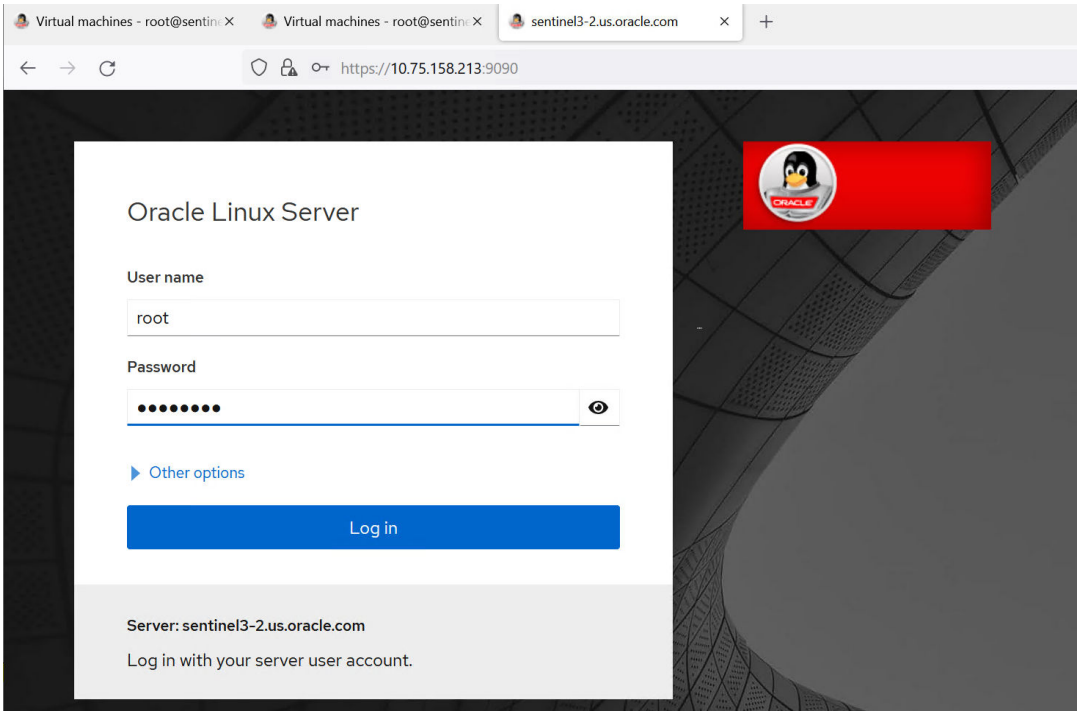
1. Run below commands on KVM host console to install cockpit GUI and its dependencies:

```
export http_proxy=http://www-proxy.us.oracle.com:80
    export https_proxy=http://www-proxy.us.oracle.com:80
    yum install cockpit
    yum install virt-viewer
    yum install virt-manager
    yum install net-tools
    yum install cockpit-machines
    systemctl start cockpit
    systemctl status cockpit
    netstat -pnltu | grep 9090
    systemctl enable --now cockpit.socket
    sudo systemctl start libvirtd
    systemctl status libvirtd.service
    systemctl start firewalld
    firewall-cmd --add-service=cockpit --permanent
    firewall-cmd --reload
```

> **Note:**
>
> The above commands need to run for the first time installation of VM on KVM hosts and later on just copy images to the `/mnt/data` directory in KVM hosts and log in to cockpit GUI → Virtual Machines → Import V.

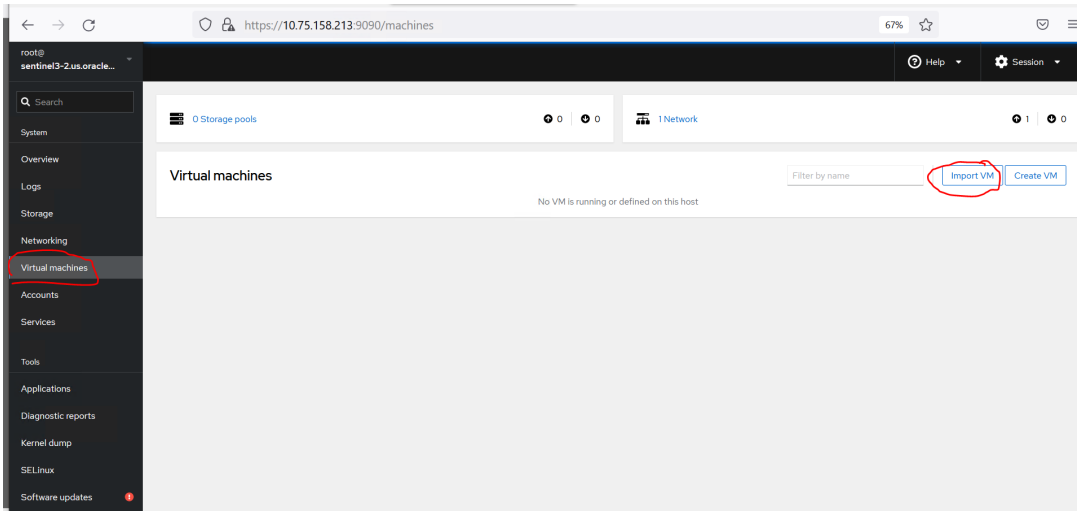
2. Log in to cockpit GUI using url, https://1KVM host ip:/9090/.

**Figure 2-1 Cockpit Graphical User Interface**



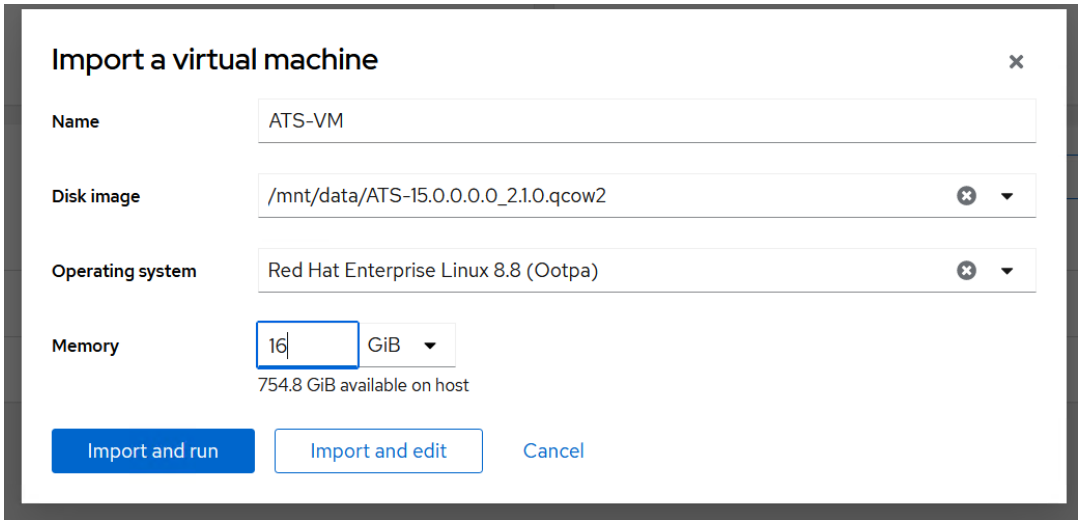

3. Click the **Virtual Machines** tab and click **Import VM**.

**Figure 2-2 Importing Virtual Machine**



4. Provide all details in the **Import VM** page as below and click **Import and Edit**. For reference, see Appendix A- Resource Requirements.

**Figure 2-3 Importing Virtual Machine**




5. Edit no of vcpus, remove default virtual network, and add configured bridge interfaces. For reference, see Appendix B- VM Networking Layout.

**Figure 2-4 Adding Virtual Network Interface**

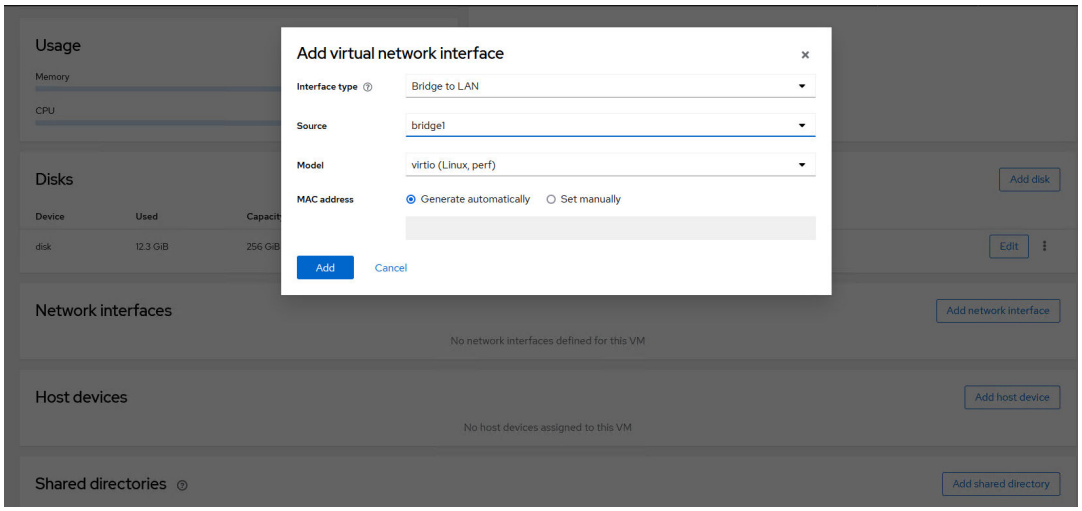
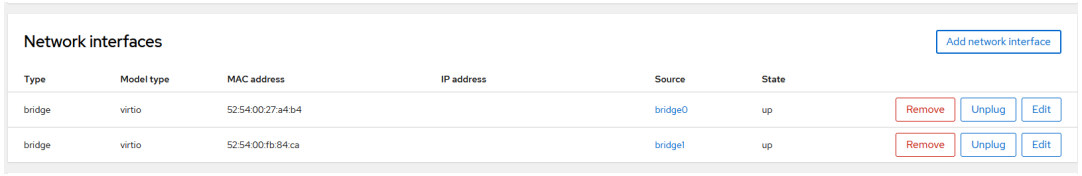



**Figure 2-5 Network Interfaces**




6. Start VM by clicking **Run** and **Console** will be displayed to check ongoing activities.

**Figure 2-6 Starting VM**

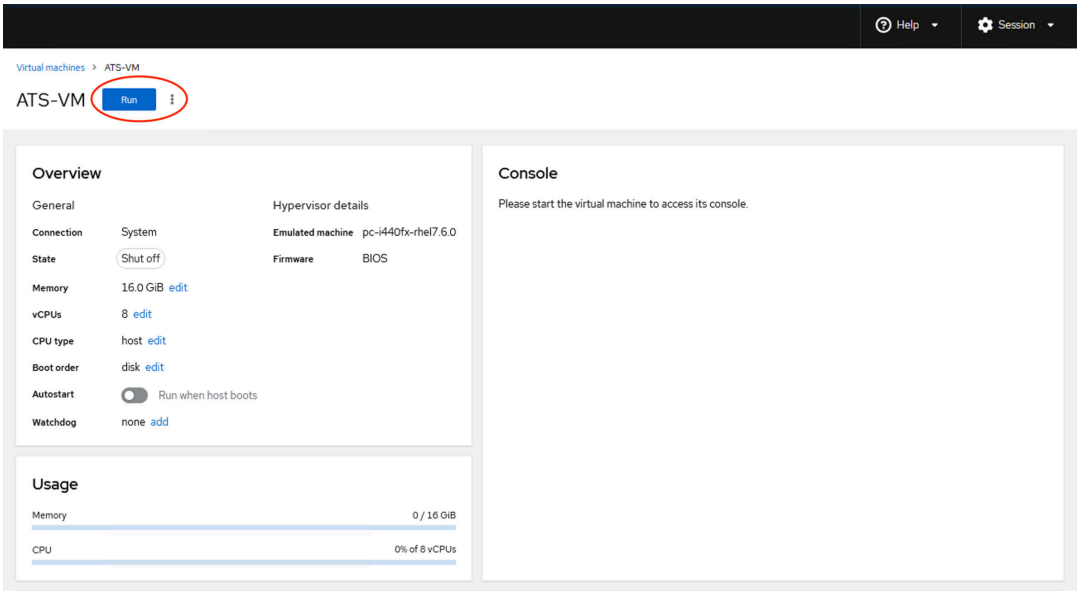
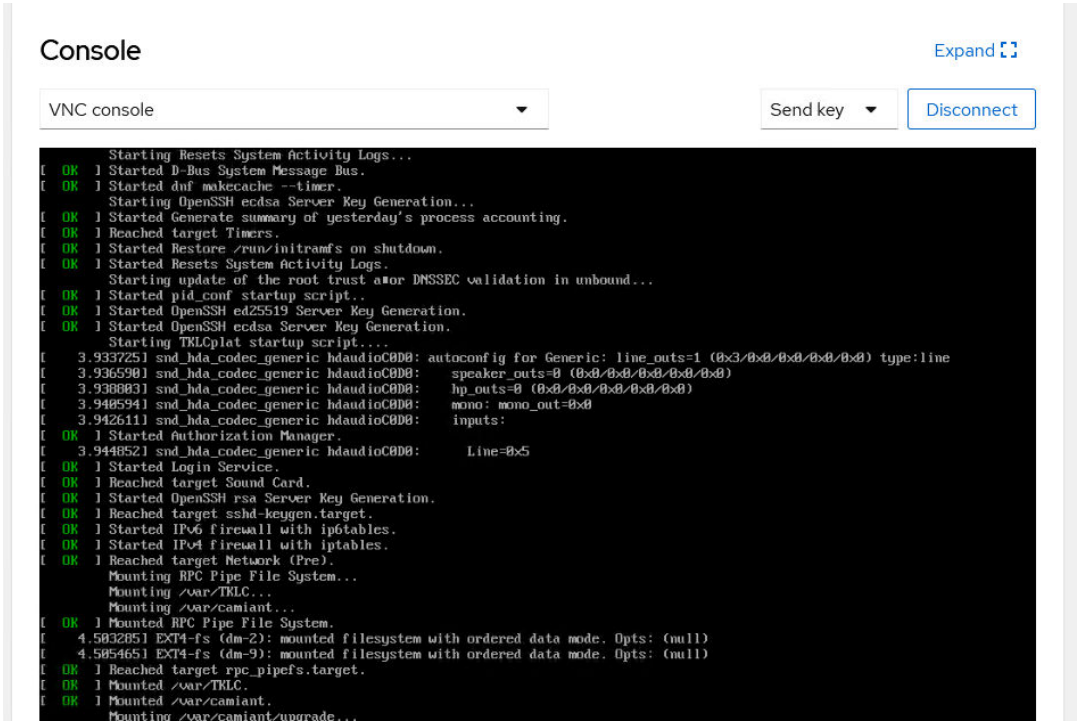
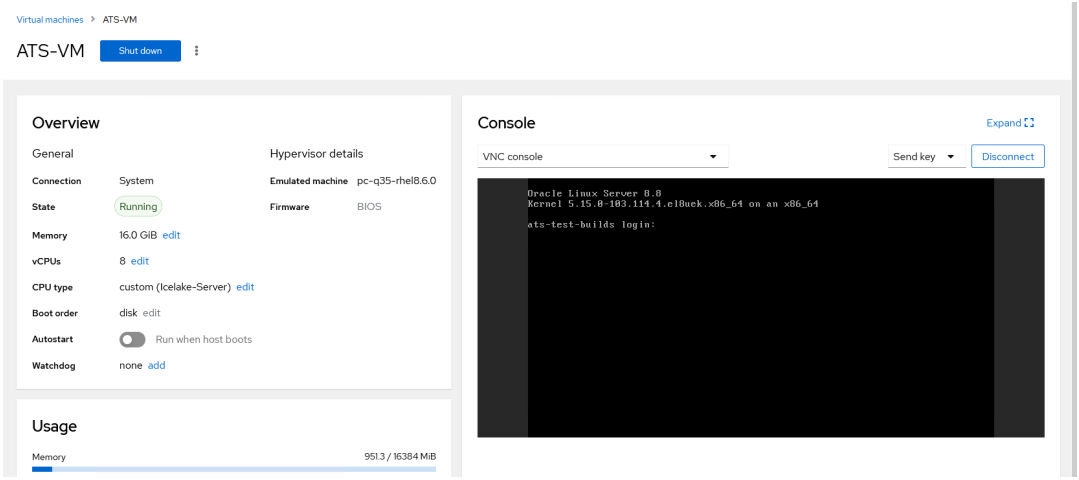



**Figure 2-7 Console**




7. Wait for few minutes to install the VM and once installation is done, the **Console** is displayed as below:

**Figure 2-8 Console**




8. Log in with cloud-user/NextGen123@.
9. Run the following commands for assigning an IP address for the ATS VM:

```
ip addr add <Ip address/subnet> dev <oam-interface-name>
```

```
ip route add default via <gateway_ip> dev <oam-interface-name>
```

For example:

```
ip addr add 10.75.204.158/24 dev eth0
```

```
ip route add default via 10.75.204.129 dev eth0
```

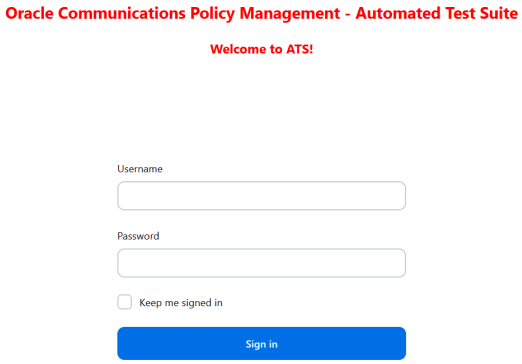
Check the IP address and subnet mask of the network interface, and ensure that the gateway IP address is within the same subnet.

# Logging into ATS

After the ATS VM is deployed, follow the below steps to log in to the ATS:

1. Open a browser and provide the IP address details and port details as https://<ATS_IP>:8443/.

**Figure 2-9 ATS Login**



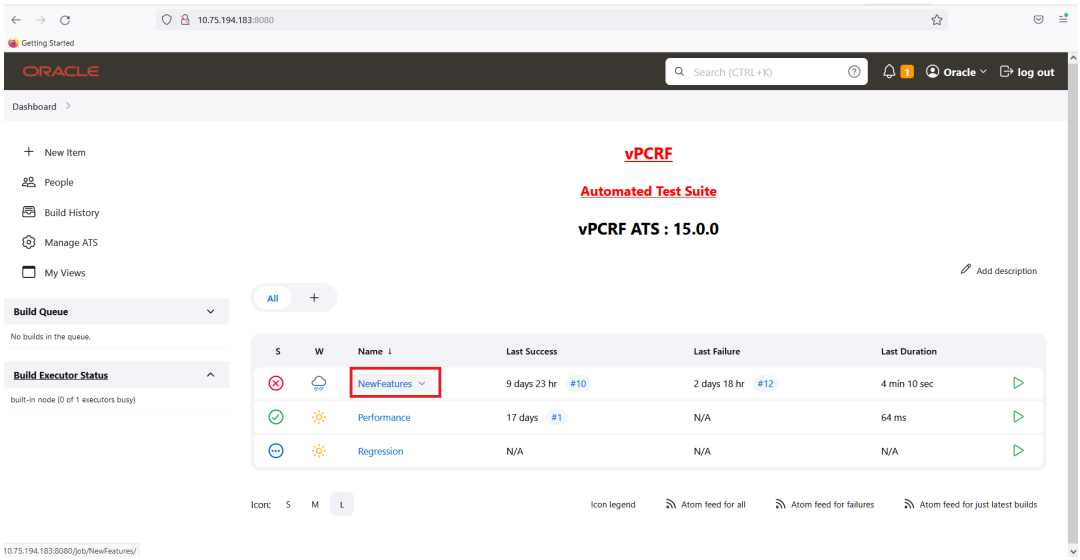

> **Note:**
>
> If TLS is not configured for ATS, then a security exception needs to be added on the browser to access ATS. To configure TLS for ATS, see Enabling ATS GUI with HTTPS.

2. Enter the log in credentials (Default Username: Oracle, Default Password: Welcome@123). Click **Sign in**.

> **Note:**
>
> You are required to change the password after the first log in.

The following ATS dashboard is displayed.

**Figure 2-10 ATS Dashboard**



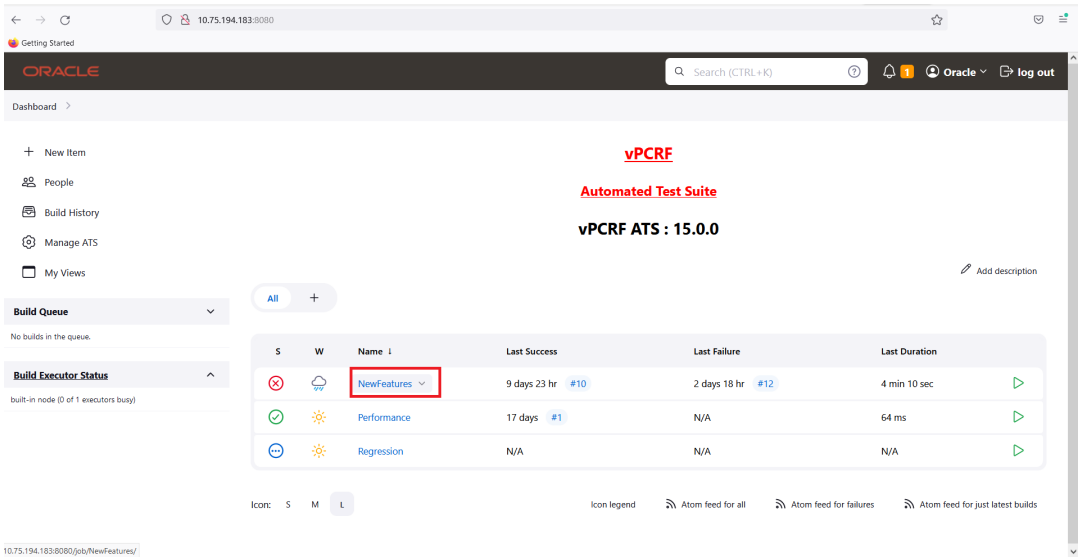

PCRF ATS has three preconfigured pipelines.

- **NewFeatures**: This pipeline has all the test cases delivered as part of the latest build.
- **Performance**: This pipeline is not operational as of now. It is reserved for future releases of ATS where lightweight performance cases will be included.
- **Regression**: This pipeline has all the test cases delivered in older builds of ATS.

# Configure IPs on ATS GUI

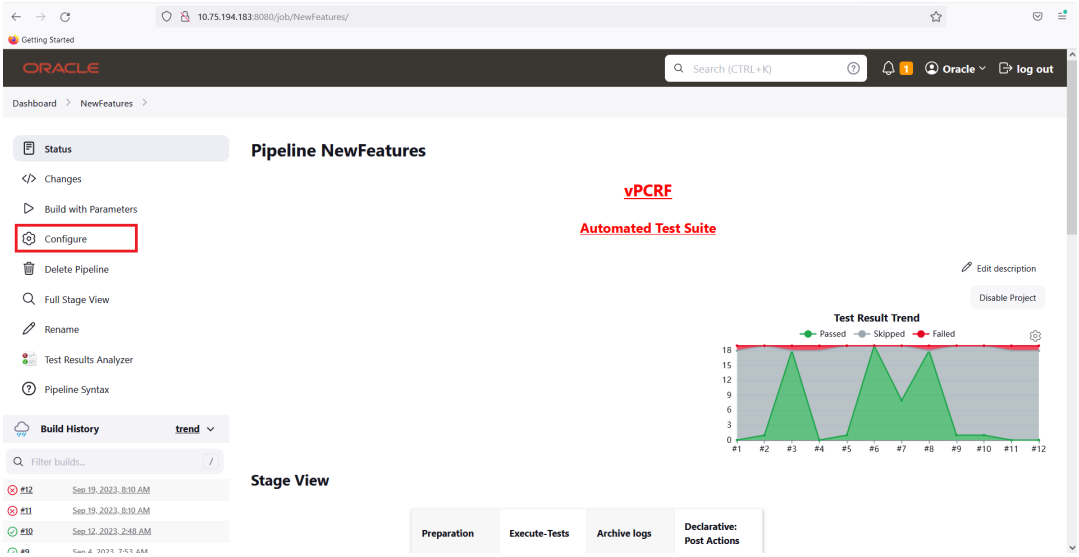
1. Click any of the pipelines(New Features/Performance/Regression) where you want to run the test cases.

**Figure 2-11 Dashboard**



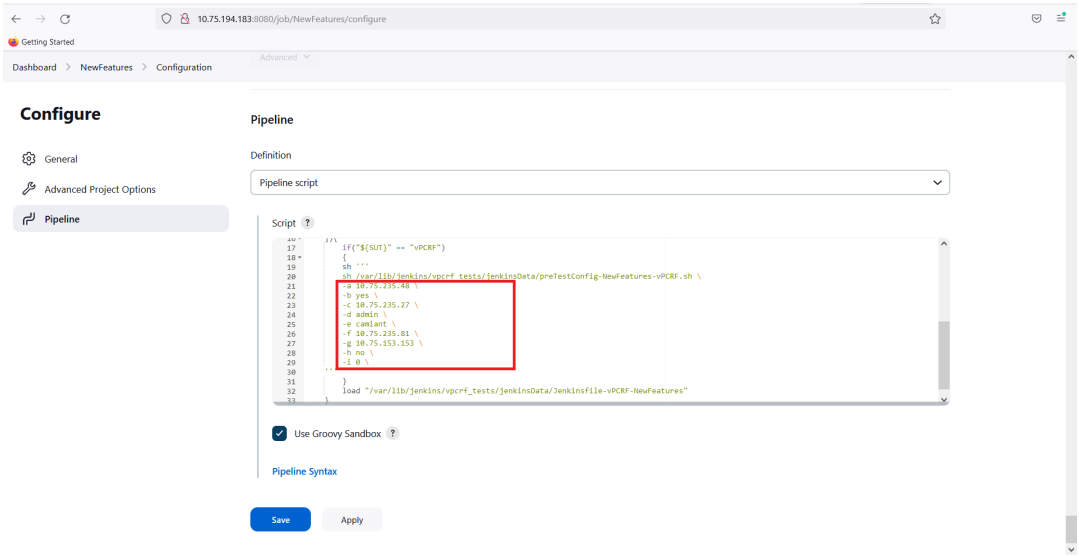

2. Click **Configure** to open the configuration section.

**Figure 2-12 Pipeline New Features**




3. Click the **Pipeline** tab and modify the script parameters depicted below.

**Figure 2-13 Pipeline Script**




The parameters are identified by the alphabets which are described in the script. Here is a detailed overview of the parameters:

**Table 2-1 Configuration parameters**

| Parameter | Description |
|---|---|
| a. MRA_SIGA_IP | SIGA IP of MRA |
| b. UseMRA | options: (yes/no)<br>If traffic is to be routed through MRA, then select this option. |

**Table 2-1 (Cont.) Configuration parameters**

| Parameter | Description |
|---|---|
| c. MPE_SIGA_IP | SIGA IP address of MPE |
| d. CMP_GUI_Username | user name to log in to CMP GUI |
| e. CMP_GUI_Password | password to log in to CMP GUI |
| f. CMP_Host_IP | CMP OAM IP |
| g. ATS_IP | IP address of current ATS Node |
| h. CleanupandReconfigure | options:(yes/no)<br>This option should be set to **yes** when ATS is to be run on a new PCRF setup or a PCRF setup with existing configurations.<br>This cleans up any existing configurations and add necessary configurations to run ATS. Once run for a setup this can be set to **no** for subsequent runs. |
| i. Re-run count | If a test case fails, this parameter decides how many times it should be rerun. |

Here is a sample configuration:

-a 10.75.235.48 \

-b yes \

-c 10.75.235.27 \

-d admin \

-e camiant \

-f 10.75.235.81 \

-g 10.75.153.153 \

-h no \

-i 0 \

> **Note:**
>
> You must provide IPv6 addresses without any square brackets.

4. Click **Save** after making the necessary changes.

# Exchange SSH-keys with PCRF

1. SSH into the ATS as a cloud-user and navigate to the `/home/cloud-user/tools` directory.
2. Ensure all PCRF IPs (atleast OAM VIP and SIG-A IPs) are reachable from ATS before exchanging SSH keys.
3. Modify the *NodeInfo.yaml* file and provide the IPs for the CMP, MPE, and MRA. If you have multiple MPE or MRA clusters in the PCRF setup, then provide the IPs for the cluster that you wish to use for ATS. If Standby blades are not present on your system, then enter N/A for the Standby nodes.
   **Sample Configuration:**

- CMP_OAM_VIP: 10.75.151.185
- Active_CMP: 10.75.151.253
- Standby CMP: N/A
- MPE_SIGA: 10.75.235.32
- Active_MPE: 10.75.151.142
- Standby_MPE: N/A
- MRA_SIGA: 10.75.235.108
- Active_MRA: 10.75.151.145
- Standby_MRA: N/A

4. Run the ssh key exchange script as a cloud-user with `./exchange_SSH_Keys.py`.
5. Enter the password of admusr in topology of PCRF system and wait for the script to complete. Try to ssh into the PCRF nodes, it should not ask for password.

**Figure 2-14 Successful SSH key exchange**

```
[cloud-user@ats-build-15001 tools]$
[cloud-user@ats-build-15001 tools]$ ./exchange_SSH_Keys.py

Enter password of admusr in PCRF topology:

Connecting......
Exchanging SSH keys with Active_CMP (10.75.151.243) [OK]
Exchanging SSH keys with Active_MPE (10.75.151.14) [OK]
Exchanging SSH keys with Active_MRA (10.75.151.159) [OK]

All SSH keys are OK
[cloud-user@ats-build-15001 tools]$
```

6. If Standby node IPs were configured, then even after the failover to the Standby blades, ATS will run properly. Only if the failover occurs to server-C Spare blades or Secondary CMP site, then the ssh key exchange has to be done again with new the IPs.

# 3
# ATS Features

This chapter describes PCRF ATS features.

## ATS Jenkins Job Queue

The ATS Jenkins Job Queue feature is to queue the second job if the current job is already running from the same or different pipelines to prevent jobs from running in parallel to one another. In Jenkins the total number of executors is one, this makes the jobs wait for resource allocation if the new pipeline is triggered.

Job/build queue status can be viewed in the left navigation pane on the ATS home page.

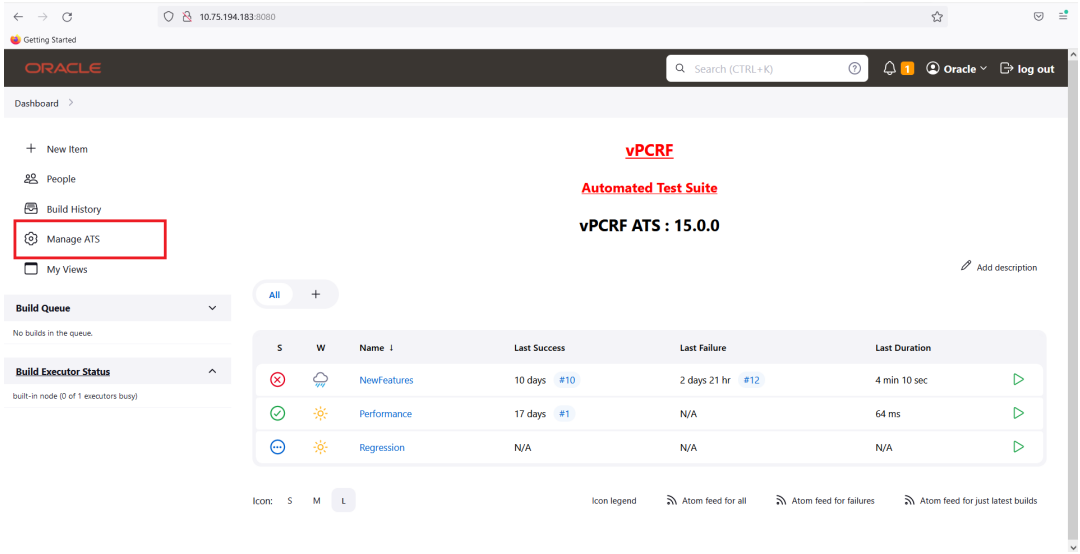
## Updating Users and Login Password

### Managing Users

To create or delete new users:

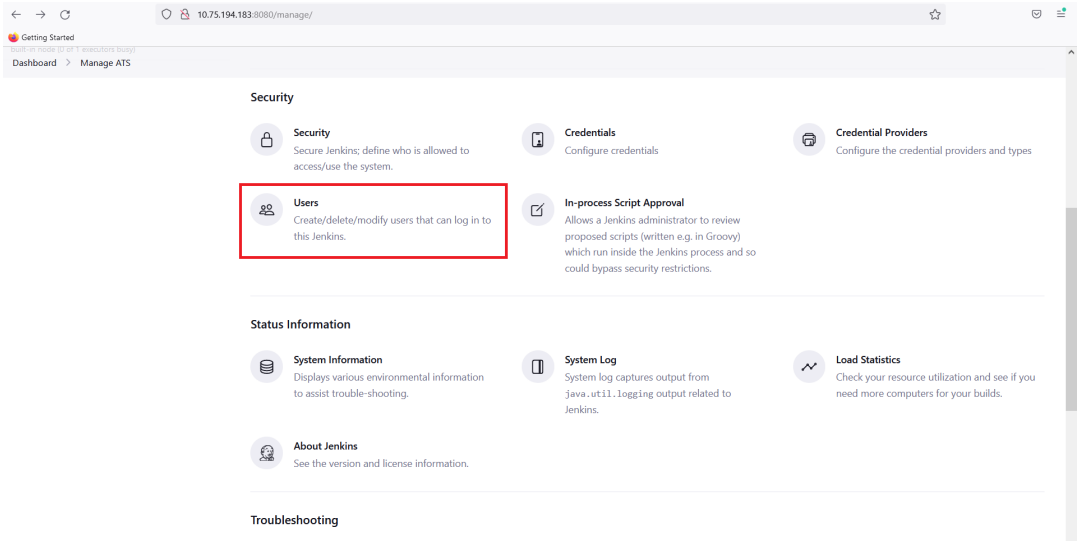
1. On the main dashboard, click **Manage ATS**.

**Figure 3-1 Manage ATS**



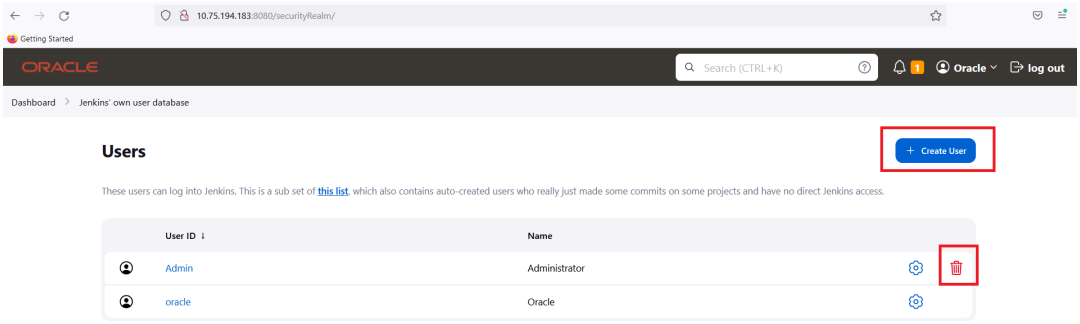

2. Scroll down and click **Users**.

**Figure 3-2 User Menu**




3. Click **+ Create User** to create a new user. Enter username, password, name, and email. Any dummy email can be provided. After entering the details, click **Save** and then the new user can be used to login.

**Figure 3-3 Create User**



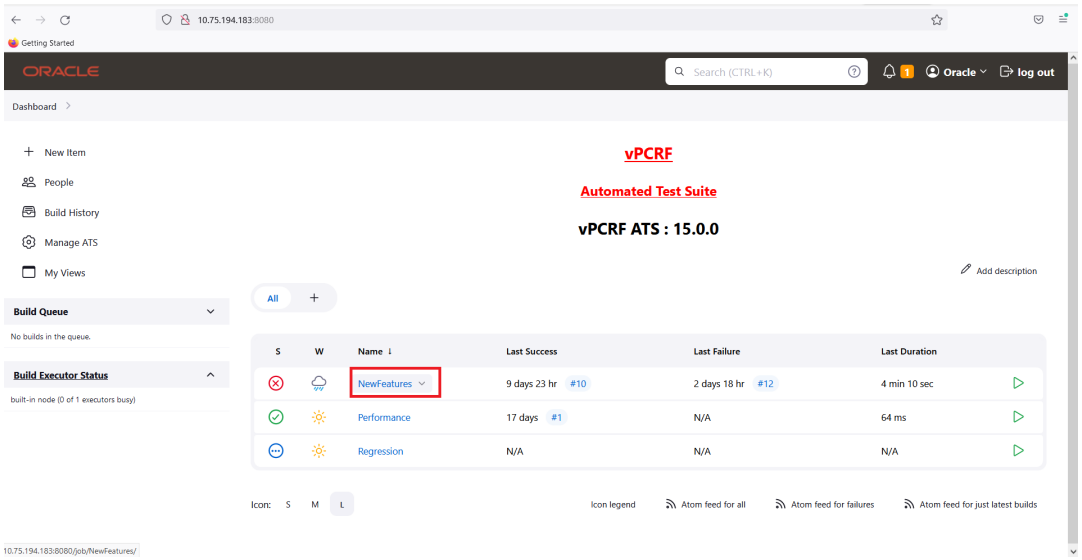

4. Click the Delete icon to delete the existing user.

# Modifying Login Password

To modify the login password:

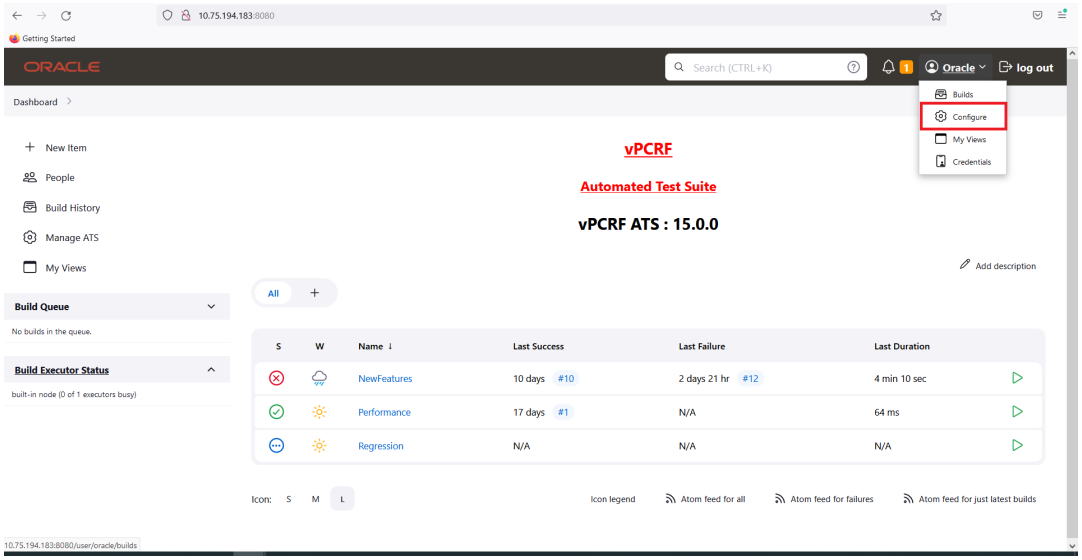
1. Log in to the ATS application using the default login credentials. The home page appears with its preconfigured pipelines as follows:

**Figure 3-4 ATS Dashboard**



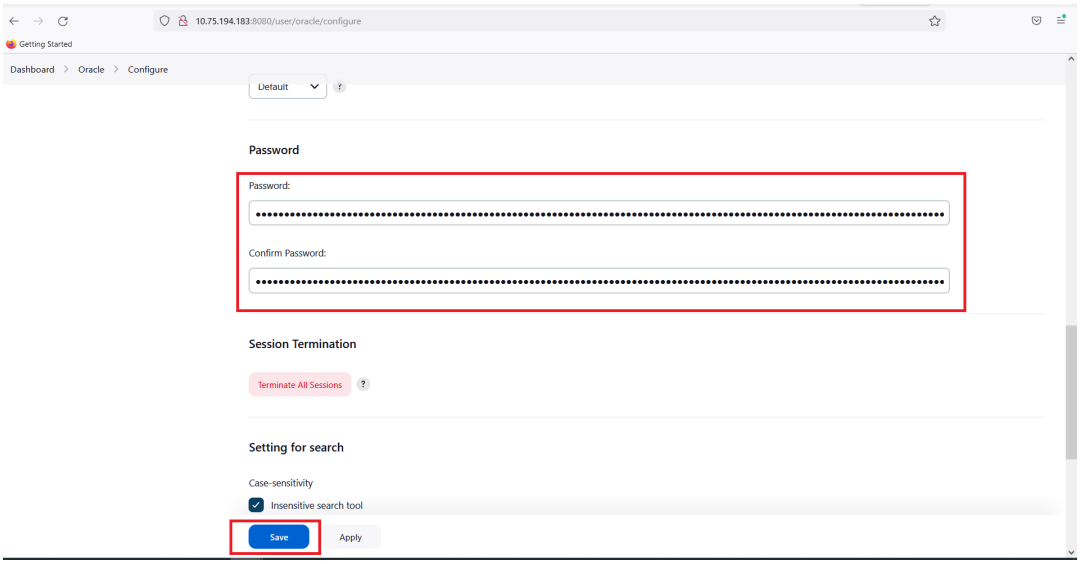

2. Hover over the user name and click the down arrow.
3. Click **Configure**.

**Figure 3-5 Configure User**




4. In the Password section, enter the new password in the Password and Confirm Password fields.

**Figure 3-6 Modify Password**



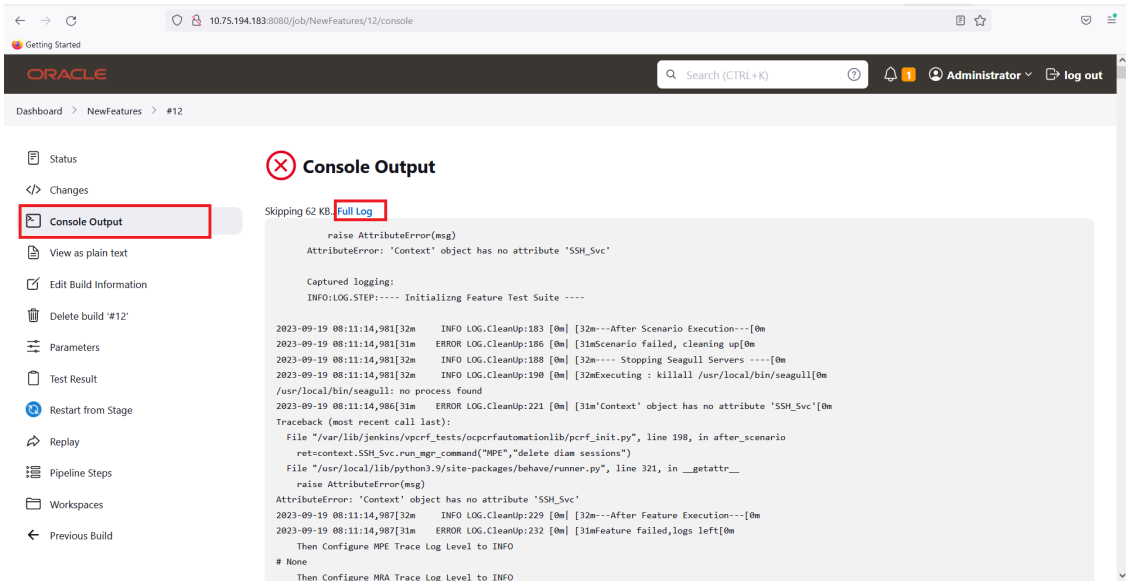

5. Click **Save**.

A new password is set for the user.

# Log Collection

After a test case run is completed, the logs for that execution can be found by clicking the **Build** and then **Console Output**. It is compressed by default, the full log can be viewed by clicking the **Full Log**. It contains a detailed description on all operations performed by ATS during the execution.

**Figure 3-7 Log Collection**




The logs captured from PCRF can be found at /var/lib/jenkins/vpcrf_tests/Logs. The logs captured from seagull can be found at /home/cloud-user/logs.

# Test Results Analyzer

The Test Results Analyzer is a plugin available in ATS to view the pipeline test results based on XML reports. It provides the test results report in a graphical format, which includes consolidated and detailed stack trace results in case of any failures. It allows you to navigate to each and every test.

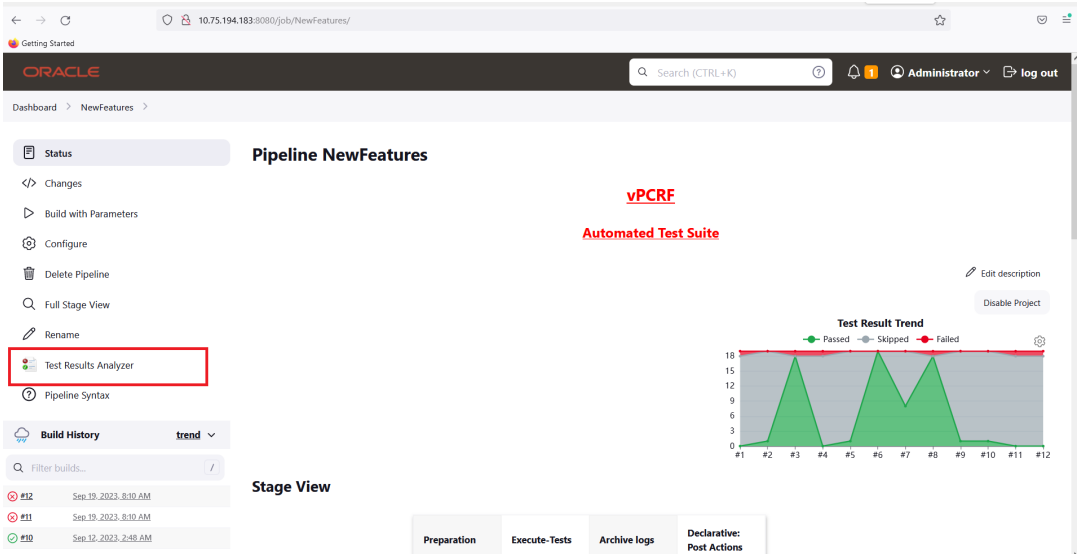
The test result report shows any one of the following statuses for each test case:

- **PASSED**: If the test case passes.
- **FAILED**: If the test case fails.
- **SKIPPED**: If the test case is skipped.
- **N/A**: If the test cases is not executed in the current build.

To access the test results analyzer feature:

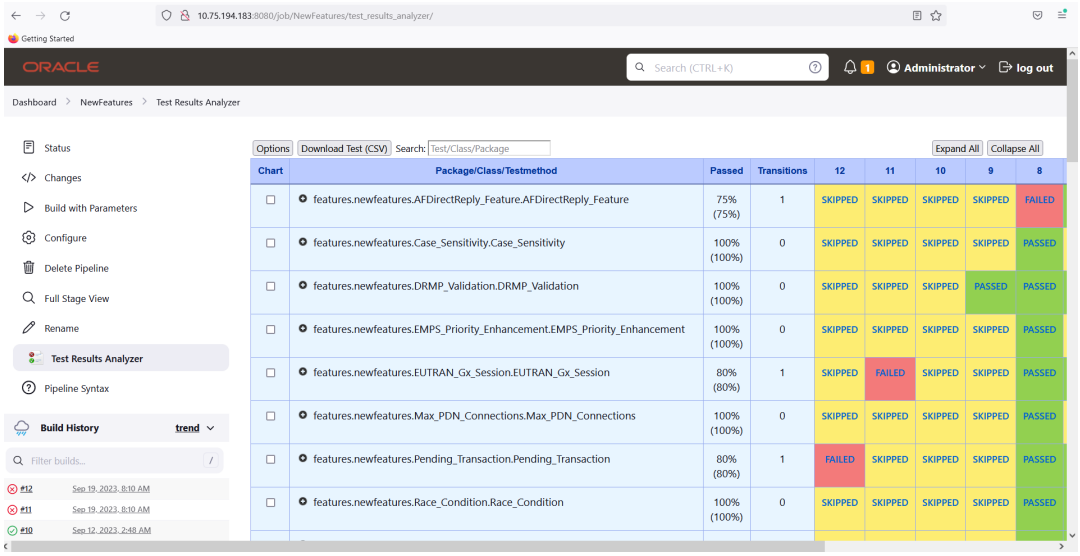
1. From the ATS dashboard, click any pipeline where you want to run this plugin.
2. In the left navigation pane, click **Test Results Analyzer**.

**Figure 3-8 Test Results Analyzer**




When the build completes, the test result report appears. A sample test result report is shown below:

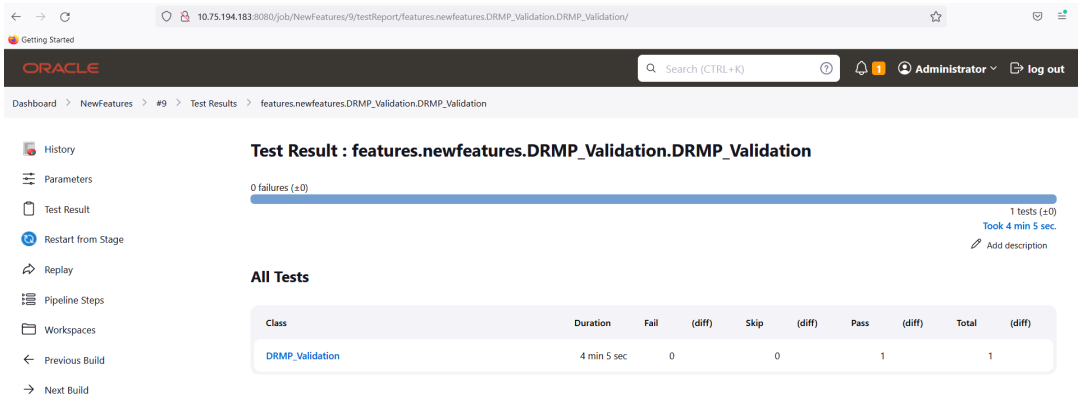
**Figure 3-9 Test Result Report**




3. Click any one of the statuses (PASSED, FAILED, SKIPPED) to view respective feature detail status report.

> **Note:**
>
> N/A Status will not show detailed reports.

**Figure 3-10 Sample Test Result**

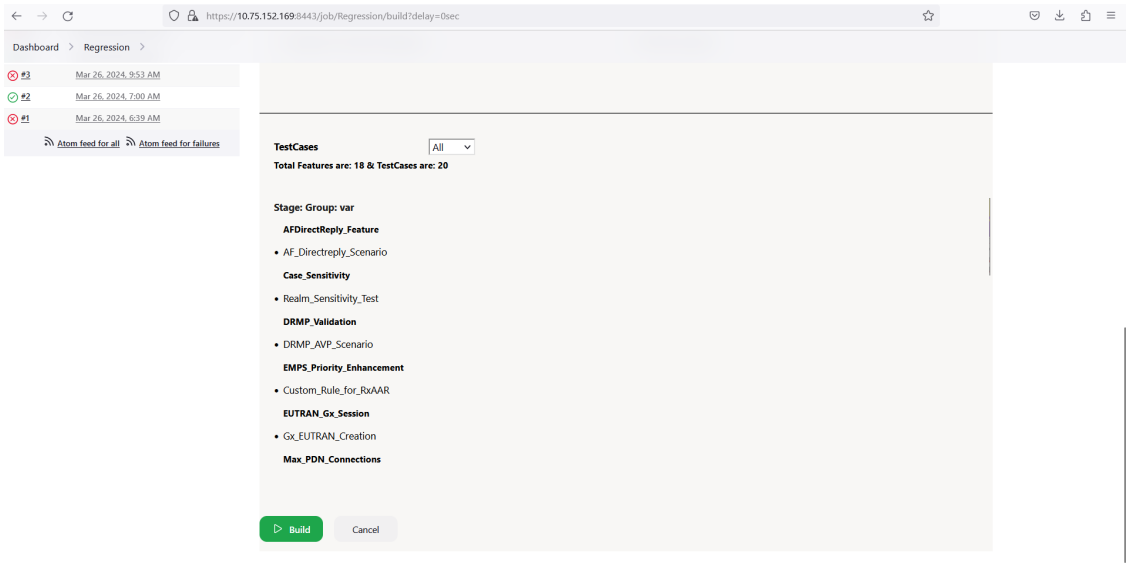



# Test Case Mapping and Count

The 'Test Case Mapping and Count' feature displays total number of features, test cases or scenarios and its mapping to each feature in the ATS GUI.

This feature can be utilized while selecting test cases to be run, the details of features and scenarios selected are listed appropriately with the total test case scenario count:

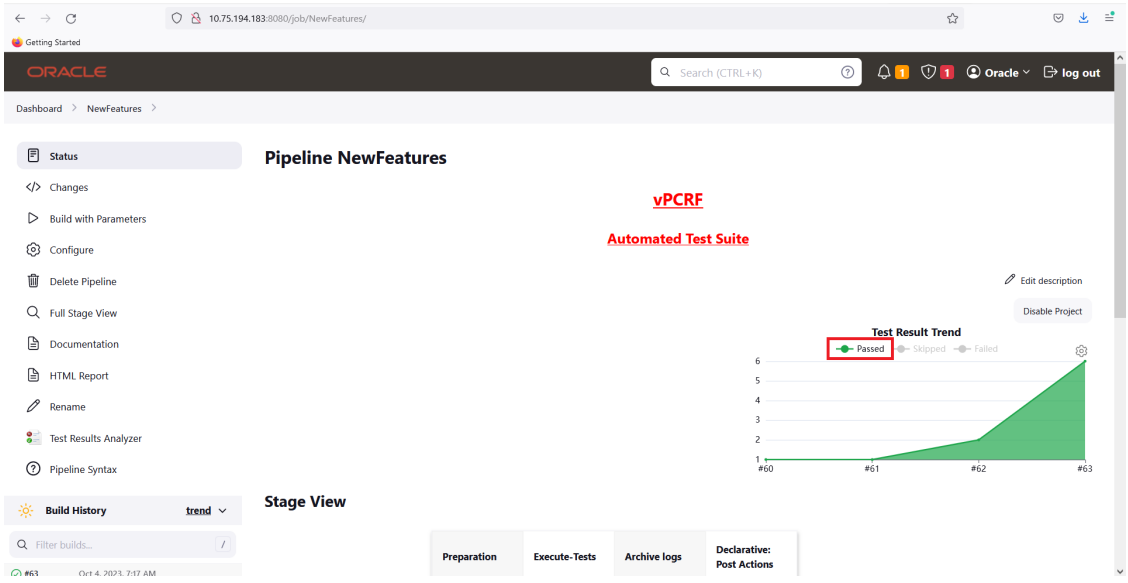
**Figure 3-11 Test Case Mapping and Count**




# Test Result Graph

The graph on the Pipeline dashboard displays the history of passed, skipped, and failed test cases for the previous runs. User can select any one option (Passed, Skipped, and Failed) at a time by clicking on it to view the results of the previous runs in graphical format. Below is a sample screen capture of test result graph:

**Figure 3-12 Test Result Graph**




# ATS Documentation

This section describes the documentation for all the pipelines.

> **Note:**
>
> Documentation is generated only after running the test cases.

To view the documentation for any of the pipelines:

1. On the ATS Dashboard, click any one of the pipelines.
2. Click **Documentation** in the left navigation pane. On clicking Documentation, the following page opens with the list of the features.

**Figure 3-13 PCRF NewFeatures-Documentation**

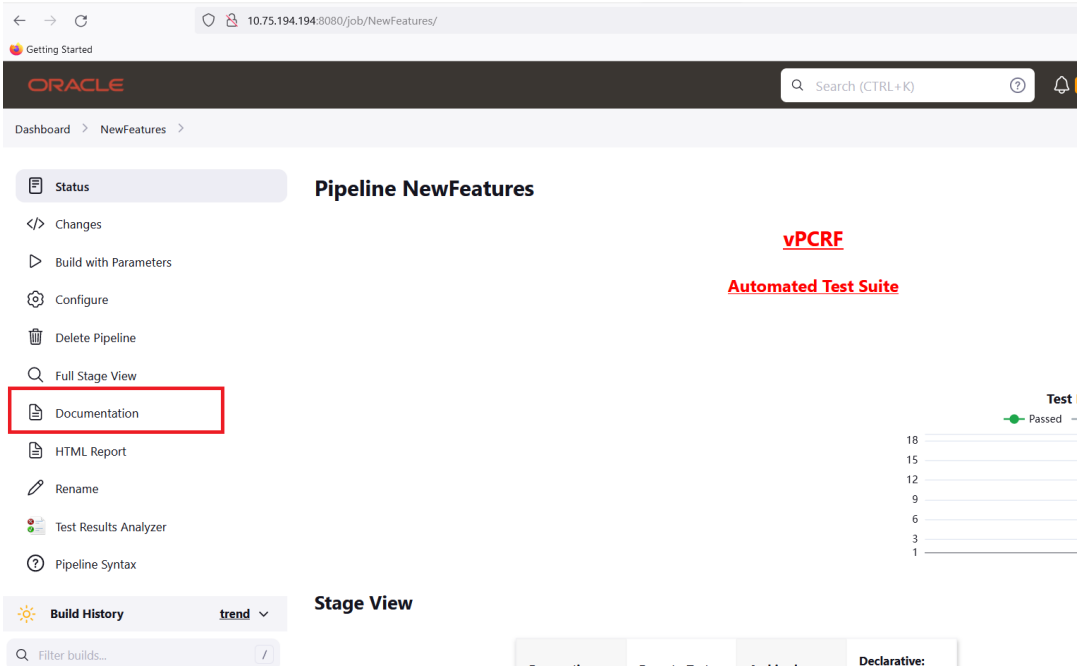
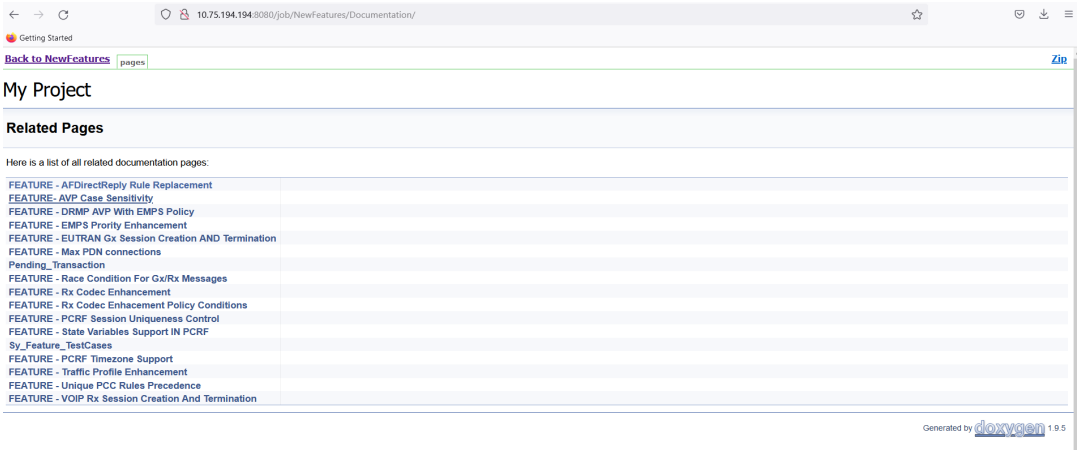



**Figure 3-14 NewFeatures-Documentation**




3. Click any feature or scenario to open documentation for that feature and scenario.

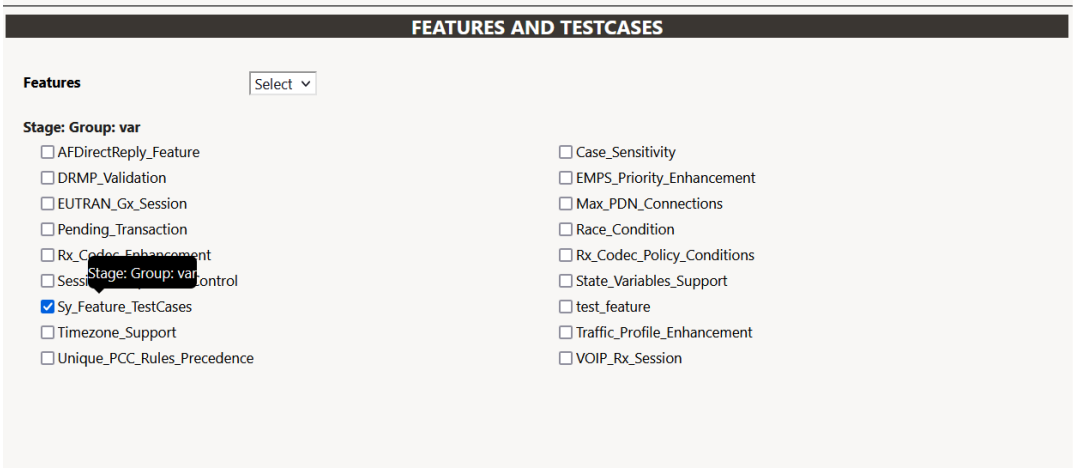
# Individual Scenario Selection

This release of ATS comes with a new feature that enables users to select not only features but individual scenarios within those features.

This feature helps the customer to run a specific test case based on their requirements. Here are the steps to follow:

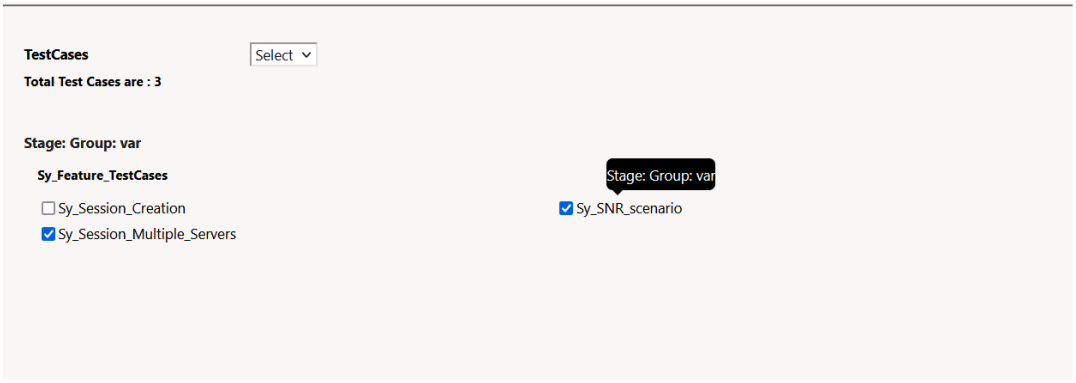
1. Select the feature that is to be run.

**Figure 3-15 Feature Selection**




2. Select the scenario that is to be run.

**Figure 3-16 Scenario Selection**




# Abort Build

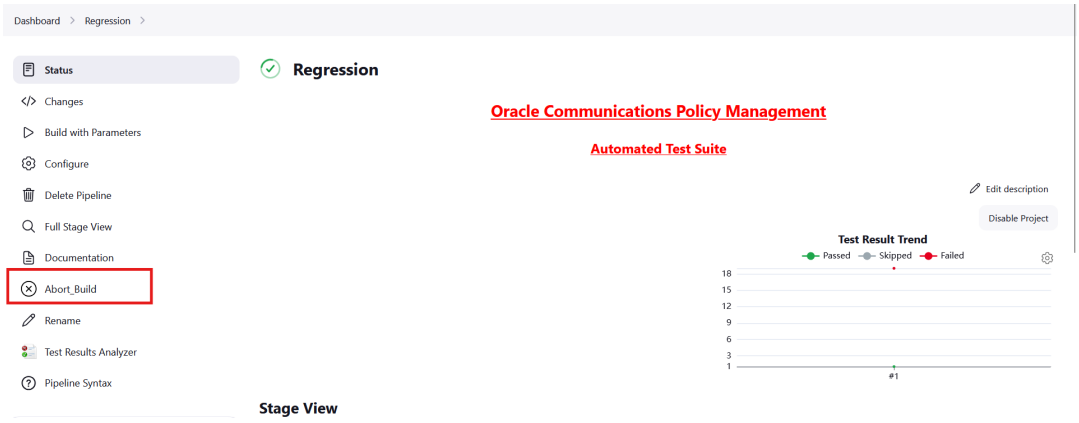
ATS provides the feature to abort running builds. The feature gracefully terminates all open connections, cleans up leftover data and skips the remaining test cases. The test cases which are already run are displayed in the test results with the appropriate status.

To abort the a running build:

1. On the ATS Dashboard, click the pipeline where the build is running.

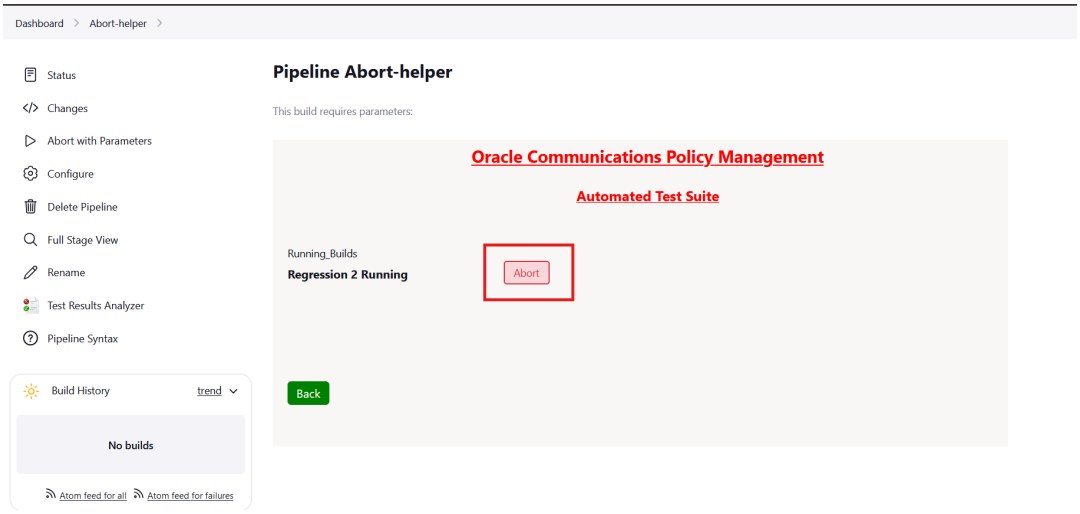
2. Click **Abort_Build** on the left-hand menu.

**Figure 3-17 Abort Build**



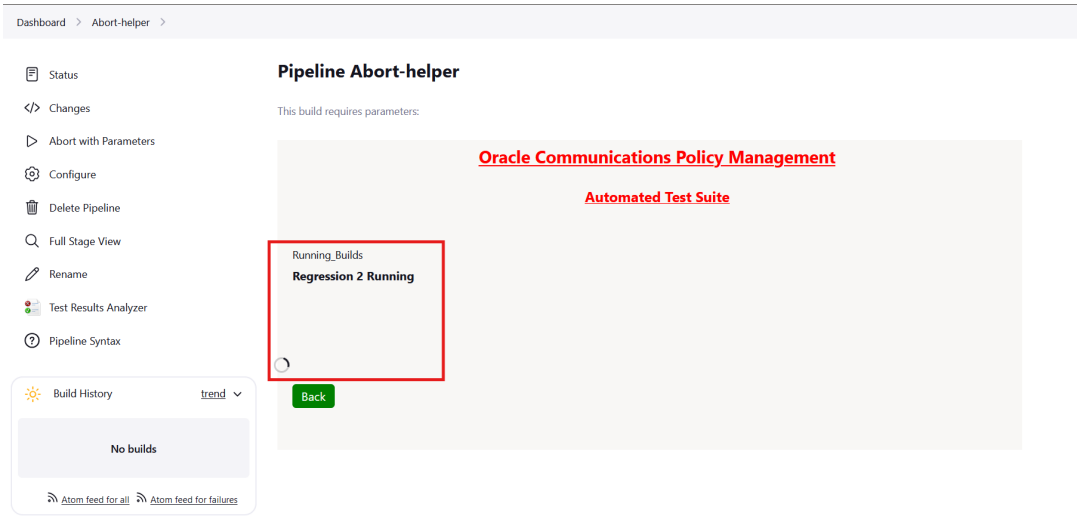

3. Select the **Abort** button next to build to be aborted.

**Figure 3-18 Abort the Build**




4. Once the abort process starts, go back to the main menu and wait for the build to be aborted.

**Figure 3-19 Main Menu**




# Support for Transport Layer Security

With the support of the TLS feature, Jenkins servers have been upgraded to support HTTPS, ensuring a secure and encrypted connection when accessing the ATS dashboard.

To provide encryption, HTTPS uses an encryption protocol known as Transport Layer Security (TLS), which is a widely accepted standard protocol that provides authentication, privacy, and data integrity between two communicating computer applications.

Now, users can access the ATS GUI with the HTTPS protocol instead of the previously used HTTP protocol.

## Deploying ATS with TLS Enabled

This section describes how to create a Java KeyStore (JKS) file and enable the ATS GUI with HTTPS.

### Generating JKS File for Jenkins Server

A Java KeyStore (JKS) file needs to be created in order for Jenkins to provide ATS GUI access through HTTPS.
Perform the following steps to generate a JKS file:

Latest versions of ATS contains a self-generated certificate that is used for all jenkins related operations. To enable TLS and add a self-signed or third-party signed certificate, the automatic certificate generation must be disabled and then the certificate should be added. To disable automatic certificate generation: comment out the line `sh /var/lib/jenkins/certs_generator.sh` in the `/home/cloud-user/jenkins_start.sh` file and save the file.

For example,

```
# nohup java -jar /usr/lib/jenkins/jenkins.war >/dev/null 2>&1 &
  # nohup java -Dhudson.model.WorkspaceCleanupThread.disabled=true -jar
  /usr/lib/jenkins/jenkins.war >/dev/null 2>&1 &
  #sh /var/lib/jenkins/certs_generator.sh
```

```
# Start Jenkins with HTTPS configuration
```

### Generate the Root Certificate

The root certificate is used to sign the application, or ATS certificate. If a root certificate, for example, caroot.cert, is not already available, a user can generate the root certificate. Users may use their own files if they have a CA signed root certificate and key or their own root certificates.

Perform the following steps to create and use self-signed certificates:

1. Generate a root key with the following command:

   ```
   openssl genrsa 2048 > <path_to_root_key>
   ```

   For example:

   ```
   openssl genrsa 2048 > caroot.key
   ```

2. Generate a "caroot" certificate with the following command:

   ```
   openssl req -new -x509 -nodes -days 1000 -key <path_to_root_key> >
   <path_to_root_certificate>
   ```

   For example:

   ```
   openssl req -new -x509 -nodes -days 1000 -key caroot.key > caroot.cer
   ```

   You will be asked to enter information that will be incorporated into your certificate request.

   You need to enter a Distinguished Name (DN). Few fields can be left blank while entering the DN. For some fields, there will be a default value. If you enter '.', the field will be left blank.

   - Country Name (2 letter code) [XX]:IN
   - State or Province Name (full name) []:KA
   - Locality Name (eg, city) [Default City]:BLR
   - Organization Name (eg, company) [Default Company Ltd]:ORACLE
   - Organizational Unit Name (eg, section) []:CGBU
   - Common Name (eg, your name or your server's hostname) []:ocats
   - Email Address []:[cloud-user@star23-bastion-1 cert]$

### Generate Application or Client Certificate

Perform the following steps to create and edit the ssl.conf file:

1. In the **alt_names** section, list the IPs, such as IP.1, IP.2, and so on, that are used to access the ATS GUI:
   [ req ]

   default_bits = 4096

   distinguished_name = req_distinguished_name

req_extensions = req_ext

[ req_distinguished_name ]

countryName = Country Name (2 letter code)

countryName_default = <Country_Name>

stateOrProvinceName = State or Province Name (full name)

stateOrProvinceName_default = <State_Name>

localityName = Locality Name (eg, city)

localityName_default = <Locality_Name>

organizationName = Organization Name (eg, company)

organizationName_default = <Org_Name>

commonName = Common Name (e.g. server FQDN or YOUR name)

commonName_max = 64

commonName_default = <helm_name>.<namespace>.svc.cluster.local

[ req_ext ]

keyUsage = critical, digitalSignature, keyEncipherment

extendedKeyUsage = serverAuth, clientAuth

asicConstraints = critical, CA:FALSE

subjectAltName = critical, @alt_names

[alt_names]

IP.1 = 127.0.0.1

IP.2 = <IP1>

IP.3 = <IP2>

DNS.1 = <helm_name>.<namespace>.svc.cluster.local

For example,

[ req ]

default_bits = 4096

distinguished_name = req_distinguished_name

req_extensions = req_ext

[ req_distinguished_name ]

countryName = Country Name (2 letter code)

countryName_default = <Country_Name>

stateOrProvinceName = State or Province Name (full name)

stateOrProvinceName_default = <State_Name>

localityName = Locality Name (eg, city)

localityName_default = <Locality_Name>

organizationName = Organization Name (eg, company)

organizationName_default = <Org_Name>

commonName = Common Name (e.g. server FQDN or YOUR

name)

commonName_max = 64

commonName_default = ocats.scpsvc.svc.cluster.local

[ req_ext ]

keyUsage = critical, digitalSignature, keyEncipherment

extendedKeyUsage = serverAuth, clientAuth

basicConstraints = critical, CA:FALSE

subjectAltName = critical, @alt_names

[alt_names]

IP.1 = 127.0.0.1

IP.2 = 10.75.217.5

IP.3 = 10.75.217.76

DNS.1 = localhost

DNS.2 = ocats.scpsvc.svc.cluster.local

> **Note:**
>
> - To access the GUI with Domain Name System (DNS), make sure that the commonName_default is the same as the DNS name being used.
> - Multiple DNS, such as DNS.1, DNS.2, and so on, can be added.
> - To support the ATS API, add the IP 127.0.0.1 to the list of IPs.

2. Create a Certificate Signing Request (CSR) with the following command:

```
openssl req -config ssl.conf -newkey rsa:2048 -days 1000 -nodes -
keyout<path_to_application_certificate_key>
><path_to_certificate_signing_request>
```

For example,

```
openssl req -config ssl.conf -newkey rsa:2048 -days 1000 -nodes -keyout
rsa_private_key_pkcs1.key >ssl_rsa_certificate.csr
```

The key name should always be `rsa_private_key_pkcs1.key`.

The following output is displayed:

Ignoring -days; not generating a certificate

Generating a RSA private key...+++++.....+++++

writing new private key to 'rsa_private_key_pkcs1.key'

---

You will be asked to enter information that will be incorporated into your certificate request.

You need to enter a Distinguished Name (DN). Few fields can be left blank while entering the DN. For some fields, there will be a default value. If you enter '.', the field will be left blank.

- Country Name (2 letter code) [IN]:
- State or Province Name (full name) [KA]:
- Locality Name (eg, city) [BLR]:
- Organization Name (eg, company) [ORACLE]:
- Common Name (e.g. server FQDN or YOUR name) [ocats]:
- Email Address []:[cloud-user@star23-bastion-1 cert]$

3. Display the components of the file and verify the configurations with the following command:

```
openssl req -text -noout -verify -in ssl_rsa_certificate.csr
```

4. Sign in to this CSR file with the root certificate with the following command:

```
openssl x509 -extfile ssl.conf -extensions req_ext -req -in
<path_to_certificate_signing_request> -days 1000 -CA
<path_to_root_certificate> -CAkey <path_to_root_key> -set_serial 04
> <path_to_application_certificate>
```

For example,

```
openssl x509 -extfile ssl.conf -extensions req_ext -req -in
ssl_rsa_certificate.csr -days 1000 -CA caroot.cer -CAkey caroot.key -
set_serial 04 >ssl_rsa_certificate.crt
```

The signed certificate name must always be `ssl_rsa_certificate.crt`.

The following output is displayed:

Signature ok

subject=C = IN, ST = KA, L = BLR, O = ORACLE, CN = ocats

Getting CA Private Key

[cloud-user@star23-bastion-1 cert]$

5. Verify that the certificate is properly signed by the root certificate with the following command:

```
openssl verify -CAfile
<path_to_root_certificate><path_to_application_certificate>
```

For example,

```
openssl verify -CAfile caroot.cer ssl_rsa_certificate.crt
```

The following output is displayed:

ssl_rsa_certificate.crt: OK

6. Save the generated application certificates and the root certificates.

7. Add the caroot.cer to the browser as a trusted author. For more information, see Enabling ATS GUI with HTTPS.
8. Generate the .p12 keystore file with the following command:

   ```
   openssl pkcs12 -inkey <path_to_application_key> -
   in<path_to_application_certificate> -export -out<path_to_p12_certificate>
   ```

   For example,

   ```
   openssl pkcs12 -inkey rsa_private_key_pkcs1.key -in
   ssl_rsa_certificate.crt -export -outcertificate.p12
   ```

   Enter password as Welcome@123.

   The following output is displayed:

   Enter Export Password:

   Verifying - Enter Export Password:
9. Convert the .p12 keystore file into a JKS format file with the following command:

   ```
   keytool -importkeystore -srckeystore <path_to_p12_certificate> -
   srcstoretype pkcs12 -destkeystore <path_to_jks_file> -deststoretypeJKS
   ```

   In the prompt, use the same password used while creating .p12 keystore file.

   In the prompt, use the password Welcome@123.

   For example,

   ```
   keytool -importkeystore -srckeystore ./certificate.p12 -srcstoretype
   pkcs12 -destkeystore jenkinsserver.jks -deststoretype JKS
   ```

   In the prompt, use the password Welcome@123.

   The following output is displayed:

   Importing keystore ./certificate.p12 to jenkinsserver.jks...

   Enter destination keystore password:

   Re-enter new password:

   Enter source keystore password:

   Entry for alias 1 successfully imported.

   Import command completed: 1 entries successfully imported, 0 entries

   failed or cancelled
10. Copy the files **rsa_private_key_pkcs1.key**, **ssl_rsa_certificate.crt**, **jenkinsserver.jks** to `/var/lib/jenkins/certificates/`.
11. Reboot ATS node to restart jenkins.

## Enabling ATS GUI with HTTPS

This section describes the procedure to enable TLS on the server and browser.

Perform the following steps to enable TLS on the server and browser:

**Adding a Certificate in Browser**

Adding a Certificate on Google Chrome in Windows Laptop:

1. In the Chrome browser, navigate to the settings and search for security.
2. Click the **security** option that appears next to **search**.
3. Click the **Manage Device Certificate** option.
4. Click the **Trusted root certification authorities** bar.
5. Import the caroot certificate.
6. Save and restart the browser.

Adding a Certificate on Google Chrome in Mac Laptop:

1. In the Chrome browser, navigate to the settings and search for security.
2. Click the **security** option that appears next to **search**.
3. Click the **Manage Device Certificate** option. The **Keychain Access** window opens.
4. Search the tab certificate and drag and drop the downloaded caroot certificate.
5. Find the uploaded certificate in the list, usually listed by a temporary name.
6. Double click the certificate and expand the **Trust** option.
7. When using this certificate option, assign it to "always trust".
8. Close the window and validate if it asks for the password.
9. Save and restart the browser.

Adding a Certificate on Mozilla Firefox for Windows and Mac Laptop:

1. In the Mozilla Firefox browser, navigate to the settings and search for certificates.
2. Click the **View Certificate** that appears next to search. This opens a **Certificate Manager** window.
3. Navigate to the **Authorities** section, click the **Import** button, and upload the caroot certificate.
4. Click the **Trust** options in the pop-up window and click **OK**.
5. Save and restart the browser.

# 4
# Running Test Cases

This chapter describes how to run PCRF test cases using ATS 15.0.

## Prerequisites for Test Case Execution

This section provides information about the prerequisites that must be achieved in the following sequence before running test cases:

1. Ensure PCRF setup contains atleast one CMP, MPE and MRA cluster defined under topology settings.
2. PCRF's CMP, MPE, MRA IPs should be pingable from ATS, that is, they should be on same network.
3. Enable the `CleanupandReconfigure` option when running test cases on a new setup or an existing setup with existing configurations.
4. Ensure there are no active alarms present.
5. SUT Requirements

**Table 4-1 Minimum SUT Requirements**

| Server | Quantity |
|---|---|
| OCPM MPE Active | 1 |
| OCPM MRA Active | 1 |
| OCPM CMP Active | 1 |

These are the minimum requirements, ATS will also work if Standby, Spare nodes are added in the MPE,MRA, and CMP clusters.

6. Ensure proper feature mode is selected when configuring CMP. Minimum requirement is Diameter 3GPP. When running specific features, ensure that the proper mode is selected. Navigate to Help→ About→ Click on Hidden button left side → Change Mode to select appropriate mode.
7. Ensure all firewalls allow connection between PCRF and ATS. If there are any firewall options configured on the PCRF, then rules should be added to permit ATS connections.

> **WARNING:**
>
> Running ATS on any PCRF setup will cause the MPE/MRA configuration and data to be deleted. Please export the system configurations and take a system backup and server backup to restore system configuration after ATS runs are done.

## Running Test Cases

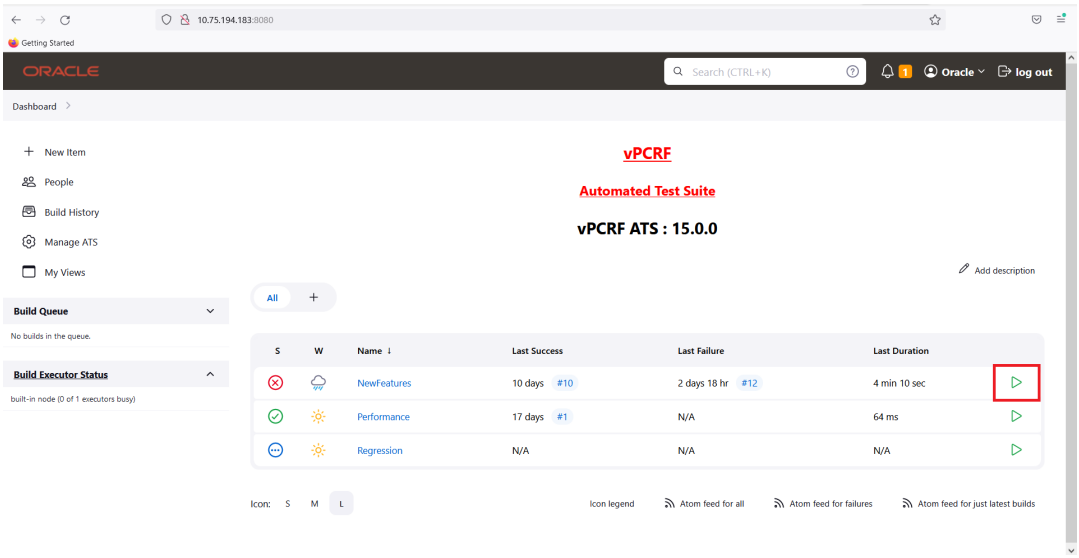
To run the test cases:

> **Note:**
>
> It is recommended to not use the CMP GUI while ATS is running. It can lead to unexpected behavior on CMP.

Complete the tasks described in the Prerequisites section before running the test cases using ATS.

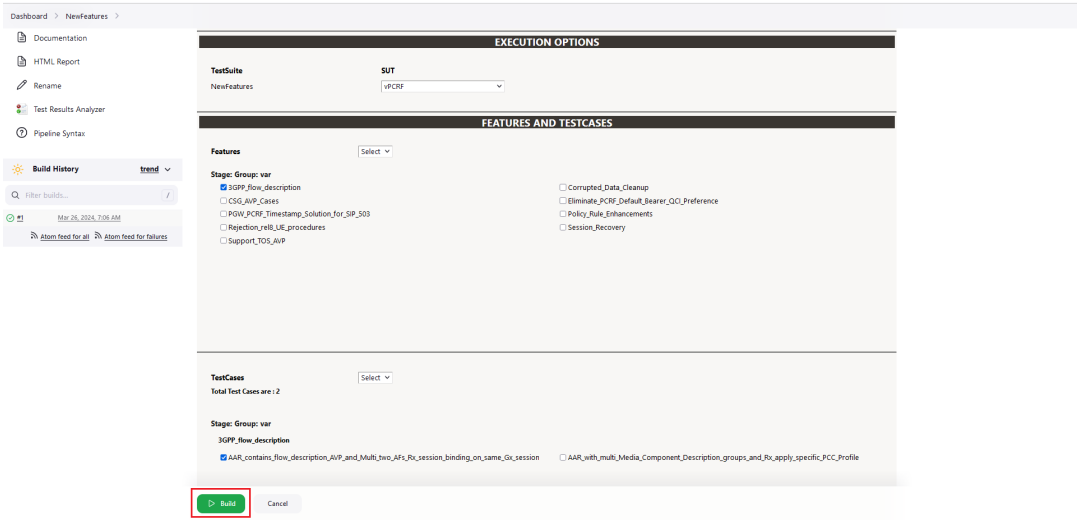
1. Go to https://<ATS_IP>:8443/.
2. Log in to the Jenkins GUI using your login credentials. The system displays the Jenkins GUI.
3. On the ATS Dashboard, select one of the pipelines to run the test cases. Click **Start** for the respective pipeline or click the pipeline name and then select **Build With Parameters**.

**Figure 4-1 Dashboard**



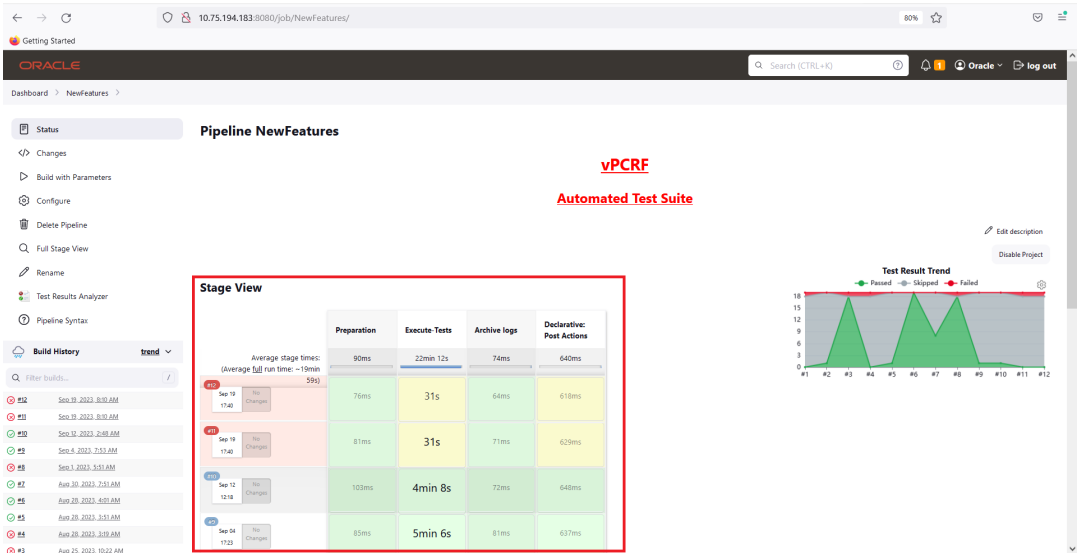

4. The test case selection screen appears, either select the **All** option to run all the test cases in the pipeline or use the **Select** option to select a few test cases to run.
   For the **Select_Option** dropdown, select any of the following values:
   - **All**: By default, all the Policy test cases are selected for execution.
   - **Select Features**: This option allows you to select any number of features that you want to run from the list of all features. Select the checkbox for each feature you want to run. Based on your selection, related test cases appear on the page.
     From the listed test cases, you can further select individual test cases to run:
   - **Select TestCases**: This option allows you to select the individual test cases or scenarios which are present under the selected feature

**Figure 4-2 Pipeline New Features**




5. Once test cases are selected, click **Build** to start the execution, the progress can be monitored on the pipeline dashboard.

**Figure 4-3 Stage View**



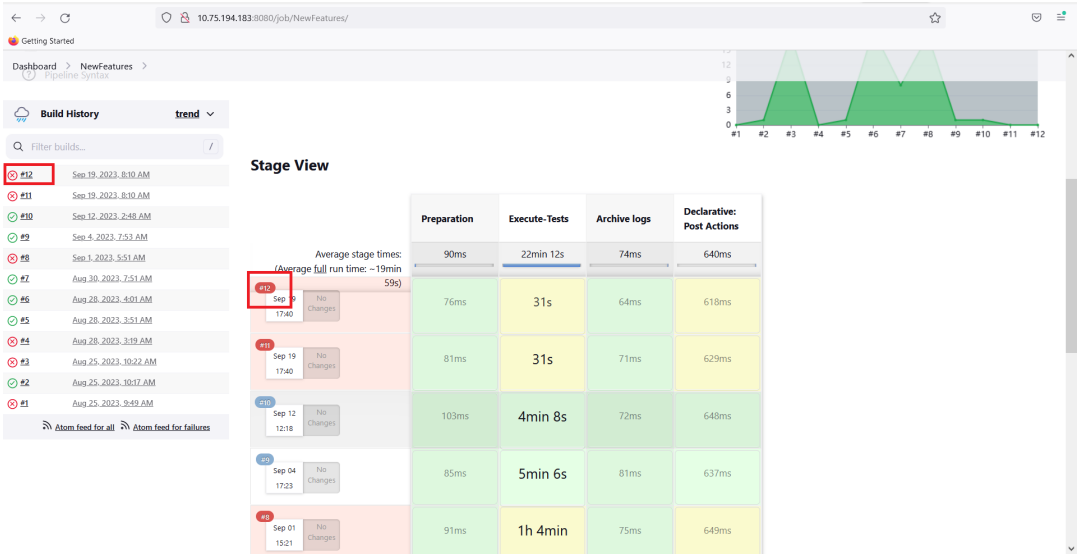

6. Once the run is finished then the build will come with a

or

symbol depicting if all test cases selected have passed or failed.

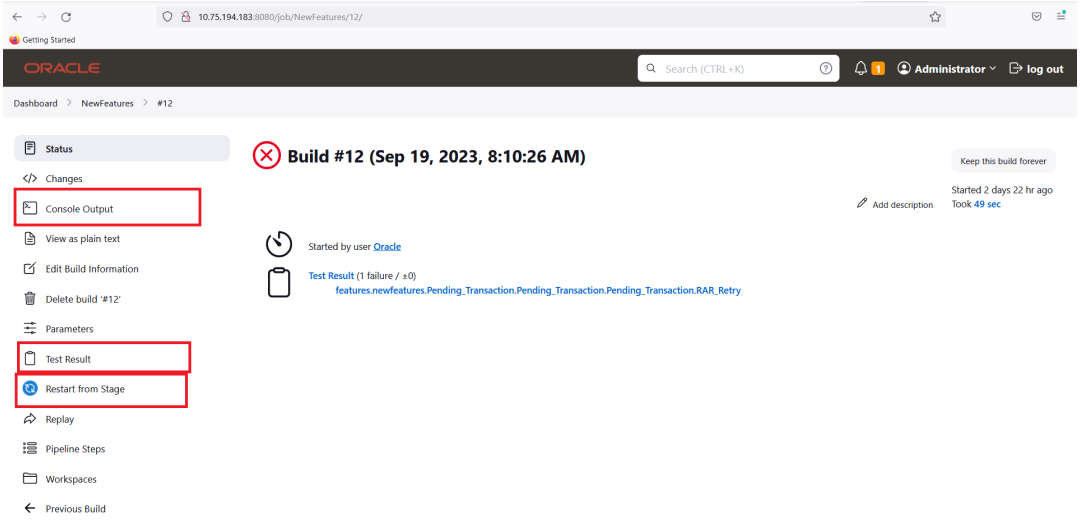
7. To get more detailed information, click on the build number and it will open the build details page.

**Figure 4-4 Stage View Details**




8. On the Build details page, the user can view the logs for the execution, see the test results to check which features have failed and passed and also restart the execution.

**Figure 4-5 Build Status**



# 5
# Troubleshooting Scenarios

This section describes the troubleshooting scenarios for PCRF ATS.

**Problem:** Slowness of MPE recreate operations and increase in ATS execution time. This scenario is seen on the PCRF application and causes the operations performed on the MPE to take more time which results in overall higher execution time for ATS. The issue arises because of how the changes are stored which results in larger config files when a lot of modifications are done on the PCRF system.

**Workaround:** The workaround for the issue is to remove the config files on the PCRF so that they can be created again. These files have to be removed repeatedly as soon as they grow large in size.

Perform the following procedure on the PCRF MPE:

1. Delete the following file on affected MPE:

   ```
   /var/TKLC/rcs/etc/camiant/logconfig/logback-rc.xml,v
   ```

2. Replace the following file with a replacement file on MPE, the replacement file can be extracted from a healthy MPE of same version:

   ```
   /etc/camiant/logconfig/logback-rc.xml
   ```

# Appendix A- Resource Requirements

**Table 1 Resource Requirements**

| Component | vCPU | RAM (GB) | Storage (GB) | vNIC |
|---|---|---|---|---|
| ATS | 8 | 16 | 256 | 1 |

# Appendix B- VM Networking Layout

**Table 2 VM Networking Layout**

| Networking Name/Function | VM vNIC |
|---|---|
| OAM | The eth name will differ depending on the ATS image used:<br>• eth0 (15.0.0.0)<br>• ensX (15.0.0.2) |