Scanning Amazon ORACLE RDS Instance with PC and VM

This document provides step-by-step guide to scanning Amazon Relational Database Service (RDS) Oracle instance for Qualys Policy Compliance and Vulnerability Management.

For more information on RDS refer to the link below.
https://aws.amazon.com/rds/

Table of Contents

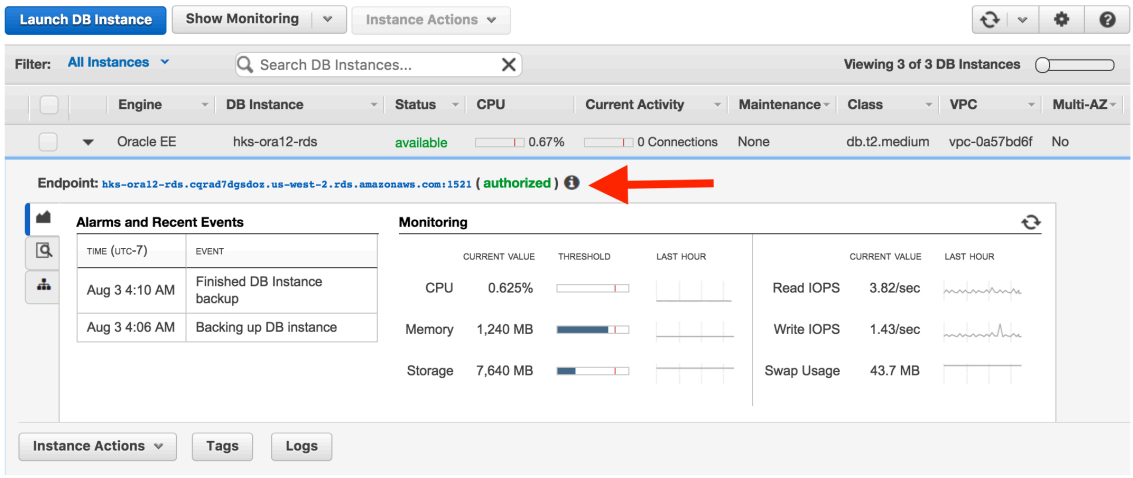
Important Notes

1. One should get a prior approval from AWS, as this process requires using non-authorized scanners.
2. Amazon RDS is a managed service for relational databases. It does not provide access to the low level infrastructure or the OS. There is no SSH, Telnet or Ping access authorized to an RDS instance. Hence OS dependent compliance checks (Windows/Unix) and OPatch checks (Unix) won't work.
3.

Background

RDS scanning is not supported via EC2 scanning today, as RDS instances are not pulled via the EC2 connector. However, one can use the public cloud scanners for RDS instances with public IP and IP based Scanner Appliance deployed in the EC2 environment for private IPs.

When you deploy an Oracle or other RDS instances you are provided with an endpoint similar to one shown in figure 1. This endpoint is internally resolved by AWS to identify your database instance and can also be resolved to either a public or private IP depending on your deployment option of publicly accessible instance or not.



Note: An RDS instance can either be setup as publicly accessible or not, which means the endpoint will resolve to a publically accessible IP or it will be only accessible via private IP.

High-level Steps for Scanning RDS Instances

The high-level steps listed below are generic can be use to scan any RDS instance technologies supported by Qualys PC and VM.

1. Obtain IP address(s) for RDS instances.
2. Add IP address(s) to subscription.
3. Add authentication records (required for PC, optional for VM).
4. Deploy Qualys Scanner Appliance (SA) to EC2 environment. Note this is the non-preauthorized one.
5. Launch PC or VM scans. (For publicly accessible IPs use the SA's in the cloud, for private IPs use SA deployed in step 4)
6. Run reports.

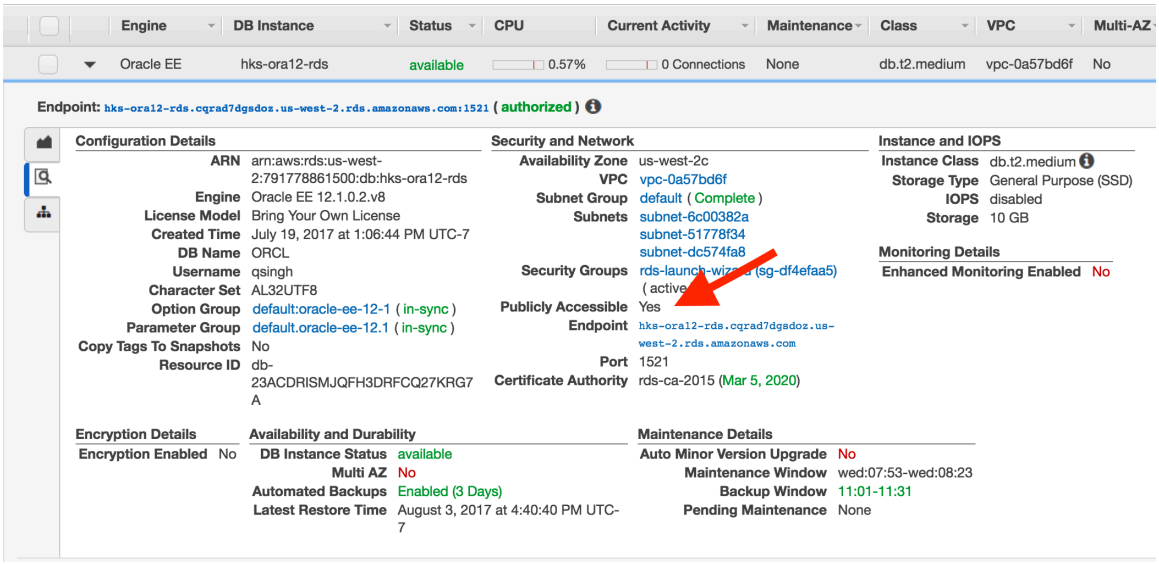
Detailed Steps

Obtaining the IP of RDS Instance

In order to scan a RDS instance for VM or PC you'll need to first resolve the RDS endpoint to an IP address. IP address is also required for the authentication record for PC scanning and is optional for VM scans.

You can obtain IP address of the endpoint by simply pinging RDS Endpoint name minus the port from anywhere. See the examples below.

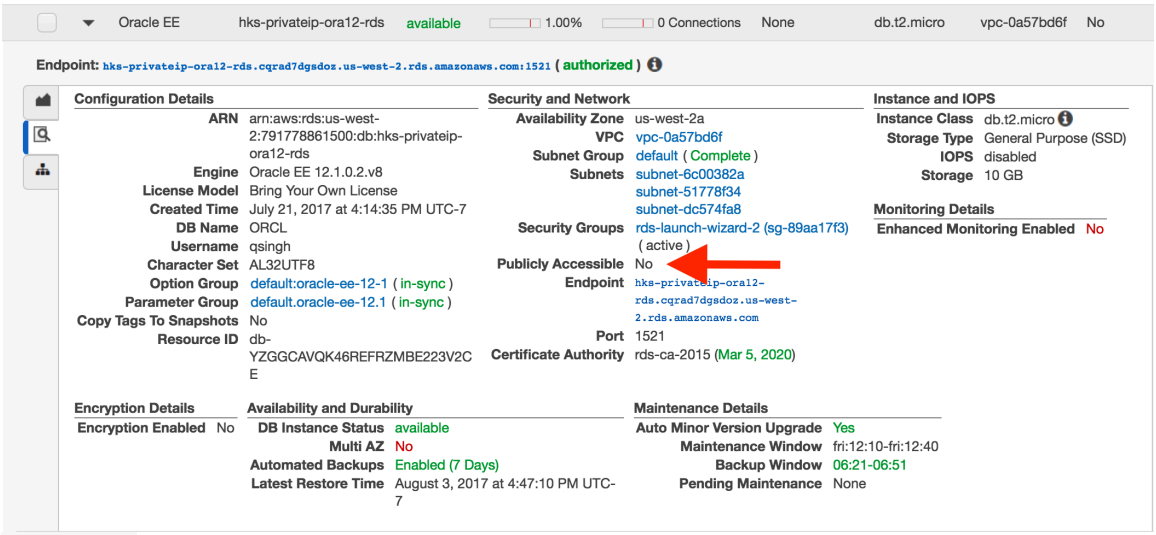
For publicly accessible endpoint:



Endpoint:
hks-ora12-rds.cqrad7dgsdoz.us-west-2.rds.amazonaws.com:1521

```
ping hks-ora12-rds.cqrad7dgsdoz.us-west-2.rds.amazonaws.com
PING ec2-52-25-163-72.us-west-2.compute.amazonaws.com
(52.25.163.72): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
```

For non-publicly available endpoint:



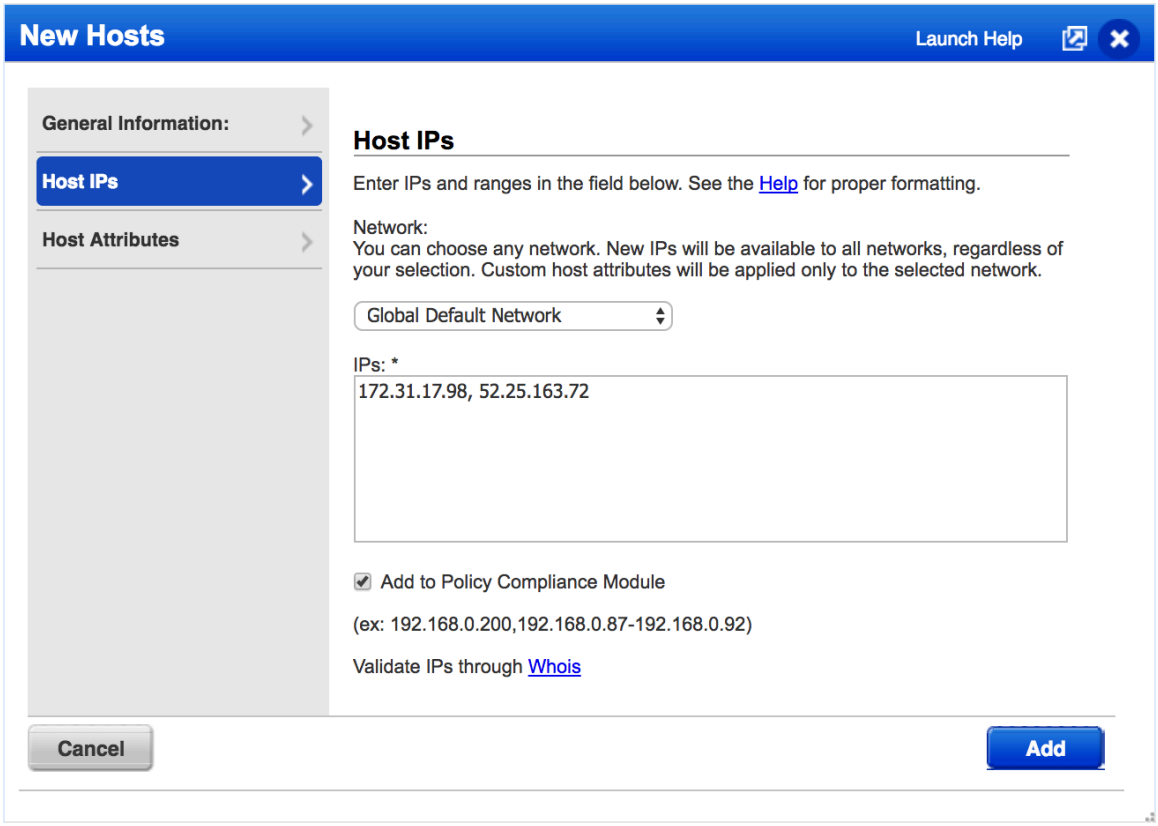
Endpoint:
hks-privateip-ora12-rds.cqrad7dgsdoz.us-west-2.rds.amazonaws.com:1521

```
ping hks-privateip-ora12-rds.cqrad7dgsdoz.us-west-
2.rds.amazonaws.com
PING hks-privateip-ora12-rds.cqrad7dgsdoz.us-west-
2.rds.amazonaws.com (172.31.17.98): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
```

Add the IPs to subscription

Before you can scan these RDS instances for VM or PC their IPs must be added to the subscription. If your AWS public and private IP ranges are already added to the subscription then you can skip this step.

To add IPs to the subscription, from VM or PC module, navigating to Assets →Host Assets → New → IP Tracked Hosts…



Note: In order to add multiple RDS instance IPs, one can automate this task using Qualys APIs.

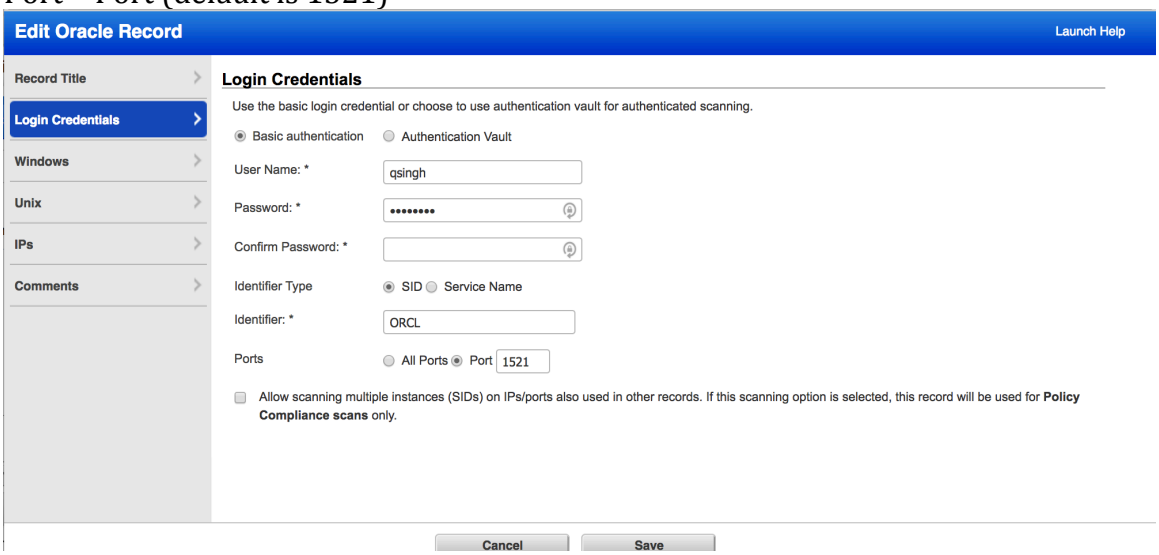
Create Authentication Record(s)

Policy Compliance (PC) scans require authentication, however for VM scan authentication is not required but recommended.

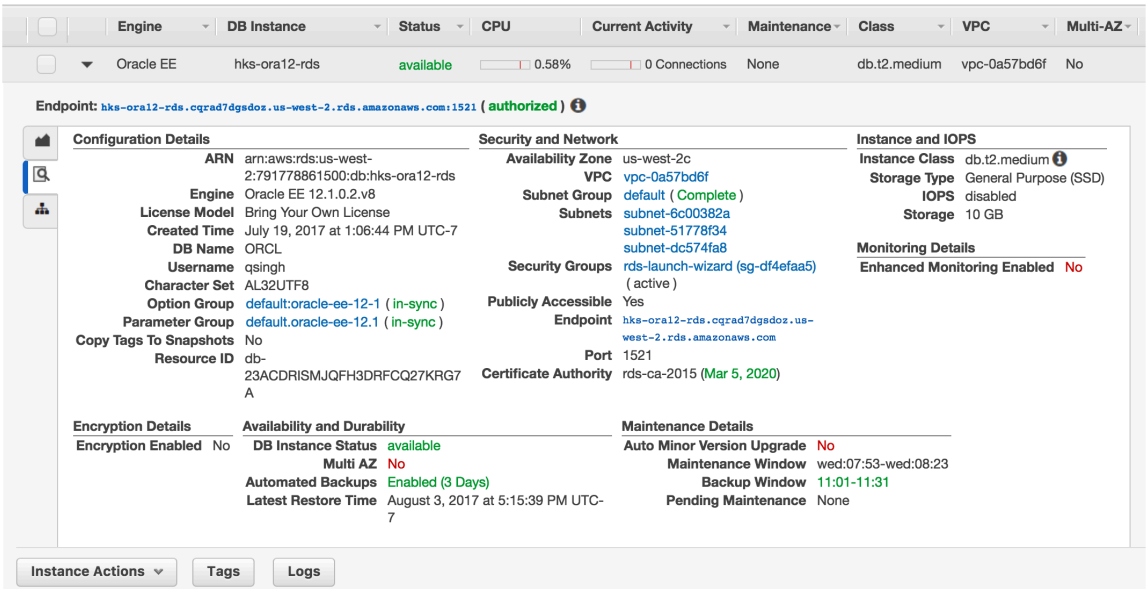
Create Oracle authentication record as follows for your RDS instance(s).

1. In the Login Credentials page enter the following info:
   - User Name = Master username specified during the instance creation or another scanning account with similar ability based on the Trusted Scanning Guide for Oracle.
   - Password = Password for the above account
   - Identifier = DB name (default is ORCL)

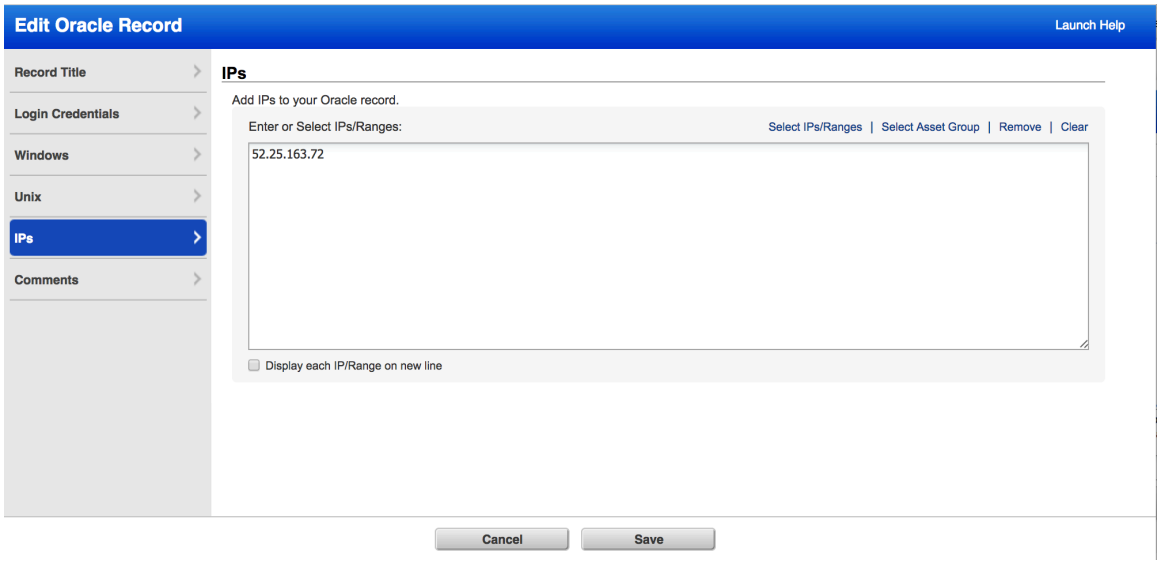
- Port = Port (default is 1521)



Note: This info can found by expanding the details of the RDS instance as shown below:



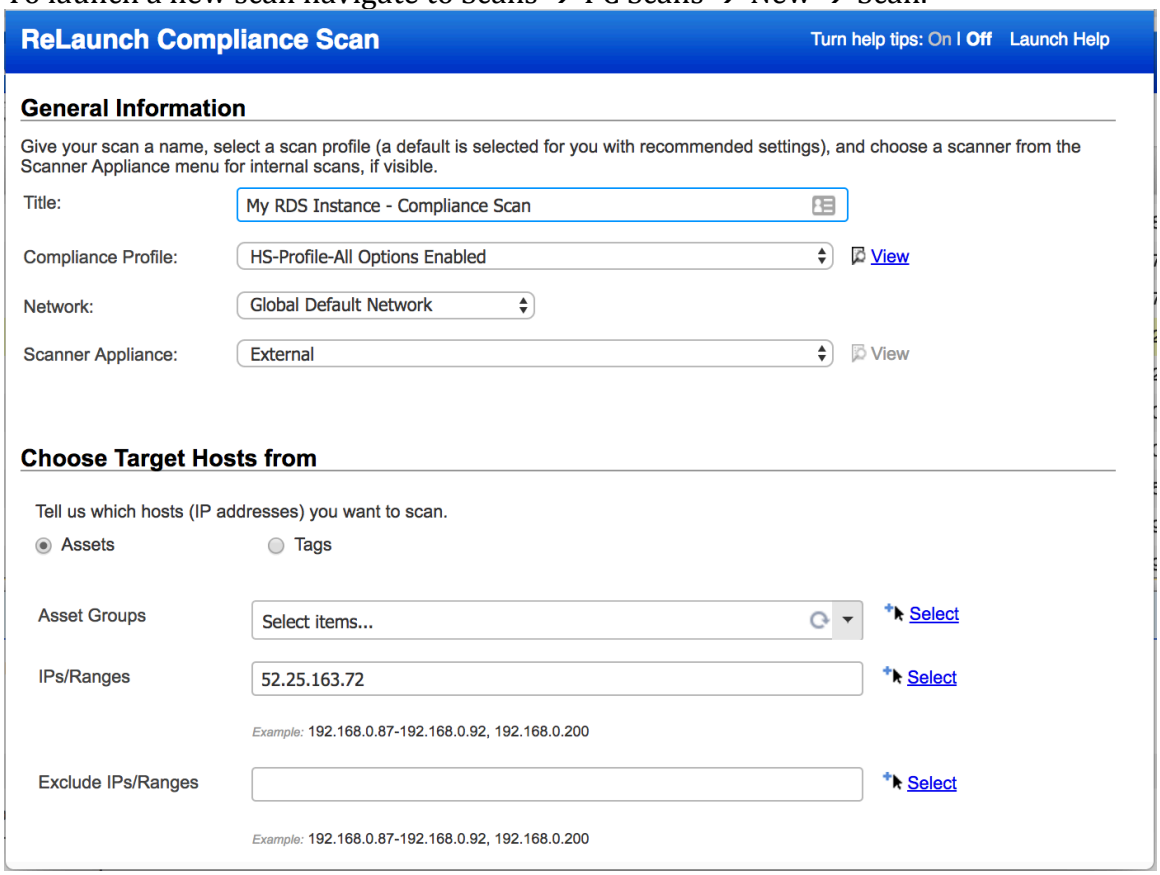
2. In the IPs page, enter either the public or private IP of the RDS endpoint, and save the authentication record.



Launch PC Scan against a publicly accessible instance

For the publicly accessible instances, you can use the Qualys Cloud Scanner(s) or your private scanners, which are able, reach the targets. Please note that you should ensure that you have proper approvals from AWS to perform such scans.

To launch a new scan navigate to Scans → PC Scans → New → Scan.

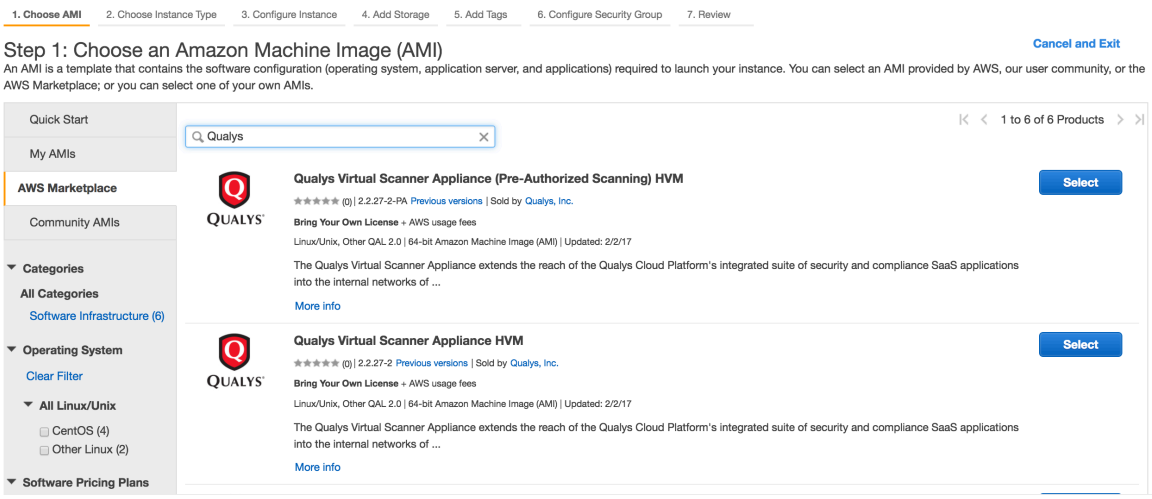


Launch PC Scan against a private RDS instance

For the non-publicly accessible instances, you must use a Qualys Scanner appliance deployed in your EC2 environment. See the section "**Deploying Qualys Scanner**" for instruction to deploy a scanner appliance for RDS instance scanning. The RDS instance must allow traffic from the scanner appliance. See the section **"Allowing Traffic from Qualys Scanner."** This is not a pre-authorized scanner so please note that you should ensure that you have proper approvals from AWS to perform such scans.

Deploying Qualys Scanner

You will need to deploy a non-preauthorized Qualys scanner appliance in order to scan non-publically accessible RDS instances. The AWS market place lists two Qualys Virtual Scanner Appliances; you will need to deploy the non-Preauthorized one. For example, the second one listed in the screenshot below.



Detailed deployment instructions can be found here: https://community.qualys.com/docs/DOC-4056-how-to-configure-a-virtual-scanner-using-amazon-ec2vpc

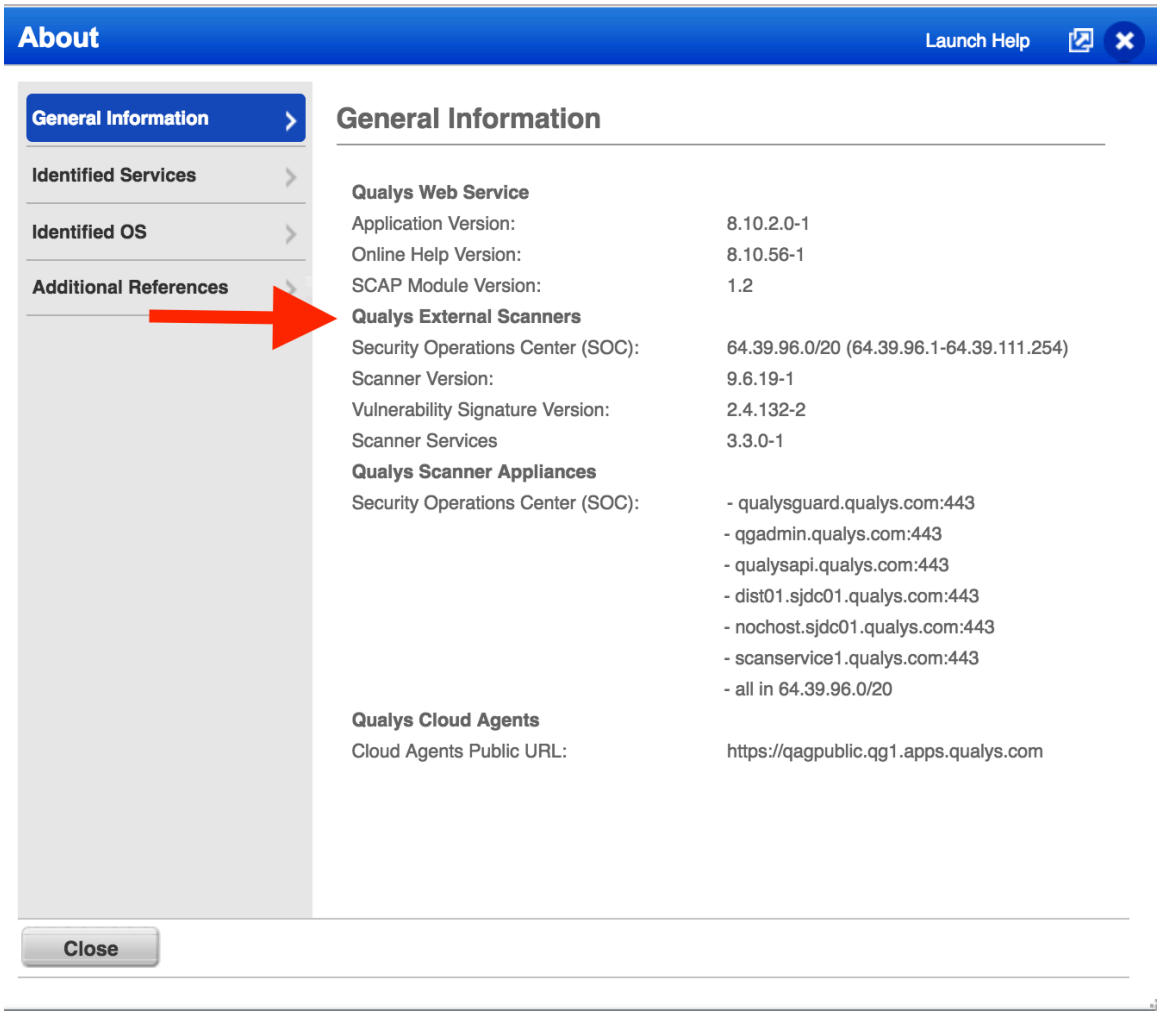
Allowing Traffic from Qualys Scanner

In order to successfully scan RDS instances for PC and VM, network traffic must be allowed from the scanner appliance(s). Access can be allowed to all ports or simply to the RDS Instance port.

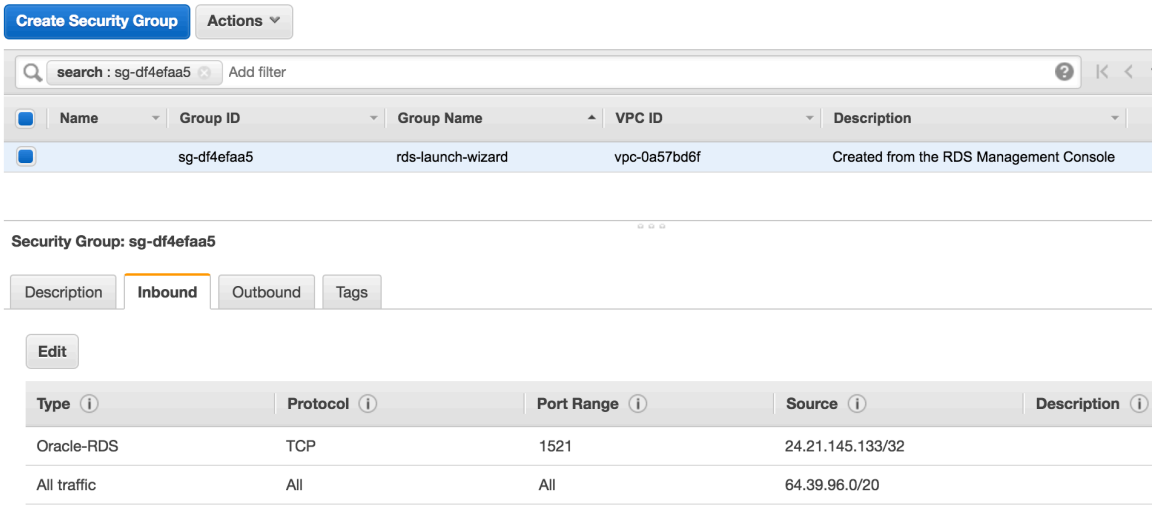
For Publicly Accessible RDS Instances

For external scanner to scan public RDS instance necessary rules should be in place in security group associated with RDS instance. You will need to allow external scanners to connect on DB port or all ports. For this, you need to obtain the IP addresses of Qualys external scanner using the steps below.

1. From your subscription navigate to Help → About.
2. Take note of the Qualys External Scanners 64.39.96.0/20 (64.39.96.1 – 64.39.111.254).

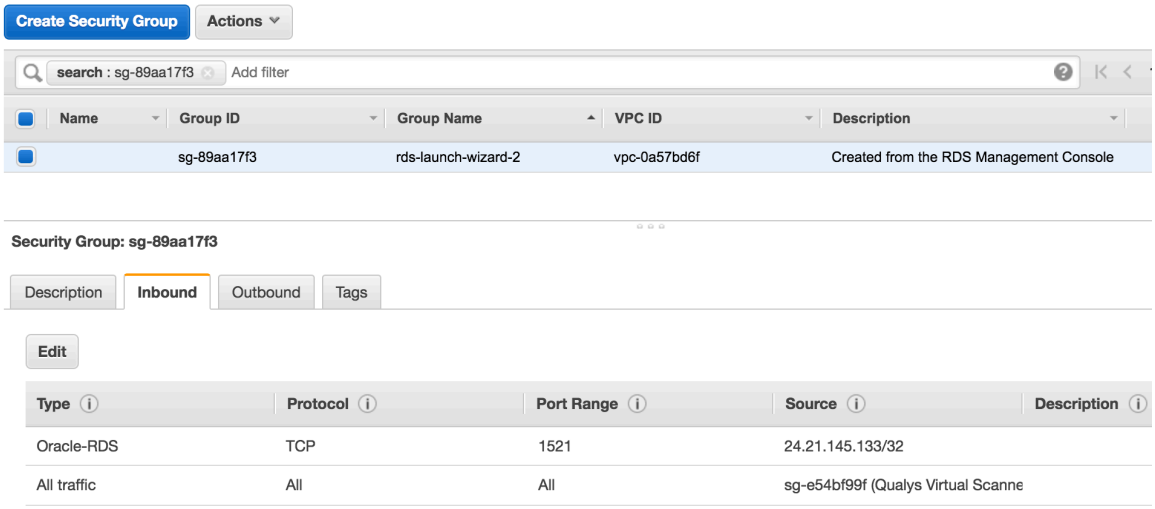


3. Screenshot below show all traffic being allowed from Qualys external scanners.



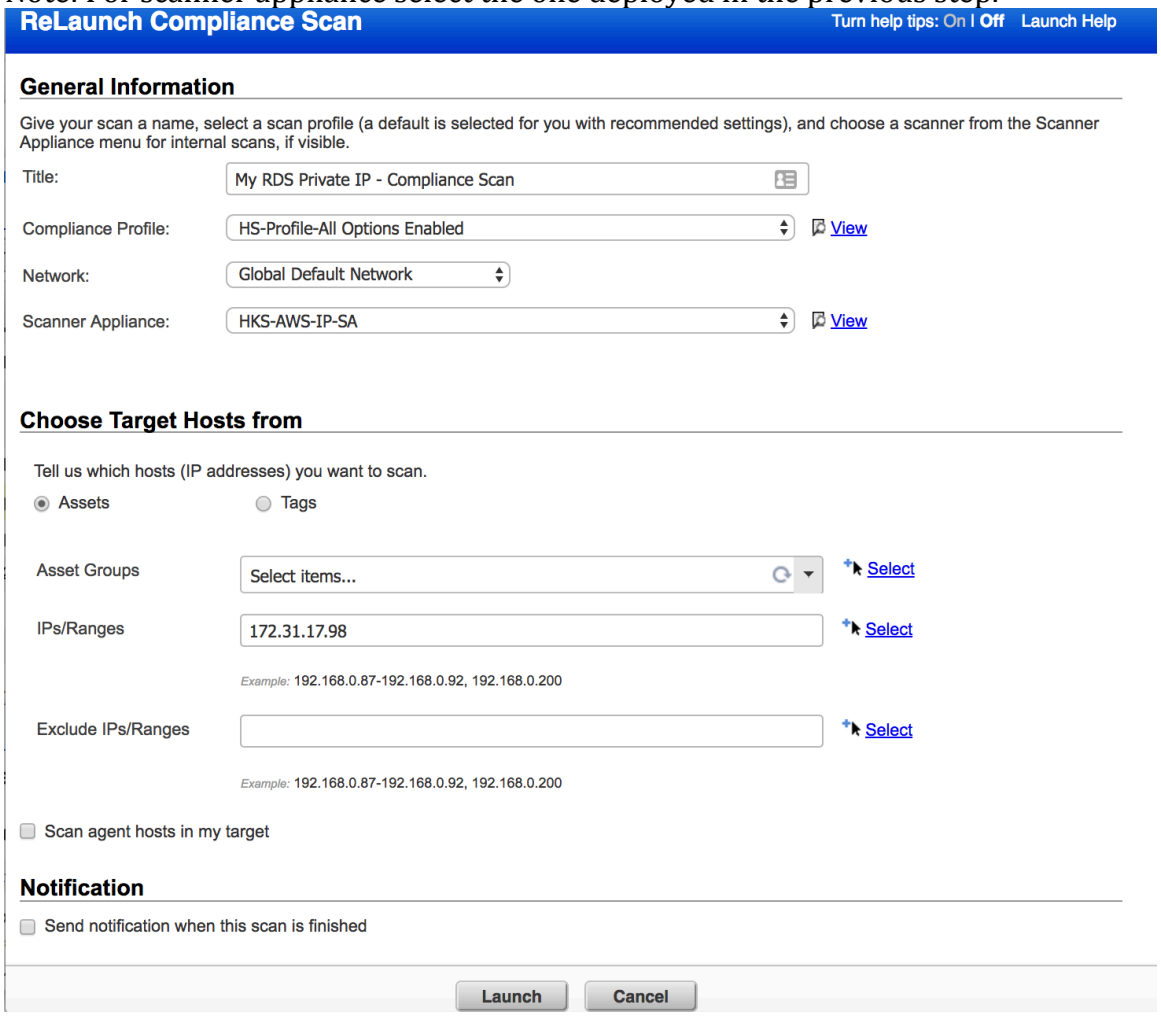
For Privately Accessible RDS Instances

Allow network traffic from the scanner security group to the RDS instances. The screenshot below shows all traffic being allowed from the Qualys Virtual Scanner security group.



Launch PC Scan

To launch a new scan navigate to Scans → PC Scans → New → Scan.
Note: For scanner appliance select the one deployed in the previous step.



Review Scan Results

Once the scan completes, ensure that authentication was successful for the database(s). In order to see data in compliance reports the authentication must be successful.

Results of the publicly accessible RDS instance:

Compliance Scan Results

File ▾ Help ▾

Report Summary

Launch Date:	07/19/2017 at 22:53:21 (GMT-0700)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	compliance/1500529944.11831
External Scanners:	64.39.99.88 (Scanner 9.4.38-1, Vulnerability Signatures 2.4.90-3)
Duration:	00:04:53
Title:	hs-externalscan 20170720
Network:	Global Default Network
Asset Groups:	-
IPs:	52.25.163.72
Excluded IPs:	-
Compliance Profile:	HS-Profile-All Options Enabled

Appendix

Target hosts found alive (IP)

52.25.163.72

Target distribution across scanner appliances

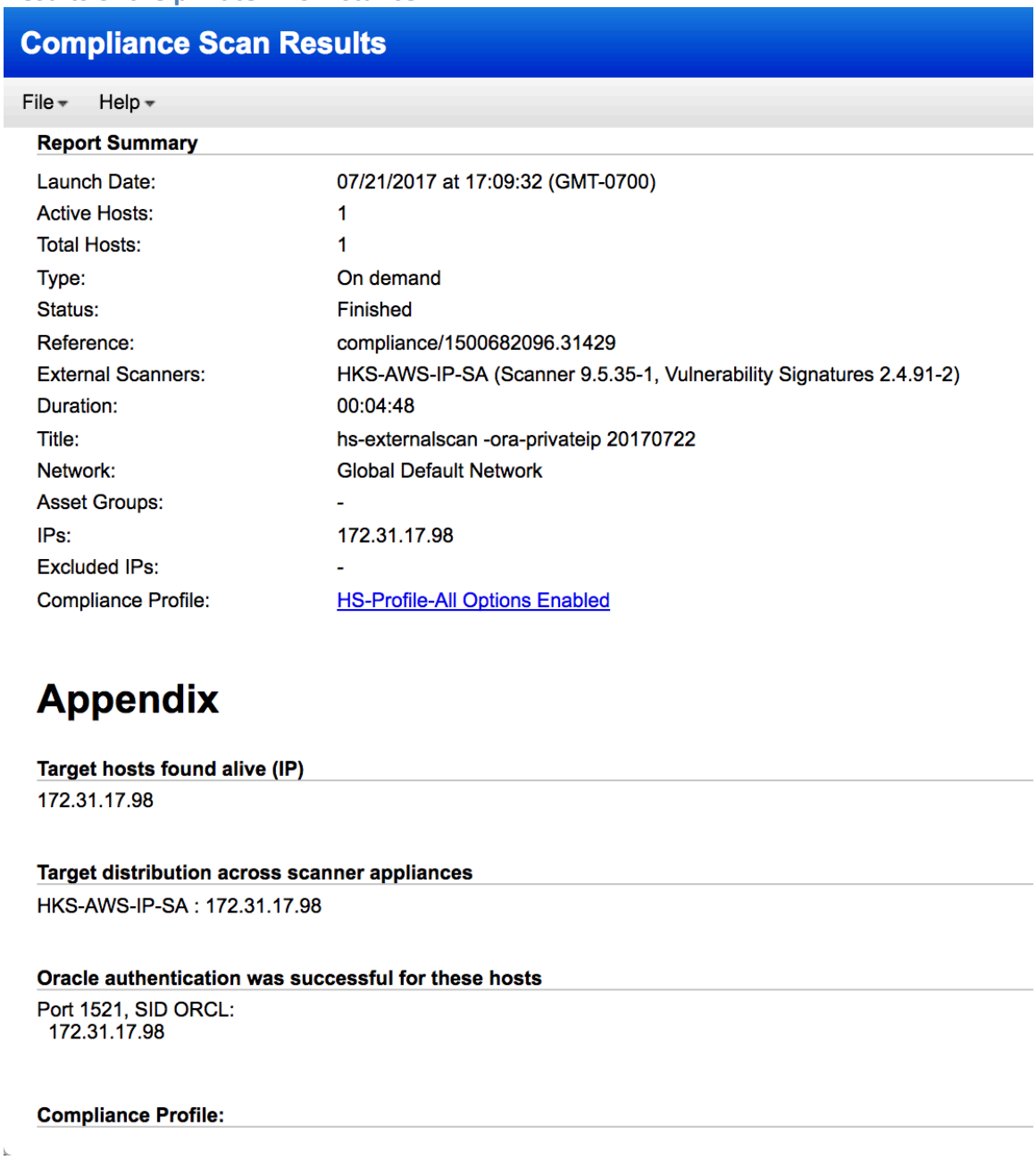
External : 52.25.163.72

Oracle authentication was successful for these hosts

Port 1521, SID ORCL:
52.25.163.72

Compliance Profile:

Results of the private RDS instance:



Compliance Scan Results

File ▾ Help ▾

Report Summary

Launch Date:	07/21/2017 at 17:09:32 (GMT-0700)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	compliance/1500682096.31429
External Scanners:	HKS-AWS-IP-SA (Scanner 9.5.35-1, Vulnerability Signatures 2.4.91-2)
Duration:	00:04:48
Title:	hs-externalscan -ora-privateip 20170722
Network:	Global Default Network
Asset Groups:	-
IPs:	172.31.17.98
Excluded IPs:	-
Compliance Profile:	HS-Profile-All Options Enabled

Appendix

Target hosts found alive (IP)

172.31.17.98

Target distribution across scanner appliances

HKS-AWS-IP-SA : 172.31.17.98

Oracle authentication was successful for these hosts

Port 1521, SID ORCL:
172.31.17.98

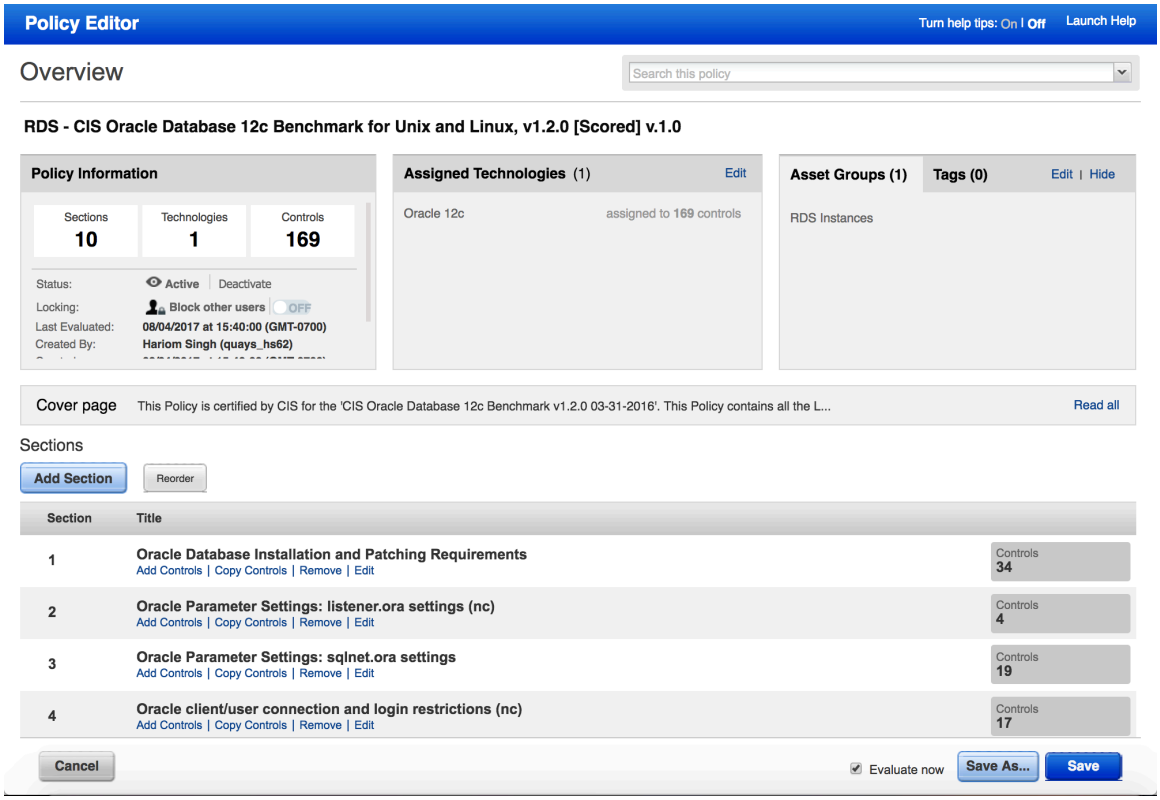
Compliance Profile:

Run Reports

In order to generate compliance reports for the RDS instances, ensure the following:

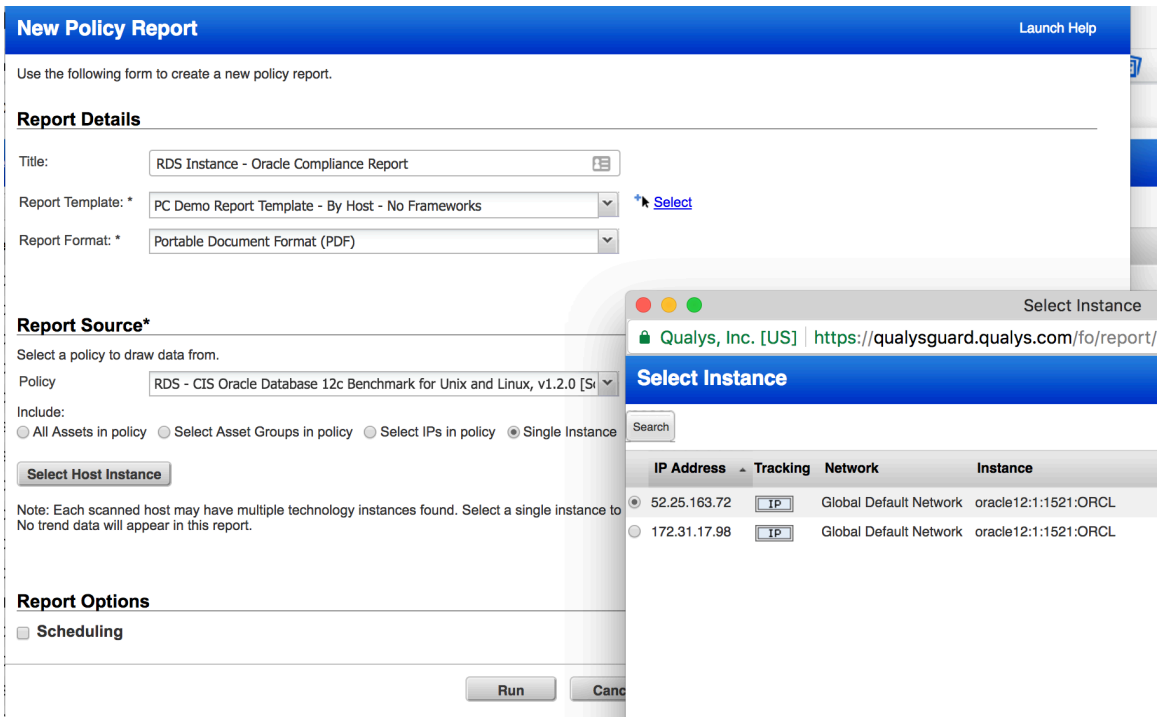
1. Create an Asset Group and add the RDS instance IPs to it.
2. Import a new policy from the library or edit an existing policy and add the Asset Group with RDS instances created in above.
3. Select “Evaluate Now” checkbox and Save the policy.

In the screenshot below, the Asset Group is called RDS instances, and Oracle 12c CIS benchmark is being used.



Run the report job

The reports can be generated normally by running a report job. You can generate reports for all of the assets assigned to the policy or select a single instance. The screenshot below shows a single instance being selected.



Public Instance Report:

Detailed Results

52.25.163.72 (ec2-52-25-163-72.us-west-2.compute.amazonaws.com) — Ubuntu / Tiny Core Linux / Linux 2.6.x

Oracle 12c

1. Oracle Database Installation and Patching Requirements

(1.1) 7989 Status of the APEX_040000 default password — **Passed** **CRITICAL**

Instance: oracle12:1:1521:ORCL

Evaluation date: 08/04/2017 at 15:52:10 (GMT-0700)

The APEX_040000 default password is set during the creation of the Oracle Application Express schema. As the default password is widely known and could allow unauthorized access to a database schema, this value should be changed in accordance with the needs of the business.

The following List String value X indicates the current status of the default password for the APEX_04000 account.

Expected	**does not contain regular expression list**
	defaultpwd
	OR, any of the selected values below:
	☑ Default password not found
	☐ Table not found
Actual	**Last Updated:07/19/2017 at 22:52:22 (GMT-0700)**
	Default password not found

(1.2) 7990 Status of the APPQOSSYS default password — **Failed** **CRITICAL**

Instance: oracle12:1:1521:ORCL

Evaluation date: 08/04/2017 at 15:52:10 (GMT-0700)

The APPQOSSYS default password applies to schema used by the Oracle Quality of Service Management for storing/ managing required data and metadata. As this is a well-known password and is vulnerable to unauthorized use, it should be changed according to the needs of the business.

Private Instance Report:

Detailed Results

172.31.17.98 (ip-172-31-17-98.us-west-2.compute.internal)	Ubuntu / Tiny Core Linux / Linux 2.6.x

Controls:	165
Passed:	79 (47.88%)
Failed:	86 (52.12%)
Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	07/21/2017 at 17:08:15 (GMT-0700)
Network:	Global Default Network
Tracking Method:	IP

Asset Tags:
MLH - Linux, WFS Linux Tag, New Host, PB - tag if any ports open and ports 22, 80, and 443 closed, PB - Not in asset group, PB - Asset updated, JDB Test 2, JDB Test Unix, MEP - Port 52311 Closed, MEP - Non-Windows OS, MEPNot45017, Internal IP Addresses (private), KAR - Zero Data, NPW Network 1, ubuntu, RFC1918, Linux Cyrille, MCW - Not 38601, Assets have DNS name, MCW - No DNS Name, draft-fbe-Internal Assets, JAG CMS Imports, JAG Search List, IP_Internal, mytag, LinuxJM, Asset Group Aa, Asset Group A_a, JAG Asset Group Test, JAG Asset Group Test 2, jg - testing not qid 45038, DynPrivMKATag, InternalIPs, RDS Instances

Oracle 12c

1. Oracle Database Installation and Patching Requirements

(1.1) 7989 Status of the APEX_040000 default password **Passed** **CRITICAL**

Instance: oracle12:1:1521:ORCL
Evaluation date: 08/04/2017 at 15:52:11 (GMT-0700)

The APEX_040000 default password is set during the creation of the Oracle Application Express schema. As the default password is widely known and could allow unauthorized access to a database schema, this value should be changed in accordance with the needs of the business.

The following List String value X indicates the current status of the default password for the APEX_04000 account.

Expected	**does not contain regular expression list**
	defaultpwd
	OR, any of the selected values below:
	☑ Default password not found
	☐ Table not found
Actual	**Last Updated:07/21/2017 at 17:08:15 (GMT-0700)**
	Default password not found

(1.2) 7990 Status of the APPQOSSYS default password **Failed** **CRITICAL**

Instance: oracle12:1:1521:ORCL
Evaluation date: 08/04/2017 at 15:52:11 (GMT-0700)

The APPQOSSYS default password applies to schema used by the Oracle Quality of Service Management for storing/ managing required data and metadata. As this is a well-known password and is vulnerable to unauthorized use, it should be changed according to the needs of the business.

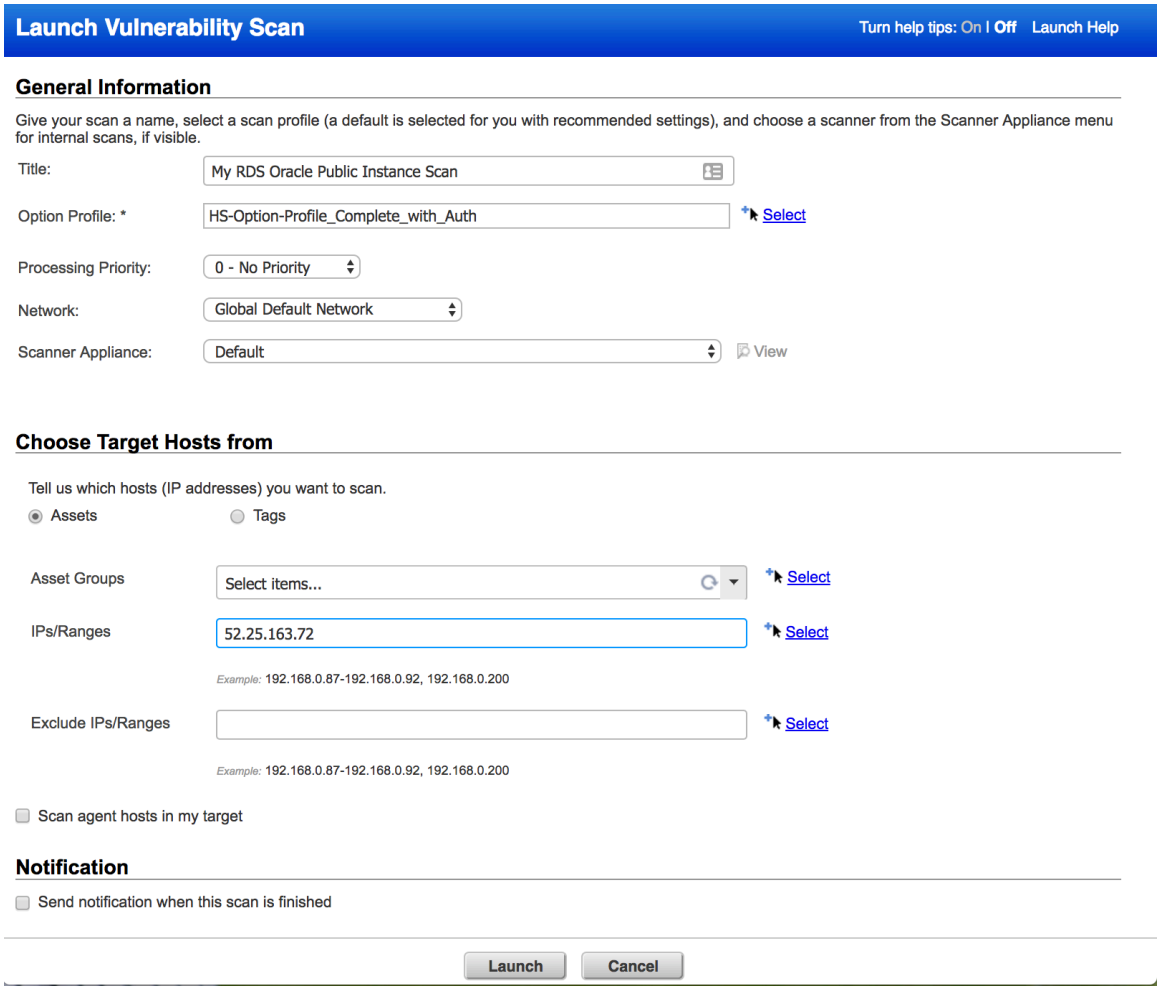
Scanning RDS Instances for VM

The scanning methodology for VM is similar to PC except that VM scans do not require authentication but is recommended, and the option profiles are different.

Scanning a publicly accessible RDS instance for VM

For the publicly accessible instances, you can use the Qualys Cloud Scanner(s) or your private scanners, which are able, reach the targets. Please note that you should ensure that you have proper approvals from AWS to perform such scans.

Note: The scanner appliance is left as "Default", a Qualys Cloud scanner appliance is automatically used for the public IP.



Results of the public RDS instance scan:

Scan Results

File ▾ View ▾ Help ▾

Report Summary

Launch Date:	08/07/2017 at 14:51:21 (GMT-0700)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1502142682.10888
External Scanners:	64.39.99.19 (Scanner 9.5.35-1, Vulnerability Signatures 2.4.103-2)
Duration:	00:06:04
Authentication:	ORACLE authentication was successful for 1 ORACLE instance
Title:	My RDS Oracle Public Instance Scan
Network:	Global Default Network
Asset Groups:	-
IPs:	52.25.163.72
Excluded IPs:	-
Option Profile:	HS-Option-Profile_Complete_with_Auth

Summary of Vulnerabilities

Total: 32 Security Risk (Avg): 4.0

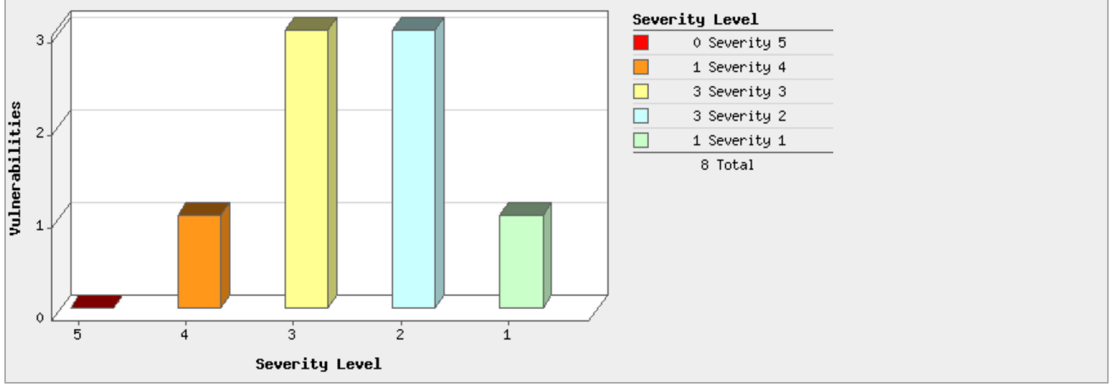
by Severity

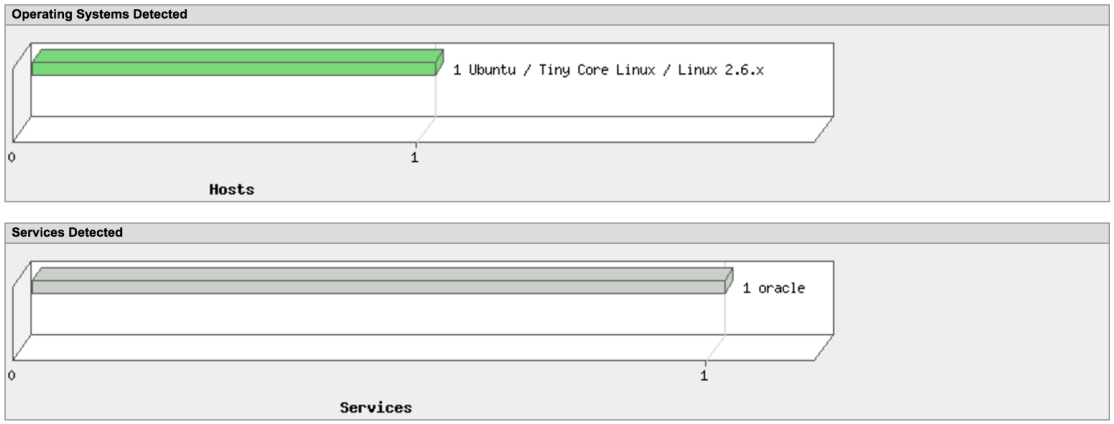
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	1	0	0	1
3	3	1	1	5
2	3	1	7	11
1	1	0	14	15
Total	**8**	**2**	**22**	**32**

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Database	8	2	11	21
Information gathering	0	0	5	5
TCP/IP	0	0	4	4
Security Policy	0	0	1	1
Firewall	0	0	1	1
Total	**8**	**2**	**22**	**32**

Vulnerabilities by Severity





Detailed Results

52.25.163.72 (ec2-52-25-163-72.us-west-2.compute.amazonaws.com, -) - Global Default Network — **Ubuntu / Tiny Core Linux / Linux 2.6.x**

Vulnerabilities (8)

4	Oracle Database July 2017 Patch Set Update (PSU) 12.1.0.2.170718 Not Installed (Patch 25755742)	port 1521/tcp
3	Oracle sql92_security Parameter is Disabled	oracle12:1:1521:ORCL
3	Oracle Server Accounts That Do Not Lockout With Failed Logon Attempts	oracle12:1:1521:ORCL
3	Oracle default_tablespace Set To SYSTEM for User Accounts	oracle12:1:1521:ORCL
2	Oracle Server Accounts With Passwords That Do Not Expire	oracle12:1:1521:ORCL
2	Oracle Server Accounts That Allow Unrestricted Password Reuse	oracle12:1:1521:ORCL
2	Oracle Server Accounts Without Password-Complexity Validation Setup	oracle12:1:1521:ORCL
1	Oracle Password Settings Do Not Conform to Recommendations	oracle12:1:1521:ORCL

Potential Vulnerabilities (2)

Information Gathered (22)

Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

52.25.163.72

Target distribution across scanner appliances

External : 52.25.163.72

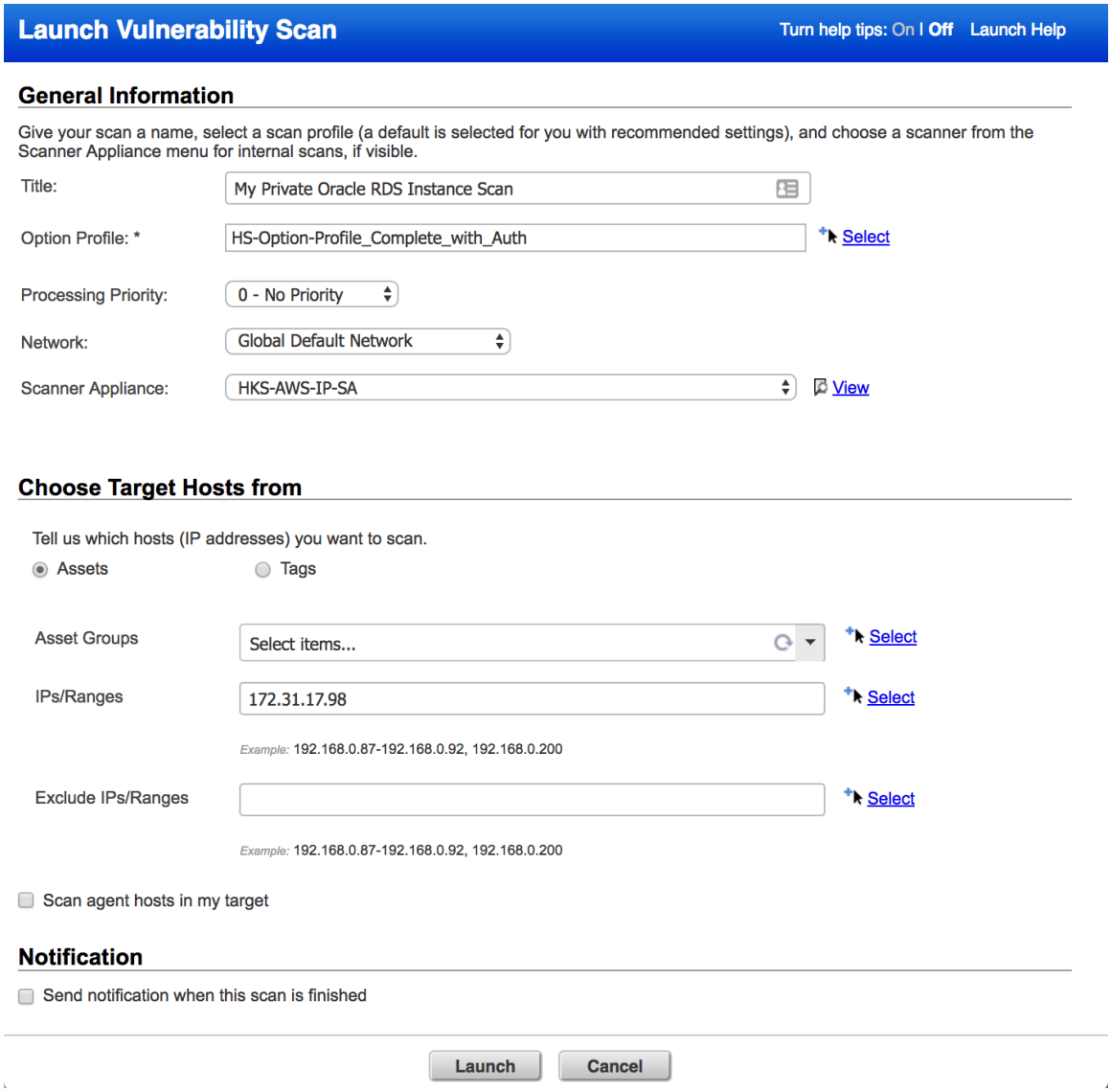
Oracle authentication was successful for these hosts (1)

Instance oracle12:1:1521:ORCL:
52.25.163.72

Scanning a private RDS instance for VM

For the non-publicly accessible instances, you must use a Qualys Scanner appliance deployed in your EC2 environment. See the section "**Deploying Qualys Scanner**" for instruction to deploy a scanner appliance for RDS instance scanning. The RDS instance must allow traffic from the scanner appliance. This is not a pre-authorized scanner; there fore please note that you should ensure that you have proper approvals from AWS to perform such scans.

Note: The non-preauthorized scanner appliance, which can reach the target RDS instance, is selected.


Launch Vulnerability Scan
Turn help tips: On | Off
Launch Help
General Information
Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.
Title:
My Private Oracle RDS Instance Scan
Option Profile: *
HS-Option-Profile_Complete_with_Auth
Select
Processing Priority:
0 - No Priority
Network:
Global Default Network
Scanner Appliance:
HKS-AWS-IP-SA
View
Choose Target Hosts from
Tell us which hosts (IP addresses) you want to scan.
Assets
Tags
Asset Groups
Select items...
Select
IPs/Ranges
172.31.17.98
Select
Example: 192.168.0.87-192.168.0.92, 192.168.0.200
Exclude IPs/Ranges
Select
Example: 192.168.0.87-192.168.0.92, 192.168.0.200
Scan agent hosts in my target
Notification
Send notification when this scan is finished
Launch
Cancel