

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 3**
- Background 3**
- High-level Steps for Scanning RDS Instances 4**
- Detailed Steps 4**
- Obtaining the IP of RDS Instance..... 4**
 - For publicly accessible endpoint:..... 4
 - For non-publicly available endpoint:..... 5
- Add the IPs to subscription 5**
- Create Authentication Record(s) 6**
- Launch PC Scan against a publicly accessible instance 8**
- Launch PC Scan against a private RDS instance 9**
 - Deploying Qualys Scanner..... 9
 - Launch PC Scan..... 13
- Review Scan Results 13**
 - Results of the publicly accessible RDS instance:..... 14*
 - Results of the private RDS instance:..... 15*
- Run Reports..... 15**
 - Run the report job..... 16
- Scanning RDS Instances for VM..... 18**
 - Scanning a publicly accessible RDS instance for VM..... 18
 - Scanning a private RDS instance for VM 21

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.

The screenshot shows the AWS Management Console interface for an Amazon RDS instance. At the top, there are buttons for 'Launch DB Instance', 'Show Monitoring', and 'Instance Actions'. Below this is a search bar and a filter set to 'All Instances'. The instance details are shown in a table with columns for Engine, DB Instance, Status, CPU, Current Activity, Maintenance, Class, VPC, and Multi-AZ. The instance 'hks-ora12-rds' is listed with a status of 'available', CPU usage of 0.67%, and 0 connections. Below the table, the endpoint is displayed as 'hks-ora12-rds.cqrad7dgsdoz.us-west-2.rds.amazonaws.com:1521 (authorized)', with a red arrow pointing to it. The console also features sections for 'Alarms and Recent Events' and 'Monitoring' with various metrics and graphs.

TIME (UTC-7)	EVENT
Aug 3 4:10 AM	Finished DB Instance backup
Aug 3 4:06 AM	Backing up DB instance

Metric	Current Value	Threshold	Last Hour
CPU	0.625%		
Memory	1,240 MB		
Storage	7,640 MB		
Read IOPS	3.82/sec		
Write IOPS	1.43/sec		
Swap Usage	43.7 MB		

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:

The screenshot displays the AWS RDS console for an Oracle EE instance named 'hks-ora12-rds'. The instance is in an 'available' state with 0.57% CPU usage and 0 connections. The endpoint is 'hks-ora12-rds.cqrad7dgsdoz.us-west-2.rds.amazonaws.com:1521' and is marked as 'authorized'. The console is divided into several sections:

- Configuration Details:** Includes ARN, Engine (Oracle EE 12.1.0.2.v8), License Model (Bring Your Own License), Created Time, DB Name (ORCL), Username (qsingh), Character Set (AL32UTF8), Option Group, Parameter Group, Copy Tags To Snapshots, and Resource ID.
- Security and Network:** Shows Availability Zone (us-west-2c), VPC (vpc-0a57bd6f), Subnet Group (default), Subnets, Security Groups (including rds-launch-wizard), Publicly Accessible (Yes), Endpoint, Port (1521), and Certificate Authority.
- Instance and IOPS:** Lists Instance Class (db.t2.medium), Storage Type (General Purpose (SSD)), IOPS (disabled), and Storage (10 GB).
- Monitoring Details:** Shows Enhanced Monitoring Enabled (No).
- Encryption Details:** Shows Encryption Enabled (No).
- Availability and Durability:** Shows DB Instance Status (available), Multi AZ (No), Automated Backups (Enabled (3 Days)), and Latest Restore Time.
- Maintenance Details:** Shows Auto Minor Version Upgrade (No), Maintenance Window, Backup Window, and Pending Maintenance (None).

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:

Oracle EE hks-privateip-ora12-rds available 1.00% 0 Connections None db.t2.micro vpc-0a57bd6f No

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

Configuration Details	Security and Network	Instance and IOPS
ARN arn:aws:rds:us-west-2:791778861500:db:hks-privateip-ora12-rds	Availability Zone us-west-2a	Instance Class db.t2.micro
Engine Oracle EE 12.1.0.2.v8	VPC vpc-0a57bd6f	Storage Type General Purpose (SSD)
License Model Bring Your Own License	Subnet Group default (Complete)	IOPS disabled
Created Time July 21, 2017 at 4:14:35 PM UTC-7	Subnets subnet-6c00382a subnet-51778f34 subnet-dc574fa8	Storage 10 GB
DB Name ORCL	Security Groups rds-launch-wizard-2 (sg-89aa17f3) (active)	Monitoring Details
Username qsingh	Publicly Accessible No	Enhanced Monitoring Enabled No
Character Set AL32UTF8	Endpoint hks-privateip-ora12-rds.cqrad7dgsdoz.us-west-2.rds.amazonaws.com	
Option Group default:oracle-ee-12.1 (in-sync)	Port 1521	
Parameter Group default:oracle-ee-12.1 (in-sync)	Certificate Authority rds-ca-2015 (Mar 5, 2020)	
Copy Tags To Snapshots No		
Resource ID YZGGCAVQK46REFRZMBE223V2C		
Encryption Details	Availability and Durability	Maintenance Details
Encryption Enabled No	DB Instance Status available	Auto Minor Version Upgrade Yes
	Multi AZ No	Maintenance Window fri:12:10-fri:12:40
	Automated Backups Enabled (7 Days)	Backup Window 06:21-06:51
	Latest Restore Time August 3, 2017 at 4:47:10 PM UTC-7	Pending Maintenance None

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...

New Hosts Launch Help

General Information:

Host IPs

Host Attributes

Host IPs

Enter IPs and ranges in the field below. See the [Help](#) for proper formatting.

Network:
You can choose any network. New IPs will be available to all networks, regardless of your selection. Custom host attributes will be applied only to the selected network.

Global Default Network

IPs: *
172.31.17.98, 52.25.163.72

Add to Policy Compliance Module
(ex: 192.168.0.200, 192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)

Cancel Add

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)

Edit Oracle Record Launch Help

Record Title > **Login Credentials**

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Basic authentication Authentication Vault

User Name: *

Password: *

Confirm Password: *

Identifier Type SID Service Name

Identifier: *

Ports All Ports Port

Allow scanning multiple instances (SIDs) on IPs/ports also used in other records. If this scanning option is selected, this record will be used for **Policy Compliance scans** only.

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

Endpoint: hks-ora12-rds.cqrad7dgdos.us-west-2.amazonaws.com:1521 (authorized)

Configuration Details	Security and Network	Instance and IOPS
ARN arn:aws:rds:us-west-2:791778861500:db:hks-ora12-rds	Availability Zone us-west-2c	Instance Class db.t2.medium
Engine Oracle EE 12.1.0.2.v8	VPC vpc-0a57bd6f	Storage Type General Purpose (SSD)
License Model Bring Your Own License	Subnet Group default (Complete)	IOPS disabled
Created Time July 19, 2017 at 1:06:44 PM UTC-7	Subnets subnet-6c00382a, subnet-51778f34, subnet-dc574fa8	Storage 10 GB
DB Name ORCL	Security Groups rds-launch-wizard (sg-df4efaa5) (active)	Monitoring Details
Username qsingh	Publicly Accessible Yes	Enhanced Monitoring Enabled No
Character Set AL32UTF8	Endpoint hks-ora12-rds.cqrad7dgdos.us-west-2.amazonaws.com	
Option Group default:oracle-ee-12-1 (in-sync)	Port 1521	
Parameter Group default:oracle-ee-12.1 (in-sync)	Certificate Authority rds-ca-2015 (Mar 5, 2020)	
Copy Tags To Snapshots No		
Resource ID db-23ACDRISMJQFH3DRFCQ27KRG7A		
Encryption Details	Availability and Durability	Maintenance Details
Encryption Enabled No	DB Instance Status available	Auto Minor Version Upgrade No
	Multi AZ No	Maintenance Window wed:07:53-wed:08:23
	Automated Backups Enabled (3 Days)	Backup Window 11:01-11:31
	Latest Restore Time August 3, 2017 at 5:15:39 PM UTC-7	Pending Maintenance None

Instance Actions

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

The screenshot shows a web interface titled "Edit Oracle Record" with a "Launch Help" link in the top right. On the left is a sidebar menu with options: "Record Title", "Login Credentials", "Windows", "Unix", "IPs" (highlighted in blue), and "Comments". The main content area is titled "IPs" and contains the instruction "Add IPs to your Oracle record." Below this is a text input field with the label "Enter or Select IPs/Ranges:" and a list of actions: "Select IPs/Ranges", "Select Asset Group", "Remove", and "Clear". The input field contains the IP address "52.25.163.72". At the bottom of the input area is a checkbox labeled "Display each IP/Range on new line". At the very bottom of the interface are two buttons: "Cancel" and "Save".

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.

ReLaunch Compliance 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 RDS Instance - Compliance Scan

Compliance Profile: HS-Profile-All Options Enabled View

Network: Global Default Network

Scanner Appliance: External View

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

Assets Tags

Asset Groups: Select items... Select

IPs/Ranges: 52.25.163.72 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

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-publicly 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.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review Cancel and Exit

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

▼ Categories

All Categories

Software Infrastructure (6)

▼ Operating System

Clear Filter

▼ All Linux/Unix

CentOS (4)

Other Linux (2)

▼ Software Pricing Plans



QUALYS

Qualys Virtual Scanner Appliance (Pre-Authorized Scanning) HVM

★★★★★ (0) | 2.2.27-2-PA [Previous versions](#) | Sold by [Qualys, Inc.](#)

Bring Your Own License + AWS usage fees

Linux/Unix, Other OAL 2.0 | 64-bit Amazon Machine Image (AMI) | Updated: 2/2/17

The Qualys Virtual Scanner Appliance extends the reach of the Qualys Cloud Platform's integrated suite of security and compliance SaaS applications into the internal networks of ...

[More info](#)

Select



QUALYS

Qualys Virtual Scanner Appliance HVM

★★★★★ (0) | 2.2.27-2 [Previous versions](#) | Sold by [Qualys, Inc.](#)

Bring Your Own License + AWS usage fees

Linux/Unix, Other OAL 2.0 | 64-bit Amazon Machine Image (AMI) | Updated: 2/2/17

The Qualys Virtual Scanner Appliance extends the reach of the Qualys Cloud Platform's integrated suite of security and compliance SaaS applications into the internal networks of ...

[More info](#)

Select

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).

About Launch Help  

General Information >

Identified Services >

Identified OS >

Additional References > 

General Information

Qualys Web Service

Application Version: 8.10.2.0-1

Online Help Version: 8.10.56-1

SCAP Module Version: 1.2

Qualys External Scanners

Security Operations Center (SOC): 64.39.96.0/20 (64.39.96.1-64.39.111.254)

Scanner Version: 9.6.19-1

Vulnerability Signature Version: 2.4.132-2

Scanner Services: 3.3.0-1

Qualys Scanner Appliances

Security Operations Center (SOC):

- qualysguard.qualys.com:443
- qqadmin.qualys.com:443
- qualysapi.qualys.com:443
- dist01.sjdc01.qualys.com:443
- nochoost.sjdc01.qualys.com:443
- scanservice1.qualys.com:443
- all in 64.39.96.0/20

Qualys Cloud Agents

Cloud Agents Public URL: <https://qagpublic.qg1.apps.qualys.com>

Close

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

Create Security Group Actions ▾

search : sg-df4efaa5 Add filter

Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/>	sg-df4efaa5	rds-launch-wizard	vpc-0a57bd6f	Created from the RDS Management Console

Security Group: sg-df4efaa5

Description

Inbound

Outbound

Tags

Edit

Type i	Protocol i	Port Range i	Source i	Description i
Oracle-RDS	TCP	1521	24.21.145.133/32	
All traffic	All	All	64.39.96.0/20	

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.

Create Security Group Actions

search : sg-89aa17f3 Add filter

Name	Group ID	Group Name	VPC ID	Description
	sg-89aa17f3	rds-launch-wizard-2	vpc-0a57bd6f	Created from the RDS Management Console

Security Group: sg-89aa17f3

Description Inbound Outbound Tags

Edit

Type	Protocol	Port Range	Source	Description
Oracle-RDS	TCP	1521	24.21.145.133/32	
All traffic	All	All	sg-e54bf99f (Qualys Virtual Scanne	

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.

ReLaunch Compliance 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:

Compliance Profile: [View](#)

Network:

Scanner Appliance: [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

Assets Tags

Asset Groups: [Select](#)

IPs/Ranges: [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

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.

Policy Editor Turn help tips: On | Off [Launch Help](#)

Overview Search this policy

RDS - CIS Oracle Database 12c Benchmark for Unix and Linux, v1.2.0 [Scored] v.1.0

Policy Information			Assigned Technologies (1) Edit	Asset Groups (1) Edit Hide	Tags (0) Edit Hide
Sections 10	Technologies 1	Controls 169	Oracle 12c assigned to 169 controls	RDS Instances	
Status: <input checked="" type="checkbox"/> Active Deactivate Locking: <input checked="" type="checkbox"/> Block other users <input type="checkbox"/> OFF Last Evaluated: 08/04/2017 at 15:40:00 (GMT-0700) Created By: Hariom Singh (quays_hs62)					

Cover page This Policy is certified by CIS for the 'CIS Oracle Database 12c Benchmark v1.2.0 03-31-2016'. This Policy contains all the L... [Read all](#)

Sections

[Add Section](#) [Reorder](#)

Section	Title	Controls
1	Oracle Database Installation and Patching Requirements Add Controls Copy Controls Remove Edit	34
2	Oracle Parameter Settings: listener.ora settings (nc) Add Controls Copy Controls Remove Edit	4
3	Oracle Parameter Settings: sqlnet.ora settings Add Controls Copy Controls Remove Edit	19
4	Oracle client/user connection and login restrictions (nc) Add Controls Copy Controls Remove Edit	17

[Cancel](#) Evaluate now [Save As...](#) [Save](#)

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.

Launch Help

New Policy Report

Use the following form to create a new policy report.

Report Details

Title:

Report Template: * [Select](#)

Report Format: *

Report Source*

Select a policy to draw data from.

Policy:

Include:

All Assets in policy
 Select Asset Groups in policy
 Select IPs in policy
 Single Instance

Note: Each scanned host may have multiple technology instances found. Select a single instance to view details. No trend data will appear in this report.

Report Options

Scheduling

Select Instance

Qualys, Inc. [US] | <https://qualysguard.qualys.com/fo/report/>

Select Instance

IP Address	Tracking	Network	Instance
<input checked="" type="radio"/> 52.25.163.72	<input type="button" value="IP"/>	Global Default Network	oracle12:1:1521:ORCL
<input type="radio"/> 172.31.17.98	<input type="button" value="IP"/>	Global Default Network	oracle12:1:1521:ORCL

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_040000 account.

Expected	does not contain regular expression list
	defaultpwd
	OR, any of the selected values below:
	<input checked="" type="checkbox"/> Default password not found
	<input type="checkbox"/> 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, InternallPs, 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_040000 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.

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: 

Option Profile: * [* Select](#)

Processing Priority: 

Network: 

Scanner Appliance:  [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

Assets Tags

Asset Groups:  [* Select](#)

IPs/Ranges: [* 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

Results of the public RDS instance scan:

Scan Results

File View Help

Report Summary

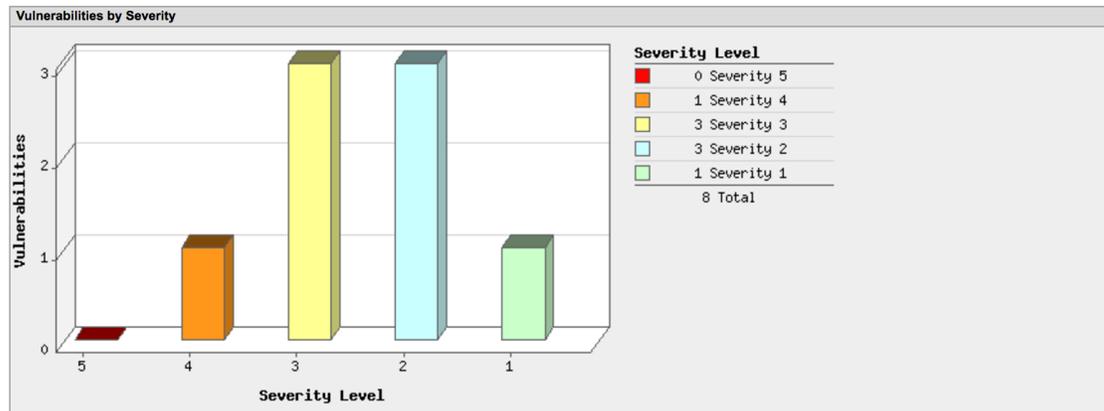
Launch Date: 08/07/2017 at 14:51:21 (GMT-0700)
 Active Hosts: 1
 Total Hosts: 1
 Type: On demand
 Status: Finished
 Reference: scan/1502142682.10888
 External Scanners: 64.39.99.19 (Scanner 9.5.35-1, Vulnerability Signatures 2.4.103-2)
 Duration: 00:06:04
 Authentication: ORACLE authentication was successful 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](#)

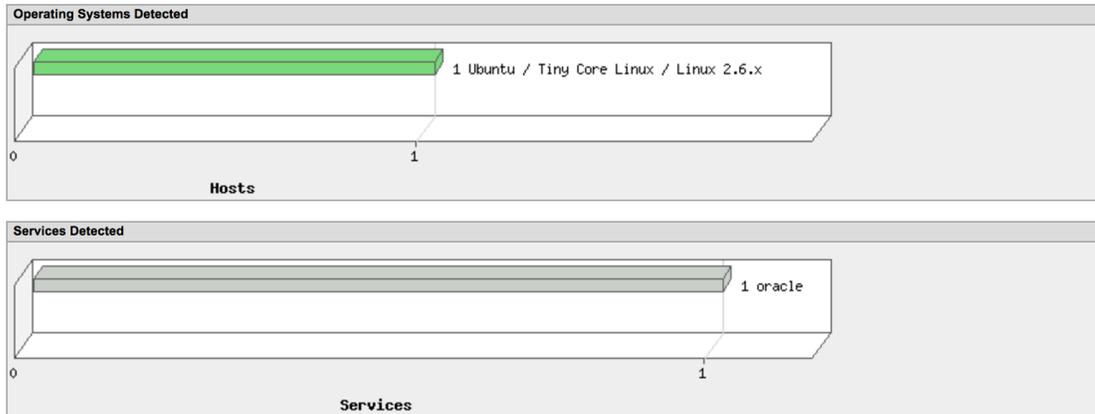
Summary of Vulnerabilities

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





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: 

Option Profile: * [* Select](#)

Processing Priority: 

Network: 

Scanner Appliance:  [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

- Assets Tags

Asset Groups  [* Select](#)

IPs/Ranges [* 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