Hewlett Packard
Enterprise

HPE Security ArcSight Investigate DB 8.1.1 for AWS

Setup Guide

March, 2018

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2018 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements: https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Warranty 2
Restricted Rights Legend 2
Copyright Notice 2
Setting Investigate Database 8.1.1 for AWS 4
Launching Vertica 8.1.1 for AWS 4
Configuring Vertica 8.1.1 for AWS 5
Starting Vertica Database 5
Changing Password 6
Running the Kafka Scheduler 7
Troubleshooting Vertica on AWS 8
Additional Information 8
Send Documentation Feedback 9

Setting Investigate Database 8.1.1 for AWS

Launching Vertica 8.1.1 for AWS

1. From the left menu go to AWS Marketplace and search for AI 2.00 - Vertica Analytic Database 8.1.1-3 (Single Host) - CentOS 7.4

2. Filter by General Purpose and select m4.4xlarge.

3. From **Configure Instance Details**, modify all corresponding items to align the instance to your needs.

> **Note:** Make sure the right network, subnet and IPs are selected.

4. You may not need to modify any setting in **Add Storage**. If you choose to increase storage volume capacity, follow the Amazon procedure to extend EBS volume once the instance is launched. Refer to the AWS User Guide and search "expanding the storage space of an EBS volume on Linux."

5. Go to **Tag Instance**, click value and enter a name for the instance.

6. From **Configure Security Group**, add any custom rules required for your environment and open the following ports:

Inbound:

Type	Use	Protocol	Port Range	Source	IP
SSH		TCP	22	My IP	0.0.0.0/0
HTTP		TCP	80	My IP	0.0.0.0/0
HTTPS		TCP	443	My IP	0.0.0.0/0
DNS (UDP)		UDP	53	My IP	0.0.0.0/0
Custom UDP	Spread	UDP	4803-4805	My IP	0.0.0.0/0
Custom TCP	Spread	TCP	4803-4805	My IP	0.0.0.0/0
Custom TCP	VSQL/SQL	TCP	5433	My IP	0.0.0.0/0
Custom TCP	Inter-node Communication	TCP	5434	My IP	0.0.0.0/0
Custom TCP		TCP	5444	My IP	0.0.0.0/0
Custom TCP	MC	TCP	5450	My IP	0.0.0.0/0
Custom TCP		TCP	8080	My IP	0.0.0.0/0

Type	Use	Protocol	Port Range	Source	IP
Custom TCP		TCP	48073	My IP	0.0.0.0/0
Custom TCP	Rsync	TCP	50000	My IP	0.0.0.0/0
ICMP	Installer	Echo Reply	N/A	My IP	0.0.0.0/0
ICMP	Installer	Traceroute	N/A	My IP	0.0.0.0/0

Outbound

Type	Protocol	Port Range	Destination	IP
All TCP	TCP	0-65535	Anywhere	0.0.0.0/0
All ICMP	ICMP	0-65535	Anywhere	0.0.0.0/0
All UDP	UDP	0-65535	Anywhere	0.0.0.0/0

7. From **Review and Launch**, correct any settings (if required), by clicking Previous and go back to the proper screen for editing. If they are correct, click Launch.

8. Go to **Create a new key pair** and click **Download Key Pair**. The key pair is required for connecting to the instance remotely. More details can be found in AWS User Guide.

9. Click **Launch Instances**. Launching Vertica AWS Elastic Compute Cloud (EC2) takes a few minutes. The progress can be monitored by accessing EC2's dashboard and clicking the Instances link on the left panel. Once the instance is running, you can continue with the configuration of ArcSight Investigate for AWS.

Configuring Vertica 8.1.1 for AWS

Perform the following steps to set a new password for Vertica's dbadmin account and a license update.

Note: This Vertica installation comes with a Community License edition.

Starting Vertica Database

1. Connect to the Vertica EC2 instance via ssh: sh -i <private_key> centos@<aws-assigned-address>

2. From root account :

    2.1 su - dbadmin

    2.2 To check the database status: $ admintools -t view_cluster

2.3 To start the database: $ admintools -t start_db -d investigate -p <dbadmin pass>

2.4 To stop the database: $ admintools -t stop_db -d investigate -p <dbadmin pass>

Changing Password

1. Connect to the Vertica EC2 instance via ssh: ssh -i <private_key> centos@<aws-assigned-address> .

2. From root account, change the user to 'dbadmin'.

2.1 su - dbadmin.

2.2 Issue vsql command. Password: cloud .

2.3 The following console must be displayed in the terminal:

Type: \h or \? for help with vsql commands.

\g or terminate with semicolon to execute query.

\q to quit.

2.4 Run the following command:

dbadmin=> alter user dbadmin IDENTIFIED BY '<NewPass>';

ALTER USER

dradmin=> \q

2.5 Verify the change has been applied by connecting to the database using

the admintools console utility: $ admintools

2.6 Select Connect to Database (Option 2).

2.7 Log in with dbadmin user and password.

3. Connect to the Vertica EC2 instance via ssh: ssh -i <private_key> centos@<aws-assigned-address>.

3.1 Using sudo access, change the user to 'dbadmin'.

3.2 Run the following commands:

NEW_PASS='<NewPass>'

sed -i /^dba_password=/c\dba_password=$(echo ${NEW_PASS} | base64) /opt/install-

vertica/vertica.properties

Note: Replace '<NewPass>' with the password of your preference.

Uploading your Entitled Vertica License

1. Connect to the Vertica EC2 instance via ssh: ssh -i <private_key> centos@<aws-assigned-address> .

2. From root account, change the user to 'dbadmin'.

    2.1 su - dbadmin.

3. Select Advanced Menu (Option 7).

4. Select Upgrade License Key (Option 5).

5. Enter your entitled license file path.

6. Wait for the upgrading license to be ready.

7. Exit admintools.

8. To verify your license:

    8.1 su - dbadmin.

    8.2 Issue vsql command. Password: cloud

    8.3 The terminal switches to :

        Type: \h or \? for help with vsql commands \g

        or terminate with semicolon to execute query \q to quit.

    8.4 Run the following command to verify your license:

        dbadmin=> SELECT DISPLAY_LICENSE();

Running the Kafka Scheduler

Create

1. Connect to the Vertica EC2 instance via ssh: ssh -i <private_key> centos@<aws-assigned-address> .

2. From root account, navigate to /opt/install-vertica

3. Run ./kafka_scheduler create <Event Broker Worker Node 1 IP>:9092 <Partition number>

    3.1 The default number of partitions is 6.

Check kafka_scheduler Status

1. Connect to the Vertica EC2 instance via ssh: ssh -i <private_key> centos@<aws-assigned-address> .

2. From root account, navigate to /opt/install-vertica

3. Run ./kafka_scheduler status

Starting & Stopping kafka_scheduler

1. Connect to the Vertica EC2 instance via ssh: ssh -i <private_key> centos@<aws-assigned-address> .

2. From root account, navigate to /opt/install-vertica

3. To start kafka_scheduler: Run ./kafka_scheduler start

4. To stop kafka_scheduler: Run ./kafka_scheduler stop

Deleting kafka_scheduler metadata

1. Connect to the Vertica EC2 instance via ssh: ssh -i <private_key> centos@<aws-assigned-address> .

2. From root account, navigate to /opt/install-vertica

3. Run ./kafka_scheduler delete

Troubleshooting Vertica on AWS

To check open ports using Netcat Utility, see Vertica Analytics documentation

Additional Information

For additional information on the use and operation of ArcSight Event Broker, see the HPE ArcSight product documentation, available from the HPE ArcSight support community at https://www.protect724.hpe.com

You can also reach HPE ArcSight Software Support at: https://softwaresupport.hpe.com

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Setup Guide (Investigate DB 8.1.1 for AWS)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!