

# SECURING CLOUD BASED FUSION MIDDLEWARE APPLICATIONS

# Vivek Kumar Sethi\* and Shrikant Lade

RKDF Institute of Science and Technology, Bhopal, India.

## ABSTRACT

Cloud computing represents the next generation of sharing computing and storage resources over a network in a self-service manner without direct involvement in how that computing and storage is resourced. Utilization of the cloud via third-party, web-based providers, such as Amazon EC2, Amazon S3 and Google App Engine, is becoming increasingly common. However, cloud computing is also available to enterprises as private clouds, meant to leverage existing investments in data centers and help overcome some of the physical and political barriers to cloud computing adoption. In general, a private cloud is a centralized shared infrastructure with automated capacity adjustment that internal business units utilize in a self-service manner.

**Keywords**: Amazon VPC, Virtual Private Cloud, AWS VPC, EC2, Security Groups, Oracle Fusion middleware App, Scalable, High availability, Cluster, ADF, Weblogic.

## **INTRODUCTION**

This document gives steps to provision a midsize virtual machine on amazon cloud EC2, there by selecting the RHEL Linux platform, setting up the Linux parameters hardening database, Installing weblogic application server and hardening weblogic server.

## System Model

All the recommendations provided are to be followed manually by administrator. Its recommended to install OS, required Application as fusion middleware app and then do the hardening followed by application hardening

## **Previous work**

A lot of articles are present in weblogic domain. However this article is mainly to address need to security when deploy the application on cloud based platform.

## PROPOSED METHODOLOGY

a. Create a virtual private cloud in AWS.

b. After making VPC ascribes an internet gateway that links virtual private cloud to internet hence, provides access to resources of amazon web services like S3.

c. Next is to form a virtual private cloud subnet in which the EC2 instances are launched.

d. To facilitate the traffic flow amid internet and subnet a routing is customary in the virtual private cloud. In the diagram the circle marked R (implied router) depicts that your VPC is routing between subnet and internet.

e. To regulate inbound and outbound traffic flow you ought to set up a security group for the instances launched by you.

f. An instance having private IP is launched into the subnet.

g. In addition, an Elastic IP is assigned to instance which is a public IP and the already assigned private IP.

h. EC2 console is available at https://console. aws.amazon.com/ec2/.

i. From EC2's dashboard click on Launch Instance.

j. From Create New Instance, choose Classic Wizard and click Continue.

k. Quick Start tab on Choose an AMI page shows list of configurations which are called Amazon Machine Images. Click your AMI and press Select.

1. To launch single micro instance in the subnet leave default value that is Micro in Instance Type menu on

Corresponding Author:- Vivek Kumar Sethi Email:- viveksavitasethi@gmail.com

m. Instance Details page.

n. Select VPC tab available under Launch Instance and make certain your subnet is checked in Subnet drop down and press Continue.

o. IP address to be used for your instance can be indicated in Advance Instance Options.

p. To use default storage click on Continue.

q. Enter tags required for instance if any and click on Continue.

r. From Create Key Pair either an existing key pair can be selected or a new one can be created.

- s. To create a new key pair:
- t. Click on Create New Key Pair.

u. Enter name for the key pair (like Virtual\_key) and press Create and Download Key Pair.

v. When the key is prompted it should be protected in a benign place on the system and click on Continue.

w. The Configuration Firewall page contains Choose one or more of the existing Security Group. Select the group created by you earlier i.e. WebserverSG.

x. Settings can be reviewed from the Review page to make sure everything is in place.

y. Click Launch in order to launch the instance.

z. All the pre-installation mandates have to be followed irrespective of the infra needs.

aa. Partition: Server should have partition for /root, /boot,/usr,/var ,/tmp,and/home. Third party should be installed on /opt

bb. Ports : all default ports should be replaced with non-default ports

## Installation tasks

- Create the database with advance option click next.
- DBCA will start automatically for configuring components.
- Assign a common password for SYS user Select OMF as file option.
- Do not fill anything in recovery area. Use UNICODE UTF-8 as CHAR set.
- Execute orainstRoot.sh and root.sh from root user.

## Security configuration

Remove tkprof from cloud system.

Change listener port from 1521 to 1526.

Change connection manager default port from 1630 to 1636 using cman in ORACLE\_HOME/network/admin. Change http port from 1158 to 1160 using ecma-reconfigure ports-DBCONTROL\_HTTP\_PORT.

Change RMI port to 5520 to 5526 ecma-reconfigure ports-DBCONTROL\_HTTP\_PORT

DB user should not be left open. They should have all the account as locked which are not being used. Check should be done against this

## SELECTACCOUNT\_STATUSFROMDBA\_USERS

Change the password to be CASE sensitive

ALTER SYSTEM SET SEC\_CASE\_SENSITIVE\_LOGON=TRUE;

Change the LISTERNER name to be a nonstandard name in listerner.ora file in \$ORACLE\_ HOME/network/admin <new listener name > = (Description =...) Listener should have logging enabled LSNRCTL> set log\_status on; LSNRCTL> save config; All the files in ORACLE\_HOME, except for bin should have the permission as 0750 or less

## PROFILE MANAGEMENT

Following profile to be used for creating users ALTER PROFILE <NAME > <PARAM> <VALUE> Param Value Failed\_login attempts 10 Password\_life\_time 60 IDLE\_TIME 180

No OS authentication to database should be allowed. ALTER PROFILE <PROFILE> LIMIT PASSWORD\_VERIFY\_FUCNTION verify\_function\_11G;

## Verify vi /etc/sysctl.conf

kernel.shmmni = 4096 kernel.sem = 250 32000 100 128 net.ipv4.ip\_local\_port\_range = 9000 65500 net.core.rmem\_default = 262144 net.core.rmem\_max = 4194304 net.core.wmem\_default = 262144 net.core.wmem\_max = 1048576

## VERIFY VI /ETC/SECURITY/LIMITS.CONF

oracle soft nproc 2047 oracle hard nproc 16384 oracle soft nofile 1024 oracle hard nofile 65536 oretail soft nofile 4096 oretail hard nofile 65536

## Securing weblogic server

Open the admin server using the http://hostname:port/console Go to the domainname -> configuration and general tab Change production mode = true, refer [1] Click save and active the changes Shutdown weblogic and start the domain

Configure the connection pool, Refer [3] start weblogic script nohup./startNodeManager.sh & nohup./startWeblogicServer.sh & Note: nohup is to ensure that execution runs in background of the server. This will be helpful if any disconnection happens. Go to config.xml in the \$WL\_HOME/config folder And change the ports <machine xsi:type="unix-machineType"> <name>lnxql99v2053</name> <node-manager> <node-manager> <listen-address>lnxql99v2053</listen-address> <listen-port>5556</listen-port> -- change this default port </node-manager> </machine>

## **Enable configuration audit**

Domain -> Configuration ->General tab

#### Figure 1. Weblogic Configuration for production mode

Configuration		Monitoring		Control	Security	Web Servi	ce Security	Notes
General	ЛА	JPA	EJB	s Web /	Applications	Logging	Log Filters	
Save								
Save								

\* Indicates required fields

*Name:	rib-hospital-domain	1
Enable Administration Port		e e e
Administration Port:	9002	i
문 Production Mode:	true	s F

Figure 3	3. Create	database	connection	using DS

Configuration		Targets	Monitoring		Control		Security	Notes		
General	Conr	nection Po	ol	Orade	ONS Transa		ransaction	Diagnostics	I	
Save										

The connection pool within a JDBC data source contains a group of JDBC connectio pool. The connection pool and the connections within it are created when the conn Server or when deploying the data source to a new target.

Use this page to define the configuration for this data source's connection pool.

Contemporation (Contemporation)	jdbc:oracle:thin:@InxqI99v2084.qualif.fr.auchan.com:1
街 Driver	oracle idbc xa client OracleXADataSource

Go to the bottom of the page Refer [4]

## **Enable SSL validation**

Click on the manage server and then go to the SSL tab Refer [5]

## **Disable Mbean attributes**

Disable the M bean attributes from Domain-> Security tab This can be done by unchecking the "autonomous adminlookup enabled" Refer [6]

## **EXPERIMENTAL RESULTS**

Access to application is disabled from all possible treats. Hardening ensures that proper throughput is achieved on the system.

## Figure 2. Manage server

Settings for Inxql99v2054

Configura	ation	Monitorin	g Not	es
General	Node N	Manager	Serve	ers

This page displays the servers that have been assigned to this Machine. You can select a server to confi

#### Customize this table

#### Servers (Filtered - More Columns Exist)

Add	Remove			
	Name 🏟	Cluster	Machine	State
	rib-hospital-wls-instance		Inxql99v2054	RUNNING

## Figure 4. enable configuration audit



## Configuration Archive Enabled

Figure 5. Enable	e SSL – sec	ure layer on	weblogic			Figure	6. I	Disabl	le M	Bean A	PI				
Configuration F	Protocols Log	ging Debug	Monitoring	Control	1	Home L	og Out	Preference	es 🔤 R	ecord Help			Q	Welcome, weblogic	c Conr
General Cluster	Services	Keystores <b>SSL</b>	Federatio	n Services	1	Home >myr hospital-wls	ealm >P instance	roviders >D > <b>rib-hosp</b>	)efaultAuti iital-dom;	nenticator >Sun ain	nmary of S	ecurity Realms	>myrealm	>Providers >DefaultAu	uthentic
Health Monitoring	Server Start	Web Services				Settings for	rib-ho	spital-do	main						
Click the Lock & E	dit button in th	e Change Center 1	o modify the	settings o	n ti	Configuratio	n M	onitoring	Control	Security	Web Ser	vice Security	Notes	1	
Save						General	Filter	Unlock L	lser Er	nbedded LDAP	Roles	Policies	SSL Certi	ficate Revocation Cheo	cking
This page lets you the security of me Identity and True Locations:	view and define ssage transmiss st Ke	e various Secure S sions. ystores Change	ockets Layer	r (SSL) sett	ing	Click the L Save This page realm for t	allows y	ou to defir	in the Ch ne the ger ain.	ange Center ti neral security s	o modify t settings for	re settings or this WebLog	n this page gic Server	e. domain. Use this page	to cha
Identity Private Key Loca	tion: fro	om Demo Identity H	(eystore			🅂 Defau	t Realı	n:		myrea	ılm 🗾			Select the security ro default (active) realr domain. More Info	ealm th m for th
Private Key Alias	: De	moldentity				🔲 街 A	nonym	ous Admi	n Looku	p Enabled				Specifies whether ar WebLogic Server MB MBeanHome API.	honymc Jeans sl More In
Private Key Pass	phrase:	•••••	•••••			Cross	Doma	in Securit	y Enable	ed .				Specifies whether or for the domain. Mo	not crore Info

## CONCLUSION

Fusion middleware application deployed on cloud console has to be secure. The above steps will ensure that database and weblogic are secured.

# REFRENCES

- 1. AMAZON EC2 white papers.
- 2. ElasTras: An elastic, Scalable and self-Managed Transactional Database for the cloud by: Sudipto das, divyakant agarwal, and amr el abbadi, University of California, Santa Barbara.