BASIC INSTALL ON AWS SERVER

1. Click on EC2



2. Click on Launch instance



3. Select the OS type



4. Select instance type and click on Review and Launch

	• type	* VCPUs ()	 Memory (GiB) 	 Instance Storage (GB) (1) 	EB
General purpo	ose t2.micro Free tier eligi	Die 1	1	EBS only	

5. Add security rule to allow HTTPS to connect to your server and to open port 4244

Туре 🛈	Protocol (i)	Port Range (i)	Source (i)			
RDP -	TCP	3389	Anywhere -	0.0.0/0	8	
HTTPS •	TCP	443	Anywhere •	0.0.0/0	8	
Custom TCP Rule	TCP	4244	Anywhere 🔻	0.0.0/0	8	

6. Review instance details and click Launch

nstance Type	ECUs	VCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance		
2 micro	Variable	1	1	EBS only	*	Low to Moderate		
curity Groups							Edit security	y grou
ecurity Groups curity group name scription	launch-w	vizard-2 vizard-2 creater	1 2015-05-04T10:27:12	.712+10:00			Edit security	y grou

7. Select or create a key pair for security purposes. Click on Launch

A key pair consists of a public key that AWS shey allow you to connect to your instance sec to obtain the password used to log into your in ecurely SSH into your instance.	stores, and a private key file that you store, curely. For Windows AMIs, the private key file in stance. For Linux AMIs, the private key file all	Together, s required ows you to
lote: The selected key pair will be added to th	he set of keys authorized for this instance. Lea	irn more
Choose an existing key pairs from a publi	IC AMI.	•
Select a key pair		
	e selected private key file (Delilah pem) and th	nat

8. The server will begin to boot up. Click on the Launch instances button to see the status of all your instances. Once it is active and running, you can get the windows password.



- 9. Use the security certificate created in the key pair step to decrypt the password. Then RDP to your instance and log in:
 - a. Start > Run > mstsc
 - b. Enter the public IP of the instance
 - c. Login as administrator using the decrypted password

10. Add a <u>new</u> inbound rule to open port 4244 and 443 for Qlik Sense. Allow connections from anywhere. Give the rule a name eg. "Qlik Sense open ports 442 & 4244" and save it.

<i>\[</i>	New Inbound	I Rule Wizard	x				
Protocol and Ports							
Specify the protocols and ports	to which this rule applies.						
Steps:	Deep this are produce TCP or LU						
 Rule Type 							
Protocol and Ports							
 Action 	O UDP						
Profile							
Name	Does this rule apply to all local p	orts or specific local ports?					
	○ All local ports						
	Specific local ports:	443, 4244					
		Example: 80, 443, 5000-5010					
Steps:							
Rule Type	What action should be taken wh	en a connection matches the specified conditions?					
Protocol and Ports	Allow the second time						
Action	This includes connections the	at are protected with IPsec as well as those are not.					
Profile	Aller 16						
 Name 	This includes only connection in will be secured using the sett Rule node.	it is secure ns that have been authenticated by using IPsec. Connections ings in IPsec properties and rules in the Connection Security					
-							
Steps:)) (han dage this side see 1-2						
Rule Type	when does this rule apply?						
Protocol and Ports							
Action	Domain	connected to its corporate domain					
Profile		connected to its corporate domain.					
Name	 Private Applies when a computer is or work place. 	connected to a private network location, such as a home					
	Public						
	Applies when a computer is o	connected to a public network location.					

Note: Do not user the existing rule for HTTPS / 443 as it is not configured correctly.

11. Turn off Internet Explorer Enhanced Security for Admins (and users if preferred)

N In	ternet Explorer Enhanced Security Configuration
Intern expos	et Explorer Enhanced Security Configuration (IE ESC) reduces the ure of your server to potential attacks from Web-based content.
Intern defaul	et Explorer Enhanced Security Configuration is enabled by t for Administrators and Users groups.
Admin	istrators:
0	O on (Recommended)
8	● Off
Users:	
0	On (Recommended)
8	⊖ off
More a	about Internet Explorer Enhanced Security Configuration
	OK Cancel

12. Setup a local account to run the Qlik Sense Services and make that user a member of the Local Administrators group

Name Full I	lame	Description
Administrator		Built-in account for administering the co
Guest		Built-in account for guest access to the c
Qlik_Service Qlik	Services	Note: Member of Local Admin Group

13. Ensure .NET Framework 4.5.1 is installed (although this should be available by default in Win2012 R2)



14. Install Qlik Sense as per the installation guide

- a) Run the install.exe as Administrator
- b) Select Quick Install



It is recommended that you close all other applications before continuing. Click on the option you wish to install.



Installs all program features. Recommended for a single node installation. Requires 300 MB of free disk space.

c) Enter user account for services

Qlik (Q ° Sense	
Service credentials	
Enter user information for starting the services.	
Warning: Not entering any user information will result in the services being installed with local system service credentials.	
Username	
.\Qlik_Service	_
Password	

Repository Service	
Select a role for the Qlik Sense Repository Service.	
Central node 🔞	

15. **IMPORTANT!** When you come to the step where the node needs to be named, ensure you use the exact server name rather than the lengthy qualified name that will default (see below)



Host name

The central node uses certificates to communicate with other servers securely. Specify the address to this machine in the same format that other machines will use to connect to this machine.

Enter the address for this machine 🚱	
WIN-ROOT7D5H5S8	
	1

... or select one of the pre-defined values below:

16. Open the Qlik sense Management Console and enter your licence details

Attps://win-root7d5h5s8/qmc/sitelice	ense 🔎 👻 🚔 🖒 🏉 Site license properties - QMC 🛪
E Site license properties	
Qlik (Q) Sense	
SITE LICENSE	. 1000
Owner organization	
Serial number	- Cana
	Mandatory. Please enter a value.
Control number	
	Mandatory. Please enter a value.

17. In the QMC, select Start > Licence and Tokens, and allocate a user tokens to the Administrator account.

()	🍯 https	s//win	-root7d5 🔎 + 🔒	🖒 🏉 User access	s allocations - Q	×				. ↔
🏫 Start	-							🕜 Help	•	administrator 🤊
💵 User	access	alloca	ations Total: 1	Showing: 1	Selected: 0			÷		
Name	٣	G	User directory	G	Status	[Ŧ	Last used	[7	License	and tokens
administr	ator		WIN-ROOT7D5F	H5S8	Allocated		2015-05-05 09:43			
									✓ User alloc	access ations
									User	

18. Test navigating to the Qlik Sense Hub as the Administrator

(-) (https://win-root	.7d5 ,Ѻ ▾ 🔒 Ĉ	🦪 Qlik Management Console	e 🧭 Qlik Sense
Qlik' Sense S	E-	administrator WIN-ROOT7D5H5S8	
My work	My work		Create new app
Administration			
Everyone	No	apps are available in	1 this view

CONFIGURE SENSE SERVER FOR ACCESS BY EXTERNAL USERS

a) To configure the Qlik Sense proxy whitelist,

- a. Open the Sense Mgt Console and select Start > Virtual Proxies.
- b. Click on the Central Proxy and select Edit
- c. Click on Advanced in the right hand side properties pane to show the advanced properties.
- b) Add the computer name, the pubic IP and the public DNS to the white list as shown below. Then click on Apply to save the details. The proxy will be restarted.

	G Add new value	
ec2-52-64-124-12	2.ap-southeast-2.compute.amazonaws.com	c
52.64.124.12		

- c) If you are using local users for authentication, then you will need to do the following for each user to enable external access using those accounts.
 - a. Create the user in Computer Management
 - b. Attempt to logon as each new user. You will get an error saying you cannot access Qlik Sense. This is because the user has no security token assigned.
 However this process will add the user to the list of users in the Qlik Sense management console. Unless you attempt to logon first the user account will not be visible and you will not be able to assign a token.
 - c. Assign a security token to the user, as was done above for the Administrator account