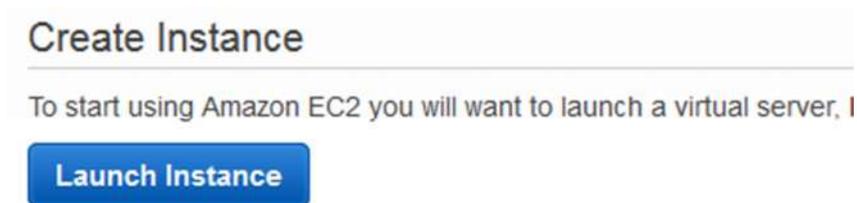


BASIC INSTALL ON AWS SERVER

1. Click on EC2



2. Click on Launch instance



3. Select the OS type



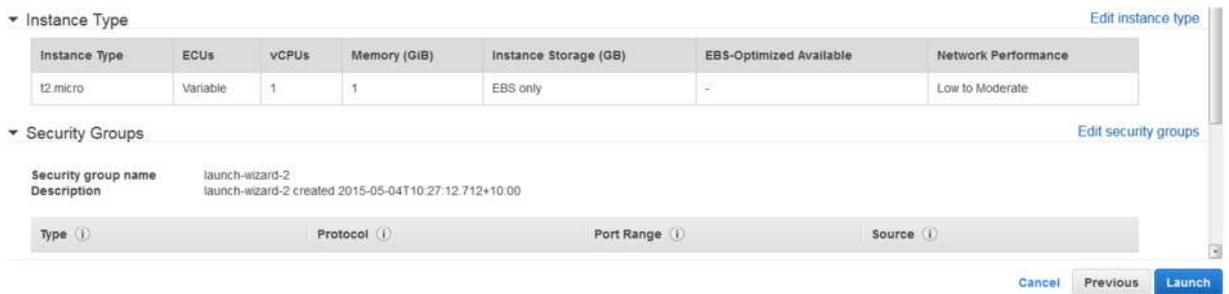
4. Select instance type and click on Review and Launch

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EB
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	

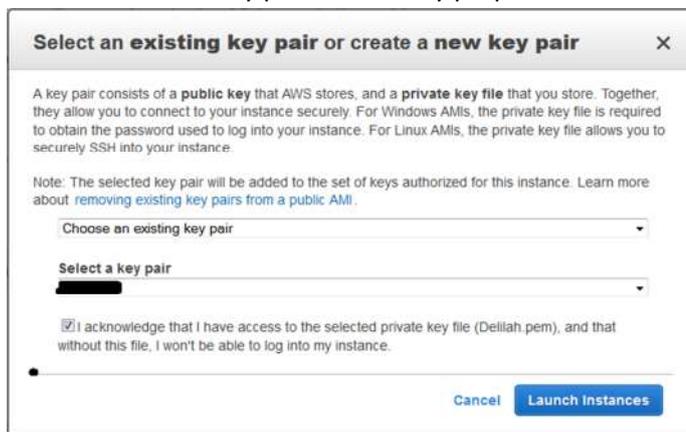
5. Add security rule to allow HTTPS to connect to your server and to open port 4244

Type	Protocol	Port Range	Source
RDP	TCP	3389	Anywhere 0.0.0.0/0
HTTPS	TCP	443	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	4244	Anywhere 0.0.0.0/0

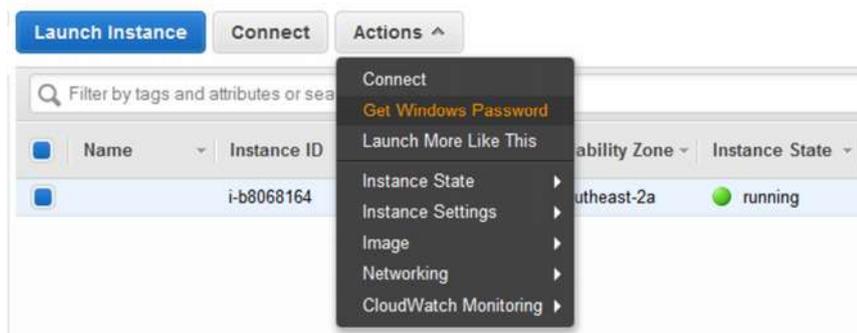
6. Review instance details and click Launch



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



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:

- Start > Run > mstsc
- Enter the public IP of the instance
- Log in as administrator using the decrypted password

10. Add a new 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.

The screenshot shows the 'New Inbound Rule Wizard' window with the 'Protocol and Ports' step selected. The window title is 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' sidebar lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main content area asks 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP. Below, it asks 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports' (selected). A text box next to 'Specific local ports' contains '443, 4244' and an example 'Example: 80, 443, 5000-5010' is shown below it.

The screenshot shows the 'New Inbound Rule Wizard' window with the 'Action' step selected. The 'Steps' sidebar lists: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main content area asks 'What action should be taken when a connection matches the specified conditions?' with radio buttons for 'Allow the connection' (selected) and 'Allow the connection if it is secure'. Descriptions are provided for each option. A 'Customize...' button is located at the bottom.

The screenshot shows the 'New Inbound Rule Wizard' window with the 'When does this rule apply?' step selected. The 'Steps' sidebar lists: Rule Type, Protocol and Ports, Action, Profile, and Name (selected). The main content area asks 'When does this rule apply?' with three checked radio buttons: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.).

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

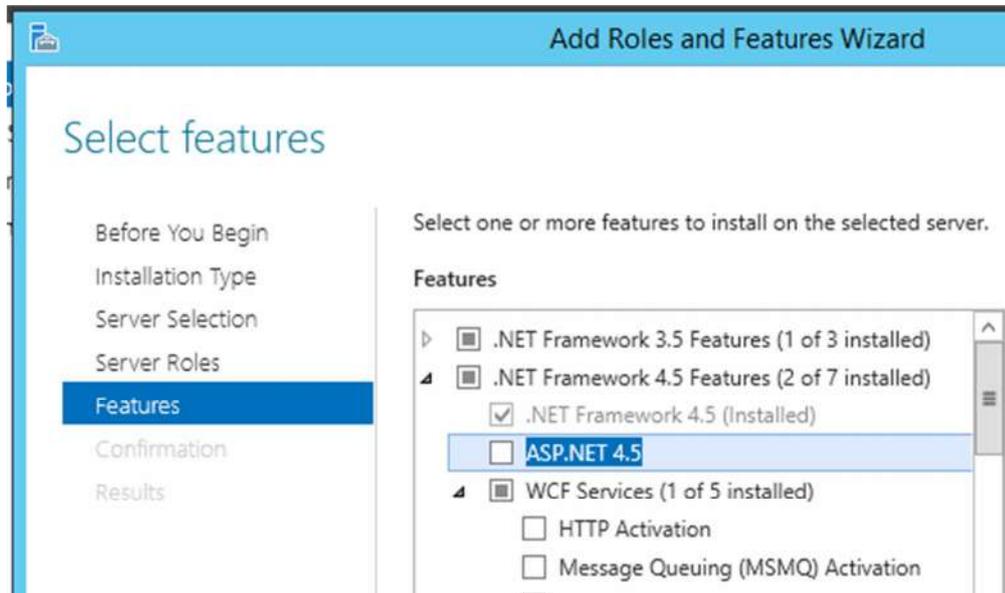
11. Turn off Internet Explorer Enhanced Security for Admins (and users if preferred)



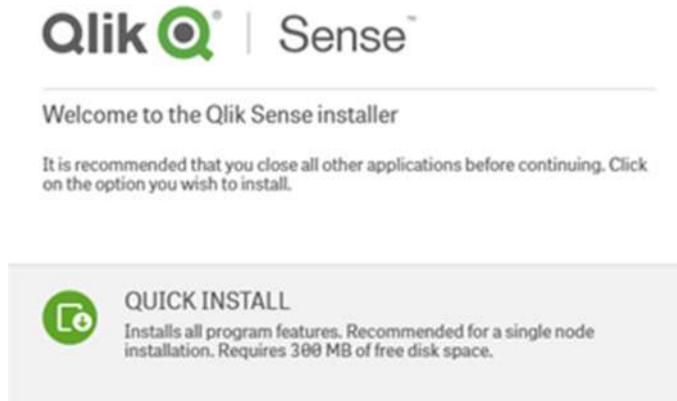
12. Setup a local account to run the Qlik Sense Services and make that user a member of the Local Administrators group

Computer Management		
Name	Full Name	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
- Run the install.exe as Administrator
 - Select Quick Install



- Enter user account for services



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

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... [?](#)

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

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

Site license properties

Qlik Sense™

SITE LICENSE

Owner name: lms

Owner organization: qlik

Serial number:
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.

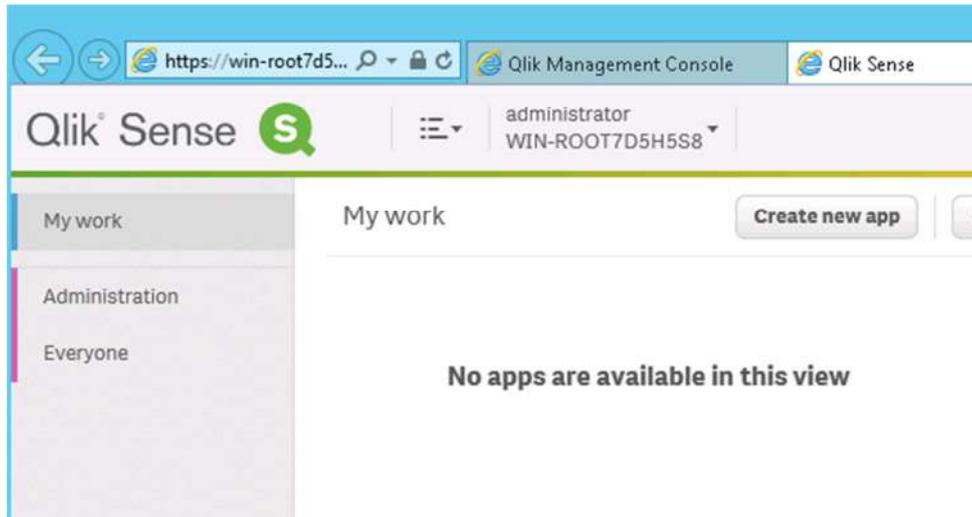
User access allocations Total: 1 Showing: 1 Selected: 0

Name	User directory	Status	Last used
administrator	WIN-ROOT7D5H5S8	Allocated	2015-05-05 09:43

License and tokens sidebar:

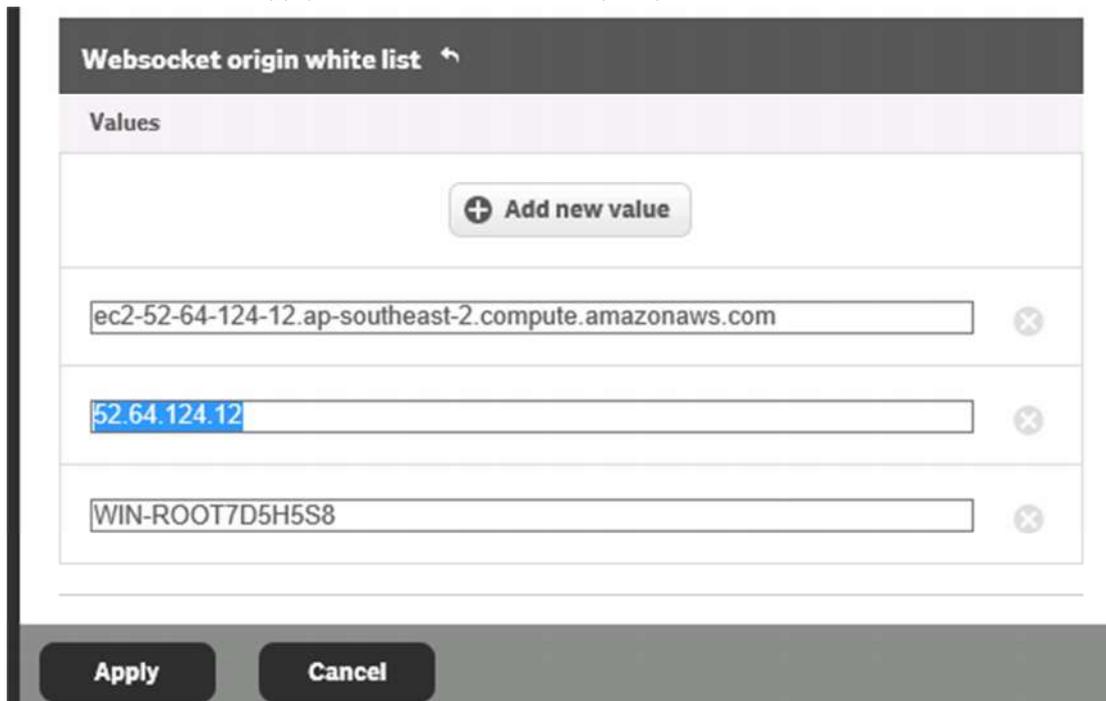
- License usage summary
- ✓ User access allocations
- User access rules

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



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 public 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.



- 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