



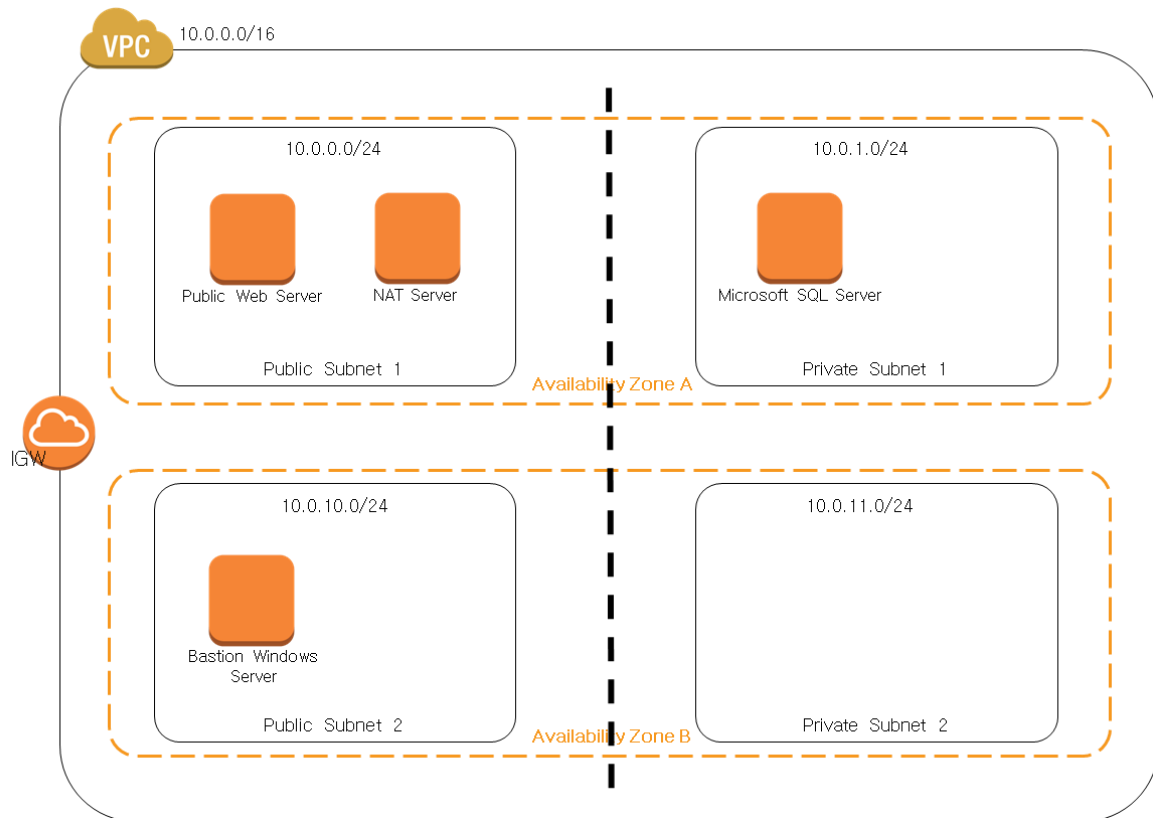
아마존 Virtual Private Cloud(VPC) 구축

Date : February 23, 2015

arang@gsneotek.co.kr

GS NEOTEK CO.,LTD

개요



- 두 개의 AZ로 나누고 분산을 통해 안정성과 가용성을 확보한다.
- 각 AZ에는 두 개의 서브넷을 만든다. Public 서브넷은 인터넷에 직접 연결되고, Private 서브넷은 VPC 내의 다른 서브넷들과 연결되지만 인터넷에는 연결되지 않는다. 가운데 점선은 이 경계를 의미한다.

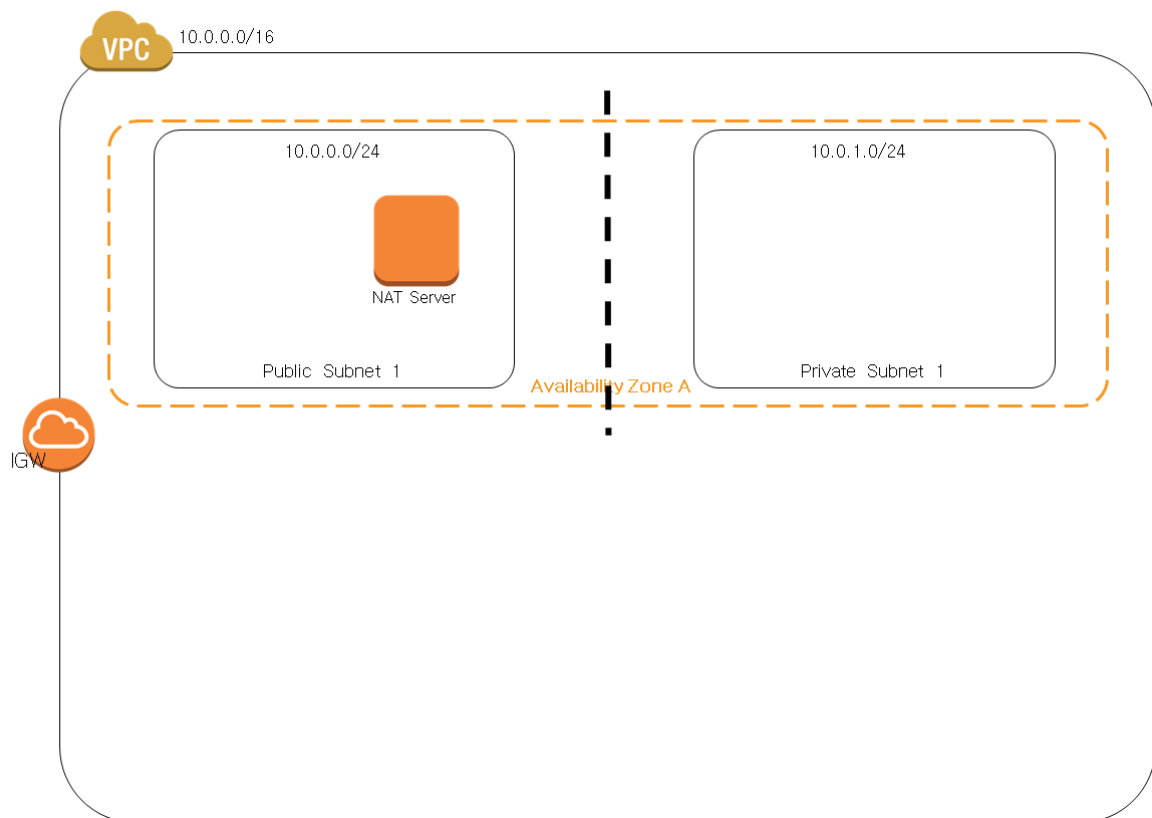
다루는 내용

- 아마존 Virtual Private Cloud (VPC) 생성하기
- 웹 서버 구축하기
- Elastic IP 주소 생성 및 할당하기
- Back-End Microsoft SQL Server 구축하기
- 서브넷 생성하기

- Bastion Windows Host 구축하기
- Bastion 서버에 연결하기

실습

VPC 생성



1. 콘솔에서 **VPC** 클릭
2. **Start VPC Wizard** 클릭
3. **VPC with Public and Private Subnet** 탭 클릭
4. **Select** 클릭
5. **VPC with Public and Private Subnets** 페이지
 - **VPC name** : *LAB VPC* 입력
 - **Availability zone** : *us-west-2a* 선택

- **Key Pair name** : *ec2_keypair* 입력
- **Create VPC** 클릭
- **OK** 클릭

웹 서버 실행

6. 콘솔에서 **EC2** 클릭
7. **Launch Instance** 클릭
8. **Choose an Amazon Machine Image (AMI)** 페이지
 - Amazon Linux AMI 선택
 - **Select** 클릭
9. **Choose an Instance Type** 페이지
 - **Next: Configure Instance Details** 클릭
10. **Configure Instance Details** 페이지
 - **Network** : LAB VPC (10.0.0.0/16) 선택
 - **Subnet** : Public Subnet (10.0.0.0/24) 선택
 - **Auto-assign Public IP** : Enable
 - **Advanced Details** 섹션의 **User data**

웹 서버 설치 및 실행을 수행하는 스크립트를 입력한다.

▼ **Advanced Details**

User data ⓘ

☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!/bin/bash
/usr/bin/yum -y install httpd
/sbin/chkconfig httpd on
/sbin/service httpd start
```

- **Next : Add Storage** 클릭

※ user data 내용이 인터넷을 사용하므로 인터넷 접속 관련 정보를 꼭 확인한다.

11. **Add Storage** 페이지

- **Next : Tag Instance** 클릭

12. Tag Instance 페이지

- **Value** : *Web Server 1*
- **Next: Configure Security Group** 클릭

13. Configure Security Group 페이지

- **Assign a security group** : Create a new security group 선택
- **Security group name** : *Web*
- Add Rule 클릭 : HTTP (80) 추가
- Add Rule 클릭 : HTTPS (443) 추가
- **Review and Launch** 클릭

Type ①	Protocol ①	Port Range ①	Source ①	
SSH ▾	TCP	22	Anywhere ▾ 0.0.0.0/0	⊗
HTTP ▾	TCP	80	Anywhere ▾ 0.0.0.0/0	⊗
HTTPS ▾	TCP	443	Anywhere ▾ 0.0.0.0/0	⊗
Add Rule				

14. Review Instance Launch 페이지

- **Launch** 클릭
- key pair 선택
- **Launch Instances** 클릭

Elastic IP 주소 생성 및 할당

15. 왼쪽 메뉴에서 **Elastic IPs** 클릭
16. **Allocate New Address** 클릭
 - **Yes, Allocate** 클릭
 - **Close** 클릭
17. 할당 받은 EIP 선택 후 **Associate Address** 클릭
 - **Instance** : Web Server 1 선택

Associate Address
✕

Select the instance OR network interface to which you wish to associate this IP address (52.10.199.240)

Instance

Network Interface

Private IP Address

☐ Reassociation

i-49879c43 (Web Server 1) (running)

i-bb908bb1 (NAT) (running)

☐ Reassociation

Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more about [public IP addresses](#).

Cancel Associate

· **Associate** 클릭

18. 인스턴스의 Public DNS로 브라우저에 접속하여 확인한다.



Back-End Microsoft SQL Server 실행

19. 콘솔에서 **EC2** 클릭
20. **Launch Instance** 클릭
21. **Choose an Amazon Machine Image (AMI)** 페이지
 - Microsoft Windows Server 2012 with SQL Server Web 선택
 - **Select** 클릭
22. **Choose an Instance Type** 페이지
 - **Next: Configure Instance Details** 클릭
23. **Configure Instance Details** 페이지
 - **Network** : LAB VPC (10.0.0.0/16) 선택
 - **Subnet** : Private Subnet (10.0.1.0/24) 선택
 - **Network interface** 섹션의 **Primary IP** : 10.0.1.99 입력

▼ **Network interfaces**

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfac ▼	subnet-06c5486 ▼	10.0.1.99	Add IP

 - **Next : Add Storage** 클릭
24. **Add Storage** 페이지
 - **Next : Tag Instance** 클릭
25. **Tag Instance** 페이지
 - **Value** : *SQL Server*
 - **Next: Configure Security Group** 클릭
26. **Configure Security Group** 페이지
 - **Assign a security group** : Create a new security group 선택
 - **Security group name** : *SQL Server*

· **Review and Launch** 클릭

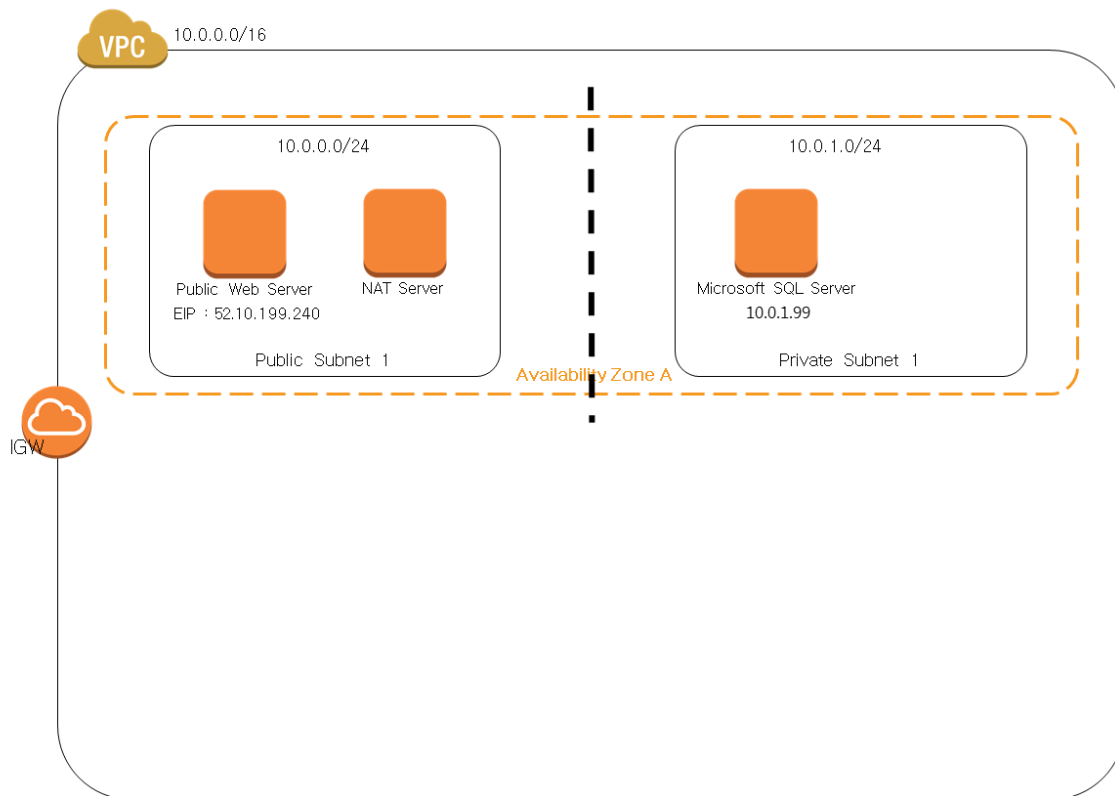
Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	
RDP ▾	TCP	3389	Anywhere ▾ 0.0.0.0/0	✕
MS SQL ▾	TCP	1433	Anywhere ▾ 0.0.0.0/0	✕
Add Rule				

27. **Review Instance Launch** 페이지

· **Launch** 클릭

· key pair 선택

· **Launch Instances** 클릭



두 개의 서브넷 추가 생성

28. 콘솔에서 **VPC** 클릭

29. 왼쪽 메뉴에서 **Subnets** 클릭

30. **Create Subnet** 클릭

public 서브넷을 추가한다.

- **Name Tag** : *Public subnet 2*
- **VPC** : LAB VPC (10.0.0.0/16) 선택
- **Availability Zone** : us-west-2b 선택 (기존 AZ와 다른 AZ)
- **CIDR block** : *10.0.10.0/24*
- **Yes, Create** 클릭

31. Create Subnet 클릭

private 서브넷을 추가한다.

- **Name Tag** : *Private subnet 2*
- **VPC** : LAB VPC (10.0.0.0/16) 선택
- **Availability Zone** : us-west-2b 선택
- **CIDR block** : *10.0.11.0/24*
- **Yes, Create** 클릭

32. Public Subnet 라우팅 변경

- Public subnet 2 (10.0.10.0/24) 선택

Summary	Route Table	Network ACL	Tags
<div>Edit</div>			
Route Table: rtb-4a42f22f			
Destination	Target		
10.0.0.0/16	local		
0.0.0.0/0	eni-1aecac7e / i-bb908bb1		

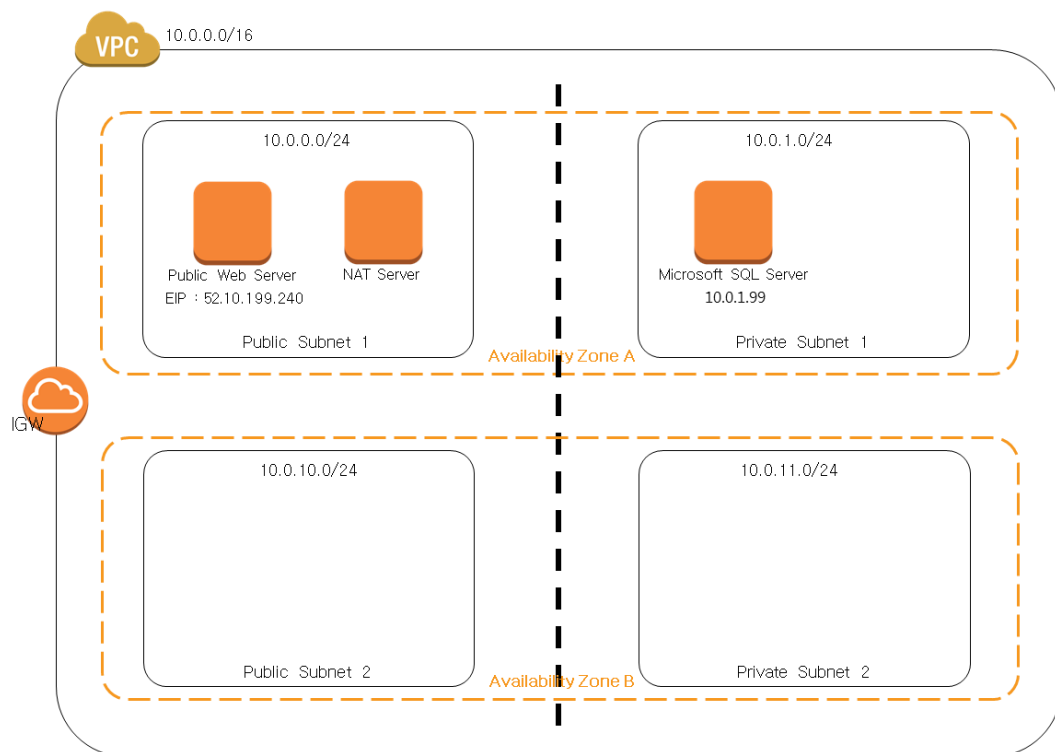
- **Edit** 클릭
- **Change to** : 다른(target이 igw인) 테이블 선택
- **Save** 클릭

Summary **Route Table** Network ACL Tags

Cancel Save

Current Route Table: [rtb-4a42f22f](#)
Change to: [rtb-5542f230](#) ▼

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-3d8a5b58



Bastion Windows 호스트 실행

33. 콘솔에서 **EC2** 클릭
34. **Launch Instance** 클릭
35. **Choose an Amazon Machine Image (AMI)** 페이지
 - Microsoft Windows Server 2012 R2 Base 선택
 - **Select** 클릭

36. **Choose an Instance Type** 페이지

- **Next: Configure Instance Details** 클릭

37. **Configure Instance Details** 페이지

- **Network** : LAB VPC (10.0.0.0/16) 선택
- **Subnet** : Public Subnet 2 (10.0.10.0/24) 선택
- **Auto-assign Public IP** : Enable
- **Next : Add Storage** 클릭

38. **Add Storage** 페이지

- **Next : Tag Instance** 클릭

39. **Tag Instance** 페이지

- **Value** : *Bastion Windows*
- **Next: Configure Security Group** 클릭

40. **Configure Security Group** 페이지

- **Assign a security group** : Create a new security group 선택
- **Security group name** : *Bastion Windows*
- **Review and Launch** 클릭

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
RDP ▾	TCP	3389	Anywhere ▾ 0.0.0.0/0 ✕
Add Rule			

41. **Review Instance Launch** 페이지

- **Launch** 클릭
- key pair 선택
- **Launch Instances** 클릭

SQL 서버에 Bastion 호스트에서만 접속 가능하도록 보안 그룹을 수정한다.

42. 왼쪽 메뉴에서 **Security Groups** 클릭

43. Group Name이 SQL Server인 보안 그룹 선택

- **Inbound** 탭 클릭
- **Edit** 클릭
- RDP의 Source를 Custom IP로 변경하고 Bastion Windows의 보안 그룹 ID 입력

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
MS SQL ▼	TCP	1433	Anywhere ▼ 0.0.0.0/0 ✕
RDP ▼	TCP	3389	Custom IP ▼ sg-9ccceef9 ✕

Add Rule Cancel Save

- **Save** 클릭

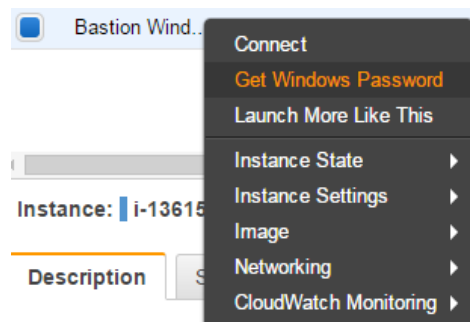
Windows 서버 접속 패스워드를 획득한다.

44. 콘솔에서 **EC2** 클릭

45. 왼쪽 메뉴에서 **Instances** 클릭

46. Bastion Windows 인스턴스 선택

47. 마우스 우클릭하여 **Get Windows Password** 선택



48. **Retrieve Default Windows Administrator Password** 창에서

- key pair 선택
- **Decrypt Password** 클릭
- 생성된 패스워드 확인 후 **Close** 클릭

You can connect remotely using this information:

Public IP 52.10.166.192

User name Administrator

Password udwew(n)Y

49. 동일한 과정으로 SQL Server의 패스워드 획득

Windows 서버에 접속한다.

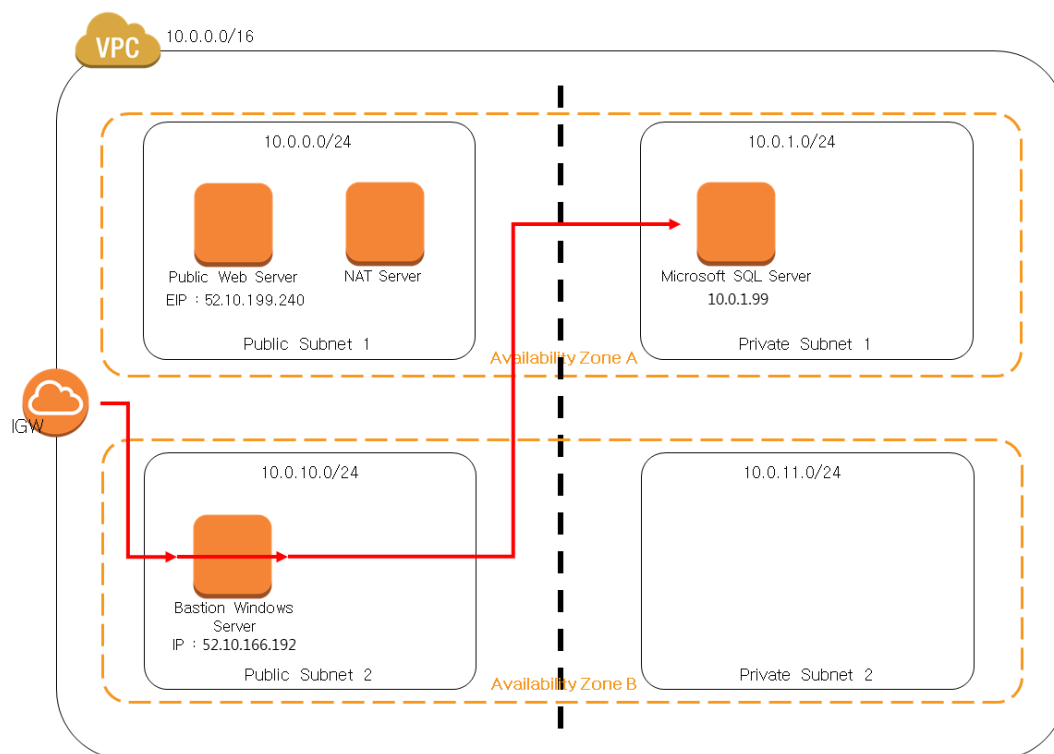
50. '윈도우 + R' 실행 창 활성화

51. **mstsc** 실행

52. bastion 호스트의 ID/PWD로 로그인

53. 동일한 방법으로 SQL Server에 접속

· Bastion에서 SQL에 접속시 IP는 Private IP를 사용한다. (예. 10.0.1.99)



참고

- <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>