



[AWS] 2. Amazon EC2와 Amazon EBS

- **References**

- AWS 공인 솔루션스 아키텍트 스터디 가이드 - 어소시에이트 3/e - 2장
- <https://inpa.tistory.com/entry/AWS-🎓-EC2-개념-사용-구축-세팅-100-정리-인스턴스-EBS-AMI>
- <https://ohgym.tistory.com/62> (EC2 인스턴스 타입 - 정리)
- <https://aws.amazon.com/ko/ec2/instance-types/> (EC2 인스턴스 타입 - AWS)
- <https://medium.com/harrythegreat/aws-가장쉽게-vpc-개념잡기-71eef95a7098> (VPC 참고)
- <https://dev.classmethod.jp/articles/ec2-summary-for-beginners-kr/>

- **EC2 (Elastic Compute Cloud) 인스턴스 개요**

- 인스턴스의 운영체제, 소프트웨어 스택(CPU 성능, Memory, 스토리지, 네트워크 등), 하드웨어 스펙, 실행 환경을 설정 가능하다

- OS는 Amazon Machine Image (AMI) 에 정의 되어 있으며, 하드웨어 사양은 인스턴스 타입에 따라 달라진다. ⇒ 인스턴스 프로비저닝
- 인스턴스의 상태는 실행 / 종료 / 중지 로 구분

실행	실행중
종료	종료(없어짐)
중지	요금이 부과되지 않음 EBS 볼륨 연결 및 분리 (*Elastic Block Store) 인스턴스로 부터 AMI를 만들 수 있는 상태

• Amazon EBS(Amazon Elastic Block Store) 개요

- 클라우드에서 사용하는 가상의 하드디스크 와 같다.
- 인스턴스는 로컬 인스턴스 스토리지와 EBS 라는 외부 스토리지로 구성
- 로컬 스토리지는 인스턴스 타입마다 제공하는 디스크 유형이나 사이즈에 차이
- EBS 는 인스턴스가 종료되어도 별개로 작동하며 네트워크로 연결 된 서비스 (로컬 스토리지에 저장된 데이터는 인스턴스 수명에 따라 삭제되지만 EBS 에 저장된 데이터는 수명과 상관없이 유지)
- EC2와 같은 AZ에 존재한다. 다른 AZ로 생성해서 EC2에 연결 하려 하면 에러가 발생
- 인스턴스가 삭제 되더라도 외부스토리지(EBS) 를 분리 하여 다른 인스턴스에서 활용 가능
- EBS 볼륨은 암호화가 가능하여 스냅샷을 생성하여 AMI와 같이 백업 가능

• AMI (Amazon Machine Image) 개요

- EC2 인스턴스 실행 비용 외 AMI 소프트웨어에 대한 시간당 비용 또는 라이선스 비용이 청구될 수 있다.

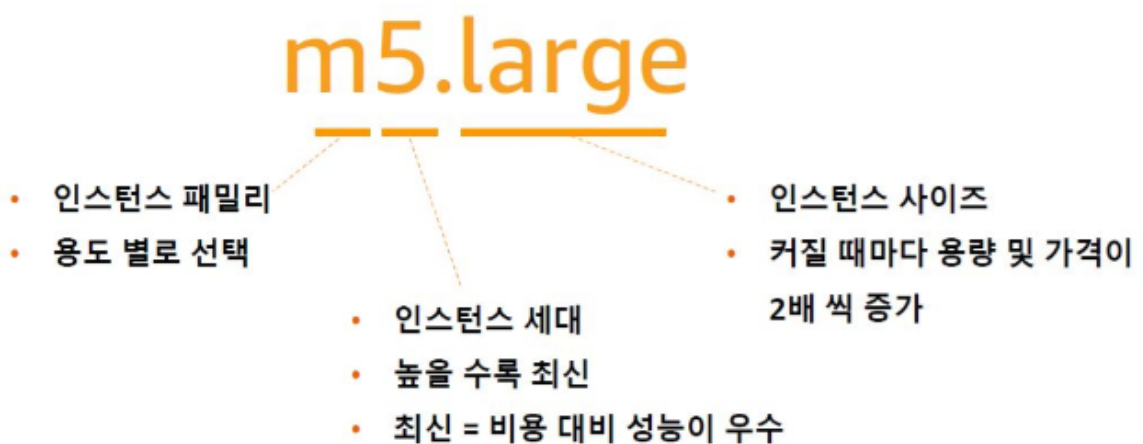
퀵 스타트 AMI	새 인스턴스 런칭 시 콘솔에 가장 먼저 등장, 리눅스, 윈도우 등 다양한 배포판 사용 가능, 최신 기능 및 공식 지원 제공
마켓플레이스 AMI	SAP, Cisco 등 기업용 소프트웨어 벤더가 지원하는 AWS 공식 상용 이미지
커뮤니티 AMI	커뮤니티 이미지, 상당수가 독립적인 벤더에 의해 특수 목적으로 개발 배포
프라이빗 AMI	직접 프라이빗 AMI를 만들어 사용, 오토스케일링 작업에 편의성을 위해 사

용 하기도 한다. 이렇게 만들어진 AMI를 AWS VM Import/Export 도구로 S3와 같은 로컬 인프라에서 VM으로 임포트하여 사용할 수 있다.

※ Amazon EC2 (Amazon Elastic Compute Cloud) 이해하기

• EC2 인스턴스 타입

범용 타입	균형에 초점을 맞춰 일반적이고 다양한 목적에서 사용하도록 설계 되었다. (T, M)
컴퓨트 최적화	고사양의 웹서버 구현 및 고성능이 요구되는 머신러닝 워크로드 처리에 적합 (C)
메모리 최적화	데이터베이스 활용, 데이터 분석, 캐싱 등의 작업, 3.9TB 의 DRAM 메모리 및 SSD 스토리지 볼륨 제공 (X)
가속 컴퓨팅	고성능의 범용 그래픽 프로세싱 유닛이 탑재된 타입 (G,P), F 타입의 경우는 FPGA (Field Programmable Gate Array) 사용 가능, 3D 시각화, 렌더링, 금융 분석, 컴퓨팅 기반 유체역학 워크로드 처리에 주로 사용
스토리지 최적화	대용량 스토리지 볼륨을 탑재한 스토리지 최적화 인스턴스 (H,I,D), I타입의 경우 60TB 의 HDD 스토리지를 선택하여 분산 파일 시스템 또는 고용량 데이터처리 어플리케이션 구현에 활용 가능하다.



• EC2 인스턴스 환경설정

- 리전 : 인스턴스, EC2 리소스는 해당 리전 내에서만 관리 할 수 있다.

- VPC : VPC는 AWS 네트워크 생성 및 관리도구이자 클라우드 인프라 관리 도구, VPC는 논리적 네트워크 구성이기에 물리적으로 분리되어 있는 AZ와 무관하게 설정 가능하다

- <https://medium.com/harrythegreat/aws-가장쉽게-vpc-개념잡기-71eef95a7098> (* 참고)

- 테넌시 모델 (Tenancy Model)

공유 테넌시 (Shared Tenancy)	런칭하는 인스턴스가 하나의 물리적 서버에서 다른 인스턴스와 동시에 실행됨, 기본설정 (Default), 가상 공간에 원격으로 존재하는 서버간 보안규정에 맞지 않는 상호작용이 발생할 가능성 존재
전용 인스턴스 (Dedicated Instance)	인스턴트가 단일 테넌트 하드웨어에서 실행, 물리적으로 분리된 구성
전용 호스트 (Dedicated Host)	인스턴스가 완전히 전용으로 사용할 EC2 인스턴스 용량을 가진 물리적 서버 (사용자가 제어할 수 있는 구성의 격리 서버) 에서 실행, 인스턴스 한개만 구성 가능한 물리적 서버

• 플ACEMENT 그룹 (Placement Groups)

- 사용자의 니즈를 반영한 서버 프로필을 정의할 수 있는 도구

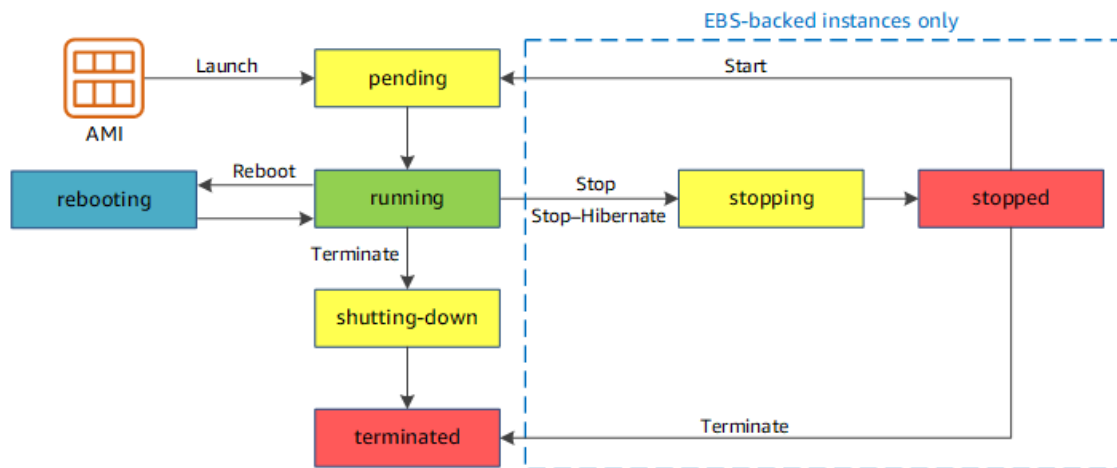
클러스터 (Cluster) 플 레이스먼트 그룹	근거리에 위치한 <u>단일 AZ에 연관 된 인스턴스를 런칭</u> , 고성능 컴퓨팅 (HPC) 애플리케이션에 적합, 상호연결형 네트워크 제공으로 전송지연이 낮음
스프레드 (Spread) 플 레이스먼트 그룹	다수의 AZ 활용으로 데이터소실, 서비스 실패 등의 위험감소, <u>서로 다른 하드웨어 랙에 인스턴스를 분산배치</u>
파티션 (Partition) 플 레이스먼트 그룹	<u>연관 인스턴스를 하나의 파티션으로 묶어 사용</u> , 파티션에 속한 인스턴스는 다른 파티션의 인스턴스와 물리적으로 분리해서 배치 가능, 스프레드 그룹에 속한 인스턴스는 동일한 물리적 서버를 공유하지 않는다는 점에서 파티션 그룹과 차이

• 인스턴스 가격 모델

온디맨드 (On-Demand)	필요에 따라 인스턴스 시작 및 종단을 시킬 수 있는 가장 유연한 방법이지만 시간당 비용은 가장 비싼 모델, 장기적 수요 예측이 힘든 경우 사용
스팟 (Spot)	경매 형식으로 시장에 남은 인스턴스를 구매해서 쓰는 방식, 고성능의 인스턴스가 필요한 경우 사용, 최고입찰가를 넘어서는 입찰자가 나타날 경우 언제 인스턴스를 반납 해야 할지 모른다는 단점이 있다.
예약 (Reserved)	미리 일정기간을 약정해서 쓰는 방식으로 1년에서 3년단위로 갱신 가능하다,

	수요예측이 확실한 경우 사용
전용 호스트 (Dedicated)	실제 물리적 서버를 임대하는 방식, 라이선스 이슈가 생길 가능성이 있다.

• 인스턴스 라이프사이클



Pending	인스턴스는 running 상태로 될 준비를 하고 있습니다. 인스턴스를 처음 시작하거나 pending 상태의 인스턴스를 다시 시작하면 stopped 상태	미청구
Running	인스턴스를 실행하고 사용할 준비가 된 상태	청구
Stopping	인스턴스가 중지 또는 중지-최대 절전 모드로 전환 준비 상태	중지 준비중인 경우 미청구 최대 절전 모드(suspend-to-disk)로 전환 준비 중인 경우 청구
Stopped	인스턴스가 종료되고 사용이 불가, 언제든지 인스턴스를 다시 시작할 수 있다.	미청구
Shutting-down	인스턴스가 종료할 준비중인 상태	미청구
Terminated	인스턴스가 영구적으로 삭제, 시작할 수 없다.	미청구

• 리소스 태그

- 리소스 관리의 복잡성으로 식별체계를 갖추기 위해 일관된 명명 규칙인 리소스 태그를 부여

- AWS 계정으로 접근 할 수 있는 거의 모든 요소에 AWS 리소스 태그를 붙일수 있다.
- 하나의 태그는 키 - 연관 값 으로 작성
- 리소스의 가시성을 높이고, 효과적인 리소스 관리 가능

• 서비스 제한 사항

- 서비스별 인스턴스 수 제한, 개별 리전마다 존재 하기도 하고 또는 글로벌 리전에 공통적으로 존재하기도 함
- 제한을 넘어서는 요청에 대해서는 AWS 측에 제한 상향 요청을 해야 한다.

※ Amazon EC2 스토리지 (EBS 볼륨 / 스토어 볼륨)

• Amazon EBS (Elastic Block Store) 타입

타입	이름	용량	사용용도
프로비전 IOPS SSD	IO2	4~16TB	수준높은 I/O 처리가 필요한 경우
범용 SSD	GP3	1~16TB	일반 범용
처리량 최적화 HDD	ST1	500GB~16TB	처리량이 중요한 워크로드에 대응할 수 있는 하둡 / OLAP DB 등
콜드 HDD	SC1	500GB~16TB	파일 저장소
마그네틱	Standard	1GB~1TB	백업 / 비주기적인 데이터 액세스

• 인스턴스 스토어 볼륨

- 비지속형 (ephemeral) 스토리지며 인스턴스 종료 시 데이터 소실
- 인스턴스 스토어 볼륨은 인스턴스 서버 호스팅 시 물리적으로 부착되는 SSD 저장 장치 이며, NVMe 인터페이스로 연결
- 인스턴스를 생성하면 자동으로 생성되며 별도의 비용 부담이 없다.

- 단기적 목적의 인스턴스 모델에 적합

※ EC2 접속 및 보안

• EC2 인스턴스 접속

- EC2 인스턴스도 유일한 IP 주소로 네트워크 상의 위치를 표시
- 프라이빗 네트워크로 사용되는 세개의 IP 주소 범위
 - 10.0.0.0 ~ 10.255.255.255
 - 172.16.0.0.0 ~ 172.31.255.255
 - 192.168.0.0 ~ 192.168.255.255
- 인스턴스에 퍼블릭 IP를 할당해서 사용 가능 (Elastic IP)

• EC2 인스턴스 보안 유지

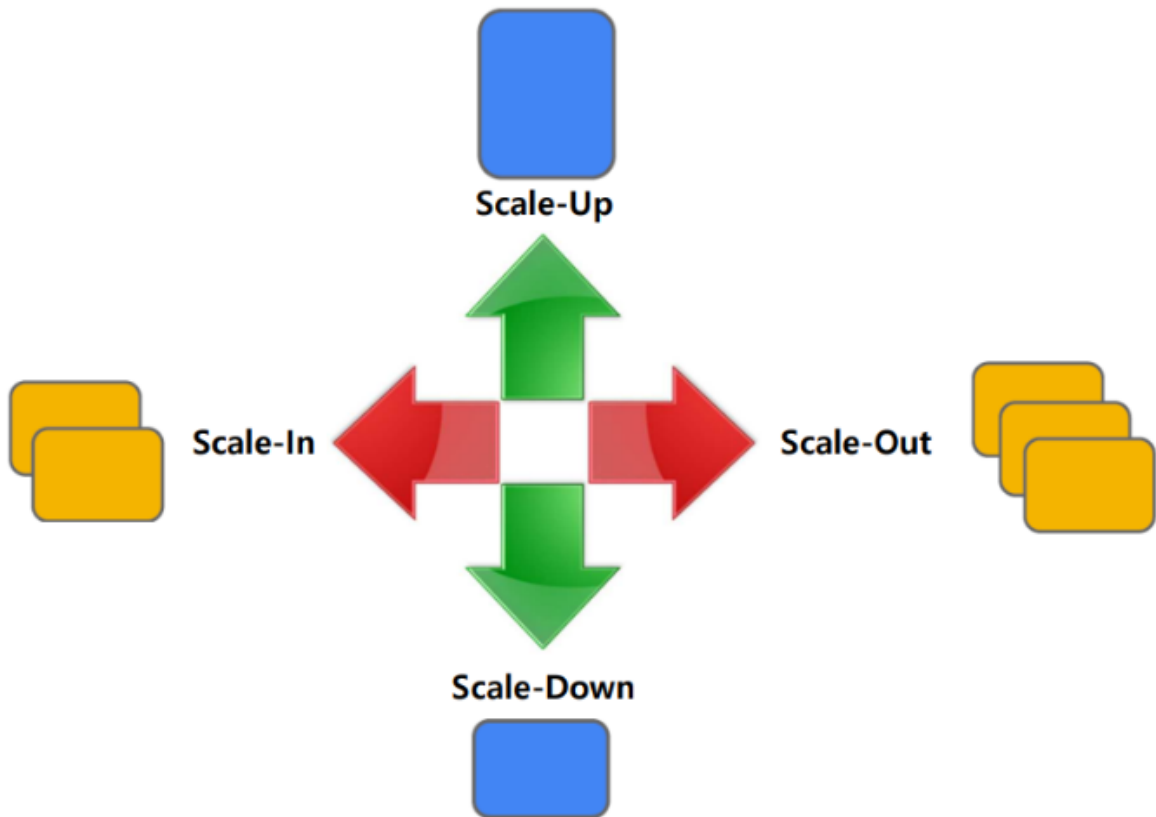
시큐리티 그룹	방화벽과 같은 역할, 정책 규칙으로 정의하여 유입 유출 트래픽 관리
IAM 롤	IAM 롤을 이용하여 EC2 인스턴스와 다른 AWS 리소스에 대한 접속 제어 가능, 특정 롤을 유저 또는 리소스에 할당하여 접근권한을 관리한다.
NAT 인스턴스, NAT 게이트웨이	NAT 디바이스를 사용하여 인터넷 연결 허용 없이 프라이빗 IP 주소를 통해 인터넷에 접속 가능
키 페어	EC2 원격 로그인 관련 보안 세션 실행 방법, EC2 인스턴스 생성 시 키페어를 생성하며, 퍼블릭 키는 EC2 서버에, 프라이빗 키는 로컬 머신에 저장하여 사용

※ EC2 Auto Scaling

• EC2 Auto Scaling 개요

- 애플리케이션 실패 및 복구 상황을 방지하기 위한 서비스
- 필요에 따라 서버사이즈를 자동으로 조절하는 서비스

- 런치 환경설정 또는 런치 템플릿을 이용하여 인스턴스의 환경을 자동으로 설정



- **Launch 환경설정**

- 인스턴스를 직접 프로비저닝 할때 지정하는 것과 동일한 정보를 담은 문서
- AWS Auto Scaling 에서만 사용 가능하며 런치 환경설정을 가지고 직접 인스턴스 생성은 불가능하다.
- 수정이 필요한 경우 새 런치환경 생성 필요

- **Launch 템플릿**

- AWS Auto Scaling, EC2 사본 생성, 스팟 플릿 생성 목적으로 사용
- 버전 기능을 제공하여 생성 후에도 수정 및 이력 관리 가능

• Auto Scaling 그룹

- Auto Scaling 이 관리하는 EC2 인스턴스 그룹
- 그룹 생성에 앞서 런치 환경설정 또는 템플릿 생성해야 한다.
- 다음 몇개의 인스턴스를 프로비전 할 것인지 지정 하고, 그룹의 최소 최대 용량 지정, 그룹 생성시 희망 인스턴스 수를 지정하는 것도 가능하다.

최소 용량 Minimum	그룹 내 최소 유지 인스턴스 수 0 으로 설정 시 새 인스턴스를 추가하지 않고 그룹 내 모든 인스턴스를 종료 시킨다.
최대 용량 Maximum	그룹 내 최대 유지 인스턴스 수 예산 제한선을 고려해 예기치 못한 수요에 의해 지나치게 많은 인스턴스가 추가되는 것을 방지한다.
희망 용량 Desired Capacity	<u>그룹 사이즈</u> 라고 한다, 그룹 내 목표 인스턴스 수, 평상시 유지 하고 있을 인스턴스 수 사용자 필요에 따라 선택 가능하며, 최소 최대 크기 범위 내 있어야 함.

• Application Load Balancer (ALB)

- Auto Scaling 그룹에서 인스턴스에 유입되는 트래픽 분산을 위해 사용
- Auto Scaling 그룹 생성 시 ALB 타겟 그룹에 연결하면 새 인스턴스 생성 시 자동으로 ALB 타겟 그룹을 추가

• 인스턴스에 대한 헬스체크

- Auto Scaling 의 인스턴스 헬스에 대한 판단 기준은 EC2 헬스 체크를 따르며 AWS 모니터링 서비스를 통해 체크

• Auto Scaling 옵션

수동 스케일링 (Manual Scaling)	Auto Scaling 그룹 생성 후 최소, 희망, 최대 용량값을 변경하면 해당 내용이 즉시 반영
동적 스케일링 (Dynamic Scaling)	CloudWatch의 경고 상황을 모니터링 한 결과에 따라 <u>희망용량을 증가시키는 방식</u> 으로 작동하며, 단순 정책, 단계별 정책 타겟 추적 정책 등 세가지가 있다. (→ 희망 용량 증가에 관한 설정)
1. 단순 스케일링 (Simple Scaling)	지표가 한계치에 도달하면 희망 용량대로 증가 타입에 따라 증가 수준 또는 속도를 조절 한다. - Change In Capacity : 지정 된 숫자 만큼 희망 용량 증가 - Exact Capacity : 현재 값에 상관 없이 용량을 지정 숫자 만큼 증가 - Percent Change In Capacity : 현재 용량의 비율을 기준으로 증가

2. 단계별 스케일링 (Step Scaling)	요구수준이 급속히 증가할 경우 리소스 누적 지표에 따른 인스턴스 추가를 위한 정책
3. 목표 추적 정책 (Target Tracking)	특정 지표와 특정 타겟을 선택하여 정책 설정 (CloudWatch Alarm 생성, 인스턴스 갯수조정을 위한 스케일링 정책 생성 등의 업무) , Scale Out 뿐만 아닌 Scale In 정책도 설정이 가능하다.
예약 된 작업 (Scheduled Actions)	워크로드의 패턴이 예측 가능한 경우 용량 변화에 선제적으로 대응하여 수요 증가 이전에 충분한 인스턴스를 확보하고자 할때 사용

• AWS System Manager

- AWS 리소스 및 온프레미스 서버의 자동 및 수동 작업 관리
- 주요 기능은 Actions, Insights

액션 (Actions)	수동 또는 자동, 개별적 또는 일괄적으로 AWS 리소스에 대한 작업을 수행 - 자동화 액션 (Automation) : AWS 리소스에 대한 작업 수행 - 명령 액션 (Command) : Linux , Window 인스턴스에 대한 작업 수행 - 정책 액션 (Policy) : 인스턴스로부터 목록 데이터 수집하는 과정 정의
자동화 액션	AWS 리소스에 대해 일괄적 작업을 수행할 수 있다. 개별 작업을 세분화 하여 처리 가능하며, 일괄적으로 전체 자동화 업무를 처리하거나 시점에 맞춰 단계별로 처리하도록 설정이 가능하다.
Run 명령	관리 대상 인스턴스에 대한 작업수행을 도우며, 로그인 없이 접속, 커스텀 스크립트 실행을 위해 서드파티 도구를 실행한다.
세션 매니저	시큐리티 그룹, NACL 에서 인바운드 포트 개방 없이 혹은 퍼블릭 서브넷에 인스턴스를 두지 않고도 Linux 와 Window 인스턴스에 대한 Bash, PowerShell 접속을 지원한다, Session Manager 플러그인 설치 필요
패치 매니저	인스턴스 패치 업무의 자동화 도구 (Window, Ubuntu, RHEL, SUSE, CentOS, Amazon Linux, Amazon Linux2 지원), Ubuntu 를 제외한 모든 OS 에서 7일후 자동 승인 설치(자동 승인 지연, Auto-approval delay), 인스턴스에 대한 동일한 패치 수준을 유지하도록 돕는 도구
스테이트 매니저	사용자가 정의한 방식대로 소프트웨어를 가져오고 환경을 설정하는 환경설정도구
인사이트 (Insights)	AWS 리소스에 대한 헬스, 컴플라이언스, 운영 세부 사항 정보를 AWS System Manager 라는 단일영역에 집약
빌트인 인사이트	기본적으로 제공하는 모니터링 내역을 담고 있다. - AWS Config Compliance AWS Config - CloudTrail Events - Personal Health Dashboard - Trusted Advisor Recommendations

인사이트 (Insights)	AWS 리소스에 대한 헬스, 컴플라이언스, 운영 세부 사항 정보를 AWS System Manager 라는 단일영역에 집약
인벤토리 매니저	- OS 이름 및 버전 - 애플리케이션 및 파일네임, 버전, 사이즈 - IP 및 MAC 주소 등 네트워크 환경설정 - Windows 업데이트, 룰, 서비스, 레지스트리 밸류 - CPU 모델, 코어, 스피드
컴플라이언스	환경 설정 규칙이 인스턴스의 패치 및 상태 관리에 어떻게 적용되고 있는지 보여 준다. - 패치 컴플라이언스 : 패치 베이스라인이 적용된 인스턴스의 수 및 설치된 패치 세부 정보를 보여준다. - 어소시에이션 컴플라이언스 : 패치작업이 성공적으로 실행된 인스턴스 수를 보여준다.