CDS-Azure

[KICE 2025년 Pilot]

문항1) A사는 Azure에 시스템을 구성하여 사용 중이다. 카카오사태로 인하여 DR시스템을 구축할 것을 권고 받아 DR을 구성하려고 한다. 현재 Korea Central Region을 사용 중에 있으며 DR의 경우 Korea South Region에 구성하려고 한다. 보기 중 적절하지 않은 것을 고르시오. [4점]

① Korea South Region에 VNET를 생성한다.
② Korea South Region에 현 Korea Central에 사용중인 모든 VM SKU가 DR에 사용가능한지 확인한다.
③ Korea South Region에 구성된 Azure DNS Private Resolver에 장애 상황을 대비하여 Korea Central Region에서 사용하는 도메인 정보를 추가한다.
④ Korea South Region에 On-Premise 데이터센터와 ExpressRoute를 구성한다.
⑤ Korea South Region에 사용하는 outbound용 public IP를 한정하기 위하여 Hub VNET에 NAT Gateway를 구성한다.

(정답) 3

(해설) Azure DNS Private Resolver 는 Korea Central Region 에서 제공하는 서비스로 Region 장애를 대비하여 Korea South Region 에는 VM 기반의 DNS 를 구성해야 한다.

(배점) 4

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Cloud Service Architecture > 시스템 비기능요건(성능, 가용성, 확장성, 비용최적화)을 반영한 구축 및 운영
- 문제제목 : Region간 가용성을 구성할 경우 유의점
- 출제의도 : Azure Region 내 가용 리소스 확인의 필요성 이해

문항2) A사는 Azure로 인프라를 마이그레이션하려고 하며 그 중 Database는 대부분 MSSQL을 사용 중에 있다. Database 마이그레이션 관련되어 아래 고객의 요구사항이 있어 부합되는 Azure의 Database서비스 및 기능을 선정하려고 한다. 보기의 내용 중 적절한 것을 선택하여 보기 번호를 답안에 작성하시오. [4점]

[요구사항]

- Region은 Korea Central을 사용해야 한다. - 주 Region인 Korea Central과 Pair Region인 Korea South에 Read Replica가 필요하다. - DR 상황 시 Application들의 Endpoint 변경이 없는 단일 Endpoint가 가능해야 한다. - Timezone 설정을 할 수 있어야 한다. - DBLink를 사용할 수 있어야 한다.

[보기]

[SQL서버 종류 및 Tier]	[고가용성 옵션]
가. Azure SQL DataBase General Purpose	**가.** Active Geo-Replication
나. Azure SQL DataBase Business Critical	**나.** Auto Failover Group
다. Azure SQL Managed Instance General Purpose	
라. Azure SQL Managed Instance Business Critical	

[답안]

(1) SQL서버 종류 및 Tier 보기선택 : _____

(2) 고가용성 옵션 보기 선택 : _____

(정답) 라, 나

(해설) Azure SQL Managed Instance 는 Active Geo-Replication 기능이 없음. Primary Region 에 Read Replica 는 기본 제공 HA 를 구성하여 사용하고, Pair Region 인 KoreaSouth 에 Read Replica 가 필요 하므로 Auto Failover Group 으로 구성함. Azure SQL DataBase 는 DBLink 를 사용할 수 없으며 Azure SQL Managed Instance 는 가능하나 MSSQL 만 가능, Timezone 은 Azure SQL Managed Instance 에서만 설정 가능하다.

(배점) 4

(난이도) 중

- 문제유형 : 단답형
- 출제영역 : Cloud Service Architecture > 요구사항기반 서비스구성요소 선정, 기반인프라 구축 및 운영
- 문제제목 : MSSQL PaaS 서비스의 제약사항 이해
- 출제의도 : MSSQL PaaS 서비스의 제약사항 이해 확인

문항3) 김선임은 C고객사의 시스템을 운영 중 Private 네트워크에서만 접근해야 하는 중요 파일 저장용 Storage Account에 퍼블릭 접근 권한을 실수로 부여하였다. 일주일 후 해당 조치가 문제가 있다는 것을 확인하여 퍼블릭 접근 권한을 회수 조치하였다. 추후 동일 이슈가 발생하지 않도록 변경사항에 대해 사전에 자동으로 모니터링 될 수 있도록 방안을 수립하기로 하였다. 다음 중 적절하지 못한 것을 고르시오. [4점]

① Azure Policy를 적용하여 퍼블릭 접근이 허용된 Storage Account에 대해 Audit Log 를 남기고 알람을 발생시키도록 한다.

② Azure Automation을 활용하여 주기적으로 퍼블릭 접근이 허용된 Storage Account을 확인하고 조치할 수 있도록 한다.

③ Azure CLI를 활용하여 Resource Graph에 질의하여 private endpoint가 구성되지 않은 Storage Account을 확인하고 수정할 수 있도록 한다.

④ Azure 활동 로그 이벤트를 수신할 수 있는 Event Grid와 Logic Apps를 활용하여 퍼블릭 접근 권한 부여되는 Storage Account을 확인하고 수정할 수 있도록 한다.

⑤ Storage Account에 진단 설정을 활성화하여 익명 요청이 성공한 Storage Account을 확인하고 수정할 수 있도록 한다.

(정답) 3

(해설)

Storage Account 에서 private endpoint 와 퍼블릭 접근 차단 설정은 별개의 설정이며, 각각 독립적으로 설정할 수 있으므로, private endpoint 구성여부로 퍼블릭 접근 가능여부를 판별 할수 없다.

(배점) 4

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Cloud Service Architecture > 요구사항기반 서비스구성요소 선정, 기반인프라 구축 및 운영
- 문제제목 : Storage Account 에 대한 리소스 구성 감사
- 출제의도 : 리소스의 변경관리를 할 수 있는 서비스 및 감사 설정에 대한 이해도 확인

문항4) A사는 차세대 프로젝트를 위해 Azure Public Cloud를 선정하였으며 금융권 Cloud 보안 요건 중 데이터센터 가용성 항목에 대응하기 위해서 Azure의 Availability Zone 기능 검토를 확인 중에 있다. 다음 내용 중 올바른 것을 고르시오. [4점]

① VM의 경우 Availability Zone내 Availability Set을 함께 구성하여 VM가용성을 극대화할 수 있다.
② Standard Load Balancer는 Frontend-ip를 Availability Zone 분산, Availability Zone지정을 할 수 있으며 Zone지정을 할 경우 Back-End VM들의 Zone과 동일하지 않아도 LB를 통한 통신을 할 수 있다.
③ Multi Subscription을 사용할 경우 각 Subscription의 Availability Zone Number는 동일한 데이터센터를 의미한다.
④ Azure Virtual Network은 Availability Zone을 사용하기 위하여 Zone별로 Subnet을 생성해야만 한다.
⑤ Azure VPN Gateway는 Availability Zone 분산(Zone Redundant)를 제공하지 않으므로 2개의 Zone을 사용하도록 각각의 VPN Gateway를 구성한다.

(정답) 2

(해설)

1) VM 의 경우 AZ 을 지정하면 AS 을 사용자가 지정할 수 없다.

2) 정답

3) Subscription 내의 Zone1, 2, 3 이 물리적 Datacenter 를 의미하는 것이 아니고 논리 적인 것이므로 Subscription 당 물리적 Datacenter 와 Zone 1, 2, 3 이 서로 다를 수 있다.

4) VNET 은 Zone Redundant 서비스 이므로 Zone 사용을 위해 별도로 존을 정의할 수 없고 자동으로 Zone 으로 확장된다.

5) Azure VPN Gateway 는 Zone-redundant 를 지원하는 SKU 가 있으므로 해당 SKU 를 사용하게 되면 2 개의 Zone 에 자동으로 2 대의 Instance 가 배포된다.

(배점) 4

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Cloud Service Architecture > 시스템 비기능요건(성능, 가용성, 확장성, 비용최적화)을 반영한 구축 및 운영
- 문제제목 : Azure 가용성에 대한 이해
- 출제의도 : Azure 리소스 가용성에 대한 이해

문항5) B사는 VM 기반 WEB / WAS 서버를 이중화 구성하였고, 대용량 파일(동영상 파일 또는 데이터 분석을 위한 로우 파일)의 저장을 위해 Azure Files를 공유 볼륨으로 구성하여 VM에 Mount하였다. 처리하는 파일 개수가 증가함에 따라 응답시간에 대한 지연이 발생하였고, 원인 분석 결과는 많은 대용량 파일의 업로드 / 다운로드로 인한 WAS 서버의 리소스 사용량이 증가였다. Azure Files의 성능 지표에서는 요청에 대한 응답 병목은 발생하지 않았다. WAS 서버의 리소스 사용량 감소를 위한 방안으로 보안을 최대한 준수하면서도 비용 효율적인 방법을 고르시오. [4점]

① WAS에 클라이언트 인증 서비스를 구성하여 인증된 클라이언트에게 Azure Files의 Access Key를 제공하여 직접 접근하여 사용하도록 한다.

② WAS에 클라이언트 인증 서비스를 구성하여 인증된 클라이언트에게 Azure Files의 SAS (Shared access signature)를 제공하여 클라이언트에서 직접 접근하여 사용하도록 한다.

③ Azure Shard Disk를 생성하여 VM에 할당하여 사용한다.

④ WAS에 클라이언트 인증 서비스를 구성하여 인증된 클라이언트에게 Azure Blob Storage의 SAS (Shared access signature)를 제공하여 클라이언트에서 직접 접근하여 사용하도록 한다.

⑤ 대용량 파일 업로드/다운로드용 Azure Function을 추가로 생성하여 사용한다.

(정답) 4

(해설) 한번만 기록하고 시퀀스 액세스로 파일을 사용하는 워크로드의 경우 Azure Files 보다 Azure Blob Storage 가 더 최적화되어 있다. 또한, 인증된 클라이언트에 SAS 를 제공하여 필요한 최소한의 권한 및 유효 기간 부여가 가능하다.

1) Access Key 는 구성과 데이터에 대한 권한을 부여하는데 사용 가능하기 때문에 보안상 문제가 발생할 수 있다.
2) Azure Files 는 랜덤 액세스 파일에 더 적합하며 동영상 파일 혹은 데이터 분석을 위한 로우 파일 저장 및 읽기에는 Blob Storage 가 더 적합하며 비용 효율적이다.
3) Azure Shard Disk 를 공유 볼륨으로 사용하려는 경우 별도의 구성이 필요하며 Azure Blob Storage 대비 비용이 비싸다.
5) Azure Function 을 사용하여 대용량 파일을 처리하는 경우 처리시간이 기본 15분, 최대 60분으로 (Azure Function 의 호스팅 옵션에 따라 다르나 추가비용 발생) 제약을 받을 수 있으며 처리할 수 있는 요청도 기본 100MB(처리량 증가 시 호스팅 옵션 설정 필요하나 비용 증가 및 비용효율성이 낮음)로 설정되어 있어 적합하지 않다.

(배점) 3

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Cloud Service Architecture> 시스템 비기능요건(성능, 가용성, 확장성, 비용최적화)을 반영한 구축 및 운영
- 문제제목 : SAS 를 사용한 Azure Blob Storage 구성

- 출제의도 : 비용과 성능 효율적인 스토리지 아키텍처 설계

문항6) VM 기반으로 구축된 웹 서비스를 운영하고 있다. 해당 서비스는 Azure Load Balancer 로 이중화 구성이 되어 있다. 서비스에 장애가 발생하여 VM 서버 확인 결과 모든 서버에서 서비스 Port 를 정상적으로 Listen 하고 있었다. 하지만 한 대의 서버에서 WAS 가 Hang 이 걸려 요청을 처리하지 못하는 상태임에도 불구하고 Azure Load Balancer 는 요청을 장애가 발생한 서버로 전달하고 있다. 다음 제시된 보기 중 장애가 발생한 VM 으로 트래픽 전달을 방지하기 위한 Azure Load Balancer 설정 중 변경해야 하는 항목과 내용이 올바른 것을 고르시오. [4점]

① Health probe 설정에서 프로토콜 항목이 TCP인 경우 HTTP나 HTTPS로 변경 후 웹 서비스의 동작확인이 가능 경로를 추가로 설정한다.

② Load balancing rule설정에서 Session persistence설정이 되어 있는 경우 None으로 변경한다.

③ Health probe 설정에서 서비스의 비정상적인 상태를 빠르게 인지하기 위하여 확인 주기를 최소 주기로 설정한다.

④ Health probe 설정에서 프로토콜 항목이 HTTP나 HTTPS인 경우 정상 응답 HTTP 상태 코드 범위를 변경한다.

⑤ Load balancing rule설정에서 Idle timeout 값을 10이하로 변경한다.

(정답) 1

(해설) TCP 로 상태를 모니터링 하는 경우 웹 서비스의 비정상적인 동작 감지가 되지 않는다. TCP 의 경우 단순 TCP 핸드셰이크 여부만을 체크한다.

1) Azure Load Balancer 로 웹 서비스의 상태를 모니터링 하기 위하여 프로토콜을 HTTP 또는 HTTPS 로 설정하는 경우 상태 체크를 위한 요청에 대한 HTTP 응답 코드가 200 (OK)으로 고정되어 있어 다른 HTTP 응답 코드 403 (Forbidden), 500 (Internal Server Error) 등이 반환되는 경우 오류 상태로 인지한다.

2) Session persistence 설정은 동일한 클라이언트에서 발생한 요청을 동일한 VM 에서 처리하도록 지정하는 옵션이며 해당 설정을 변경한다고 하여도 일부 요청은 기존과 동일하게 장애가 발생한 서버로 전달된다.

3) 상태 체크 확인 주기를 변경한다고 하여도 VM 서버가 서비스 Port 를 정상적으로 Listen 하고 있기 때문에 기존과 동일하게 장애가 발생 서버로 요청이 전달된다.

4) Azure Load Balance 의 경우 정상 응답 HTTP 상태 코드의 범위를 지정하는 옵션이 존재 하지 않는다. 해당 옵션은 Application Gateway 에서 제공한다.

5) Idle timeout 값은 Azure Load Balance 에 연결된 클라이언트가 요청없이 일정 시간이 경과하는 경우 자동으로 연결을 종료하는 기능이다.

(배점) 4

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Cloud Service Architecture> 시스템 비기능요건(성능, 가용성, 확장성, 비용최적화)을 반영한 구축 및 운영

[2025년 Pilot]

- 문제 제목: Load balancer 구성 항목 중 Health probe 의 이해
- 출제 의도: Load balancer 구성 항목 중 Health probe 의 이해 여부 확인

문항7) K 책임은 G 고객사의 클라우드 MSP 를 수행하는 담당자이다. 디스크 변경 작업을 검토한 내용 중 잘못 설명된 보기를 고르시오. [3점]

① VM에 데이터 디스크를 추가로 attach 하기 위해서는 VM을 중지시키지 않고 구성이 가능하기 때문에 별도의 서비스 중단 시간을 고려하지 않고 작업을 진행할 수 있다.

② 데이터 디스크를 동일한 유형의 더 큰 사이즈로 resize 하는 경우 VM을 중지시키지 않고 작업이 가능하여 별도의 서비스 중단 시간을 고려하지 않고 작업을 진행할 수 있다.

③ 데이터 디스크가 공유 디스크로 다수의 VM에 할당된 경우 사이즈 조정을 위해서는 모든 VM에서 detach 이후 진행을 해야 하기 때문에 서비스 중단 시간을 확보한 이후 작업을 진행할 수 있다.

④ VM에 attach되었지만 볼륨을 구성하지 않았던 데이터 디스크에 대한 삭제 요청 시에는 VM을 중지시키지 않고 detach가 가능하기 때문에 별도의 서비스 중단 시간을 고려하지 않고 작업을 진행할 수 있다.

⑤ 할당된 데이터 디스크의 사이즈의 축소를 요청하는 경우 용량 문제가 없다면 해당 데이터 디스크에서 직접 용량을 줄일 수 있으므로 서비스 중단 시간을 고려하지 않고 작업을 진행할 수 있다.

(정답) 5
(해설) 데이터 디스크의 사이즈를 직접 줄일 수 없다. 데이터 디스크의 사이즈를 축소하고자 하는 경우 신규 디스크를 추가한 후 기존 데이터를 신규 디스크에 복제 후 기존 데이터 디스크를 삭제하는 방식(마이그레이션)을 통해서 진행을 해야 한다.
(배점) 3
(난이도) 하

- 문제유형 : 선다형
- 출제영역 : Cloud Service Architecture > 시스템 비기능요건(성능, 가용성, 확장성, 비용최적화)을 반영한 구축 및 운영
- 문제제목 : Azure Managed Disks 의 디스크 분리, 확장의 이해
- 출제의도 : Azure Managed Disks 의 디스크 분리, 확장의 이해 여부 확인

문항8) Azure Public 클라우드와 On-premise간 전용선 연결 구성을 하려고 한다. 보기의 전용선 구축 전 고려해야 할 내용중 적절하지 않은 것을 고르시오. [4점]

① Korea Central Region의 Azure ExpressRoute Circuit(Premium SKU)을 Japan EAST Region에 있는 구축된 Express Route Gateway와 연결 후 On-Premise와 Japan EAST Region의 VNET간의 통신이 가능하다.

② Korea Central Region의 Azure ExpressRoute Circuit(Standard SKU)을 Korea South Region에 있는 Express Route Gateway와 연결 후 On-Premise와 South Region의 VNET간의 통신이 가능하다.

③ Korea Central Region의 Azure ExpressRoute Circuit과 연결된 On-Premise와 Korea South Region의 Azure ExpressRoute Circuit과 연결된 On-Premise는 서로 통신이 가능하므로 On-Premise간 통신을 위해 별도의 전용회선 연결이 불필요 하다.

④ Azure Express Route Circuit Private Peering과 Express Route Gateway간에는 QoS 설정 기능이 없기 때문에 ExpressRoute Gateway에 여러 개의 VNET이 Peering되어 연결된 경우 하나의 VNET에서 전용선 대역폭을 모두 사용하여 다른 VNET에 영향을 끼치지 않도록 설계 시 고려가 필요하다.

⑤ Azure Express Route Circuit과 Azure Express Route Gateway를 통해 두 개의 VNET이 연결되어 있는 경우 Express Route Circuit자체의 라우팅 기능을 통해 VNET간 직접 통신이 가능하다.

(정답)3

(해설) Circuit 만으로는 불가능 하며 Global Reach 를 추가 구성하여 사용해야 가능하다.

(배점)4

(난이도)중

- 문제유형 : 선다형
- 출제영역 : Cloud Service Architecture > Hybrid Cloud 설계 및 구축
- 문제제목 : On-premise 연동시 필요한 ExpressRoute 에 대한 이해
- 출제의도 : On-premise 연동시 필요한 ExpressRoute 에 대한 이해 확인

문항 9) B 사의 김선임은 Kubernetes 기반으로 구축된 홈쇼핑 서비스를 운영하고 있다. 조회용 API 서비스 로그를 확인해보니 간헐적으로 에러가 발생하였으며 원인을 추적한 결과 서비스의 기능 개선 및 오류 수정을 위한 배포 시 POD 시작/종료 시점에 에러가 발생하고 있었다. 조치사항으로 잘못된 것을 고르시오. [4 점]

① POD 종료 시 에러는 PreStop Hook를 설정하여 Graceful ShutDown을 통해 해결한다.

② ReadinessProbe의 설정을 조정하여 서비스가 정상 기동 후에 K8S Service에 등록되도록 한다.

③ StartUpProbe를 활용하여 LivenessProbe와 ReadinessProbe가 서비스가 정상 기동 후에 동작하도록 한다.

④ Ingress 컨트롤러에서 Internal Error(500) 오류 발생시 Retry 를 적용하여 End-User 에러 발생 빈도를 현저히 감소시킬 수 있다.

⑤ Service Mesh를 사용하고 에러가 발생하는 서버에서 다른 Micro Service Pod의 조회 API를 호출하는 경우 Circuit Breaker의 Retry 설정을 확인하여 다른 Micro Service 배포 시 발생할 수 있는 에러를 줄일 수 있다.

(정답)4

(해설) (4) Internal Error 의 경우 Application 자체에 문제가 있는 경우이며, Retry 로 해결되지 않는다. Bad Gateway 의 경우에는 Retry 로 개선이 가능할 수 있다.

(배점)4

(난이도)중

- 문제유형 : 선다형
- 출제영역 : Cloud Native Architecture > K8S 기반 MSA Outer 구축 및 운영
- 문제제목: K8S MSA Outer 영역에서 무중단 서비스 구축 방안
- 출제의도 : 무중단 서비스 구축을 위한 Outer 영역별 점검 및 설계 포인트의 이해도 측정

문항 10) 다음 제시된 보기 중 Azure Cache for Redis 를 활용하는 예시로 잘못 설명된 보기를 고르시오. [3 점]

① DB에서 데이터를 빈번하게 조회하는 경우 DB에 부하를 주어 성능이 저하될 수 있으므로 해당 서비스를 데이터 캐시로 사용하여 애플리케이션 응답성을 높일 수 있다.

② 해당 서비스를 세션저장소로 사용하여 WAS 간 세션 클러스터링을 구성할 수 있다.

③ 애플리케이션이 비동기 처리를 해야 하나 별도의 Queue 가 존재하지 않는 경우 해당 서비스를 활용하여 Queue 서비스를 대체할 수 있다.

④ 해당 서비스는 데이터를 메모리에만 저장하며, Ehcache 와 같은 로컬 Cache 보다 속도가 빠르므로 어플리케이션에서 데이터 캐시 사용 필요시 성능 측면에서 해당 서비스를 우선적으로 사용하여야 한다.

⑤ 해당 서비스는 Premium Tier 사용시 Scale Up/Down 뿐 아니라 Scale In/Out도 적용할 수 있어 부하증가에 따라 유연하게 대응이 가능하다.

(정답)4

(해설) (4) 로컬 Cache 는 네트워크 구간을 거치지 않으므로 일반적으로 더 성능이 우수하다. 다만 서버의 메모리 자원등을 공유하고, 여러 개의 서버가 있을 경우 캐시 데이터를 공유하기 위한 별도의 구성이 필요하다. 따라서 캐시 데이터의 동기화가 중요한 경우에는 외부 캐시 사용을 고려하여야 한다. Redis 의 경우 데이터 안정성을 위해 데이터를 주기적으로 디스크에 저장하는 기능도 지원한다.

(배점)3

(난이도)하

- 문제유형 : 선다형
- 출제영역 : Cloud Native Architecture > K8S 기반 MSA Outer 구축 및 운영
- 출제구분: 신규
- 문제제목 : Azure Cache for Redis 활용 방안의 이해
- 출제의도 : Azure Cache for Redis 활용 방안 이해도 측정

[2025년 Pilot]

문항 11) A 선임은 Kubernetes 환경의 SpringBoot 2.7.18 (JDK 8u441)로 구성된 Pod 에 장애가 자주 발생하는 것을 조치하기 위해 투입되었다. Deployment.yaml 파일에서 수정되어야 할 부분을 찾아 Line Number 를 작성하시오. [4 점]

[추가 확인 사안 및 제한]

장애가 발생 중인 Pod 의 SpringBoot 가 사용하는 Max Heap Memory size 는 1GB 이다. 원인 파악 진행 중 POD 장애 시 Out Of Memory 관련 로그를 확인하였다. configmap 과 service.yaml 을 수정하지 않는 선에서 조치를 수행해야 한다.

[Pod Describe]

```
State: Waiting
Reason: CrashLoopBackOff
Last State: Terminated
Reason: OOMKilled
        Exit Code: 137
```

```
# configmap.yaml
apiVersion: v1
data:
  _JAVA_OPTIONS: -Xmx1g
metadata:
  name: cm-backend
  namespace: default

# service.yaml
apiVersion: v1
metadata:
  name: svc-backend
  namespace: default
spec:
  ports:
  - name: http
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: backend
```

Line	[deployment.yaml]
1	apiVersion: apps/v1
2	kind: Deployment
3	metadata:
4	name: backend
5	spec:
6	replicas: 2
6	selector:
8	matchLabels: backend
9	template:
10	metadata:
11	labels:
12	app: backend
13	spec:
14	containers:
15	- name: backend
16	image: backend:1.14.2
17	imagePullPolicy: Always
18	envFrom:
19	- configMapRef:
20	name: cm-backend
21	resources:
22	requests:
23	cpu: 500m
24	memory: 500Mi
25	limits:
26	cpu: 500m
27	memory: 500Mi

답 Line : __

Secret

(정답)27
(해설) Limits.memory 사양을 지정한 힙사이즈보다 크게 설정해야 한다
(배점)4
(난이도)중

- 문제유형 : 단답형
- 출제영역 : Cloud Native Architecture > K8S 기반 MSA Outer 구축 및 운영
- 문제제목 : K8S 환경 운영시 발생할 수 있는 장애 조치
- 출제의도: Application 메모리 증가를 위한 Heap Memory 조정시 Pod 의 자원도 함께 변경이 필요하며, 그렇지 않으면 장애를 유발할 수 있음.

문항 12) 아래 제시된 AzureRM Resource Provider 를 사용하여 구성한 AKS Terraform 코드에 대해서 설명한 내용 중 잘못 설명한 것을 고르시오. [4 점]

[Terraform tfvars 파일]

```
AKSCluster = {
        ... 중략 ...
        default_node_pool = {
            name = "np-default"
            vm_size = "Standard_D2_v2"
            zones = [1]
            enable_auto_scaling = true
            max_count = 5
            min_count = 2
            node_count = 2
            kubelet_disk_type = "OS"
            orchestrator_version = "1.31.7"
            os_sku = "Ubuntu"
            node_subnet_name = "sbn-aks"
            type = "VirtualMachineScaleSets"
        }
        ... 중략 ...
        kubernetes_version = "1.31.7"
        network_profile = {
            network_plugin = "azure"
            network_mode = "transparent"
            network_policy = "calico"
            service_cidrs = ["10.1.0.0/24"]
            dns_service_ip = "10.1.0.20"
        }
        ... 중략 ...
}
```

① default_node_pool 은 추가적인 Pod Scheduling 요청이 발생하더라도, 최대 5 개의 Node 까지만 Scale-out 이 가능하다.

② 해당 AKS Cluster 의 kubernetes version 은 이미 수명 종료가 되어 상위 버전으로 업데이트가 필요하다.

③ 해당 default_node_pool 은 단일 Zone 으로 구성되어 있어 해당 Zone 장애발생 시 해당 Cluster 상에서 구동되는 Application 은 서비스 불가 상태에 빠질 수 있다.

④ 해당 AKS Cluster 에는 OS 가 Ubuntu 인 Container 이미지만 배포가 가능하다.

⑤ AKS Cluster 는 Pod 간 네트워크 통신을 제어할 수 있는 Network Policy 로 calico 를 사용한다.

(정답)4

(해설)

(4) os_sku 에 설정될 수 있는 값은 AzureLinux, Ubuntu, Windows2019 and Windows2022 이며, 해당 설정은 Node Pool 에 공급되는 VM 의 기본 OS 에 관련된 것이며, 컨테이너의 OS 와는 관계가 없다.

(배점)4

(난이도)중

- 문제유형 : 선다형
- 출제영역 : Cloud Native Architecture > Container Management
- 문제제목 : IaC 기반 AKS 구현 및 설계
- 출제의도 : IaC 기반 AKS 구현 및 설계 역량 측정

[2025년 Pilot]

문항13) 아래와 같이 한개의 Node Pool로 구성된 AKS클러스터를 업그레이드하려고 한다. 업그레이드를 위해 제시된 작업 목록을 확인하여 작업해야 하는 순서를 답안에 맞게 순서대로 기재하시오. [4점]

Node pool	Provisioning state ⓘ	Power state ⓘ	Node count	Mode	Kubernetes version	Node size
agentpool	Succeeded	Running	3/3 ready	System	1.25.5	Standard_D2as_v4

[제약 조건]

- Node Pool 업그레이드시 서비스 영향도는 최소화되어야 한다. 무중단 또는 중단시간이 0 에 가까워야 한다.
- 해당 클러스터는 Public 이 아닌 Private 환경으로 구성되어 있다.
- 포탈에 접속하는 단말과 AKS 를 제어하는 단말은 망분리에 따라 분리되어 있다.
- 개발, 사용자테스트, 통합테스트, 운영 환경으로 각각 동일한 사이즈로 분리되어 구성되어 있다.
- 반복하는 작업을 위해서 매뉴얼 작업이 필요하여 스크립트 작성이 필요하다.
- 기존 NodePool 기준으로 모니터링이 구성되어 있어, NodePool 이름은 agentpool 로 유지하여야 한다.

[작업 순서]

1. 컨트롤 플레인을 업그레이드한다.
2. 임시 NodePool(Name: newagentpool)을 클러스터에 신규로 추가한다.
3. _____
4. _____
5. _____
6. 기존 NodePool(Name: agentpool)을 업그레이드한다.
7. _____
8. _____
9. _____
10. 기존 NodePool(Name: agentpool)로 모든 Pod 가 이동되었고, 서비스가 정상적인지 확인한다.
11. 임시 NodePool(Name: newagentpool)을 삭제한다.

가. 기존 NodePool(Name: agentpool)의 Node AutoScaling 을 활성화한다.
나. 기존 NodePool(Name: agentpool)의 Node AutoScaling 을 비활성화 한다.
다. 기존 NodePool(Name: agentpool)에 Pod 스케쥴링을 활성화한다.
라. 기존 NodePool(Name: agentpool)에 Pod 스케쥴링을 비활성화 하고 Drain 작업을 수행하여 Pod 를 임시 NodePool(Name: newagentpool)로 스케쥴링 되도록 한다.
마. 임시 NodePool(Name: newagentpool)에 Pod 스케쥴링을 비활성화 하고 Drain 작업을 수행하여 Pod 를 기존 NodePool(Name: agentpool)로 스케쥴링 되도록 한다.

Secret

바. 임시 NodePool(Name: newagentpool)로 모든 Pod 가 이동되었고, 서비스가 정상적인지 확인한다.

답안 : 기호없이 6 글자를 이어서 작성(예: 가나다라마바)

1 – 2 - ( ) – ( ) – ( ) – 6 – ( ) – ( ) – ( ) – 10 – 11

정답

1 – 2 - (나) – (라) – (바) – 6 – (가) – (다) – (마) – 10 – 11

(정답) 나라바가다마

(해설) AKS 를 안정적으로 업그레이드 하기 위해서는 컨트롤 플레인에 대해서 사전 업데이트를 진행한 이후에 버전 업그레이드가 진행되는 경우 롤백이 불가능한 상황을 고려하여 과거 버전의 Node Pool 을 유지한 상태로 신규 Node Pool 을 추가하여 서비스가 정상적으로 동작하는 것을 확인 한 이후 과거 버전의 Node Pool 의 버전 업그레이드를 진행함

작업순서는 아래와 같다.

1. 컨트롤 플레인을 업그레이드한다.
2. 임시 NodePool(Name: newagentpool)을 클러스터에 신규로 추가한다.
3. 기존 NodePool(Name: agentpool)의 Node AutoScaling 을 비활성화 한다.
4. 기존 NodePool(Name: agentpool)에 Pod 스케쥴링을 비활성화 하고 Drain 작업을 수행하여 Pod 를 임시 NodePool(Name: newagentpool)로 스케쥴링 되도록 한다.
5. 임시 NodePool(Name: newagentpool)로 모든 Pod 가 이동되었고, 서비스가 정상적인지 확인한다.
6. 기존 NodePool(Name: agentpool)을 업그레이드한다.
7. 기존 NodePool(Name: agentpool)의 Node AutoScaling 을 활성화한다.
8. 기존 NodePool(Name: agentpool)에 Pod 스케쥴링을 활성화한다.
9. 임시 NodePool(Name: newagentpool)에 Pod 스케쥴링을 비활성화 하고 Drain 작업을 수행하여 Pod 를 기존 NodePool(Name: agentpool)로 스케쥴링 되도록 한다.
10. 기존 NodePool(Name: agentpool)로 모든 Pod 가 이동되었고, 서비스가 정상적인지 확인한다.
11. 임시 NodePool(Name: newagentpool)을 삭제한다.

(배점)4

(난이도)중

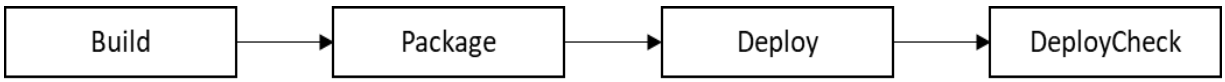
- 문제유형 : 단답형
- 출제영역 : Cloud Native Architecture > Container Management
- 문제제목 : K8S 환경 운영시 NodePool 업그레이드 절차
- 출제의도 : K8S 환경 운영시 NodePool 업그레이드 절차에 대한 이해도 측정

문항 14) Github Action 을 이용하여 다음과 같은 Pipeline 을 구성하고자 하였다. 아래에 제시된 Pipeline 단계 및 설명과 코드를 보고 빈칸에 들어갈 내용을 작성하여 파이프라인 코드를 완성하시오. [4 점]

[답안]

답안 : _____

[Pipeline 단계 및 설명]



- Build : Gradle 빌드 결과물로 jar 파일 생성
- Package : Build 단계에서 생성된 jar 파일을 사용하여 Docker Image 생성 후 ACR 에 Push
- Deploy : Helm Chart 를 통해 AKS 에 Deploy
- DeployCheck : Helm Chart Deploy 가 정상적으로 수행되었는지 확인

[Dockerfile]

```
FROM openjdk:8-jdk

COPY artifact/app.jar /sorc001/app.jar
RUN chmod +x /sorc001/app.jar
EXPOSE 8080

CMD ["./docker-entrypoint.sh"]
```

[Pipeline 코드]

```
... 생략 ...
env:
  BASE_URL: tct.azurecr.io
  CLUSTER_NAME: tct-cluster

jobs:
  Build:
    runs-on: ubuntu-latest
    container:
    steps:
      - uses: actions/checkout@v3
```

```
        - run: chmod +x gradlew
        - run: ./gradlew build
        - uses: actions/upload-artifact@v3
            with:
              name: build-artifact
              path: |
                build/libs
              retention-days: 1
  Package:
    if: ${{ github.ref == 'refs/heads/main' }}
    needs: [ build ]
    runs-on: ubuntu-latest
    env:
      IMAGE_NAME: tct/app
      DOCKER_FILE_NAME: ./docker/Dockerfile
    steps:
    - uses: actions/checkout@v3
    - uses: (답안)_____
          with:
            name: build-artifact
            path: artifact
    - name: Build Container
      run: docker build . -t ${{ env.BASE_URL }}/${{ env.IMAGE_NAME }}:${GITHUB_SHA} -f
${{ env.DOCKER_FILE_NAME }}
    - name: Tag Container
      run: docker tag ${{ env.BASE_URL }}/${{ env.IMAGE_NAME }}:${GITHUB_SHA}
    - name: Push Container Image to ACR
      run: |
        docker push ${{ env.BASE_URL }}/${{ env.IMAGE_NAME }}:${GITHUB_SHA}

  Deploy:
    ... 생략 ...

  DeployCheck:
    ... 생략 ...
```

(정답) actions/download-artifact@v3

[2025년 Pilot]

(해설) Job 간에 생성된 파일은 공유가 되지 않으므로, Github Actions 의 Artifact-Upload/Artifact-Download Action 을 통해 Artifact 공유가 필요함

(배점)4

(난이도)중

- 문제유형 : 단답형
- 출제영역 : Cloud Native Architecture > DevOps(CI/CD, 테라폼 IaC) Pipeline
- 문제제목 : Github Action 에서 Job, Step 간 데이터 전달방법
- 출제의도 : Devops 파이프라인 구성시 중요개념에 대한 구현 및 이슈해결 역량 측정

문항 15) 다음과 같은 상황에서 발생할 수 있는 보안 이슈를 방지할 수 있는 방안을 설명한 보기 중 적절하지 않는 것을 고르시오. [4 점]

<상황>

A 프로젝트는 Git 기반으로 소스 형상 관리를 하고 있으며, 소스 변경 시 파이프라인을 통해 Azure VM 에 어플리케이션이 배포된다. 개발자가 StorageAccount 에 데이터 업로드시 Access 권한을 획득하기 위한 방법을 TA 에게 문의하였다. TA 는 Azure 경험이 부족하여 Service Principal 을 생성하고 현재 사용하고 있는 Subscription 에 Owner RBAC 권한을 부여한 후 개발자에게 전달하였다. 개발자는 전달받은 Service Principal Object ID 및 Secret 을 소스코드에 포함하여 업무 로직을 작성하였다. 이후 해당 Service Principal 이 탈취되어 해킹사고가 발생하였다.

① 프로젝트 소스코드가 저장된 Repository 에서 주기적으로 소스 정적 분석을 수행하여, Password, Token, Secret AccessKey 등의 패턴으로 저장되어 있는 값이 있는지 확인하여 사전 조치할 수 있도록 한다.

② StorageAccount 에 대한 접근은 StorageAccount 전용 AccessKey 를 발급하여 사용하도록 가이드 하면 키가 탈취되더라도 해킹범위를 해당 StorageAccount 로 제한할 수 있다.

③ 어플리케이션이 배포될 Azure VM 에 Managed Identity 를 부여하여 StorageAccount 에 접근할 수 있도록 가이드 했다면 Service Principal 정보를 제공하지 않아도 된다.

④ 이미 commit 된 적이 있는 소스에서 Service Principal Secret 를 삭제한 후 source 를 commit 하더라도 Service Principal 정보 탈취를 방지할 수 없어, 추가적인 조치가 필요하다.

⑤ 생성된 Service Principal 에 Owner RBAC 권한 부여시 Subscription 전체에 권한을 할당한 것이 문제이며, Resource Group 에 Owner RBAC 를 할당했다면 문제가 되지 않았을 것이다.

(정답)5

(해설) (5) Resource Group 에 한정한다고 하더라도 소스에 비밀정보가 저장되어 있어, 여전히 해킹의 위험이 있고, Storage Account 외 다른 리소스에 대한 권한도 허용되므로 위험하다.

(배점)4

(난이도)중

- 문제유형 : 선다형
- 출제영역 : Cloud Native Architecture > DevOps(CI/CD, 테라폼 IaC) Pipeline
- 문제제목 : Devops 소스코드 보안 적용 방안
- 출제의도 : Devops 환경에서 소스코드 내 비밀정보 보관 방지를 위한 방안

문항 16) A 고객사는 Azure에 시스템을 구성하고자 한다. 고객의 보안 요구 사항이 아래와 같을 때 Azure Native로 해결할 수 있는 사항으로 적절하지 않은 것을 고르시오. [4점]

[요구사항]

1. RDP(3389), SSH(22) 등 주요 포트들은 Inbound 접근 통제가 이루어 져야 하며 접속 시도들은 로깅을 통해 모니터링하고자 한다.
2. 유지관리 작업 시 관리자들이 RDP, SSH 포트를 통해 접속할 수 있도록 일시적인 접근이 필요하다.
3. 인터넷으로 나가는 통신은 Azure방화벽을 통하여야 한다.
4. Azure 시스템은 A 고객사의 On-Premise와 안정적인 연결을 위한 전용선이 필요하고 네트워크 트래픽
   도청이나 데이터 유출 방지를 위해 L3이상의 통신 암호화를 적용하여야 한다.
5. Azure Open AI등 PaaS 서비스는 On-Premise와 Private한 통신이 가능하여야 한다.

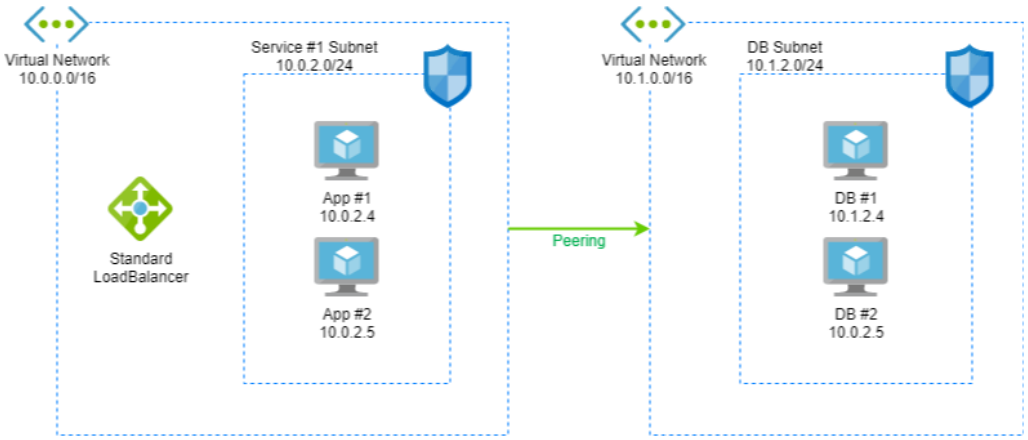
① Network Watcher의 NSG(네트워크 보안 그룹) 흐름 로그를 구성하여 주요 포트들에 대한 로그를 확인한다.
② Public Endpoint로 구성 후 PaaS서비스의 Firewall 설정을 On-Premise Private CIDR만를 연결하도록 구성한다.
③ Azure에서 외부 인터넷으로 나가는 트래픽은 Azure Firewall을 경유하도록 User Defined Routes를 설정한다.
④ Microsoft Defender의 JIT(Just-In-Time) 액세스를 통해, 특정 사용자에게 지정된 시간 동안 선택한 포트에 대한 액세스를 허용한다.
⑤ On-Premise와 연결 시 ExpressRoute Gateway와 VPNGateway를 추가하여 VPN을 함께 구성한다.

(정답)2
(해설) Public Endpoint 도 Azure Backborn 을 이용하지만 Public IP 를 사용하기 때문에 인터넷에 노출이 되며 PaaS 의 Firewall 구성에는 PrivateIP 가 구성되지 않는다.
(배점)4
(난이도)중

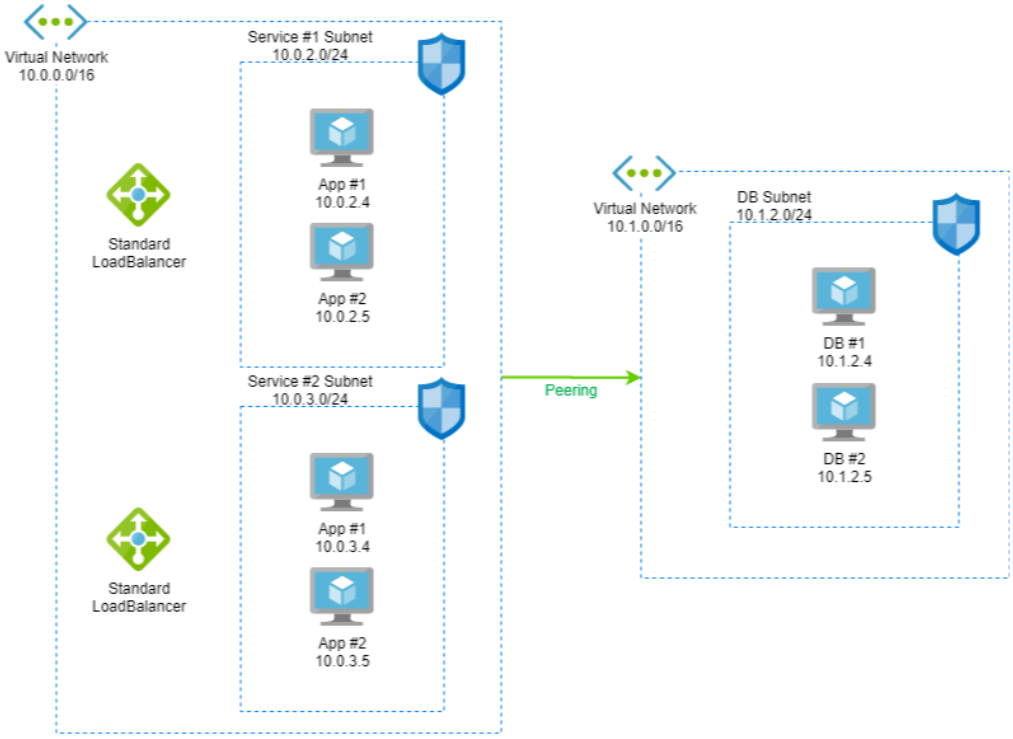
- 문제유형 : 선다형
- 출제영역 : Cloud Security Architecture > 서비스 인프라 보안(서비스구간, 서버, 스토리지) 구축 및 운영
- 문제제목 : 클라우드 보안요건 구현 방안
- 출제의도 : 클라우드 보안요건 구현 방안

문항 17) A사는 Azure를 사용하고 있으며 아래와 같이 Application과 Database를 별도의 Virtual Network로 Peering을 통해 운영하고 있다. 같은 Database를 사용하는 신규 서비스 추가가 필요하여 아래와 같이 Standard Load Balancer와 Subnet을 생성했다. Database에 Application VM만 접근 가능하도록 Database Network Security Group의 Inbound Rule을 조정해야 한다. Database는 서비스 포트로 3306을 사용하고 있다.

[As-Is]



[To-Be]



Service1, Service2, Database의 각 VM들은 ASG-Service1, ASG-Service2, ASG-Database 라는 이름의 Application Security Group으로 구성되어 있다. 다음 중 Service1, Service2의 VM들이 Database에 접근하기 위한 Rule로 최소한의 권한 법칙에 가장 충족한 것을 고르시오. [4점]

①

Port	Protocol	Source	Destination	Action
3306	TCP	10.0.2.0/24 10.0.3.0/24	10.1.0.0/16	Allow

②

Port	Protocol	Source	Destination	Action
3306	TCP	ASG-Service1 ASG-Service2	10.1.2.0/24	Allow

③

Port	Protocol	Source	Destination	Action
3306	TCP	10.0.2.0/24 10.0.3.0/24	ASG-Database	Allow

④

Port	Protocol	Source	Destination	Action
3306	TCP	ASG-Service1 ASG-Service2	ASG-Database	Allow

⑤

Port	Protocol	Source	Destination	Action
3306	TCP	10.0.0.0/16	10.1.2.0/24	Allow

(정답)3

(해설) Application Security Group 은 Associated VM 이 속한 Virtual Network 내에서만 유효하다.

(배점)4

(난이도)중

- 문제유형 : 선다형
- 출제영역 : Cloud Security Architecture > 서비스 인프라 보안(서비스구간, 서버, 스토리지) 구축 및 운영
- 문제제목 : NSG, ASG 설정
- 출제의도 : NSG, ASG 를 적절히 사용할 수 있는지 여부 확인

문항18) A책임은 프로젝트에서 AKS 기반환경에서 MSA 프로젝트를 진행중이다. 구축되는 시스템의 보안요건을 만족시키기 위해서 데이터 전송 및 저장 시 암호화를 적용하여야 한다. 이를 위해서 다음과 같이 아키텍처 설계서를 작성하였다. 이를 구현하기 위한 방안 중 잘못된 것을 고르시오. [4점]

구분	적용대상	암호화 방안
전송시 암호화	외부 인터넷 -> WAF 구간	mTLS 및 SSL/TLS 1.2 버전 이상 통신 암호화 적용
	WAF -> F/W 구간	SSL/TLS 1.2 버전 이상 통신 암호화 적용
	MSA Service <-> 타 시스템 호출 구간	SSL/TLS 1.2 버전 이상 통신 암호화 적용
저장시 암호화	응용 어플리케이션	Always Encrypted 및 Dynamic data masking 기능 사용
	DBMS – SQL Managed Instance	TDE (Transparent data encryption)을 이용한 스토리지 암호화
	Azure Files	SSE에 CMK를 사용하여 암호화
	Azure Blob Storage	Azure Key Vault에 저장된 CMK를 사용하여 암호화

① WAF_v2 SKU에서 TLS 프로토콜 수신기를 REST API, PowerShell 및 포털에서 생성하여 상호 인증 구성이 가능하다.

② Azure Firewall을 Premium SKU로 생성하여 구성이 가능하다.

③ 응용 어플리케이션은 Always Encrypted를 지원하는 드라이버로 변경하여 Always Encrypted와 Dynamic data masking을 동시에 사용할 수 있다.

④ Azure Files는 Azure Key Vault에 키를 저장하고 스토리지 계정에 부여된 ID에 wrapkey, unwrapkey, get 권한을 부여 하여 구성이 가능하다.

⑤ Azure Blob Storage에 파일을 업로드 할 때는 클라이언트 어플리케이션의 보안 취약성을 완화하기 위하여 SSE 기능을 사용하는 것으로 구성한다.

(정답) 3

(해설) Dynamic data masking 은 서버에 설정을 통하여 구현되며 Always Encrypted 를 사용하기 위해서는 드라이버 변경 이외에도 데이터 베이스 연결 문자열 수정이 필요하다.

(배점) 4

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Cloud Security Architecture > 어플리케이션 기반 보안 구축 및 운영
- 문제제목 : Application 암호화 요건
- 출제의도 : 프로젝트의 보안 요건에 맞도록 Application 보안 적용방안에 대한 이해도를 측정 하기위한 문항

문항19) B 책임은 AKS를 이용하여 시스템 구축을 계획하고 있다. AKS 보안 설계를 위해서 검토 중인 사항 중 잘못된 내용을 고르시오. [4점]

① PSA(Pod Security Admission)를 이용해서 보안정책에 위반되는 POD는 생성을 차단하도록 한다.

② PSA(Pod Security Admission)는 단일 클러스터 구현을 위한 기본 제공 정책 솔루션이기 때문에 가급적 Azure Policy를 적용하도록 한다.

③ Secrets Store를 사용하여 Pod에서 안전하게 비밀, 키 및 인증서를 사용하도록 구성한다.

④ POD내의 프로세스가 Root로 실행되는 것을 방지하기 위서서 "Security Context"에 "runasuser"를 0이 아닌 값으로 설정한다.

⑤ AKS 네트워크 정책은 POD간에는 서로 제약없이 통신이 가능하다. POD간 통신 제어를 위해서는 Azure Network Policy Manager를 사용한다.

(정답) 3

(해설) Kubernetes Secret 오브젝트는 비밀을 Base64 인코딩하여 etcd 에 저장하여 기본적인 보안을 제공하지만 etcd 에 접근할 수 있는 권한을 가진 사용자는 모든 Secret 을 디코딩하여 볼 수 있어 안전하지 않다. 또한, 감사 기능을 제공하지 않아 직접 구현하여야 한다.

(배점) 4

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Cloud Security Architecture > 어플리케이션 기반 보안 구축 및 운영
- 문제제목 : AKS 보안강화
- 출제의도 : AKS 보안 적용을 위해 AKS 특성과 보안에 대한 이해도 측정

문항 20) A 사는 AWS 에 시스템을 구성하여 서비스 중이다. 해당 AWS 환경은 A 사가 보유한 데이터센터와 전용선(DirectConnect)을 통해 연결되어 있으며, 레거시 시스템과 주기적으로 데이터를 주고받고 있다. 또한 사용자 접근도 전용선을 통해 하고 있다. 최근 A 사의 전략 방향에 따라 신규로 구성되는 시스템은 Azure 에 올리기로 결정하였고, 기존 AWS 에 구성되어 있는 시스템도 Azure 로 이관해야 한다고 전달받았다. 이에 따라 시스템 담당자는 현재 구성된 AWS 시스템을 Azure 로 이관하는 작업을 준비 중이다. 시스템 담당자가 고려해야 할 사항으로 올바르지 않은 것을 고르시오. [4 점]

① AWS에서는 RDS(MariaDB)를 사용하고 있었지만, Azure의 PaaS DB인 Azure Database for MariaDB는 앞으로 제공되지 않을 예정이므로 Azure Database for MySQL로 DB를 생성하고 데이터를 이관하여 구성할 예정이다.
② VM의 경우 현재 Amazon Linux를 사용하고 있어 Azure에서 사용이 불가능 하므로 Azure에서 공식으로 제공하는 Linux OS로 변경 구성하고 소스 및 데이터만 이관하여 테스트하려고 한다.
③ 이미 오픈된 시스템으로 레거시 시스템과 연계 구성 때문에 내부 IP 변경이 어려운 상황으로 Azure에 동일 내부 IP를 부여하였다. Azure에서 시스템을 오픈하기 전까지는 레거시 시스템과 통신이 되지 않도록 On-Premise에서 ExpressRoute에 해당 레거시 IP 대역에 대해 BGP routing 전파를 하지 않고 ExpressRoute에서 전파되는 BGP Routing은 On-Premise에서 차단하고 있다가 오픈 시점에 추가할 예정이다.
④ Public DNS 마이그레이션의 경우 DNS 전파 지연으로 인한 영향을 최소화하기 위해 미리 기 레코드의 TTL값을 줄이도록 한다.
⑤ 외부 웹서버용 SSL인증서들은 MS가 CA(Certificate Authority)공급자 이므로 Azure KeyVault에서 신규 SSL인증서를 생성하여 적용 및 관리하도록 한다.

(정답)5
(해설) Azure 는 CA 공급자가 아니며 따라서 Azure Key Vault 는 인증된 CA SSL 인증서를 생성할 수 없다
(배점)4
(난이도)중

- 문제유형 : 선다형
- 출제영역 : Cloud Migration> 요건기반 시스템 Cloud 전환 구축
- 문제 제목: CSP 간 마이그레이션시 유의사항
- 출제 의도: CSP 간 마이그레이션시 유의사항 체크 여부 확인

[2025년 Pilot]

문항21) B사에 운영중인 시스템에 고객사의 요청에 의해 설정 추가 및 변경작업을 진행하려 한다. 아래 표에서 각 요청에 따른 예상되는 이슈에 대해서 정리한 내용 중 기술적으로 적절하지 않은 것을 고르시오. [4점]

<table>
<tr><th>번호</th><th>구분</th><th>내용</th></tr>
<tr><td>①</td><td>요청</td><td>아래와 같이 서브넷에 할당되어 있는 기본 인바운드 NSG Rule에 Deny All 정책을 우선순위가 64000으로 Rule 추가
<table>
<tr><th>Priority</th><th>Name</th><th>Port</th><th>Protocol</th><th>Source</th><th>Destination</th><th>Action</th></tr>
<tr><td>65000</td><td>AllowVnetInBound</td><td>Any</td><td>Any</td><td>VirtualNetwork</td><td>VirtualNetwork</td><td>Allow</td></tr>
<tr><td>65001</td><td>AllowAzureLoadBalancerInBound</td><td>Any</td><td>Any</td><td>AzureLoadBalancer</td><td>Any</td><td>Allow</td></tr>
<tr><td>65500</td><td>DenyAllInBound</td><td>Any</td><td>Any</td><td>Any</td><td>Any</td><td>Deny</td></tr>
</table></td></tr>
<tr><td></td><td>이슈</td><td>VM이 Loadbalancer의 Backend Pool로 지정되어 있는 경우 상태 프로브가 비정상적으로 표기되어 부하 분산 이슈가 발생함</td></tr>
<tr><td>②</td><td>요청</td><td>비 중요 시스템의 백업 비용을 절감하기 위하여 백업 데이터에 대한 복제 유형을 Geo-redundant에서 Locally-redundant로 변경 적용</td></tr>
<tr><td></td><td>이슈</td><td>데이터 복제 유형은 백업 정책을 생성시에 지정하며 이후 수정이 불가능 하여 복제 유형을 변경하려는 경우 새로운 백업 정책을 적용해야 하기 때문에 기존 백업 데이터를 삭제해야 함</td></tr>
<tr><td>③</td><td>요청</td><td>특정 VM의 데이터 디스크의 사용률이 높아 데이터 디스크의 추가 생성 및 할당</td></tr>
<tr><td></td><td>이슈</td><td>디스크 증설시에는 OS 디스크와 동일한 유형과 동일한 스토리지 유형의 디스크만 생성이 가능하고 VM에 할당할 수 있음</td></tr>
<tr><td>④</td><td>요청</td><td>보안 규정 준수를 하여 모든 스토리지 계정에 공용 네트워크 접근 제한</td></tr>
<tr><td></td><td>이슈</td><td>공용 네트워크 접근 제한시에는 VM 부팅 실패를 진단하는 디버깅에 제약이 발생할 수 있음</td></tr>
<tr><td>⑤</td><td>요청</td><td>프라이빗으로 구성한 DEV 및 TEST AKS 클러스터를 비용 절감 차원에서 업무 시간에만 사용하고 이외의 시간에는 중지</td></tr>
<tr><td></td><td>이슈</td><td>프라이빗 클러스터가 중지되고 다시 시작되는 경우 기존 프라이빗 링크 서비스가 제거되고 다시 생성되어 프라이빗 엔드포인트와 클러스터 간의 연결이 끊어져 프라이빗 엔포인트를 다시 생성해야 함</td></tr>
</table>

(정답) 3

(해설) VM 에 디스크를 추가하는 경우 VM 이 지원해주는 스토리지 유형의 디스크를 추가 할 수 있음

예) Standard F2s v2 의 경우 OS 디스크가 Premium SSD LRS 인 경우 데이터 디스크는 Premium SSD 이외 Standard SSD 와 Standard HDD 를 사용 할 수 있음

(배점) 4

(난이도) 중

- 문제유형 : 선다형
- 출제영역 : Troble Shooting & New Technology > (시스템 전환 및 구축 운영 시 포함) 아키텍처 이슈/문제해결
- 문제 제목: Cloud 운영 시 문제 해결
- 출제 의도: 운영중인 환경의 리소스 변경 요청에 따른 이슈를 사전에 파악하여 이슈 발생에 따른 서비스 장애 상황을 회피 할 수 있는지 확인

문항22) Azure 전용선 서비스인 ExpressRoute는 2회선의 물리 전용선을 사용하여 하나의 ExpressRoute Location내 이중화를 제공하였으나 이 경우 ExpressRoute Location의 이슈가 생겼을 경우 ExpressRoute서비스를 사용할 수 없는 단점이 있었다. 이에 MS는 이 부분을 해결하기위한 신규 서비스를 제공 예정 중에 있다 동일한 2회선의 물리 전용선을 사용하여 ExpressRoute Location의 가용성을 제공할 수 있는 서비스명을 작성하시오. [3점]

정답) _____

(정답) ExpressRoute Metro | Metro
(해설) ExpressRoute Metro 는 동일 Azure 리전 내 Multi ExpressRoute Location 을 제공하여 각 ER Location 에 1 회선씩 물리 회선을 연결하여 Availability Zone 과 유사한 기능을 제공 하여 ER Location 에 대한 가용성을 확보할 수 있다
(배점) 3
(난이도) 하

- 문제유형 : 단답형
- 출제영역 : Troble Shooting & New Technology>CSP New Tech(CSP 신규 서비스, Data Pipeline, AI/Data platform 등)
- 문제 제목: ExpressRoute Metro 서비스의 이해
- 출제 의도: ExpressRoute Metro 서비스의 이해