4/01

비즈니스에서 워크로드를 AWS로 이동하려고 합니다. 최고 정보 보안 책임자(CIO)는 클라우드에 저장된 모든 데이터를 미사용 시 암호화할 것을 요구합니다. 조직은 암호화 키 수명 주기 관리 프로세스를 완전히 제어하기를 원합니다.
조직은 AWS CloudTrail과 별도로 키 자료를 즉시 삭제하고 키 사용을 감사할 수 있어야 합니다. 선택한 서비스는 다른 AWS 스토리지 서비스와 인터페이스해야 합니다.

이러한 보안 표준을 준수하는 서비스는 무엇입니까?

A. CloudHSM 클라이언트가 있는 AWS CloudHSM

B. AWS CloudHSM을 사용한 AWS 키 관리 서비스(AWS KMS)

C. 외부 키 구성 요소 출처가 있는 AWS Key Management Service(AWS KMS)

D. AWS 관리형 고객 마스터 키(CMK)가 있는 AWS Key Management Service(AWS KMS)

주요 키워드 Cloud HSM / KMS

문제 상황 분석

저장된 데이터 암호화, 암호화 키 관리 프로세스 제어권한, 키사용 감사, 다른 AWS 스토리지 서비스와 연계

틀린 이유

처음보는 서비스라서 풀 수 없음. 일단 찍음

풀이 과정

Cloud HSM(Hardware Security Module): 클라우드에 하드웨어 보안 모듈을 제공해 암호화 작업을 처리하고 암호화 키에 보안 스토리지를 제공하는 서비스. 암호화 키를 생성하고 제어하기 위한 관리형 서비스를 원하지만 자체 HSM 은 원하지 않거나 운영할 필요가 없는 경우 AWS Key Management Service 사용을 고려해 보십시오.

https://docs.aws.amazon.com/ko_kr/cloudhsm/latest/userguide/introduction.html

AWS Key Management Service: 데이터를 보호하는 데 사용하는 암호화 키를 쉽게 생성하고 제어할 수 있게 해주는 관리형 서비스. AWS KMS 는 데이터를 암호화하는 대부분의 기타 AWS 서비스와 통합됩니다. AWS KMS 는 또한 감사, 규제 및 규정 준수 요구사항에 따라 KMS 키 사용을 기록하기 위해 AWS CloudTrail 과 통합됩니다.

https://docs.aws.amazon.com/ko_kr/kms/latest/developerguide/overview.html

저장된 데이터 암호화, 암호화 키 관리 프로세스 제어권한, > Cloud HSM

키사용 감사, 다른 AWS 스토리지 서비스와 연계 > AWS KMS. 모두 제공하는 솔루션 조합은 **B**

A. Cloud HSM 단독으로는 데이터 암호화랑 별개로 키 제어가 불가능. 따라서 탈락

C. 외부키 구성요소 출처가 있는 KMS > 이미 기존에 사용하는 키가 있을경우, 그것을 KMS 로 불러오는 방식.

https://docs.aws.amazon.com/ko_kr/kms/latest/developerguide/importing-keys.html

D. *고객 마스터 키(CMK)*라는 용어가 *AWS KMS key*과 *KMS 키*로 바뀌었습니다. > 따흐흑

https://docs.aws.amazon.com/ko_kr/kms/latest/developerguide/dochistory.html

기업은 Amazon Web Services를 활용하여 3계층 애플리케이션의 모든 구성 요소를 호스팅합니다. 조직은 환경 내부의 가능한 보안 취약성을 자동으로 식별하기를 원합니다. [redacted] 관리자에게 경고하기를 원합니다.

어떤 솔루션이 이러한 기준을 충족합니까?

A. 의심스러운 웹 트래픽을 평가하도록 AWS WAF를 설정합니다. AWS Lambda 함수를 생성하여 Amazon CloudWatch의 모든 결과를 기록하고 관리자에게 이메일 알림을 보냅니다.

B. AWS Shield를 설정하여 의심스러운 웹 트래픽을 평가합니다. AWS Lambda 함수를 생성하여 Amazon CloudWatch의 모든 결과를 기록하고 관리자에게 이메일 알림을 보냅니다.

C. Amazon Inspector를 배포하여 환경을 모니터링하고 Amazon CloudWatch에서 결과를 생성합니다. Amazon EventBridge(Amazon CloudWatch Events) 규칙을 구성하여 Amazon Simple Notification Service(Amazon SNS) 주제에 메시지를 게시하여 이메일로 관리자에게 알립니다.

D. Amazon GuardDuty를 배포하여 환경을 모니터링하고 Amazon CloudWatch에서 결과를 생성합니다. Amazon EventBridge(Amazon CloudWatch Events) 규칙을 구성하여 Amazon Simple Notification Service(Amazon SNS) 주제에 메시지를 게시하여 이메일로 관리자에게 알립니다.

주요 키워드 WAF&Shield / Cloudwatch / Event Bridge / Inspector / SNS

문제 상황 분석

환경 내부의 보안 취약성을 자동으로 식별 > 관리자에게 경고 메시지 전달

풀이 과정

내부의 보안 취약성을 자동으로 식별한다길래 조사관(Inspector) 서비스를 골라서 쭉따라감. **C**

Amazon Inspector 는 지속적으로 스캔하는 취약성 관리 서비스입니다. AWS 취약성을 위한 워크로드 Amazon Inspector 는 Amazon ECR (Amazon 엘라스틱 컨테이너 레지스트리)에 있는 Amazon EC2 인스턴스와 컨테이너 이미지를 자동으로 검색하여 소프트웨어 취약성과 의도하지 않은 네트워크 노출이 있는지 검사합니다. https://docs.aws.amazon.com/ko_kr/inspector/latest/user/what-is-inspector.html

A. WAF(Web Application Firewall)은 들어오는 트래픽을 분석함. 내부환경 분석 X

AWS WAF 는 웹 어플리케이션 방화벽으로서 다음 서비스들에 전달되는 HTTP, HTTPS 요청을 모니터링 하고 컨텐츠 접근을 제어합니다. .Amazon CloudFront, Amazon API Gateway REST API, Application Load Balancer 또는 AWS AppSyncGraphQL API https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

B. Shield 는 WAF 에 대한 추가 서비스로, DDOS 방어수단임. 환경 분석 X

https://docs.aws.amazon.com/ko_kr/waf/latest/developerguide/shield-chapter.html

A,B: Lambda 함수로 Cloudwatch 결과 전달 > 외부의 보안 공격에 대한 모니터링 기록을 전달. 환경 분석 X

D. GuardDuty 는 들어오는 데이터 흐름을 분석해 보안 결함을 찾는 서비스. 환경 분석 X

GuardDuty 는 다음 데이터 원본들을 분석하고 처리하는 지속적 보안 모니터링 서비스입니다; VPC 흐름 로그, AWS CloudTrail 관리 이벤트 로그, CloudTrail S3 데이터 이벤트 로그, EKS 감사 로그 및 DNS 로그 악성 IP 주소 및 도메인 목록 https://docs.aws.amazon.com/ko_kr/guardduty/latest/ug/what-is-guardduty.html

기업은 시장 분석 관리를 제3자 파트너에게 아웃소싱합니다. 공급업체는 회사 계정의 리소스에 대한 제한된 프로그래밍 방식 액세스를 요구합니다. 허용 가능한 액세스를 보장하기 위해 필요한 모든 정책이 수립되었습니다.

공급업체에 계정에 대한 가장 안전한 액세스를 제공하는 새로운 구성 요소는 무엇입니까?

A. IAM 사용자를 생성합니다.

B. 서비스 제어 정책(SCP) 구현

C. 외부 ID가 있는 교차 계정 역할을 사용합니다.

D. SSO(Single Sign-On) ID 공급자를 구성합니다.

주요 키워드 IAM 및 하위 서비스들(SCP, 교차 계정 역할, SSO)

문제 상황 분석

외부사용자(제 3 자 파트너) 접근 허가. 제한된 프로그래밍 방식 액세스. 필요한 정책은 모두 준비됨

풀이 과정

A. IAM 사용자 계정은 같은 AWS 계정 내에서의 접근권한 관리. > 제 3 자 접근 X

B. SCP 는 권한에 대한 권한을 설정하는 느낌..

SCP(서비스 제어 정책)는 조직의 권한을 관리하는 데 사용할 수 있는 조직 정책 유형입니다. SCP 는 조직의 모든 계정에 사용 가능한 최대 권한을 중앙에서 제어합니다. SCP 만으로는 조직 내 계정에 권한을 부여하기에 충분하지 않습니다. SCP 는 어떠한 권한도 부여하지 않습니다. SCP 는 계정 관리자가 영향을 받는 계정의 IAM 사용자 및 역할에 위임할 수 있는 작업에 대해 권한 범위를 정의하거나 제한을
설정합니다 https://docs.aws.amazon.com/ko_kr/organizations/latest/userguide/orgs_manage_policies_scps.html

C. 문제상황에 맞음

타사가 조직의 AWS 리소스에 액세스해야 하는 경우 역할을 사용하여 해당 사용자에게 그에 대한 액세스 권한을 위임할 수 있습니다. https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html

D. SSO 는 AWS 내 계정과 어플리케이션에 대한 통합 접속관리 시스템> 제 3 자 접근 X

4/04

기업은 TCP 기반 애플리케이션을 회사의 가상 사설 클라우드(VPC)로 이전하려고 합니다. 이 프로그램은 회사 데이터 센터에 있는 물리적 장치를 통해 지원되지 않는 TCP 포트를 통해 대중에게 제공됩니다. 이 공용 엔드포인트의 지연 시간은 3밀리초 미만이며 초당 최대 3백만 개의 요청을 처리할 수 있습니다. 조직이 동일한 수준의 성능으로 작동하려면 AWS의 새로운 퍼블릭 엔드포인트가 필요합니다.

이 요구 사항을 충족하려면 어떤 솔루션 아키텍처 접근 방식을 권장해야 합니까?

A. NLB(네트워크 로드 밸런서)를 배포합니다. 애플리케이션에 필요한 TCP 포트를 통해 공개적으로 액세스할 수 있도록 NLB를 구성합니다.

B. 애플리케이션 로드 밸런서(ALB)를 배포합니다. 애플리케이션에 필요한 TCP 포트를 통해 공개적으로 액세스할 수 있도록 ALB를 구성하십시오.

C. 애플리케이션에 필요한 TCP 포트에서 수신 대기하는 Amazon CloudFront 배포를 배포합니다. Application Load Balancer를 오리진으로 사용합니다.

D. 애플리케이션에 필요한 TCP 포트로 구성된 Amazon API Gateway API를 배포합니다. 프로비저닝된 동시성을 사용하여 AWS Lambda 함수를 구성하여 요청을 처리합니다.

주요 키워드 ELB(NLB, ALB)

문제 상황 분석

TCP 기반 애플리케이션, 최대 3 백만개의 요청, 퍼블릭 엔드포인트 필요

풀이 과정

TCP/UDP > OSI 7 레이어 중 4 계층 통신 방법, NLB 가 4 계층 로드 밸런서

HTTP/HTTPS > OSI 7 레이어 중 7 계층 통신 방법, ALB 가 7 계층 로드 밸런서

따라서 ALB 들어간건 배제하고 NLB 들어간거 골랐습니다.. **A**

Network Load Balancer 는 오픈 시스템 상호 연결(OSI) 모델의 네 번째 계층에서 작동합니다. 초당 수백만 개의 요청을 처리할 수 있습니다 TCP 연결을 열려고 시도합니다.
https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/network/introduction.html#network-load-balancer-overview

B.

Application Load Balancer 는 개방형 시스템 간 상호 연결(OSI) 모델의 일곱 번째 계층인 애플리케이션 계층에서 작동합니다.
https://docs.aws.amazon.com/ko_kr/elasticloadbalancing/latest/application/introduction.html

C. CDN 을 포함하려면 정적데이터에 관련된 언급이 들어갔어야 했을 듯.

D. API 게이트웨이는 뭔가 프로그램적으로 작동하니까 퍼블릭엔드포인트가 없지않을까요? 아마그래서 X?

Amazon API Gateway 는 규모와 관계없이 REST 및 WebSocket API 를 생성, 게시, 유지, 모니터링 및 보호하기 위한 AWS 서비스입니다. API 개발자는 AWS 또는 다른 웹 서비스를 비롯해 AWS 클라우드에 저장된 데이터에 액세스하는 API 를 생성할 수 있습니다.

동일한 AWS 계정 내에서 회사는 us-west-2 리전에 위치한 두 개의 VPC를 가지고 있습니다. 비즈니스는 이러한 VPC 간의 네트워크 통신을 허용해야 합니다. 매월 약 500GB의 데이터가 VPC 간에 전송됩니다.

이러한 VPC를 연결하는 데 가장 비용 효율적인 접근 방식은 무엇입니까?

A. AWS Transit Gateway를 구현하여 VPC를 연결합니다. VPC 간 통신에 전송 게이트웨이를 사용하도록 각 VPC의 라우팅 테이블을 업데이트합니다.

B. VPC 간에 AWS Site-to-Site VPN 터널을 구현합니다. VPC 간 통신에 VPN 터널을 사용하도록 각 VPC의 라우팅 테이블을 업데이트합니다.

C. VPC 간에 VPC 피어링 연결을 설정합니다. VPC 간 통신에 VPC 피어링 연결을 사용하도록 각 VPC의 라우팅 테이블을 업데이트합니다.

D. VPC 간에 1GB AWS Direct Connect 연결을 설정합니다. VPC 간 통신에 Direct Connect 연결을 사용하도록 각 VPC의 라우팅 테이블을 업데이트합니다.

주요 키워드 VPC 간 데이터 통신서비스들(Transit Gateway, Site-to-Site tunnel, Peering, Direct Connect)

문제 상황 분석

문제 상황에 맞는 적절한 VPC 데이터 통신 서비스 선정.

동일 계정 내에서 동일 리전내 2 개의 VPC. 매월 약 500GB 정도의 데이터가 전송

풀이 과정

A. Transit Gateway 는 온프레미스 VPC 간 상호 연결> VPC 간 연결 X

Transit Gateway 는 가상 사설 클라우드(VPC)와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브. https://docs.aws.amazon.com/ko_kr/vpc/latest/tgw/what-is-transit-gateway.html

B. Site to Site VPN 은 VPC 와 자체 온프레미스 네트워크를 연결하는 서비스, A.는 이의 하위개념> VPC 간 연결 X

https://docs.aws.amazon.com/ko_kr/vpn/latest/s2svpn/VPC_VPN.html

C. VPC peering 이 VPC 간 연결을 위한 서비스

VPC 피어링 연결은 프라이빗 IPv4 주소 또는 IPv6 주소를 사용하여 두 VPC 간에 트래픽을 라우팅할 수 있도록 하기 위한 두 VPC 사이의 네트워킹 연결 https://docs.aws.amazon.com/ko_kr/vpc/latest/peering/what-is-vpc-peering.html

D. Direct Connect 는 온프레미스와 VPC 간의 직접연결을 제공하는 서비스, 1GB 인거도 고려요소일 듯?

https://docs.aws.amazon.com/ko_kr/directconnect/latest/UserGuide/Welcome.html

한 기업이 여러 가용 영역에 분산된 Amazon EC2 인스턴스에서 작동할 웹 기반 애플리케이션을 개발 중입니다. 온라인 애플리케이션을 통해 900TB 이상의 텍스트 콘텐츠 컬렉션에 액세스할 수 있습니다. 회사는 온라인 지원에 대한 수요가 많을 것으로 예상합니다. 솔루션 설계자는 텍스트 문서 스토리지 구성 요소가 항상 애플리케이션의 요구 사항을 충족하도록 확장할 수 있음을 보장해야 합니다. 회사는 솔루션의 총 비용에 대해 우려하고 있습니다.

비용 효율성 측면에서 이러한 기준을 가장 잘 충족하는 스토리지 시스템은 무엇입니까?

A. Amazon Elastic Block Store(Amazon EBS)

B. Amazon Elastic File System(Amazon EFS)

C. Amazon Elasticsearch Service(Amazon ES)

D. 아마존 S3

주요 키워드 스토리지 서비스(EBS, EFS, S3), ES

문제 상황 분석

여러 가용영역 분산, 900TB 이상의 텍스트콘텐츠(정적데이터), 온라인 접속 필요, 확장성

풀이 과정

A. EBS 여러가용영역에서 탈락 (단일가용영역 사용가능)

B. EFS 사용가능성이 없는건 아니지만 비용 효율성에서 탈락 (저렴순 S3<EBS<EFS)

C. ES 일단 Elasticsearch 는 21 년 9 월 Openseach 로 개명당함 https://docs.aws.amazon.com/ko_kr/opensearch-service/latest/developerguide/release-notes.html

OpenSearch 는 로그 분석, 실시간 애플리케이션 모니터링, 클릭 스트림 분석 같은 사용 사례를 위한 완전한 오픈 소스 검색 및 분석 엔진입니다. https://docs.aws.amazon.com/ko_kr/opensearch-service/latest/developerguide/what-is.html

D. S3 정적데이터라는 측면에서도 가산점, 무제한 저장용량도 가산점