



AWS Trusted Advisor

© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

이 강의에서는 AWS Trusted Advisor를 소개합니다.

교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- AWS Trusted Advisor를 설명합니다.
- AWS Trusted Advisor에서 제시한 다섯 가지 범주의 권장 사항을 알아봅니다.
- Trusted Advisor의 기능을 알아봅니다.
- AWS Trusted Advisor 권장 사항을 해석합니다.



이 모듈에서는 AWS Trusted Advisor와 점검 항목을 알아봅니다.

AWS Trusted Advisor 소개

AWS Trusted Advisor는 모범 실무 또는 점검을 다음과 같이 다섯 가지 범주로 제공합니다.



초록색: 탐지된 문제 없음



노란색: 조사가 권장됨



빨간색: 조치가 권장됨



AWS Trusted Advisor는 AWS 환경을 최적화함으로써 비용을 절감하고, 성능과 내결함성을 향상하며, 보안을 강화하는 데 도움이 되는 온라인 리소스입니다. 모범 실무 또는 점검을 다음과 같은 5가지 범주로 제공합니다.

1. **비용 최적화** - 사용되지 않는 유휴 리소스를 제거하거나 예약 용량을 약정하여 AWS에서 비용을 절감하는 방법
2. **성능** - 서비스 한도를 점검하고, 프로비저닝된 처리량을 활용하도록 하며, 초과 사용되는 인스턴스를 모니터링하여 서비스 성능 개선
3. **보안** - 간극을 메우고, 다양한 AWS 보안 기능을 사용하며, 권한을 점검하여 애플리케이션 보안 개선
4. **내결함성** - 오토스케일링, 상태 확인, 여러 가용 영역, 백업 기능을 활용하여 AWS 애플리케이션의 가용성과 중복성 증대
5. **서비스 한도** - 서비스 한도의 80%가 넘는 사용량 검사

점검 상태는 대시보드 페이지에서 서로 다른 색상으로 표시됩니다.

- **빨간색**(빨간색 느낌표) - 조치가 권장됨
- **노란색**(노란색 느낌표) - 조사가 권장됨
- **초록색**(초록색 확인 표시) - 탐지된 문제 없음

AWS Trusted Advisor 사용

모든 고객에게 여섯 가지 핵심 점검이 제공됩니다.

1. 서비스 한도
2. 보안 그룹 - 제한 없는 특정 포트
3. AWS Identity 및 Access Management(IAM) 사용
4. 루트 계정의 다중 인증(MFA)
5. Amazon Elastic Block Store(Amazon EBS) 퍼블릭 스냅샷
6. Amazon Relational Database Service(Amazon RDS) 퍼블릭 스냅샷

AWS Trusted Advisor는 모든 AWS 고객에게 인기 있는 성능 및 보안 권장 사항을 제공합니다. 다음 Trusted Advisor 점검이 모든 고객에게 무료로 제공됩니다.

1. 서비스 한도
2. 보안 그룹 - 제한 없는 특정 포트
3. AWS Identity 및 Access Management(IAM) 사용
4. 루트 계정의 다중 인증(MFA)
5. Amazon Elastic Block Store(Amazon EBS) 퍼블릭 스냅샷
6. Amazon Relational Database Service(Amazon RDS) 퍼블릭 스냅샷

점검 및 지침의 전체 세트는 Business Support 및 Enterprise Support 플랜 고객에게 제공됩니다. AWS Trusted Advisor는 모범 실무에 따라 AWS 리소스를 프로비저닝하도록 지원합니다. 이 기능을 사용하면 시스템 성능과 신뢰성을 높이고, 보안을 강화하며, 비용을 절감할 기회를 모색할 수 있습니다.

Trusted Advisor 모범 실무를 자세히 알아보려면 AWS Support 웹 페이지에서 'AWS Trusted Advisor 모범 사례 체크리스트' (<https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/>)를

참조하십시오.

Trusted Advisor 기능

AWS Trusted Advisor는 여러분이 권장 사항을 사용자 지정하고 AWS 리소스를 사전에 모니터링할 수 있도록 다양한 기능을 제공합니다.



5

aws re/start

AWS Trusted Advisor는 여러분이 권장 사항을 사용자 지정하고 AWS 리소스를 사전에 모니터링할 수 있도록 다양한 기능을 제공합니다.

- **Trusted Advisor 알림** - AWS 리소스 배포를 가장 최신 상태로 유지하는 데 도움이 됩니다. 이 서비스에 옵트인하면 매주 이메일 메시지를 통해 알림이 전달됩니다.
- **AWS Identity 및 Access Management(IAM)** - 특정 점검 또는 점검 범주에 대한 액세스를 제어할 수 있습니다.
- **AWS Support 애플리케이션 프로그래밍 인터페이스(API)** - Trusted Advisor 결과를 프로그래밍 방식으로 검색하고 새로 고칠 수 있습니다.
- **작업 링크** - Trusted Advisor 보고서 내의 항목에 하이퍼링크가 있어 콘솔로 직접 연결됩니다. 콘솔에서 Trusted Advisor 권장 사항을 구현할 수 있습니다.
- **최근 변경 사항** - 콘솔 대시보드에서 점검 상태의 최근 변경 사항을 추적할 수 있습니다. 변경 사항에 주목할 수 있도록 가장 최근에 변경된 사항이 목록 상단에 표시됩니다.
- **항목 제외** - Trusted Advisor 보고서를 사용자 지정할 수 있습니다. 관련이 없는 항목은 점검 결과에서 제외할 수 있습니다.
- **모두 새로 고침** - 점검 사항을 개별적으로 새로 고치거나 요약 대시보드의 우측 상단에 있는 **Refresh All**을 선택하여 모든 점검 사항을 한꺼번에 새로 고칠 수 있습니다. 점검은 마지막으로 새로 고침된 후 **5분 간격으로 새로 고침**되도록 할 수 있습니다.

Trusted Advisor를 자세히 알아보려면 AWS Support 웹 페이지의 [AWS Trusted](#)

[Advisor](#)를 참조하십시오.

Trusted Advisor 사용 방법

Trusted Advisor를 사용하려면 어떻게 해야 하나요?



6

aws re/start

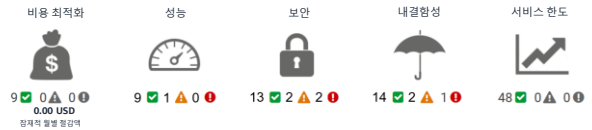
YouTube에서 Trusted Advisor 데모를 시청할 수 있습니다.
<https://www.youtube.com/watch?v=i0lkKN9NoPk>

활동

AWS Trusted Advisor 권장 사항 해석

7

Trusted Advisor 대시보드



aws re/start

여러분의 친구가 AWS Trusted Advisor를 처음으로 사용했습니다. 이 친구는 클라우드 환경을 개선하기 위해 권장 사항을 해석하려고 하는데, 여러분의 도움이 필요합니다.

화면에 보이는 것이 친구의 대시보드입니다. 다 괜찮아 보이지만 **비용 최적화**와 **서비스 한도** 범주에 몇 가지 권장 사항이 표시되어 있습니다. 여러분은 이 권장 사항을 조사하여 친구가 보안을 강화하는 데 도움을 주고자 합니다.

이 친구가 다음 권장 사항을 해석하도록 도와주십시오.

활동: 권장 사항 1

루트 계정의 MFA

설명: 루트 계정을 점검하여 다중 인증(MFA)이 활성화되지 않은 경우 경고합니다. 보안을 강화하려면 MFA를 사용하여 계정을 보호하는 것이 좋습니다. MFA를 사용하면 사용자는 AWS Management Console 및 관련 웹 사이트와 상호 작용할 때 MFA 하드웨어 또는 가상 디바이스에서 받은 고유 인증 코드를 입력해야 합니다.

알림 기준: 루트 계정에서 MFA가 활성화되지 않았습니다.

권장 조치: 루트 계정에 로그인하여 MFA 장치를 활성화하십시오.

이 권장 사항과 관련해 다음 질문에 답하십시오.

- 어떤 상태입니까?
- 무엇이 문제입니까?
- 구체적인 환경 세부 정보는 무엇입니까?
- 모범 실무는 무엇입니까?
- 권장되는 작업은 무엇입니까?

활동: 권장 사항 2

IAM 암호 정책

설명: 계정에 대한 암호 정책을 점검하며 암호 정책이 활성화되지 않았거나 암호 콘텐츠 요구 사항이 활성화되지 않은 경우 경고합니다. 암호 콘텐츠 요구 사항은 강력한 사용자 암호 생성을 적용하여 AWS 환경 전반의 보안을 높입니다. 암호 정책을 생성하거나 변경하면 변경 사항은 새로운 사용자에게 즉시 적용되지만 기존 사용자는 암호를 변경하지 않아도 됩니다.

알림 기준: 암호 정책이 활성화되었지만, 콘텐츠 요구 사항이 1개 이상 활성화되지 않았습니다.

권장 조치: 일부 콘텐츠 요구 사항이 활성화되지 않은 경우 활성화하는 것이 좋습니다. 활성화할 암호 정책이 없다면 정책을 생성하여 구성하십시오. IAM 사용자의 계정 암호 정책 설정을 참조하십시오.

이 권장 사항과 관련해 다음 질문에 답하십시오.

- 어떤 상태입니까?
- 무엇이 문제입니까?
- 구체적인 환경 세부 정보는 무엇입니까?
- 모범 실무는 무엇입니까?
- 권장되는 작업은 무엇입니까?

활동: 권장 사항 3

! 보안 그룹 - 제한 없는 액세스

설명: 리소스에 대한 제한 없는 액세스를 허용하는 규칙의 보안 그룹을 점검합니다. 제한 없는 액세스는 악의적인 활동(해킹, DoS 공격, 데이터 손실) 기회를 증가시킵니다.

알림 기준: 25, 80, 443 이외의 포트에 대한 접미사가 /0인 소스 IP 주소가 보안 그룹 규칙에 있습니다.

권장 조치: 필요한 IP 주소로만 액세스를 한정하십시오. 특정 IP 주소로만 액세스를 한정하려면 접미사를 /32로 설정하십시오(예: 192.0.2.10/32). 액세스가 더욱 제한적인 규칙을 생성한 후에는 액세스를 지나치게 허용하는 규칙을 반드시 삭제해야 합니다.

리전	보안 그룹 이름	보안 그룹 ID	프로토콜	포트	상태	IP 범위
us-east-1	WebServerSG	sg-xxxxxx1 (vpc-xxxxxx1)	TCP	22	빨간색	0.0.0.0/0
us-west-2	DatabaseServerSG	sg-xxxxxx2 (vpc-xxxxxx2)	TCP	8080	빨간색	0.0.0.0/0

이 권장 사항과 관련해 다음 질문에 답하십시오.

- 어떤 상태입니까?
- 무엇이 문제입니까?
- 구체적인 환경 세부 정보는 무엇입니까?
- 모범 실무는 무엇입니까?
- 권장되는 작업은 무엇입니까?

활동: 권장 사항 4

Amazon S3 버킷 로깅

설명: Amazon Simple Storage Service(Amazon S3) 버킷의 로깅 구성을 점검합니다. 서버 액세스 로깅이 활성화된 경우 자세한 액세스 로그가 한 시간마다 선택한 버킷으로 전송됩니다. 액세스 로그 레코드는 요청 유형, 요청에 지정된 리소스, 요청이 처리된 시간 및 날짜와 같은 요청에 대한 세부 정보를 포함합니다. 기본적으로 버킷 로깅은 활성화되지 않습니다. 보안 감사를 수행하거나 사용자 및 사용 패턴에 대해 자세히 알아보려면 로깅을 활성화해야 합니다.

알림 기준:

노란색: 버킷에 서버 액세스 로깅이 활성화되어 있지 않습니다.

노란색: 대상 버킷 권한에 소유자 계정이 포함되어 있지 않습니다. Trusted Advisor가 이를 점검할 수 없습니다.

권장 조치:

대부분의 버킷에 대해 버킷 로깅을 활성화하십시오.

대상 버킷 권한에 소유자 계정이 포함되어 있지 않은 경우 Trusted Advisor가 로깅 상태를 점검할 수 있게 하려면 소유자 계정을 권한 부여 대상으로 추가하십시오.

리전	버킷 이름	대상 이름	대상 존재 여부	동일 소유자 여부	쓰기 활성화 여부	이유
us-east-2	my-hello-world-bucket		아니요	아니요	아니요	로깅이 활성화되지 않음

이 권장 사항과 관련해 다음 질문에 답하십시오.

- 어떤 상태입니까?
- 무엇이 문제입니까?
- 구체적인 환경 세부 정보는 무엇입니까?
- 모범 실무는 무엇입니까?
- 권장되는 작업은 무엇입니까?

핵심 사항



© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

12

- AWS Trusted Advisor는 AWS 모범 실무에 따라 리소스를 **프로비저닝, 최적화, 보호**하는 데 도움이 되도록 실시간 지침을 제공하는 온라인 도구입니다.
- Trusted Advisor **보안 점검 및 조언**의 예는 다음과 같습니다.
 - **보안 그룹**이 무제한 액세스를 포트를 열어두지 않게 함
 - **AWS Identity 및 Access Management(IAM) 권한** 사용을 점검하여 AWS 리소스에 대한 액세스를 제어함
 - 루트 계정을 점검하여 **다중 인증(MFA)**이 활성화되지 않은 경우 경고함
 - Amazon Simple Storage Service(Amazon S3) 버킷에서 **로깅**이 활성화되어 있는지 점검함



이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- AWS Trusted Advisor는 AWS 모범 실무에 따라 리소스를 **프로비저닝, 최적화, 보호**하는 데 도움이 되도록 실시간 지침을 제공하는 온라인 도구입니다.
- Trusted Advisor **보안 점검 및 조언**의 예는 다음과 같습니다.
 - 보안 그룹이 무제한 액세스를 포트를 열어두지 않게 함
 - AWS Identity 및 Access Management(IAM) 권한 사용을 점검하여 AWS 리소스에 대한 액세스를 제어함
 - 루트 계정을 점검하여 **다중 인증(MFA)**이 활성화되지 않은 경우 경고함
 - Amazon Simple Storage Service(Amazon S3) 버킷에서 **로깅**이 활성화되어 있는지 점검함