사용자 가이드

AWS Well-Architected Tool

AWS Well-Architected Tool: 사용자 가이드

Table of Contents

Well-Architected Framework의 새 버전을 출시했습니다. 또한 Lens Catalog에 새 렌즈와 업데이트된 렌즈를 추가했습니다. 변경 사항에 대해 자세히 알아보세요.

AWS Well-Architected Tool란 무엇인가요?

AWS Well-Architected Tool(AWS WA Tool)은 AWS 모범 사례를 사용해 아키텍처를 측정할 수 있도록 일관된 프로세스를 제공하는 클라우드 서비스입니다. AWS WA Tool은 다음과 같이 제품 수명 주기에서 도움이 됩니다.

- 결정한 사항 문서화 지원
- 모범 사례를 기반으로 워크로드를 개선하는 권장 사항 제공
- 워크로드의 신뢰성, 보안, 효율성 및 비용 효율성 향상 안내

AWS WA Tool을 사용하여 AWS Well-Architected Framework의 모범 사례를 이용해 워크로드를 문서화하고 측정할 수 있습니다. 이러한 모범 사례는 AWS 솔루션즈 아키텍트가 다양한 기업에서 수년간 솔루션을 개발하며 쌓은 경험을 바탕으로 개발되었습니다. 이 프레임워크는 아키텍처를 평가하는 일관된 접근 방식을 제공할 뿐 아니라, 나중에 필요에 따라 확장되는 설계를 구현하도록 안내합니다.

AWS 모범 사례 외에도 사용자 지정 렌즈를 사용하여 자체 모범 사례로 워크로드를 측정할 수 있습니다. 특정 기술에 맞게 또는 조직 내 거버넌스 요구 사항을 충족하는 데 도움이 되도록 사용자 지정 렌즈에서 질문을 조정할 수 있습니다. 사용자 지정 렌즈는 AWS 렌즈가 제공하는 지침을 확장합니다.

AWS Trusted Advisor과 AWS Service Catalog AppRegistry의 통합으로 AWS Well-Architected Tool 검토 질문에 답하는 데 필요한 정보를 더 쉽게 찾을 수 있습니다.

이 서비스는 최고 기술 책임자(CTO), 아키텍트, 개발자, 운영 팀원 등 기술 제품 개발에 관련된 사람들을 대상으로 합니다. AWS 고객은 AWS WA Tool을 사용해 아키텍처를 문서화하고, 제품 출시 거버넌스를 제공하고, 기술 포트폴리오의 위험을 이해 및 관리합니다.

주제

- AWS Well-Architected Framework란 무엇입니까?
- AWS Well-Architected Tool 용어집

AWS Well-Architected Framework란 무엇입니까?

AWS Well-Architected 프레임워크에는 특정 아키텍처와 클라우드 모범 사례가 얼마나 일치하는지 살펴볼 수 있는 몇 가지 기본 질문이 포함되어 있습니다. 이 프레임워크는 현대의 클라우드 기반 시스템에 기대되는 품질과 비교하여 시스템을 평가하는 일관된 접근 방식을 제공합니다. 아키텍처의 상태를 토대로, 프레임워크가 보다 효과적으로 이 품질에 도달할 수 있는 개선 사항을 제안합니다.

이 프레임워크를 사용하여 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례를 살펴볼 수 있습니다. 또한 모범 사례와 비교하여 아키텍처를 지속적으로 측정하고 개선할 영역을 파악할 수 있습니다. 프레임워크는 운영 우수성, 보안, 안정성, 성능 효율성, 비용 최적화, 지속 가능성 등 여섯 가지 원칙을 토대로 합니다.

워크로드를 설계할 때는 비즈니스 요건에 따라 이 5가지 원칙을 절충합니다. 이러한 비즈니스 의사결정에 따라 엔지니어링 우선 순위가 달라질 수 있습니다. 예를 들어 개발 환경에서는 안정성을 상쇄하여 비용을 줄이는 데 최적화할 수 있습니다. 미션 크리티컬 솔루션에서는 안정성을 최적화하는 대신 비용 증가를 기꺼이 감수할 수도 있습니다. 전자 상거래 솔루션이라면 고객 만족이 수익 증대로 이어질 수 있기 때문에 성능 우선순위를 높이기도 합니다. 보안 및 운영 우수성은 일반적으로 다른 원칙과 절충 관계에 있지 않습니다.

프레임워크에 대한 자세한 내용은 AWS Well-Architected 웹사이트를 참조하세요.

AWS Well-Architected Tool 용어집

다음에서는 AWS WA Tool 및 AWS Well-Architected Framework에서 사용되는 일반적인 용어를 정의합니다.

- 워크로드는 비즈니스 가치를 창출하는 구성 요소를 식별합니다. 일반적으로 비즈니스 리더와 기술 리더가 교환하는 세부적인 정보 수준을 나타냅니다. 마케팅 웹 사이트, 전자 상거래 웹 사이트, 모바일 앱 백엔드, 분석 플랫폼 등이 워크로드에 해당합니다. 워크로드는 아키텍처의 복잡성 수준에 따라 다양합니다. 정적 웹사이트처럼 간단할 수도 있고, 데이터 스토어와 구성 요소가 매우 많은 마이크로서비스 아키텍처처럼 복잡할 수도 있습니다.
- 마일스톤은 설계, 테스트, 개시, 프로덕션 등 제품 수명 주기 전반에 걸쳐 아키텍처가 발전함에 따라 나타나는 아키텍처의 주요 변경 사항을 보여줍니다.
- 렌즈를 사용하면 모범 사례를 기준으로 아키텍처를 지속적으로 평가하고 개선할 영역을 파악할 수 있습니다.

  AWS에서 제공하는 렌즈 외에도 직접 렌즈를 생성하여 사용하거나 나에게 공유된 렌즈를 사용할 수도 있습니다.
- HRI(고위험 문제)는 AWS에서 발견한 아키텍처 및 운영 선택 사항으로 비즈니스에 상당히 부정적인 영향을 미칠 수 있습니다. 이러한 HRI는 조직 운영, 자산 및 개인에 영향을 미칠 수 있습니다.
- MRI(중간 위험 문제)는 AWS에서 발견한 아키텍처 및 운영 선택 사항으로 비즈니스에 부정적인 영향을 미칠 수 있지만, 그 영향이 HRI보다 적습니다.

  자세한 내용은 HRI(고위험 문제) 및 MRI(중간 위험 문제) 섹션을 참조하세요.

AWS Well-Architected Tool 시작

AWS Well-Architected Tool 사용을 시작하려면 먼저 사용자, 그룹 및 역할에 적절한 권한을 제공하고 AWS WA Tool에 사용하려는 AWS 서비스에 대한 지원을 활성화합니다. 다음으로 워크로드를 정의하고 문서화합니다. 워크로드의 현재 상태에 대한 마일스톤을 저장할 수도 있습니다.

다음 주제는 AWS WA Tool을 사용하여 시작하는 방법에 대해 설명합니다. AWS Well-Architected Tool 사용 방법을 보여주는 단계별 자습서는 자습서: AWS Well-Architected Tool 워크로드 문서화를 참조하세요.

주제

- AWS WA Tool에 대한 사용자, 그룹 또는 역할의 액세스 권한 제공
- 다른 AWS 서비스에 대한 AWS WA Tool 지원 활성화
- AWS WA Tool에서 워크로드 정의
- AWS WA Tool에서 워크로드 문서화
- AWS Well-Architected Framework로 워크로드 검토
- 워크로드에 대한 Trusted Advisor 검사 보기
- AWS WA Tool에서 워크로드에 대한 마일스톤 저장

AWS WA Tool에 대한 사용자, 그룹 또는 역할의 액세스 권한 제공

사용자, 그룹 또는 역할에 AWS Well-Architected Tool에 대한 전체 제어 또는 읽기 전용 액세스 권한을 부여할 수 있습니다.

AWS WA Tool에 대한 액세스 권한을 제공

1. 액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

   - AWS IAM Identity Center의 사용자 및 그룹:

     권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따릅니다.
   - 보안 인증 공급자를 통해 IAM에서 관리되는 사용자:

     ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.

- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

2. 전체 제어 권한을 부여하려면 권한 집합 또는 역할에 WellArchitectedConsoleFullAccess 관리형 정책을 적용하세요.

   전체 액세스는 보안 주체에게 AWS WA Tool에서의 모든 작업을 허용합니다. 워크로드를 정의하고, 삭제하고, 확인하고, 업데이트하려면 이 권한이 필요합니다.

3. 읽기 전용 액세스 권한을 부여하려면 권한 집합이나 역할에 WellArchitectedConsoleReadOnlyAccess 관리형 정책을 적용하세요. 이 역할이 부여된 보안 주체는 리소스 확인만 가능합니다.

이러한 정책에 대한 자세한 내용은 AWS Well-Architected Tool의 AWS 관리형 정책 섹션을 참조하세요.

다른 AWS 서비스에 대한 AWS WA Tool 지원 활성화

조직 액세스를 활성화하면 AWS Well-Architected Tool이 조직 구조에 대한 정보를 수집하여 리소스를 더 쉽게 공유할 수 있습니다(자세한 내용은 the section called “AWS Organizations 내에서 리소스 공유 활성화” 참조). 검색 지원을 활성화하면 AWS Trusted Advisor, AWS Service Catalog AppRegistry 및 관련 리소스(예: AppRegistry 리소스 컬렉션의 AWS CloudFormation 스택)에서 정보를 수집하여 Well-Architected 검토 질문에 답하고 워크로드에 맞게 Trusted Advisor 검사를 조정하는 데 필요한 정보를 더 쉽게 찾을 수 있습니다.

AWS Organizations 지원 활성화 또는 검색 지원 활성화를 통해 계정에 대한 서비스 연결 역할을 자동으로 생성할 수 있습니다.

AWS WA Tool이 상호 작용할 수 있는 다른 서비스에 대한 지원을 사용하려면 설정으로 이동하세요.

1. AWS Organizations에서 정보를 수집하려면 AWS Organizations 지원 활성화를 사용 설정하세요.
2. 검색 지원 활성화를 사용 설정하여 다른 AWS 서비스 및 리소스에서 정보를 수집하세요.
3. 서비스 연결 역할 권한 또는 신뢰 관계 정책을 보려면 역할 권한 보기를 선택합니다.
4. 설정 저장을 선택합니다.

워크로드에 대한 AppRegistry 활성화

AppRegistry를 사용하는 것은 선택 사항이며, AWS Business 및 Enterprise Support 고객은 워크로드별로 앱을 활성화할 수 있습니다.

검색 지원이 설정되고 AppRegistry가 새 워크로드 또는 기존 워크로드에 연결될 때마다 AWS Well-Architected Tool이 서비스 관리형 속성 그룹을 생성합니다. AppRegistry의 메타데이터 속성 그룹에는 워크로드 ARN, 워크로드 이름 및 워크로드와 관련된 위험이 포함됩니다.

- 검색 지원이 설정되어 있는 경우 워크로드가 변경될 때마다 속성 그룹이 업데이트됩니다.
- 검색 지원이 해제되거나 애플리케이션이 워크로드에서 삭제되면 AWS Service Catalog에서 워크로드 정보가 삭제됩니다.

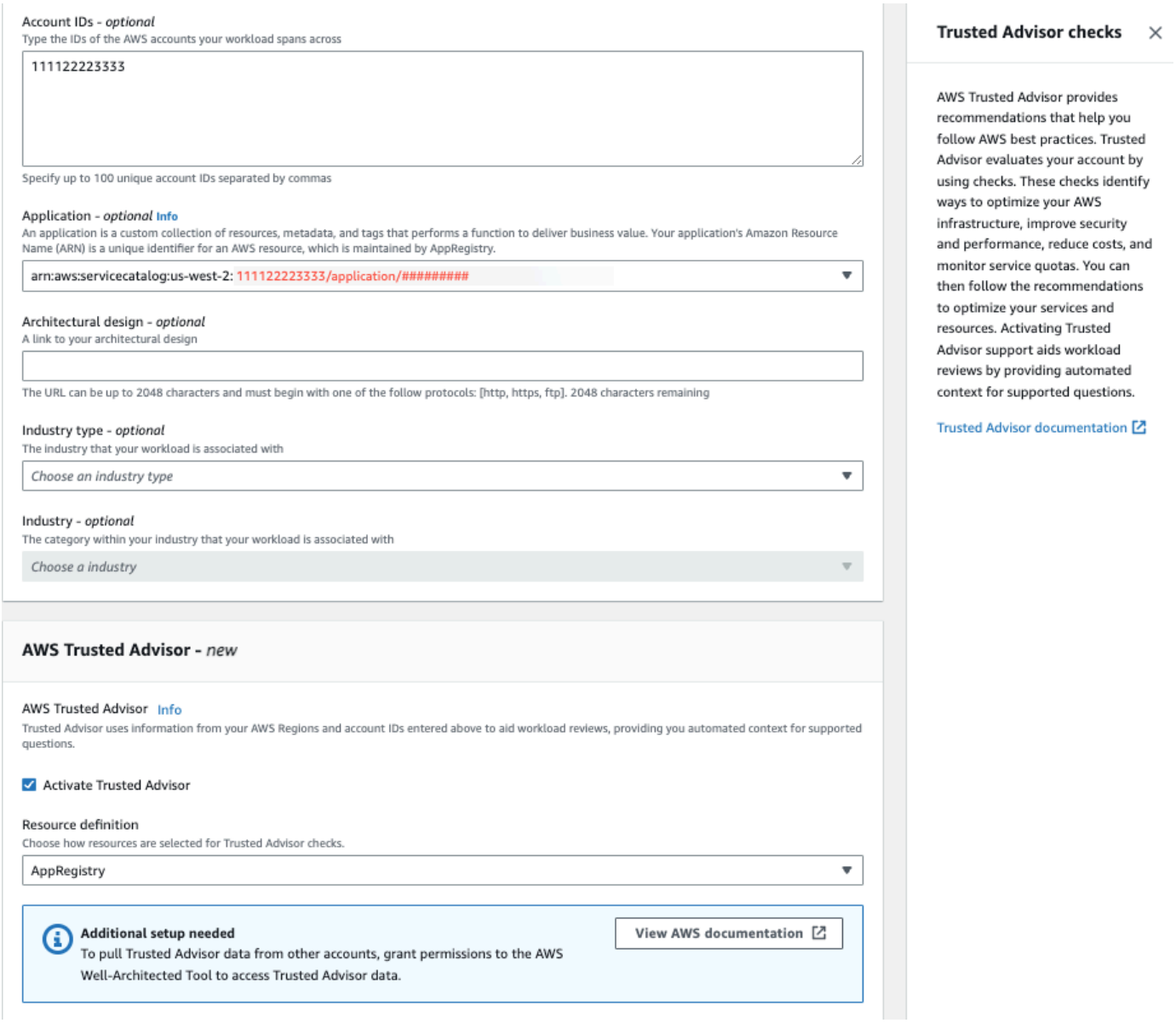
AppRegistry 애플리케이션이 Trusted Advisor에서 가져온 데이터를 구동하도록 하려면 워크로드 리소스 정의를 AppRegistry 또는 모두로 설정합니다. the section called “IAM에서 Trusted Advisor 활성화”의 지침에 따라 애플리케이션의 리소스를 소유한 모든 계정의 역할을 생성합니다.

워크로드에 대해 AWS Trusted Advisor 활성화

AWS Trusted Advisor와의 통합은 선택 사항이며 AWS Business 및 Enterprise Support 고객의 경우 워크로드별로 활성화할 수 있습니다. Trusted Advisor와 AWS WA Tool의 통합 비용은 없지만 Trusted Advisor 가격 세부 정보는 AWS 지원 플랜을 참조하세요. 워크로드에 대해 Trusted Advisor를 활성화하면 AWS 워크로드를 검토하고 최적화하는 보다 포괄적이고 자동화 및 모니터링된 접근 방식을 제공할 수 있습니다. 이를 통해 워크로드의 신뢰성, 보안, 성능 및 비용 최적화를 개선할 수 있습니다.

워크로드에 대해 Trusted Advisor를 활성화하려면

1. Trusted Advisor를 활성화하기 위해 워크로드 소유자는 AWS WA Tool을 사용하여 기존 워크로드를 업데이트하거나 워크로드 정의를 선택하여 새 워크로드를 생성할 수 있습니다.
2. 계정 ID 필드에 Trusted Advisor에서 사용하는 계정 ID를 입력하거나, 애플리케이션 필드에서 애플리케이션 ARN을 선택하거나, 둘 다 선택하여 Trusted Advisor를 활성화합니다.
3. AWS Trusted Advisor 섹션에서 Trusted Advisor 활성화를 선택합니다.



4. IAM 서비스 역할이 생성됩니다 알림은 워크로드에 대해 Trusted Advisor가 처음 활성화될 때 표시됩니다. 권한 보기를 선택하면 IAM 역할 권한이 표시됩니다. 역할 이름은 물론 IAM에서 JSON이 자동으로 생성한 권한 및 신뢰 관계를 확인할 수 있습니다. 역할을 생성한 후 Trusted Advisor를 활성화하는 후속 워크로드에 대해서는 추가 설정 필요 알림만 표시됩니다.
5. 리소스 정의 드롭다운에서 워크로드 메타데이터, AppRegistry 또는 모두를 선택할 수 있습니다. 리소스 정의 선택은 Well-Architected 모범 사례에 매핑되는 워크로드 검토 시 상태 검사를 제공하기 위해 AWS WA Tool이 Trusted Advisor에서 데이터를 가져올 대상을 정의합니다.

   워크로드 메타데이터 - 워크로드는 계정 ID로 정의되고 워크로드에 AWS 리전이 지정됩니다.

AppRegistry - 워크로드는 워크로드와 연결된 AppRegistry 애플리케이션에 있는 리소스(예: AWS CloudFormation 스택)에 의해 정의됩니다.

모두 — 워크로드는 워크로드 메타데이터와 AppRegistry 리소스 모두에 의해 정의됩니다.

6. 다음을 선택합니다.
7. AWS Well-Architected Framework를 워크로드에 적용하고 워크로드 정의를 선택합니다. Trusted Advisor 검사는 AWS Well-Architected Framework에만 연결되며 다른 렌즈에는 연결되지 않습니다.

AWS WA Tool은 IAM에서 생성된 역할을 사용하여 Trusted Advisor에서 정기적으로 데이터를 가져옵니다. IAM 역할은 워크로드 소유자에 대해 자동으로 생성됩니다. 하지만 Trusted Advisor 정보를 보려면 워크로드에 연결된 계정의 소유자가 IAM으로 이동하여 역할을 생성해야 합니다. 자세한 내용은 ??? 섹션을 참조하세요. 이 역할이 없는 경우 AWS WA Tool은 해당 계정에 대한 Trusted Advisor 정보를 얻을 수 없으며 오류가 표시됩니다.

AWS Identity and Access Management(IAM)에서의 역할 생성에 대한 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 역할 생성(콘솔)을 참조하세요.

IAM에서 워크로드에 대해 Trusted Advisor 활성화

> **Note**
>
> 워크로드 소유자는 Trusted Advisor 워크로드를 생성하기 전에 계정에 대한 검색 지원을 활성화해야 합니다. 검색 지원 활성화를 선택하면 워크로드 소유자에게 필요한 역할이 생성됩니다. 연결된 다른 모든 계정에 대해서는 다음 단계를 따르세요.

Trusted Advisor가 활성화된 워크로드와 연결된 계정 소유자는 IAM에서 역할을 생성해야 AWS Well-Architected Tool에서 Trusted Advisor 정보를 볼 수 있습니다.

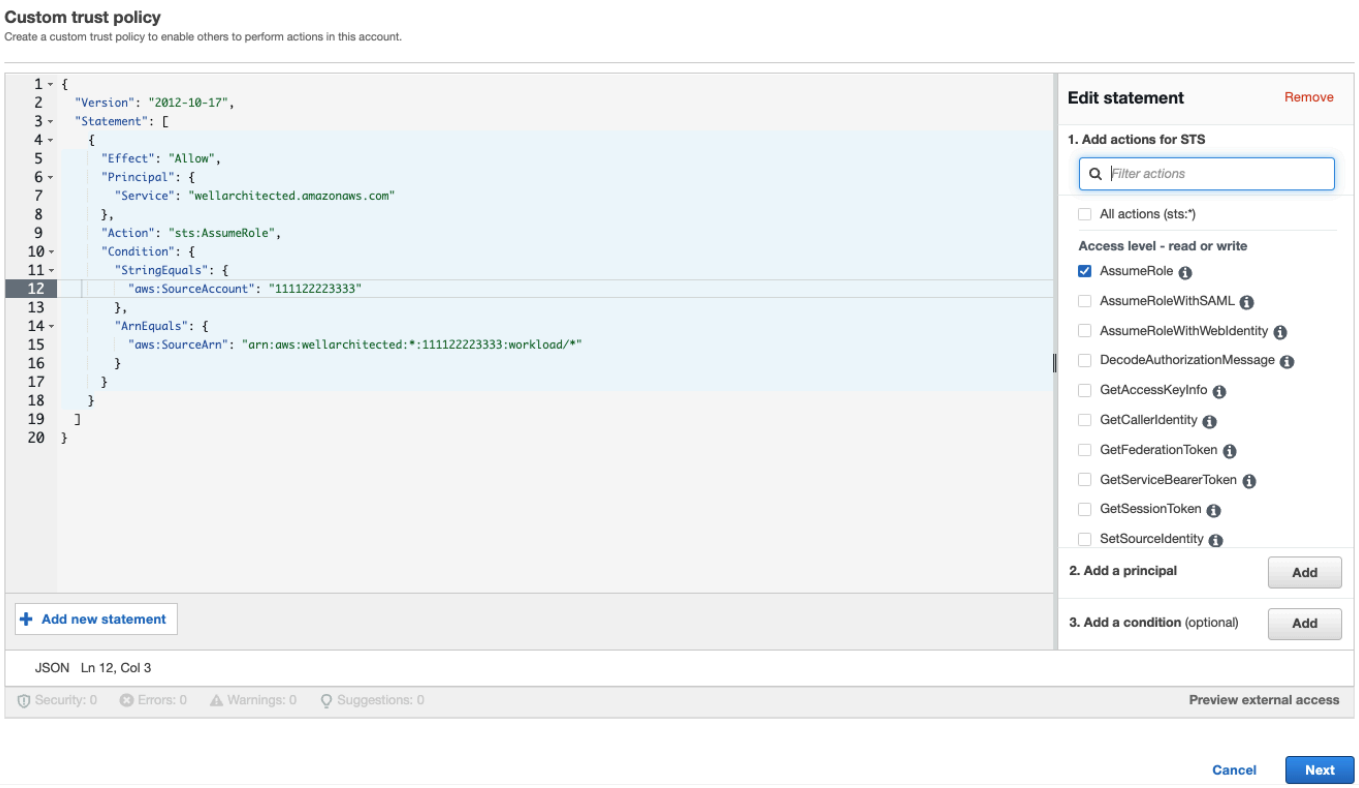
Trusted Advisor에서 정보를 가져올 수 있도록 IAM에서 AWS WA Tool에 대한 역할을 생성하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 유형에서 사용자 지정 신뢰 정책을 선택합니다.

4. 다음 이미지에 표시된 것처럼 다음 사용자 지정 신뢰 정책을 복사하여 IAM 콘솔의 JSON 필드에 붙여넣습니다. *WORKLOAD_OWNER_ACCOUNT_ID*를 워크로드 소유자의 계정 ID로 바꾸고 다음을 선택합니다.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:wellarchitected:*:111122223333:workload/*"
                }
            }
        }
    ]
}
```



Note

이전 사용자 지정 신뢰 정책에 대한 조건 블록의 `aws:sourceArn`은 `"arn:aws:wellarchitected:*:`*WORKLOAD_OWNER_ACCOUNT_ID*`:workload/*"`이며, AWS WA Tool에서 이 역할이 모든 워크로드 소유자의 워크로드에 사용될 수 있다는 일반 조건이 있습니다. 하지만 특정 워크로드 ARN 또는 워크로드 ARN 집합으로 액세스 범위를 좁힐 수 있습니다. 여러 ARN을 지정하려면 다음 신뢰 정책 예제를 참조하세요.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
```

```
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "aws:SourceArn": [
                    "arn:aws:wellarchitected:us-
east-1:111122223333:workload/WORKLOAD_ID_1",
    "arn:aws:wellarchitected:us-
east-1:111122223333:workload/WORKLOAD_ID_2"
                    ]
                }
            }
        }
    ]
}
```

5. 권한 추가 페이지에서 권한 정책에 대해 Trusted Advisor의 데이터를 읽을 수 있는 AWS WA Tool 액세스 권한을 부여할 수 있도록 정책 생성을 선택합니다. 정책 생성을 선택하면 새 창이 열립니다.

> **Note**
>
> 또한 역할을 생성하는 동안 권한 생성을 건너뛰고, 역할을 생성한 후 인라인 정책을 생성할 수도 있습니다. 역할 생성 성공 메시지에서 역할 보기를 선택하고 권한 탭의 권한 추가 드롭다운에서 인라인 정책 생성을 선택합니다.

6. 다음 권한 정책을 복사해 JSON 필드에 붙여 넣습니다. `Resource` ARN에서 *YOUR_ACCOUNT_ID*를 자체 계정 ID로 바꾸고 리전 또는 별표(*)를 지정한 다음 다음: 태그를 선택합니다.

   ARN 형식에 대한 자세한 내용은 AWS 일반 참조 안내서의 Amazon 리소스 이름(ARN)을 참조하세요.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeCheckRefreshStatuses",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeRiskResources",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeRisk",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeRisks",
                "trustedadvisor:DescribeCheckItems"
            ],
            "Resource": [
                "arn:aws:trustedadvisor:*:111122223333:checks/*"
            ]
        }
    ]
}
```

7. Trusted Advisor가 워크로드에 대해 활성화되고 리소스 정의가 AppRegistry 또는 모두로 설정된 경우, 워크로드에 연결된 AppRegistry 애플리케이션에서 리소스를 소유한 모든 계정이 해당 Trusted Advisor 역할의 권한 정책에 다음 권한을 추가해야 합니다.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DiscoveryPermissions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ListAssociatedResources",
                "tag:GetResources",
                "servicecatalog:GetApplication",
                "resource-groups:ListGroupResources",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources"
            ],
            "Resource": "*"
        }
    ]
}
```

8. (선택 사항) 태그를 추가합니다. 다음: 검토를 선택합니다.
9. 정책을 검토하고 정책 이름을 추가한 다음 정책 생성을 선택합니다.
10. 역할의 권한 추가 페이지에서 방금 생성한 정책 이름을 선택하고 다음을 선택합니다.
11. 다음 `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* 구문을 사용해야 하는 역할 이름을 입력하고 역할 생성을 선택합니다. *`WORKLOAD_OWNER_ACCOUNT_ID`*를 워크로드 소유자의 계정 ID로 바꿉니다.

    페이지 상단에 역할이 생성되었음을 알리는 성공 메시지가 표시됩니다.
12. 역할 및 관련 권한 정책을 보려면 왼쪽 탐색 창의 액세스 관리에서 역할을 선택하고 `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* 이름을 검색합니다. 역할 이름을 선택하여 권한 및 신뢰 관계가 올바른지 확인합니다.

워크로드에 대해 Trusted Advisor 비활성화

워크로드에 대해 Trusted Advisor를 비활성화하려면

워크로드를 편집하고 Trusted Advisor 활성화를 선택 취소하여 AWS Well-Architected Tool에서 모든 워크로드에 대해 Trusted Advisor를 비활성화할 수 있습니다. 워크로드 편집에 대한 자세한 내용은 the section called “워크로드 편집” 섹션을 참조하세요.

AWS WA Tool에서 Trusted Advisor를 비활성화해도 IAM에서 생성한 역할은 삭제되지 않습니다. IAM에서 역할을 삭제하려면 별도의 정리 조치가 필요합니다. 워크로드 소유자 또는 관련 계정의 소유자는 Trusted Advisor 가 AWS WA Tool에서 비활성화되었을 때 생성된 IAM 역할을 삭제하거나 워크로드에 대한 AWS WA Tool의 Trusted Advisor 데이터 수집을 중단해야 합니다.

IAM에서 **`WellArchitectedRoleForTrustedAdvisor`**를 삭제하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택합니다.
3. `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*를 검색하여 역할 이름을 선택합니다.
4. 삭제를 선택합니다. 팝업 창에서 역할의 이름을 입력하여 삭제를 확인하고 삭제를 다시 선택합니다.

IAM에서 역할을 삭제하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 삭제(콘솔)를 참조하세요.

AWS WA Tool에서 워크로드 정의

워크로드는 비즈니스 가치를 창출하는 구성 요소입니다. 마케팅 웹 사이트, 전자 상거래 웹 사이트, 모바일 앱 백엔드, 분석 플랫폼 등이 워크로드에 해당합니다. 워크로드를 정확하게 정의하면 AWS Well-Architected Framework 요소에 대한 포괄적인 검토를 보장하는 데 도움이 됩니다.

워크로드를 정의하는 방법

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. AWS WA Tool을 처음 사용하는 경우, 서비스의 기능을 소개하는 페이지가 나타납니다. 워크로드 정의 섹션에서 워크로드 정의를 선택합니다.

   또는 왼쪽 탐색 창에서 워크로드와 워크로드 정의를 차례대로 선택합니다.

   AWS에서 워크로드 데이터를 사용하는 방법에 대한 자세한 내용은 AWS에서 이 데이터가 필요한 이유는 무엇이며 어떻게 사용됩니까?를 선택하세요.
3. 이름 상자에 워크로드 이름을 입력합니다.

   > **Note**
   >
   > 이름은 3~100자 이내로 작성해야 합니다. 문자 3개 이상이 공백이어서는 안 됩니다. 워크로드 이름은 고유해야 합니다. 고유성 여부를 확인할 때 공백과 대문자는 무시합니다.
4. 설명 상자에 워크로드에 대한 설명을 입력합니다. 설명은 3~250자 이내로 작성해야 합니다.
5. 검토 소유자 상자에 워크로드 검토 프로세스를 소유한 기본 그룹 또는 개인의 이름, 이메일 주소 또는 식별자를 입력합니다.
6. 환경 상자에서 워크로드 환경을 선택합니다.
   - 프로덕션 - 워크로드가 프로덕션 환경에서 실행됩니다.
   - 사전 프로덕션 - 워크로드가 사전 프로덕션 환경에서 실행됩니다.
7. 리전 섹션에서 워크로드의 리전을 선택합니다.
   - AWS 리전 - 워크로드가 실행되는 AWS 리전을 한 번에 하나씩 선택합니다.
   - AWS 외부 리전 - 워크로드가 실행되는 AWS 외부 리전의 이름을 입력합니다. 고유 리전을 5개까지 쉼표로 구분하여 지정할 수 있습니다.

   워크로드에 필요하다면 두 옵션을 모두 사용하십시오.

8. (선택 사항) 계정 ID 상자에 워크로드와 연결되는 AWS 계정를 입력합니다. 고유 계정 ID를 최대 100개까지 쉼표로 구분하여 지정할 수 있습니다.

   Trusted Advisor가 활성화되면 지정된 모든 계정 ID가 Trusted Advisor에서 데이터를 가져오는 데 사용됩니다. IAM 내에서 사용자를 대신하여 Trusted Advisor 데이터를 가져올 AWS WA Tool 권한을 부여하려면 워크로드에 대해 AWS Trusted Advisor 활성화를 참조하세요.

9. (선택 사항) 애플리케이션 상자에 이 워크로드에 연결할 AWS Service Catalog AppRegistry 애플리케이션의 애플리케이션 ARN을 입력합니다. 워크로드당 ARN을 하나만 지정할 수 있으며 애플리케이션과 워크로드는 동일한 리전에 있어야 합니다.

10. (선택 사항) 아키텍처 설계 상자에 아키텍처 설계의 URL을 입력합니다.

11. (선택 사항) 산업 유형 상자에서 워크로드와 연결할 산업 유형을 선택합니다.

12. (선택 사항) 산업 상자에서 워크로드와 가장 일치하는 산업을 선택합니다.

13. (선택 사항) Trusted Advisor 섹션에서 워크로드에 대한 Trusted Advisor 검사를 활성화하려면 Trusted Advisor 활성화를 선택합니다. 워크로드와 관련된 계정에는 추가 설정이 필요할 수 있습니다. 사용자 대신 Trusted Advisor 데이터를 가져올 수 있는 AWS WA Tool 권한을 부여하려면 the section called “Trusted Advisor 활성화” 섹션을 참조하세요. 리소스 정의에서 워크로드 메타데이터, AppRegistry 또는 모두를 선택하여 AWS WA Tool이 Trusted Advisor 검사를 실행하는 데 사용할 리소스를 정의합니다.

14. (선택 사항) Jira 섹션에서 워크로드에 대한 워크로드 수준 Jira 동기화 설정을 활성화하려면 계정 수준 설정 재정의를 선택합니다. 워크로드와 관련된 계정에는 추가 설정이 필요할 수 있습니다. 커넥터 설정 및 구성을 시작하려면 AWS Well-Architected Tool Connector for Jira를 참조하세요. 워크로드 동기화 안 함, 워크로드 동기화 - 수동, 워크로드 동기화 - 자동에서 선택하고, 선택적으로 동기화할 Jira 프로젝트 키를 입력합니다.

   > **Note**
   >
   > 계정 수준 설정을 재정의하지 않으면 워크로드는 계정 수준 Jira 동기화 설정으로 기본 설정됩니다.

15. (선택 사항) 태그 섹션에서 워크로드에 연결할 태그를 추가합니다.

    태그에 대한 자세한 내용은 AWS WA Tool 리소스에 태그 지정 섹션을 참조하세요.

16. 다음을 선택합니다.

    필수 입력 상자가 비어있거나 지정된 값이 잘못된 경우에는 계속하기 전에 먼저 문제를 해결해야 합니다.

17. (선택 사항) 프로필 적용 단계에서 기존 프로필을 선택하거나, 프로필 이름을 검색하거나, 프로필 생성을 선택하여 프로필을 생성해 워크로드에 프로필을 연결합니다. 다음을 선택합니다.
18. 이 워크로드에 적용되는 렌즈를 선택합니다. 최대 20개의 렌즈를 워크로드에 추가할 수 있습니다. 공식 AWS 렌즈에 대한 설명은 렌즈를 참조하세요.

    렌즈는 사용자 지정 렌즈(직접 생성했거나 AWS 계정과 공유한 렌즈), Lens Catalog(모든 사용자가 사용할 수 있는 AWS 공식 렌즈) 또는 둘 다에서 선택할 수 있습니다.

    > **Note**
    >
    > 사용자 지정 렌즈를 생성하지 않았거나 사용자 지정 렌즈를 공유하지 않은 경우 사용자 지정 렌즈 섹션은 비어 있습니다.

    > **면책 조항**
    >
    > 다른 AWS 사용자 또는 계정에서 생성된 사용자 지정 렌즈에 액세스하거나 이를 적용하면 다른 사용자가 생성하여 나에게 공유한 사용자 지정 렌즈가 AWS 고객 계약에 정의된 제3자 콘텐츠임을 인정하는 것으로 간주됩니다.

19. 워크로드 정의를 선택합니다.

    필수 입력 상자가 비어 있거나, 혹은 지정된 값이 잘못된 경우에는 워크로드를 정의하기 전에 먼저 문제를 해결해야 합니다.

AWS WA Tool에서 워크로드 문서화

AWS Well-Architected Tool에서 워크로드를 정의한 후 워크로드 검토 페이지를 열어 워크로드의 상태를 문서화할 수 있습니다. 이를 통해 워크로드를 평가하고 시간 경과에 따른 진행 상황을 추적할 수 있습니다.

워크로드의 상태를 문서화하려면

1. 처음 워크로드를 정의한 후에는 현재 워크로드 세부 정보가 표시된 페이지가 나타납니다. Start reviewing(검토 시작)을 선택하여 시작합니다.

   그렇지 않으면 왼쪽 탐색 창에서 Workloads(워크로드)를 선택한 후 워크로드 이름을 선택하여 워크로드 세부 정보 페이지를 엽니다. Continue reviewing(검토 계속)을 선택합니다.

(선택 사항) 프로필이 워크로드와 연결된 경우 왼쪽 탐색 창에는 워크로드 검토 프로세스를 가속화하는 데 사용할 수 있는 우선순위가 지정된 워크로드 검토 질문 목록이 표시됩니다.

2. 이제 첫 번째 질문에 표시됩니다. 질문이 표시될 때마다 다음과 같이 실행합니다.

   a. 질문을 읽고 워크로드에 적용되는 질문인지 결정합니다.

      추가 지침을 보고 싶다면 정보를 선택하여 도움말 패널에서 정보를 확인합니다.

      - 질문이 워크로드에 적용되지 않는다면 질문이 이 워크로드에 적용되지 않음을 선택합니다.
      - 적용된다면 목록에서 현재 따르고 있는 모범 사례를 선택합니다.

        현재 따르는 모범 사례가 없으면 None of these(여기에 없음)를 선택합니다.

      항목에 대한 추가 지침을 보고 싶다면 정보를 선택하여 도움말 패널에서 정보를 확인합니다.

   b. (선택 사항) 워크로드에 적용할 수 없는 모범 사례가 하나 이상 있는 경우 이 워크로드에 적용되지 않는 모범 사례 표시를 선택하고 해당 항목을 선택합니다. 선택한 각 모범 사례에 대해 필요한 경우 이유를 선택하고 추가 세부 정보를 제공할 수 있습니다.

   c. (선택 사항) 노트 상자를 사용해 질문과 관련된 정보를 기록합니다.

      예를 들어, 질문이 적용되지 않는 이유를 설명하거나 선택한 모범 사례의 세부 정보를 입력할 수 있습니다.

   d. 다음을 선택하여 다음 질문으로 계속 이어갑니다.

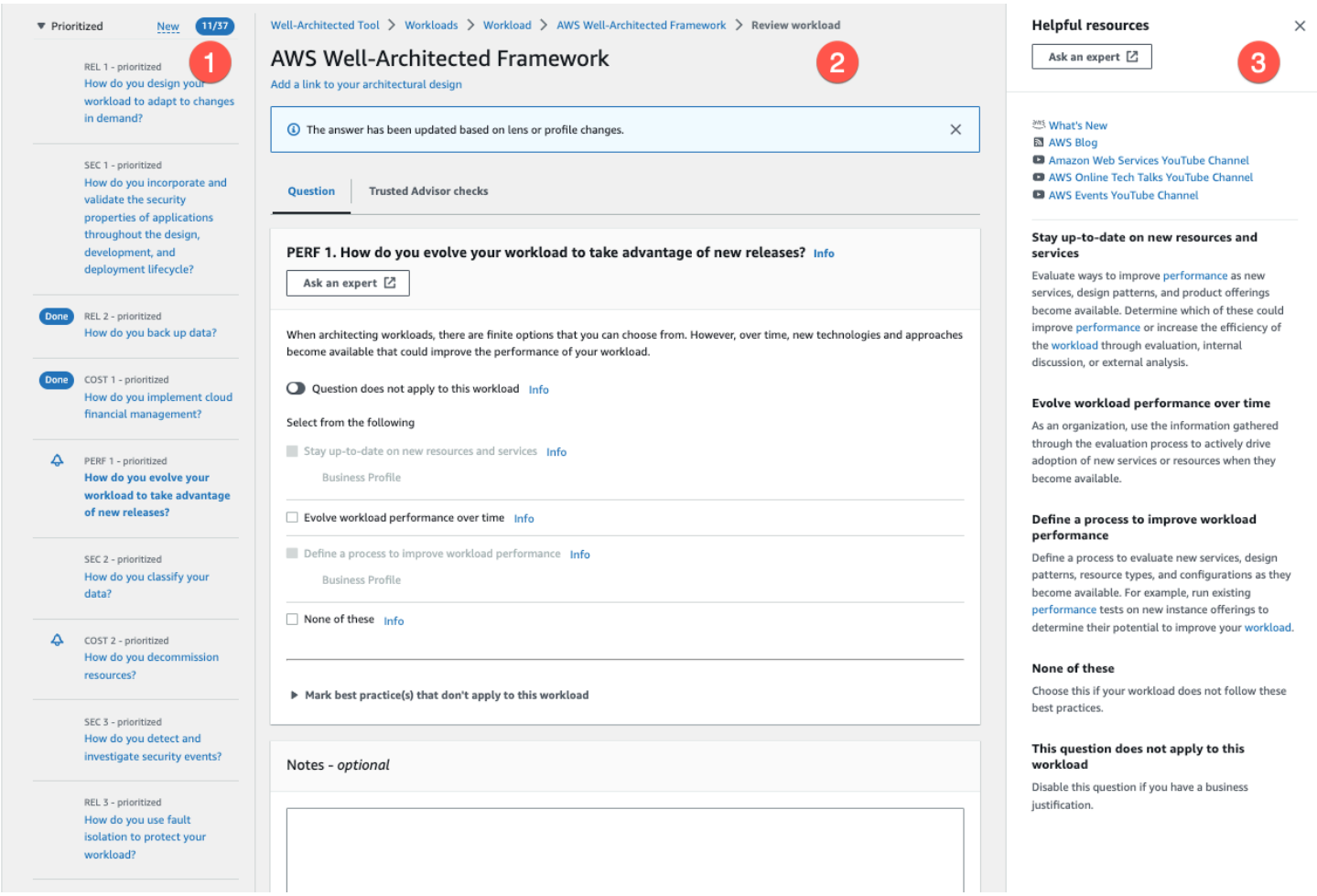
   각 항목의 질문마다 위의 단계를 반복합니다.

3. 언제든지 저장 후 나가기를 선택하여 변경 사항을 저장하고 워크로드 문서화를 일시 중지할 수 있습니다.

워크로드를 문서화한 후 언제든지 질문으로 돌아가서 계속 검토할 수 있습니다. 자세한 내용은 AWS Well-Architected Framework를 사용한 워크로드 검토를 참조하세요.

AWS Well-Architected Framework로 워크로드 검토

워크로드 검토 페이지의 콘솔에서 워크로드를 검토할 수 있습니다. 이 페이지에서는 워크로드 성능에 대한 모범 사례와 유용한 리소스를 제공합니다.



1. 워크로드 검토 페이지를 열려면 워크로드 세부 정보 페이지에서 계속 검토를 선택합니다. 왼쪽 탐색 창에는 각 원칙에 대한 질문이 표시됩니다. 답변한 질문은 완료로 표시됩니다. 원칙 이름 옆에는 각 원칙에서 응답한 질문의 수가 표시됩니다.

   원칙 이름과 응답할 질문을 차례대로 선택하면 다른 원칙의 질문으로 이동할 수 있습니다.

   (선택 사항) 프로필이 워크로드와 연결되어 있는 경우 AWS WA Tool은 프로필의 정보를 사용하여 워크로드 검토에서 우선순위가 지정된 질문과 비즈니스에 적합하지 않은 질문을 판단합니다. 왼쪽 탐색 창에서 우선순위가 지정된 질문을 사용하여 워크로드 검토 프로세스를 가속화할 수 있습니다. 우선순위가 지정된 질문 목록에 새로 추가된 질문 옆에는 알림 아이콘이 표시됩니다.
2. 중간 패널에는 현재 질문이 표시됩니다. 따르고 있는 모범 사례를 선택합니다. 정보를 선택하면 질문이나 모범 사례에 대한 추가 정보를 얻을 수 있습니다. 전문가에게 물어보기를 선택하여 AWS Well-Architected 전용 AWS re:Post 커뮤니티에 액세스합니다. AWS re:Post는 AWS 포럼을 대체하는 주제 기반 Q&A 커뮤니티입니다. re:Post를 사용하면 답변을 찾고, 질문에 답하고, 그룹에 가입하고, 인기 주제를 팔로우하고, 좋아하는 질문과 답변에 투표할 수 있습니다.

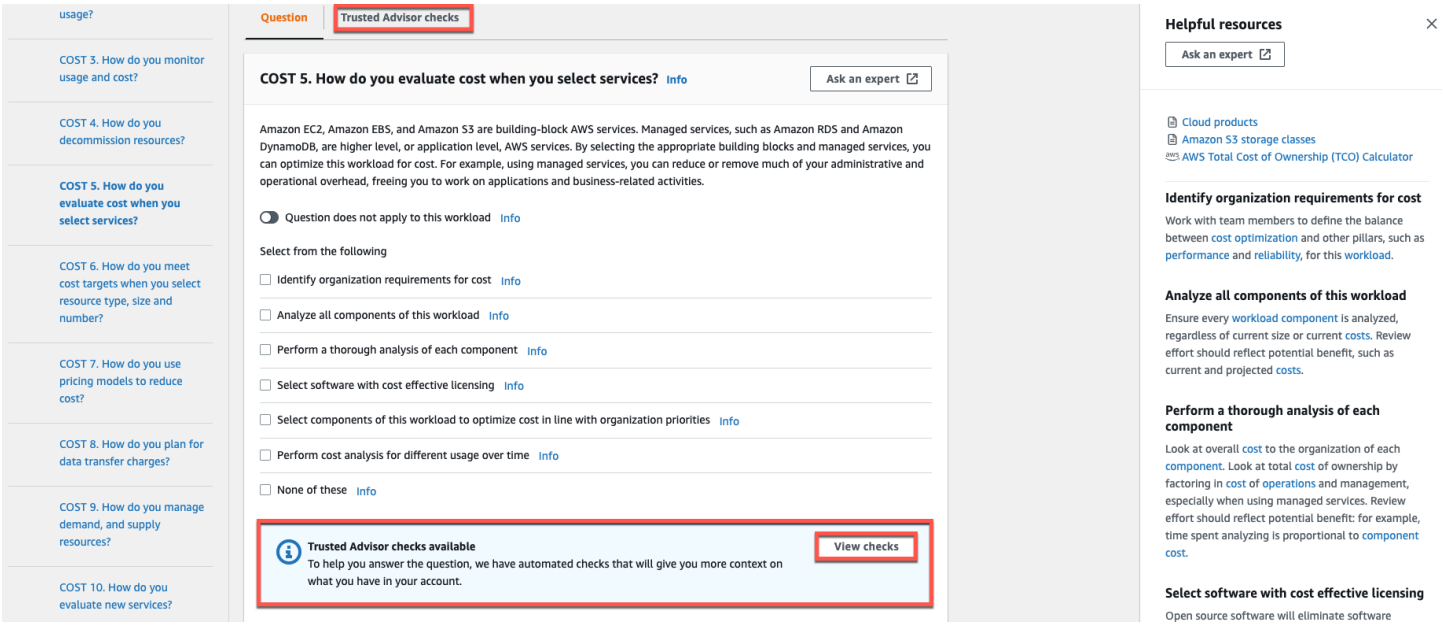
(선택 사항) 적용할 수 없는 하나 이상의 모범 사례를 표시하려면 이 워크로드에 적용되지 않는 모범 사례 표시를 선택하고 해당 항목을 선택합니다.

이 패널 하단에 있는 버튼을 사용하면 다음 질문으로 이동하거나, 이전 질문으로 돌아가거나, 변경 사항을 저장하고 나갈 수 있습니다.

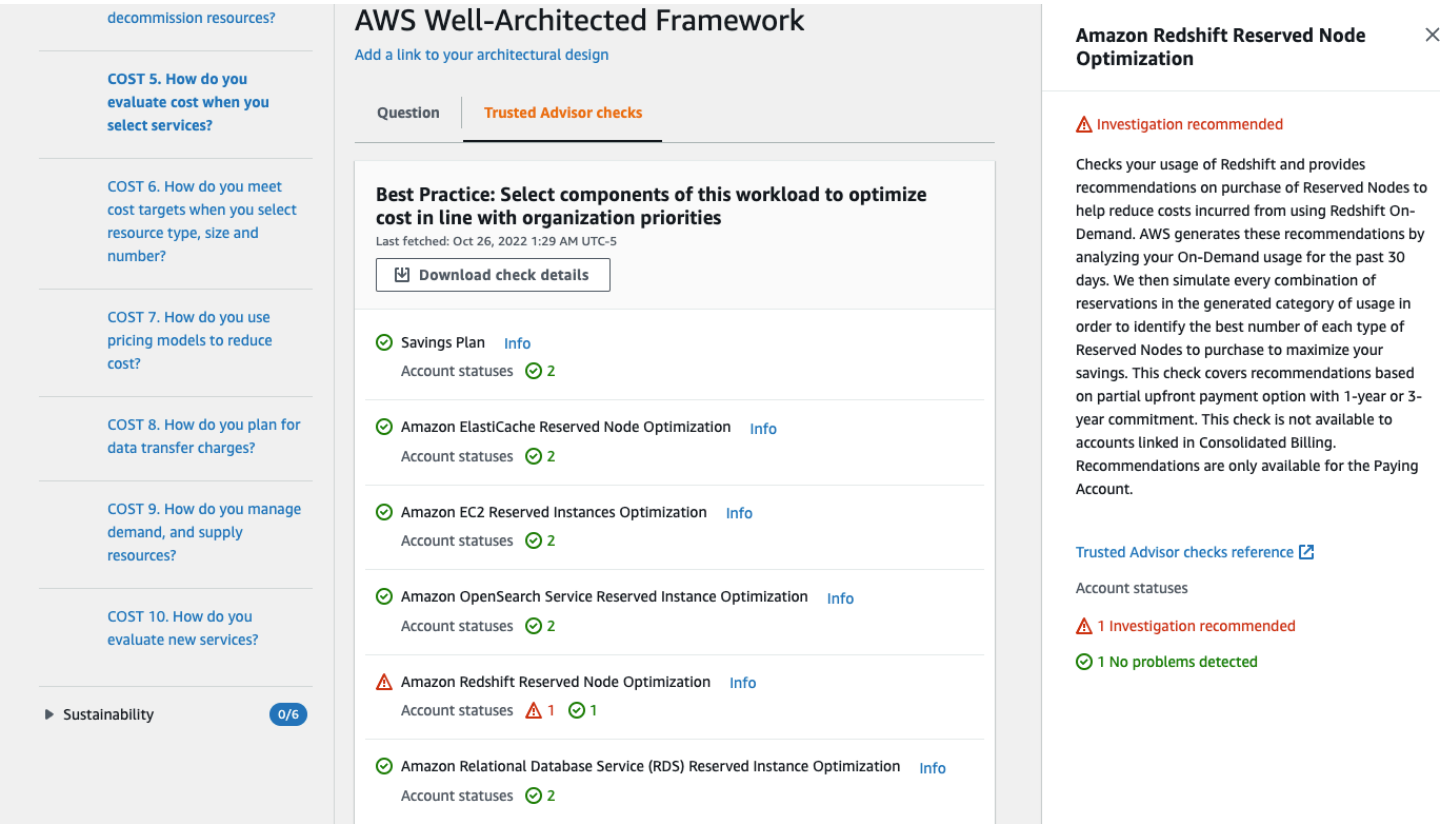
3. 오른쪽 도움말 패널에는 추가 정보와 유용한 리소스가 표시됩니다. 전문가에게 물어보기를 선택하여 AWS Well-Architected 전용 AWS re:Post 커뮤니티에 액세스하세요. 이 커뮤니티에서는 AWS에서의 워크로드 설계, 구축, 배포 및 운영과 관련된 질문을 할 수 있습니다.

워크로드에 대한 Trusted Advisor 검사 보기

워크로드에 대해 Trusted Advisor가 활성화된 경우 질문 옆에 Trusted Advisor 검사 탭이 표시됩니다. 모범 사례에 사용할 수 있는 검사 항목이 있는 경우 질문 선택 이후에 이용 가능한 Trusted Advisor 검사가 있다는 알림이 표시됩니다. 검사 보기를 선택하면 Trusted Advisor 검사 탭으로 이동합니다.



Trusted Advisor 검사 탭에서는 Trusted Advisor의 모범 사례 검사에 대한 자세한 정보를 보거나, 도움말 리소스 창의 Trusted Advisor 문서 링크를 보거나, 각 모범 사례에 대한 Trusted Advisor 검사 및 상태를 CSV 파일 보고서로 제공하는 검사 세부 정보를 다운로드할 수 있습니다.



Trusted Advisor의 검사 카테고리는 색상이 지정된 아이콘으로 표시되며 각 아이콘 옆의 숫자는 해당 상태의 계정 수를 나타냅니다.

- 작업 권장(빨간색) – Trusted Advisor가 검사 작업을 권장합니다.
- 조사 권장(노란색) – Trusted Advisor가 검사 대상이 될 수 있는 문제를 감지합니다.
- 문제가 감지되지 않음(녹색) – Trusted Advisor가 검사의 문제를 감지하지 않습니다.
- 제외된 항목(회색) - 제외된 항목(예: 검사에서 무시할 리소스)이 있는 검사의 수입니다.

Trusted Advisor가 제공하는 검사에 대한 자세한 내용은 지원 사용 설명서의 검사 카테고리 보기를 참조하세요.

각 Trusted Advisor 검사 옆의 정보 링크를 선택하면 도움말 리소스 창에 검사에 대한 정보가 표시됩니다. 자세한 정보는 지원 사용 설명서의 AWS Trusted Advisor 검사 참조를 참조하세요.

AWS WA Tool에서 워크로드에 대한 마일스톤 저장

언제든지 워크로드에 대한 마일스톤을 저장할 수 있습니다. 마일스톤은 현재 워크로드 상태를 기록합니다.

마일스톤을 저장하는 방법

1. 워크로드 세부 정보 페이지에서 마일스톤 저장을 선택합니다.
2. 마일스톤 이름 상자에 마일스톤 이름을 입력합니다.

> **Note**
>
> 이름은 3~100자 이내로 작성해야 합니다. 문자 3개 이상이 공백이어서는 안 됩니다. 워크로드와 연결되는 마일스톤 이름은 고유해야 합니다. 고유성 여부를 확인할 때 공백과 대문자는 무시합니다.

3. 저장을 선택합니다.

마일스톤이 저장된 후에는 이 마일스톤에 캡처된 워크로드 데이터를 변경할 수 없습니다.

자세한 내용은 마일스톤 섹션을 참조하세요.

자습서: AWS Well-Architected Tool 워크로드 문서화

이 자습서에서는 AWS Well-Architected Tool을 이용한 워크로드 문서화 및 측정을 설명합니다. 이 예에서는 소매 전자 상거래 웹 사이트의 워크로드를 정의하고 문서화하는 방법을 단계별로 보여줍니다.

주제

1단계: 워크로드 정의

워크로드 정의부터 시작합니다. 워크로드를 정의하는 방법에는 두 가지가 있습니다. 이 자습서에서는 검토 템플릿에서 워크로드를 정의하지 않습니다. 검토 템플릿에서 워크로드를 정의하는 방법에 대한 자세한 내용은 the section called “워크로드 정의” 섹션을 참조하세요.

워크로드를 정의하는 방법

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.

   > **Note**
   >
   > 워크로드 상태를 문서화하는 사용자는 AWS WA Tool에 대한 전체 액세스 권한이 있어야 합니다.

2. 워크로드 정의 섹션에서 워크로드 정의를 선택합니다.
3. 이름 상자에 **`Retail Website - North America`**를 워크로드 이름으로 입력합니다.
4. 설명 상자에 워크로드에 대한 설명을 입력합니다.
5. 검토 소유자 상자에 워크로드 검토 프로세스 담당자의 이름을 입력합니다.
6. 환경 상자에서 워크로드가 프로덕션 환경에서 실행되도록 지정합니다.
7. 워크로드는 AWS와 로컬 데이터 센터 모두에서 실행됩니다.

   a. AWS 리전을 선택한 후 북미 지역에서 워크로드가 실행되는 리전 2곳을 선택합니다.

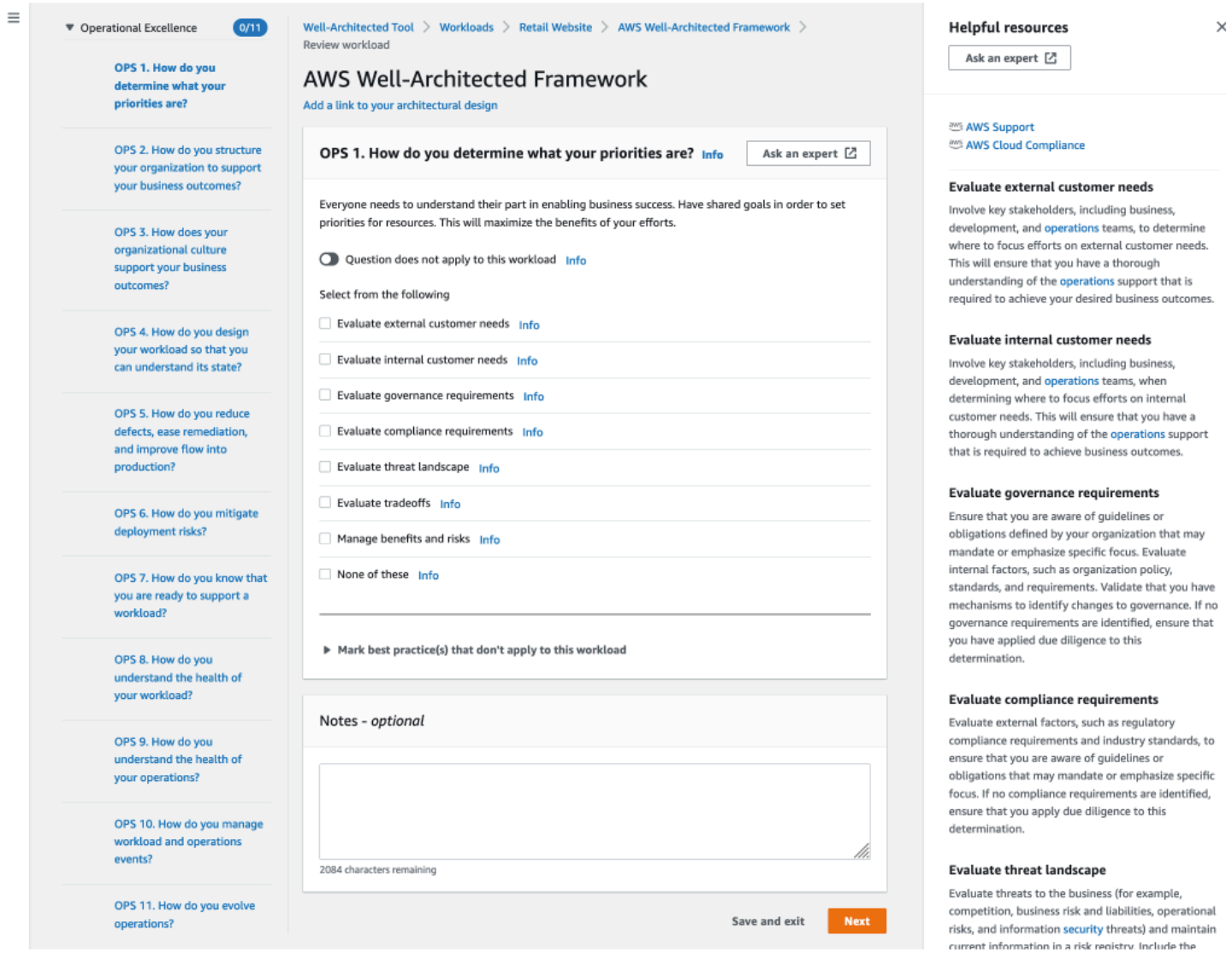
   b. 또한 AWS 외부 리전을 선택한 후 로컬 데이터 센터 이름을 입력합니다.
8. 계정 ID 상자는 선택 사항입니다. 이 워크로드에 어떠한 AWS 계정도 연결하지 마세요.
9. 애플리케이션 상자는 선택 사항입니다. 이 워크로드에는 애플리케이션 ARN을 입력하지 마세요.
10. 아키텍처 다이어그램 상자는 선택 사항입니다. 아키텍처 다이어그램을 이 워크로드에 연결하지 마세요.
11. 산업 유형 및 산업 상자는 선택 사항이며 이 워크로드에 지정되지 않았습니다.
12. Trusted Advisor 섹션은 선택 사항입니다. 이 워크로드에 대해서는 Trusted Advisor 지원 활성화를 하지 마세요.
13. Jira 섹션은 선택 사항입니다. 이 워크로드에 대한 Jira 섹션의 계정 수준 설정을 재정의하지 마세요.
14. 이 예시에서는 워크로드에 어떠한 태그도 적용하지 마세요. Next(다음)를 선택합니다.
15. 프로필 적용 단계는 선택 사항입니다. 이 워크로드에는 프로필을 적용하지 마세요. Next(다음)를 선택합니다.
16. 이 예제에서는 자동으로 선택되는 AWS Well-Architected Framework 렌즈를 적용합니다. 워크로드 정의를 선택하여 이 값을 저장하고 워크로드를 정의합니다.
17. 워크로드 정의를 마쳤으면 이제 검토 시작을 선택하여 워크로드 상태 문서화를 시작합니다.

2단계: 워크로드 상태 문서화

워크로드의 상태를 문서화하기 위해서는 운영 우수성, 보안, 안정성, 성능 효율성, 비용 최적화, 지속 가능성 등 AWS AWS Well-Architected Framework의 원칙에 걸쳐 특정 렌즈에 대한 질문에 답해야 합니다.

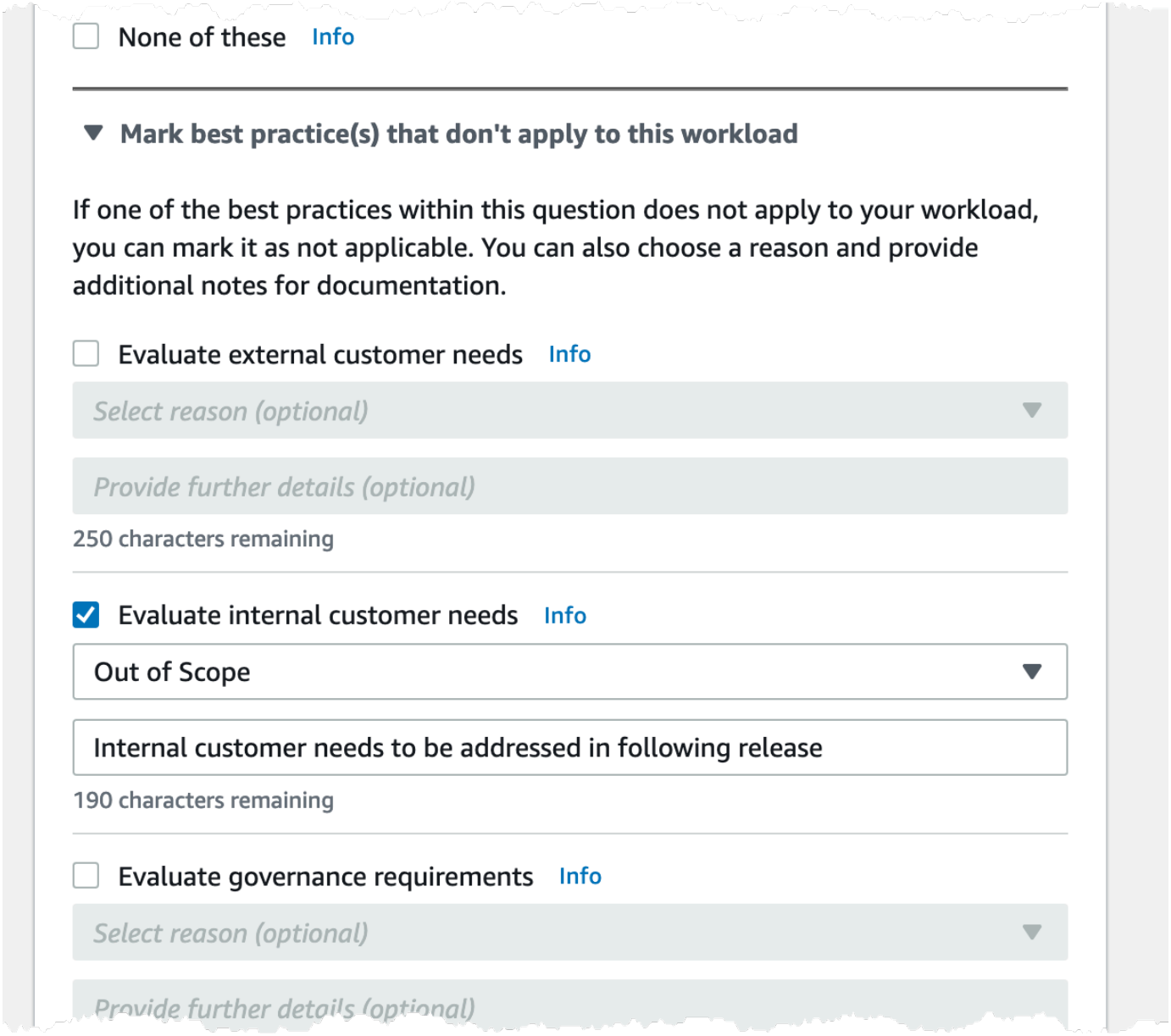
제시된 목록에서 현재 따르고 있는 모범 사례를 질문마다 선택합니다. 모범 사례에 대한 세부 정보가 필요하다면 정보를 선택하여 오른쪽 패널에서 추가 정보 및 리소스를 확인합니다.

전문가에게 물어보기를 선택하여 AWS Well-Architected 전용 AWS re:Post 커뮤니티에 액세스하세요. 이 커뮤니티에서는 AWS에서의 워크로드 설계, 구축, 배포 및 운영과 관련된 질문을 할 수 있습니다.



1. 다음을 선택하여 다음 질문으로 넘어갑니다. 왼쪽 패널에서는 같은 원칙에 속한 다른 질문이나 다른 원칙에 속한 질문으로 이동할 수 있습니다.
2. 질문이 이 워크로드에 적용되지 않음 또는 해당 사항 없음을 선택하는 경우, AWS에서 노트 상자에 이유를 입력하는 것이 좋습니다. 여기에 입력하는 노트는 워크로드 보고서에도 포함되어 앞으로 워크로드가 변경되었을 때 유용하게 사용될 수 있습니다.

> **Note**
>
> 선택적으로 하나 이상의 개별 모범 사례를 해당 사항 없음으로 표시할 수 있습니다. 이 워크로드에 적용되지 않는 모범 사례 표시를 선택하고 적용되지 않는 모범 사례를 선택합니다. 필요한 경우 이유를 선택하고 추가 세부 정보를 제공할 수 있습니다. 적용되지 않는 각 모범 사례에 대해 이 과정을 반복합니다.



> **Note**
>
> 저장 및 종료를 선택하여 언제든지 이 프로세스를 일시 중지할 수 있습니다. 나중에 다시 시작하려면 AWS WA Tool 콘솔을 열고 왼쪽 탐색 창에서 워크로드를 선택합니다.

3. 워크로드의 이름을 선택하여 워크로드 세부 정보 페이지를 엽니다.
4. Continue reviewing(검토 계속)을 선택하고 멈췄던 위치로 이동합니다.

5. 모든 질문에 대답한 후에는 워크로드 개요 페이지가 나타납니다. 여기에서 세부 정보를 검토하거나, 나중에 왼쪽 탐색 창에서 Workloads(워크로드)를 선택한 후 워크로드 이름을 선택하여 이 세부 정보로 이동할 수 있습니다.

처음 워크로드의 상태를 문서화한 후에는 마일스톤을 저장하고 워크로드 보고서를 생성해야 합니다.

마일스톤은 현재 워크로드의 상태를 캡처하기 때문에 사용자가 개선 계획에 따라 워크로드를 변경하면서 진행 상황을 측정할 수 있습니다.

워크로드 세부 정보 페이지에서:

1. 워크로드 개요 섹션에서 마일스톤 저장 버튼을 선택합니다.
2. 마일스톤 이름으로 **`Version 1.0 - initial review`**를 입력합니다.
3. 저장을 선택합니다.
4. 워크로드 보고서를 생성하려면 원하는 렌즈를 선택하고 보고서 생성을 선택합니다. 그러면 PDF 파일이 생성됩니다. 워크로드의 상태, 식별된 위험 수, 제안된 개선 사항 목록이 이 파일에 포함됩니다.

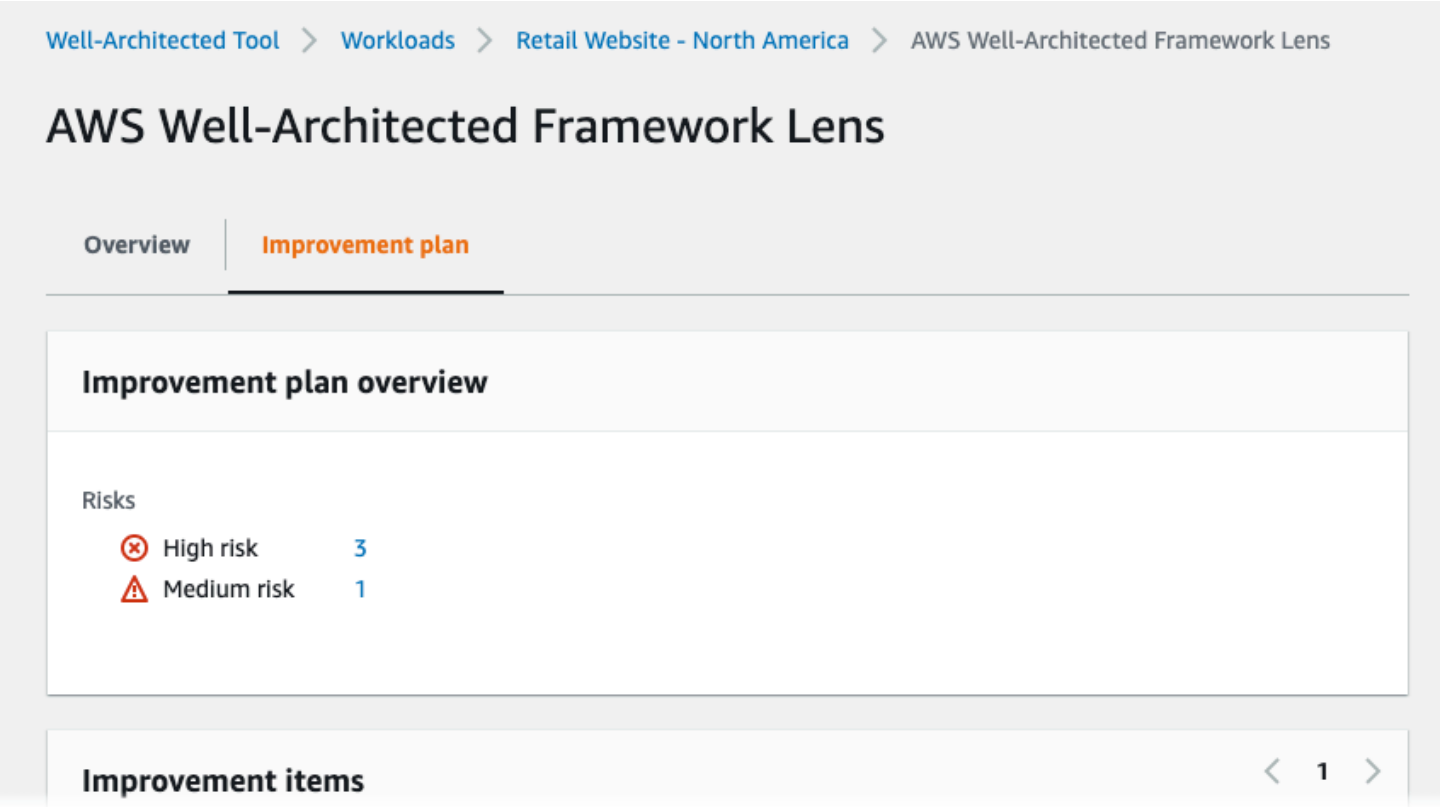
3단계: 개선 계획 검토

AWS WA Tool은 선택한 모범 사례에 따라 AWS Well-Architected Framework 렌즈를 기준으로 위험도가 높음/중간인 영역을 찾습니다.

개선 계획을 검토하려면

1. 개요 페이지의 렌즈 섹션에서 AWS Well-Architected Framework를 선택합니다.
2. 그런 다음 개선 계획을 선택합니다.

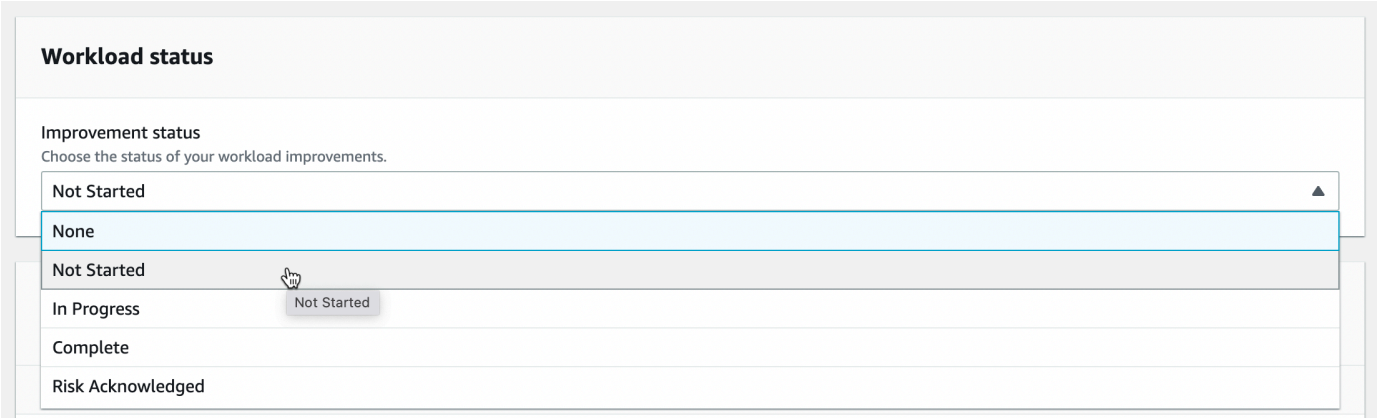
이 특정 예제 워크로드에서는 AWS Well-Architected Framework 렌즈를 통해 위험도 높음 문제 3개와 위험도 중간 문제 1개를 찾았습니다.



워크로드의 개선 상태를 업데이트하여 워크로드 개선이 아직 시작되지 않았음을 나타냅니다.

개선 상태를 변경하려면

1. 개선 계획에서 페이지 상단의 브레드크럼에 있는 워크로드 이름(**`Retail Website - North America`**)을 클릭합니다.
2. 속성 탭을 클릭합니다.
3. 워크로드 상태 섹션으로 이동한 다음 드롭다운 목록에서 시작되지 않음을 선택합니다.



4. 개요 탭을 클릭한 다음 렌즈 섹션에서 AWS Well-Architected Framework 링크를 클릭하여 속성 탭에서 개선 계획으로 돌아갑니다. 그런 다음 페이지 상단의 개선 계획 탭을 클릭합니다.

개선 항목 섹션에는 워크로드에서 식별된 권장 개선 항목이 표시됩니다. 질문은 앞에서 설정한 원칙 우선순위에 따라 순서가 결정되며, 위험도 높음 문제가 위험도 중간 문제보다 먼저 나열됩니다.

Recommended improvement items(권장 개선 항목)를 확장하여 질문에 맞는 모범 사례를 표시합니다. 권장 개선 작업은 각각 자세한 전문가 지침으로 연결되기 때문에 식별된 위험을 제거하거나, 혹은 적어도 완화하는 데 효과적입니다.

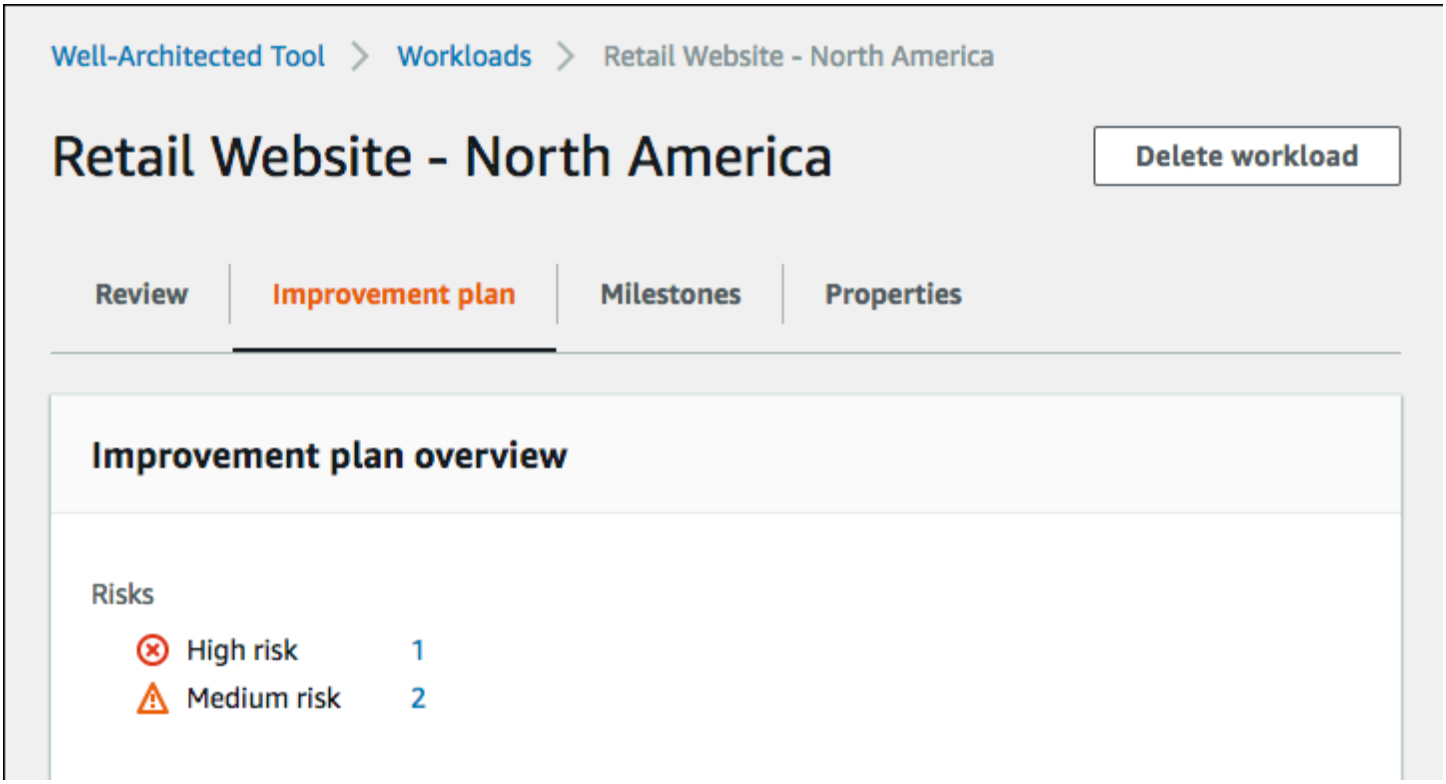
프로필이 워크로드와 연결된 경우 개선 계획 개요 섹션에 우선순위가 지정된 위험 수가 표시되고 프로필별로 우선순위가 지정됨을 선택하여 개선 항목 목록을 필터링할 수 있습니다. 개선 항목 목록에는 우선순위가 지정된 레이블이 표시됩니다.

4단계: 개선 및 진행 상황 측정

이 개선 계획의 일환으로 워크로드에 Amazon CloudWatch 및 AWS Auto Scaling 지원을 추가하여 위험도 높음 문제 하나를 해결했습니다.

개선 항목 섹션:

1. 관련 질문을 선택한 후 선택한 모범 사례를 업데이트하여 변경 사항을 반영합니다. 개선 사항을 기록하기 위한 노트가 추가됩니다.
2. 그런 다음 저장 후 종료를 선택하여 워크로드 상태를 업데이트합니다.
3. 변경을 마친 후 개선 계획으로 돌아가 워크로드 변경 결과를 확인할 수 있습니다. 이 예제에서는 이러한 조치를 통해 위험 프로필이 개선되어 고위험 문제의 수를 3개에서 단 1개로 줄였습니다.



이때 마일스톤을 저장한 후 Milestones(마일스톤)로 이동하여 워크로드가 어떻게 개선되었는지 확인할 수 있습니다.

워크로드

워크로드란 고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음을 말합니다.

워크로드는 단일 AWS 계정 계정에서 리소스 하위 집합으로 구성되거나, 혹은 여러 AWS 계정 계정에 적용되는 다수의 리소스 컬렉션이 될 수도 있습니다. 중소기업은 워크로드가 소수일 수 있지만 대기업에서는 워크로드가 수천 개에 이르기도 합니다.

왼쪽 탐색 창에서 사용할 수 있는 Workloads(워크로드) 페이지는 워크로드 및 사용자와 공유된 워크로드에 대한 정보를 제공합니다.

각 워크로드마다 표시되는 정보는 다음과 같습니다.

명칭

워크로드 이름입니다

소유자

워크로드를 소유하고 있는 AWS 계정 ID입니다.

답변한 질문

답변한 질문 수입니다.

높은 수준의 위험

확인된 HRI(고위험 문제) 수입니다.

중간 수준의 위험

확인된 MRI(중간 위험 문제) 수입니다.

개선 상태

워크로드에 설정되어 있는 개선 상태입니다.

- None
- 시작 안 됨
- 진행 중
- 완료

- 승인된 위험

최종 업데이트 날짜

워크로드가 마지막으로 업데이트된 날짜와 시간입니다.

목록에서 워크로드를 선택한 후 가능한 작업은 다음과 같습니다.

- 워크로드의 세부 정보를 검토하려면 세부 정보 보기를 선택합니다.
- 워크로드의 속성을 변경하려면 편집을 선택합니다.
- 다른 AWS 계정, 사용자 또는 조직 단위(OU)에 대한 워크로드 공유를 관리하려면 세부 정보 보기를 선택한 다음 공유를 선택합니다.
- 워크로드와 워크로드의 마일스톤을 모두 삭제하려면 삭제를 선택합니다. 워크로드의 소유자에게만 삭제 권한이 있습니다.

> **Warning**
>
> 워크로드 삭제는 실행 취소할 수 없습니다. 워크로드와 연결된 데이터까지 모두 삭제됩니다.

HRI(고위험 문제) 및 MRI(중간 위험 문제)

AWS Well-Architected Tool에서 식별된 HRI(고위험 문제)는 AWS에서 발견한 아키텍처 및 운영 선택 사항으로 비즈니스에 상당히 부정적인 영향을 미칠 수 있습니다. 이러한 HRI는 조직 운영, 자산 및 개인에 영향을 미칠 수 있습니다. MRI(중간 위험 문제)도 비즈니스에 부정적인 영향을 미칠 수 있지만, HRI보다 정도는 덜합니다. 이러한 문제는 AWS Well-Architected Tool의 응답을 기반으로 합니다. 해당하는 모범 사례는 AWS 및 AWS 고객에 의해 광범위하게 적용됩니다. 이러한 모범 사례는 AWS Well-Architected Framework 및 렌즈에서 정의한 지침입니다.

> **Note**
>
> 이는 지침일 뿐이며 고객은 모범 사례를 구현하지 않은 경우 비즈니스에 미치는 영향을 평가하고 측정해야 합니다. 특정 기술적 또는 업무상의 이유로 인해 모범 사례를 워크로드에 적용할 수 없는 경우 위험 수준이 표시된 것보다 낮을 수 있습니다. AWS는 고객이 워크로드 노트에 그 이유가 무엇인지, 이러한 이유가 모범 사례에 어떤 영향을 미치는지 문서화하도록 제안합니다. 확인된 모든 HRI 및 MRI에 대해 AWS는 고객이 AWS Well-Architected Tool에 정의된 모범 사례를 구현할 것을 제안합니다. 모범 사례를 구현하면, 모범 사례가 AWS Well-Architected Tool에서 충족된 것으로 표시하여 문제가 해결되었음을 나타냅니다. 고객이 모범 사례를 구현하지

않기로 선택하면, AWS는 해당 비즈니스 수준 승인과 이를 구현하지 않는 이유를 문서화할 것을 제안합니다.

AWS Well-Architected Tool에서 워크로드 정의

워크로드를 정의하는 방법에는 두 가지가 있습니다. AWS WA Tool의 워크로드 페이지에서 템플릿 없이 워크로드를 정의할 수 있습니다. 또는 검토 템플릿 페이지에서 기존 검토 템플릿을 사용하거나 새 템플릿을 생성하여 워크로드를 정의할 수 있습니다.

워크로드 페이지에서 워크로드를 정의하려면

1. 왼쪽 탐색 창에서 워크로드를 선택합니다.
2. 워크로드 정의 드롭다운을 선택합니다.
3. 워크로드 정의를 선택합니다. 또는 검토 템플릿을 생성한 후 이 템플릿에서 워크로드를 정의하려면 검토 템플릿에서 정의를 선택합니다.
4. the section called “워크로드 정의”의 지침에 따라 워크로드 속성을 지정하거나, 원하는 경우 프로필과 렌즈를 적용합니다.

검토 템플릿 페이지에서 워크로드를 정의하려면

1. 왼쪽 탐색 창에서 검토 템플릿을 선택합니다.
2. 기존 검토 템플릿의 이름을 선택하거나, the section called “검토 템플릿 생성”의 지침에 따라 새 검토 템플릿을 생성합니다.
3. 템플릿에서 워크로드 정의를 선택합니다.
4. the section called “템플릿에서 워크로드 정의”의 지침에 따라 검토 템플릿에서 워크로드를 생성합니다.

AWS Well-Architected Tool에서 워크로드 보기

자신이 소유한 워크로드 및 사용자와 공유된 워크로드의 세부 정보를 볼 수 있습니다.

워크로드를 확인하는 방법

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 다음 중 한 가지 방법으로 확인할 워크로드를 선택합니다.
   - 워크로드 이름을 선택합니다.
   - 워크로드와 세부 정보 보기를 차례대로 선택합니다.

워크로드 세부 정보 페이지가 표시됩니다.

> **Note**
>
> 검토 프로세스를 관리하는 기본 담당자 또는 그룹을 쉽게 식별할 수 있도록 하기 위해 필수 필드인 검토 소유자가 추가되었습니다.
> 이 필드가 추가되기 전에 정의된 워크로드를 처음 확인할 때 이 변경에 대한 알림을 받게 됩니다. 편집을 선택하여 검토 소유자 필드를 설정합니다. 이때 추가적인 작업이 필요하지 않습니다.
> 승인을 선택하여 검토 소유자 필드 설정을 연기합니다. 다음 60일 동안 필드가 비어 있음을 알려주는 배너가 표시됩니다. 배너를 제거하려면 워크로드를 편집하고 검토 소유자를 지정합니다.
> 지정된 날짜까지 필드를 설정하지 않으면 워크로드에 대한 액세스가 제한됩니다. 워크로드를 여전히 확인하고 삭제할 수는 있지만 검토 소유자 필드를 설정하는 것을 제외하고는 워크로드를 편집할 수 없습니다. 액세스가 제한되는 동안 워크로드에 대한 공유 액세스는 영향을 받지 않습니다.

AWS Well-Architected Tool에서 워크로드 편집

소유한 워크로드의 세부 정보를 편집할 수 있습니다.

워크로드를 편집하는 방법

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 편집할 워크로드를 선택하고 편집을 선택합니다.
4. 워크로드를 변경합니다.

   각 필드의 설명은 AWS WA Tool에서 워크로드 정의 단원을 참조하세요.

> **Note**
>
> 기존 워크로드를 업데이트할 때 Trusted Advisor를 활성화하여 워크로드 소유자의 IAM 역할을 자동으로 생성할 수 있습니다. Trusted Advisor가 활성화된 워크로드의 연결 계정 소유자는 IAM에서 역할을 생성해야 합니다. 세부 정보는 the section called “IAM에서 Trusted Advisor 활성화”을 참조하세요.

5. 저장을 선택하여 워크로드 변경 사항을 저장합니다.

   필수 입력 필드가 비어있거나, 혹은 지정된 값이 잘못된 경우에는 워크로드 변경 사항을 저장하기 전에 먼저 문제를 해결해야 합니다.

AWS Well-Architected Tool에서 워크로드 공유

소유한 워크로드를 같은 AWS 리전의 다른 AWS 계정, 사용자, 조직 및 조직 단위(OU)에 공유할 수 있습니다.

> **Note**
>
> 워크로드는 동일한 AWS 리전 내에서만 공유할 수 있습니다.
> 다른 AWS 계정에 워크로드를 공유할 때 수신자에게 `wellarchitected:UpdateShareInvitation` 권한이 없으면 수신자가 공유 초대를 수락할 수 없습니다. 권한 정책 예제는 the section called “AWS WA Tool에 대한 액세스 권한 제공” 섹션을 참조하세요.

다른 AWS 계정 및 사용자에게 워크로드를 공유하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 다음 방법 중 하나로 소유한 워크로드를 선택합니다.
   - 워크로드 이름을 선택합니다.
   - 워크로드와 세부 정보 보기를 차례대로 선택합니다.
4. 공유를 선택합니다. 그런 다음 생성 및 사용자 또는 계정에 대한 공유 생성을 선택하여 워크로드 초대를 생성합니다.

5. 워크로드를 공유할 사용자의 12자리 AWS 계정 ID 또는 ARN을 입력합니다.
6. 부여할 권한을 선택합니다.

   읽기 전용

   워크로드에 대한 읽기 전용 액세스를 제공합니다.

   기고자

   답변 및 해당 노트에 대한 업데이트 액세스 및 나머지 워크로드에 대한 읽기 전용 액세스를 제공합니다.
7. 생성을 선택하여 지정된 AWS 계정 또는 사용자에게 워크로드 초대를 보냅니다.

7일 이내에 워크로드 초대를 수락하지 않으면 초대가 자동으로 만료됩니다.

사용자와 사용자의 AWS 계정 모두 워크로드 초대를 받은 경우 가장 높은 수준의 권한을 가진 워크로드 초대가 사용자에게 적용됩니다.

> **Important**
>
> 워크로드를 조직 또는 조직 단위(OU)에 공유하기 전에 AWS Organizations 액세스를 활성화해야 합니다.

워크로드를 조직 또는 OU에 공유하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 다음 방법 중 하나로 소유한 워크로드를 선택합니다.
   - 워크로드 이름을 선택합니다.
   - 워크로드와 세부 정보 보기를 차례대로 선택합니다.
4. 공유를 선택합니다. 그런 다음 생성 및 Organizations에 대한 공유 생성을 선택합니다.
5. 워크로드 공유 생성 페이지에서 전체 조직에 권한을 부여할지 아니면 하나 이상의 OU에 권한을 부여할지 선택합니다.
6. 부여할 권한을 선택합니다.

읽기 전용

워크로드에 대한 읽기 전용 액세스를 제공합니다.

기고자

답변 및 해당 노트에 대한 업데이트 액세스 및 나머지 워크로드에 대한 읽기 전용 액세스를 제공합니다.

7. 생성을 선택하여 워크로드를 공유합니다.

워크로드에 대한 액세스 권한을 공유한 사람을 확인하려면 AWS Well-Architected Tool에서 워크로드 세부 정보 보기 페이지에서 공유를 선택합니다.

엔터티가 워크로드를 공유하지 못하게 하려면 `wellarchitected:CreateWorkloadShare` 작업을 거부하는 정책을 연결합니다.

소유한 사용자 지정 렌즈를 같은 AWS 리전의 다른 AWS 계정, 사용자, 조직 및 OU에 공유할 수도 있습니다. 자세한 내용은 AWS WA Tool에서 사용자 지정 렌즈 공유 섹션을 참조하세요.

AWS Well-Architected Tool 워크로드 공유 시 고려 사항

워크로드는 최대 20개의 서로 다른 AWS 계정 및 사용자와 공유할 수 있습니다. 워크로드는 워크로드와 동일한 AWS 리전에 있는 계정 및 사용자에게만 공유할 수 있습니다.

2019년 3월 20일 이후에 도입된 리전에서 워크로드를 공유하려면 사용자 및 공유를 받은 AWS 계정 모두 AWS Management Console에서 리전을 사용하도록 설정해야 합니다. 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

워크로드를 AWS 계정, 계정의 개별 사용자 또는 둘 모두와 공유할 수 있습니다. AWS 계정와 워크로드를 공유하면 해당 계정의 모든 사용자에게 워크로드에 대한 액세스 권한이 부여됩니다. 계정의 특정 사용자만 액세스가 필요한 경우 최소 권한을 부여하는 모범 사례를 따르고 해당 사용자와 개별적으로 워크로드를 공유합니다.

AWS 계정와 계정의 사용자 모두에게 워크로드 초대가 있는 경우 가장 높은 수준의 권한이 있는 워크로드 초대에 따라 워크로드에 대한 사용자의 권한이 결정됩니다. 사용자에 대한 워크로드 초대를 삭제하면 사용자의 액세스는 AWS 계정의 워크로드 초대에 따라 결정됩니다. 워크로드에 대한 사용자 액세스를 제거하려면 두 워크로드 초대를 모두 삭제합니다.

워크로드를 조직 또는 하나 이상의 조직 단위(OU)에 공유하기 전에 AWS Organizations 액세스를 활성화해야 합니다.

조직 및 하나 이상의 OU에 워크로드를 공유하는 경우 가장 높은 수준의 권한을 가진 워크로드 초대에 따라 해당 워크로드에 대한 계정의 권한이 결정됩니다.

AWS Organizations 공유를 활성화하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. AWS Organizations 지원 활성화를 선택합니다.
4. 설정 저장을 선택합니다.

AWS Well-Architected Tool에서 공유 액세스 삭제

워크로드 초대를 삭제할 수 있습니다. 워크로드 초대를 삭제하면 워크로드에 대한 공유 액세스 권한이 제거됩니다.

워크로드에 대한 공유 액세스를 삭제하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 다음 중 한 가지 방법으로 워크로드를 선택합니다.
   - 워크로드 이름을 선택합니다.
   - 워크로드와 세부 정보 보기를 차례대로 선택합니다.
4. 공유를 선택합니다.
5. 삭제할 워크로드 초대를 선택하고 삭제를 선택합니다.
6. [삭제]를 선택하여 확인합니다.

사용자와 사용자의 AWS 계정에 워크로드 초대가 있는 경우 워크로드에 대한 사용자의 권한을 제거하려면 두 워크로드 초대를 모두 삭제해야 합니다.

AWS Well-Architected Tool에서 공유 액세스 수정

보류 중이거나 수락된 워크로드 초대를 수정할 수 있습니다.

워크로드에 대한 공유 액세스를 수정하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 다음 방법 중 하나로 소유한 워크로드를 선택합니다.
   - 워크로드 이름을 선택합니다.
   - 워크로드와 세부 정보 보기를 차례대로 선택합니다.
4. 공유를 선택합니다.
5. 수정할 워크로드 초대를 선택하고 편집을 선택합니다.
6. AWS 계정 또는 사용자에게 부여할 새 권한을 선택합니다.

   읽기 전용

   워크로드에 대한 읽기 전용 액세스를 제공합니다.

   기고자

   답변 및 해당 노트에 대한 업데이트 액세스 및 나머지 워크로드에 대한 읽기 전용 액세스를 제공합니다.
7. Save(저장)를 선택합니다.

수정된 워크로드 초대가 7일 이내에 수락되지 않으면 자동으로 만료됩니다.

AWS Well-Architected Tool에서 워크로드 초대 수락 및 거부

워크로드 초대는 다른 AWS 계정가 소유한 워크로드를 공유하라는 요청입니다. 워크로드 초대를 수락하면 워크로드 및 대시보드 페이지에 워크로드가 추가됩니다. 워크로드 초대를 거부하면 워크로드 초대 목록에서 제거됩니다.

7일 이내에 워크로드 초대를 수락할 수 있습니다. 7일 이내에 수락하지 않은 초대는 자동으로 만료됩니다.

> **Note**
>
> 워크로드는 동일한 AWS 리전 내에서만 공유할 수 있습니다.

워크로드 초대를 수락하거나 거부하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 Workload invitations(워크로드 초대)를 선택합니다.
3. 수락하거나 거부할 워크로드 초대를 선택합니다.
   - 워크로드 초대를 수락하려면 적용을 선택합니다.

     워크로드가 Workloads(워크로드) 및 대시보드 페이지에 추가됩니다.
   - 워크로드 초대를 거부하려면 거부를 선택합니다.

     워크로드 초대가 목록에서 제거됩니다.

워크로드 초대를 수락한 후 공유 액세스를 거부하려면 해당 워크로드의 AWS Well-Architected Tool에서 워크로드 세부 정보 보기 페이지에서 공유 거부를 선택합니다.

AWS Well-Architected Tool에서 워크로드 삭제

더 이상 필요 없는 워크로드는 삭제할 수 있습니다. 워크로드를 삭제하면 마일스톤 및 워크로드 공유 초대를 포함하여 워크로드와 연결된 모든 데이터가 제거됩니다. 워크로드의 소유자에게만 삭제 권한이 있습니다.

> **Warning**
>
> 워크로드 삭제는 실행 취소할 수 없습니다. 워크로드와 연결된 데이터가 모두 영구적으로 제거됩니다.

워크로드를 삭제하는 방법

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 삭제할 워크로드를 선택하고 삭제를 선택합니다.
4. 삭제 창에서 삭제를 선택하여 워크로드와 마일스톤의 삭제를 확인합니다.

엔티티가 워크로드를 삭제하지 못하게 하려면 `wellarchitected:DeleteWorkload` 작업을 거부하는 정책을 연결합니다.

AWS Well-Architected Tool에서 워크로드 보고서 생성

렌즈에 대한 워크로드 보고서를 생성할 수 있습니다. 보고서에는 워크로드 질문에 대한 응답, 노트, 식별된 현재 위험도 높음 및 중간 수가 포함됩니다. 질문에 식별된 위험이 1개 이상 있으면 이 질문의 개선 계획에 해당 위험을 완화하기 위해 취할 수 있는 조치가 나열됩니다.

워크로드에 연결된 프로필이 있는 경우 프로필 개요 정보와 우선순위가 지정된 위험이 워크로드 보고서에 표시됩니다.

보고서를 생성하면 AWS Well-Architected Tool에 대한 액세스 권한이 없는 다른 사용자들과 워크로드의 세부 정보를 공유할 수 있습니다.

워크로드 보고서를 생성하는 방법

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 원하는 워크로드와 세부 정보 보기를 차례로 선택합니다.
4. 보고서를 생성할 렌즈를 선택하고 Generate report(보고서 생성)를 선택합니다.

   보고서가 생성되어 다운로드하거나 직접 볼 수 있습니다.

AWS Well-Architected Tool에서 워크로드 세부 정보 보기

워크로드 세부 정보 페이지는 워크로드 마일스톤, 개선 계획 및 워크로드 공유를 포함하여 워크로드에 대한 정보를 제공합니다. 페이지 상단에 있는 탭은 다른 세부 정보 섹션으로 이동하는 데 사용됩니다.

워크로드를 삭제하려면 워크로드 삭제를 선택합니다. 워크로드의 소유자에게만 삭제 권한이 있습니다.

공유 워크로드에 대한 액세스 권한을 제거하려면 공유 거부를 선택합니다.

주제

- AWS Well-Architected Tool 개요 탭
- AWS Well-Architected Tool 마일스톤 탭

- AWS Well-Architected Tool 속성 탭
- AWS Well-Architected Tool 공유 탭

AWS Well-Architected Tool 개요 탭

워크로드를 처음에 보면 개요 탭의 정보가 가장 먼저 표시됩니다. 전반적인 워크로드 상태에 이어 각 렌즈의 상태가 이 탭에 표시됩니다.

질문에 아직 모두 답하지 않았다면 배너가 나타나 워크로드를 시작하거나 계속 문서화하도록 알려 줍니다.

워크로드 개요 섹션에는 현재 전체 워크로드의 상태와 이전에 입력한 워크로드 노트가 모두 표시됩니다. 편집을 선택하여 상태 또는 노트를 업데이트합니다.

현재 워크로드의 상태를 캡처하려면 마일스톤 저장을 선택합니다. 마일스톤은 변경이 불가능하기 때문에 저장된 이후에는 바꿀 수 없습니다.

계속해서 워크로드 상태를 문서화하려면 검토 시작을 선택하고 원하는 렌즈를 선택합니다.

AWS Well-Architected Tool 마일스톤 탭

워크로드에 연결된 마일스톤을 표시하려면 마일스톤 탭을 선택합니다.

마일스톤을 선택한 후에는 보고서 생성을 선택하여 마일스톤과 연결된 워크로드 보고서를 생성합니다. 보고서에는 워크로드 질문에 대한 응답, 노트, 마일스톤 저장 시점에 워크로드의 위험도 높음 및 중간 수가 포함됩니다.

특정 마일스톤 시점에서 다음 중 한 가지 방법을 사용해 워크로드 상태에 대한 세부 정보를 확인할 수 있습니다.

- 마일스톤 이름을 선택합니다.
- 원하는 마일스톤과 View milestone(마일스톤 보기)를 차례대로 선택합니다.

AWS Well-Architected Tool 속성 탭

워크로드의 속성을 표시하려면 속성 탭을 선택합니다. 처음에 이러한 속성은 워크로드가 정의될 때 지정된 값입니다. 편집을 선택하여 변경합니다. 워크로드의 소유자에게만 변경 권한이 있습니다.

속성에 대한 자세한 내용은 AWS WA Tool에서 워크로드 정의 섹션을 참조하세요.

AWS Well-Architected Tool 공유 탭

워크로드 초대를 표시하거나 수정하려면 Shares(공유) 탭을 선택합니다. 이 탭은 워크로드 소유자에게만 표시됩니다.

워크로드에 대한 공유 액세스 권한이 있는 각 AWS 계정 및 사용자에게 다음 정보가 표시됩니다.

보안 주체

워크로드에 대한 공유 액세스 권한이 있는 AWS 계정 ID 또는 사용자 ARN입니다.

상태 표시기

워크로드 초대의 상태입니다.

- 보류중

  초대가 수락 또는 거부되기를 기다리고 있습니다. 7일 이내에 워크로드 초대를 수락하지 않으면 자동으로 만료됩니다.

- 수락됨

  초대를 수락했습니다.

- 거부됨

  초대를 거부했습니다.

- 만료됨

  초대가 7일 이내에 수락되거나 거부되지 않았습니다.

권한

AWS 계정 또는 사용자에게 부여된 권한입니다.

- 읽기 전용

  보안 주체는 워크로드에 대한 읽기 전용 액세스 권한을 가집니다.

- 기고자

  보안 주체는 답변과 해당 노트를 업데이트할 수 있으며 나머지 워크로드에 대한 읽기 전용 액세스 권한을 갖습니다.

권한 세부 정보

권한에 대한 자세한 설명입니다.

워크로드를 동일한 AWS 리전의 다른 AWS 계정 또는 사용자와 공유하려면 생성을 선택합니다. 워크로드는 최대 20개의 서로 다른 AWS 계정 및 사용자와 공유할 수 있습니다.

워크로드 초대를 삭제하려면 초대를 선택하고 삭제를 선택합니다.

워크로드 초대를 수정하려면 초대를 선택하고 편집을 선택합니다.

AWS WA Tool에서 렌즈 사용

AWS Well-Architected Tool에서 렌즈를 사용하면 모범 사례를 기준으로 아키텍처를 지속적으로 평가하고 개선할 영역을 파악할 수 있습니다. 워크로드가 정의되면 AWS Well-Architected Framework 렌즈가 자동으로 적용됩니다.

한 워크로드에 하나 이상의 렌즈가 적용될 수 있습니다. 각 렌즈에는 고유한 질문, 모범 사례, 노트 및 개선 계획이 있습니다.

워크로드에 적용할 수 있는 렌즈에는 Lens Catalog 렌즈와 사용자 지정 렌즈라는 두 가지 종류가 있습니다.

- Lens Catalog: AWS에서 생성 및 유지 관리하는 공식 렌즈입니다. Lens Catalog는 모든 사용자가 사용할 수 있으며 사용하기 위해 추가 설치가 필요하지 않습니다.
- 사용자 지정 렌즈: AWS 공식 콘텐츠가 아닌 사용자가 정의한 렌즈입니다. 자체 원칙, 질문, 모범 사례 및 개선 계획을 사용하여 사용자 지정 렌즈를 생성하고 사용자 지정 렌즈를 다른 AWS 계정과 공유할 수 있습니다.

워크로드당 한 번에 5개의 렌즈를 추가할 수 있으며, 워크로드당 최대 20개의 렌즈를 적용할 수 있습니다.

워크로드에서 렌즈를 제거해도 렌즈와 연관된 데이터는 그대로 유지됩니다. 렌즈를 워크로드에 다시 추가하면 데이터가 복원됩니다.

AWS WA Tool에서 워크로드에 렌즈 추가

워크로드에 렌즈를 추가하면 아키텍처의 강점과 약점을 더 잘 이해하고, 개선 사항을 식별하고, 워크로드가 모범 사례를 따르도록 하는 데 도움이 됩니다.

워크로드에 렌즈를 추가하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 원하는 워크로드와 세부 정보 보기를 차례로 선택합니다.
4. 추가할 렌즈를 선택하고 저장을 선택합니다.

   렌즈는 사용자 지정 렌즈, 렌즈 카탈로그 또는 둘 다에서 선택할 수 있습니다.

최대 20개의 렌즈를 워크로드에 추가할 수 있습니다.

AWS Lens Catalog에 대한 자세한 내용은 AWS Well-Architected 렌즈를 참조하세요. Lens Catalog에서 모든 렌즈 백서가 렌즈로 제공되는 것은 아니라는 점에 유의하세요.

> **면책 조항**
>
> 다른 AWS 사용자 또는 계정에서 생성된 사용자 지정 렌즈에 액세스하거나 이를 적용하면 다른 사용자가 생성하여 나에게 공유한 사용자 지정 렌즈가 AWS 고객 계약에 정의된 제3자 콘텐츠임을 인정하는 것으로 간주됩니다.

AWS WA Tool에서 워크로드의 렌즈 제거

렌즈가 더 이상 워크로드와 관련이 없는 경우 제거할 수 있습니다.

워크로드에서 렌즈를 제거하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 워크로드를 선택합니다.
3. 원하는 워크로드와 세부 정보 보기를 차례로 선택합니다.
4. 제거할 렌즈의 선택을 해제하고 저장을 선택합니다.

   AWS Well-Architected Framework 렌즈는 워크로드에서 제거할 수 없습니다.

렌즈와 연관된 데이터는 유지됩니다. 렌즈를 워크로드에 다시 추가하면 데이터가 복원됩니다.

AWS WA Tool에서 워크로드에 대한 렌즈 세부 정보 보기

AWS Well-Architected Tool 콘솔에서 렌즈에 대한 세부 정보를 볼 수 있습니다. 렌즈에 대한 세부 정보를 보려면 렌즈를 선택합니다.

개요 탭

개요 탭에는 답변된 질문 수와 같은 렌즈에 대한 일반 정보가 나와 있습니다. 이 탭에서 워크로드 검토를 계속하거나, 보고서를 생성하거나, 렌즈 노트를 편집할 수 있습니다.

개선 계획 탭

개선 계획 탭에는 워크로드를 개선하기 위한 권장 작업 목록이 나와 있습니다. 위험과 원칙을 기준으로 권장 사항을 필터링할 수 있습니다.

공유 탭

사용자 지정 렌즈의 경우 공유 탭에는 렌즈가 공유된 IAM 보안 주체 목록이 제공됩니다.

AWS WA Tool의 워크로드에 대한 사용자 지정 렌즈

자체 원칙, 질문, 모범 사례 및 개선 계획을 사용하여 사용자 지정 렌즈를 생성할 수 있습니다. AWS 제공 렌즈를 적용하는 것과 같은 방식으로 사용자 지정 렌즈를 워크로드에 적용할 수 있습니다. 자신이 만든 사용자 지정 렌즈를 다른 AWS 계정에 공유할 수도 있고, 다른 사람이 소유한 사용자 지정 렌즈가 나에게 공유될 수도 있습니다.

사용자 지정 렌즈로 특정 기술에 맞게 질문을 조정하거나, 조직 내 거버넌스 요구 사항을 충족하는 데 도움을 주거나, Well-Architected Framework 및 AWS 렌즈에서 제공하는 지침을 확장할 수 있습니다. 기존 렌즈와 마찬가지로 마일스톤을 생성하여 시간 경과에 따른 진행 상황을 추적하고, 보고서를 생성하여 주기적 상태를 제공할 수 있습니다.

주제

AWS WA Tool에서 사용자 지정 렌즈 보기

내가 소유한 사용자 지정 렌즈 및 나에게 공유된 사용자 지정 렌즈의 세부 정보를 볼 수 있습니다.

렌즈를 보려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.

   > **Note**
   >
   > 사용자 지정 렌즈를 생성하지 않았거나 사용자 지정 렌즈를 공유하지 않은 경우 사용자 지정 렌즈 섹션은 비어 있습니다.

3. 확인할 사용자 지정 렌즈를 선택합니다.
   - 내 소유 - 내가 생성한 사용자 지정 렌즈를 보여줍니다.
   - 나와 공유됨 - 나에게 공유된 사용자 지정 렌즈를 보여줍니다.
4. 확인할 사용자 지정 렌즈를 다음 중 한 가지 방법으로 선택합니다.
   - 렌즈의 이름을 선택합니다.
   - 렌즈를 선택하고 세부 정보 보기를 선택합니다.

AWS WA Tool에서 워크로드에 대한 렌즈 세부 정보 보기 페이지가 표시됩니다.

사용자 지정 렌즈 페이지에는 다음과 같은 필드가 있습니다.

명칭

렌즈의 이름입니다.

소유자

사용자 지정 렌즈를 소유한 AWS 계정 ID입니다.

상태 표시기

게시됨 상태는 사용자 지정 렌즈가 게시되었으며 이를 워크로드에 적용하거나 다른 AWS 계정에 공유할 수 있음을 의미합니다.

초안 상태는 사용자 지정 렌즈가 생성되었지만 아직 게시되지 않았음을 의미합니다. 사용자 지정 렌즈를 워크로드에 적용하거나 공유하려면 먼저 게시해야 합니다.

버전

사용자 지정 렌즈의 버전 이름입니다.

최종 업데이트 날짜

사용자 지정 렌즈가 마지막으로 업데이트된 날짜와 시간입니다.

AWS WA Tool에서 워크로드에 대한 사용자 지정 렌즈 생성

사용자 지정 렌즈를 생성하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 사용자 지정 렌즈를 선택합니다.
4. 파일 다운로드 선택하여 JSON 템플릿 파일을 다운로드합니다.
5. 선호하는 텍스트 편집기로 JSON 템플릿 파일을 열고 사용자 지정 렌즈에 대한 데이터를 추가합니다. 이 데이터에는 원칙, 질문, 모범 사례, 개선 계획 링크가 포함됩니다.

   자세한 내용은 AWS WA Tool의 렌즈 형식 사양 섹션을 참조하세요. 사용자 지정 렌즈의 크기는 500KB를 초과할 수 없습니다.
6. 파일 선택을 선택하여 JSON 파일을 선택합니다.
7. (선택 사항) 태그 섹션에서 사용자 지정 렌즈에 연결할 태그를 추가합니다.
8. 사용자 지정 렌즈를 미리 보려면 제출 및 미리 보기기를 선택하고, 미리 보기 없이 사용자 지정 렌즈를 제출하려면 제출을 선택합니다.

   사용자 지정 렌즈 제출 및 미리 보기를 선택한 경우 다음을 선택하여 렌즈 미리 보기를 통해 탐색하거나 미리 보기 종료를 선택하여 사용자 지정 렌즈로 돌아갈 수 있습니다.

검증이 실패하면 JSON 파일을 수정하고 사용자 지정 렌즈를 다시 생성해 보세요.

AWS WA Tool이 JSON 파일의 유효성을 검사하면 사용자 지정 렌즈가 사용자 지정 렌즈에 표시됩니다.

생성된 사용자 지정 렌즈는 초안 상태입니다. 렌즈를 워크로드에 적용하거나 다른 AWS 계정와 공유하려면 먼저 렌즈를 게시해야 합니다.

하나의 AWS 계정에 최대 15개의 사용자 지정 렌즈를 생성할 수 있습니다.

> **면책 조항**
>
> 사용자 지정 렌즈 내에서 또는 렌즈를 통해 최종 사용자 또는 기타 식별 가능한 개인의 개인 식별 정보(PII)를 포함하거나 수집하지 마세요. 내 사용자 지정 렌즈 또는 나에게 공유되어 내 계정에서 사용되는 사용자 지정 렌즈에 PII가 포함되거나 수집되는 경우, 포함된 PII가 관련 법률에 따라 처리되도록 하고, 적절한 개인 정보 보호 고지를 제공하고, 해당 데이터를 처리하는 데 필요한 동의를 얻을 책임은 나에게 있습니다.

AWS WA Tool에서 워크로드에 대한 사용자 지정 렌즈 미리 보기

사용자 지정 렌즈를 미리 보려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 초안 상태의 렌즈만 미리 볼 수 있습니다. 원하는 초안 사용자 지정 렌즈를 선택하고 미리 보기 경험을 선택합니다.
4. 다음을 선택하여 렌즈 미리 보기를 통해 탐색합니다.
5. (선택 사항) 미리 보기의 각 질문 내에서 모범 사례를 선택하여 개선 계획을 검토하고, 답변에 기반하여 업데이트를 선택하여 위험 논리를 테스트할 수 있습니다. 변경이 필요한 경우 게시하기 전에 JSON 템플릿의 위험 규칙을 업데이트할 수 있습니다.
6. 사용자 지정 렌즈로 돌아가려면 미리 보기 종료를 선택합니다.

> **Note**
>
> 사용자 지정 렌즈 생성 시 제출 및 미리 보기를 선택하여 사용자 지정 렌즈를 미리 볼 수도 있습니다.

AWS WA Tool에서 사용자 지정 렌즈를 최초로 게시

사용자 지정 렌즈를 게시하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 원하는 사용자 지정 렌즈를 선택하고 렌즈 게시를 선택합니다.
4. 버전 이름 상자에 버전 변경에 대한 고유 식별자를 입력합니다. 이 값은 최대 32자까지 가능하며 영숫자와 마침표(“.”)만 포함해야 합니다.
5. 사용자 지정 렌즈 게시를 선택합니다.

   사용자 지정 렌즈가 게시된 후에는 게시됨 상태가 됩니다.

이제 사용자 지정 렌즈를 워크로드에 적용하거나 다른 AWS 계정 또는 다른 사용자와 공유할 수 있습니다.

AWS WA Tool에서 사용자 지정 렌즈에 업데이트 게시

기존 사용자 지정 렌즈에 업데이트를 게시하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 원하는 사용자 지정 렌즈를 선택하고 편집을 선택합니다.
4. 업데이트된 JSON 파일이 준비되지 않은 경우 파일 다운로드를 선택하여 현재 사용자 지정 렌즈의 사본을 다운로드하세요. 자주 사용하는 텍스트 편집기로 다운로드된 JSON 파일을 편집하고 원하는 대로 변경합니다.
5. 파일 선택을 선택하여 업데이트된 JSON 파일을 선택하고 제출 및 미리 보기를 선택하여 사용자 지정 렌즈를 미리 보거나 제출을 선택하여 미리 보기를 거치지 않고 사용자 지정 렌즈를 제출하세요.

   사용자 지정 렌즈의 크기는 500KB를 초과할 수 없습니다.

   AWS WA Tool이 JSON 파일의 유효성을 검사하면 사용자 지정 렌즈가 초안 상태로 사용자 지정 렌즈에 표시됩니다.
6. 사용자 지정 렌즈를 다시 선택하고 렌즈 게시를 선택합니다.
7. 게시 전에 변경 사항 검토를 선택하여 사용자 지정 렌즈에 대한 변경 사항이 올바른지 확인하세요. 여기에는 다음과 같은 검증이 포함됩니다.

   - 사용자 지정 렌즈의 이름
   - 원칙 이름

- 새 질문, 업데이트된 질문, 삭제된 질문

다음을 선택합니다.

8. 버전 변경의 유형을 지정합니다.

   메이저 버전

   렌즈가 대폭 변경되었음을 나타냅니다. 사용자 지정 렌즈의 의미에 영향을 미치는 변경에 사용합니다.

   렌즈가 적용된 모든 워크로드에 새 버전의 사용자 지정 렌즈를 이용할 수 있다는 알림이 전송됩니다.

   메이저 버전 변경 사항은 렌즈를 사용하는 워크로드에 자동으로 적용되지 않습니다.

   마이너 버전

   렌즈가 약간 변경되었음을 나타냅니다. 텍스트 변경이나 URL 링크 업데이트와 같은 사소한 변경에 사용합니다.

   마이너 버전 변경 사항은 사용자 지정 렌즈를 사용하는 워크로드에 자동으로 적용됩니다.

   다음을 선택합니다.

9. 버전 이름 상자에 버전 변경에 대한 고유 식별자를 입력합니다. 이 값은 최대 32자까지 가능하며 영숫자와 마침표(“.”)만 포함해야 합니다.
10. 사용자 지정 렌즈 게시를 선택합니다.

    사용자 지정 렌즈가 게시된 후에는 게시됨 상태가 됩니다.

이제 업데이트된 사용자 지정 렌즈를 워크로드에 적용하거나 다른 AWS 계정 또는 다른 사용자와 공유할 수 있습니다.

업데이트가 메이저 버전 변경인 경우 이전 버전의 렌즈가 적용된 모든 워크로드에 새 버전을 사용할 수 있다는 알림이 전송되고 업그레이드 옵션이 제공됩니다.

마이너 버전 업데이트가 알림 없이 자동으로 적용됩니다.

최대 100개의 사용자 지정 렌즈 버전을 생성할 수 있습니다.

AWS WA Tool에서 사용자 지정 렌즈 공유

사용자 지정 렌즈를 다른 AWS 계정, 다른 사용자, AWS Organizations, 조직 단위(OU)에 공유할 수 있습니다.

사용자 지정 렌즈를 다른 AWS 계정 및 다른 사용자와 공유하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 공유할 사용자 지정 렌즈를 선택하고 세부 정보 보기를 선택합니다.
4. AWS WA Tool에서 워크로드에 대한 렌즈 세부 정보 보기 페이지에서 공유를 선택합니다. 그런 다음 생성 및 사용자 또는 계정에 대한 공유 생성을 선택하여 렌즈 공유 초대를 생성합니다.
5. 사용자 지정 렌즈를 공유할 사용자의 12자리 AWS 계정 ID 또는 ARN을 입력합니다.
6. 지정한 AWS 계정 또는 사용자에게 렌즈 공유 초대를 보내려면 생성을 선택합니다.

최대 300명의 AWS 계정 또는 사용자에게 사용자 지정 렌즈를 공유할 수 있습니다.

7일 이내에 렌즈 공유 초대를 수락하지 않으면 초대가 자동으로 만료됩니다.

> **Important**
>
> 사용자 지정 렌즈를 조직 또는 조직 단위(OU)에 공유하기 전에 AWS Organizations 액세스를 활성화해야 합니다.

사용자 지정 렌즈를 조직 또는 OU에 공유하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 공유할 사용자 지정 렌즈를 선택합니다.
4. AWS WA Tool에서 워크로드에 대한 렌즈 세부 정보 보기 페이지에서 공유를 선택합니다. 그런 다음 생성 및 Organizations에 대한 공유 생성을 선택합니다.
5. 사용자 지정 렌즈 공유 생성 페이지에서 전체 조직에 권한을 부여할지 아니면 하나 이상의 OU에 권한을 부여할지 선택합니다.

6. 생성을 선택하여 사용자 지정 렌즈를 공유합니다.

사용자 지정 렌즈에 대한 액세스 권한을 공유한 사람을 확인하려면 AWS WA Tool에서 워크로드에 대한 렌즈 세부 정보 보기 페이지에서 공유를 선택합니다.

> **면책 조항**
>
> 사용자 지정 렌즈를 다른 AWS 계정에 공유하면 AWS가 사용자 지정 렌즈를 다른 계정에서 사용할 수 있도록 승인하는 것으로 간주됩니다. 사용자가 자체 AWS 계정에서 사용자 지정 렌즈를 삭제하거나 AWS 계정를 해지하더라도 이러한 다른 계정에서는 공유된 사용자 지정 렌즈에 계속 액세스하여 사용할 수 있습니다.

AWS WA Tool에서 사용자 지정 렌즈에 태그 추가

사용자 지정 렌즈에 태그를 추가하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 업데이트할 사용자 지정 렌즈를 선택합니다.
4. 태그 섹션에서 태그 관리를 선택합니다.
5. 추가할 각 태그에 대해 새 태그 추가를 선택하고 키와 값을 입력합니다.
6. 저장을 선택합니다.

태그를 제거하려면 제거하려는 태그 옆에 있는제거를 선택합니다.

AWS WA Tool에서 사용자 지정 렌즈 삭제

사용자 지정 렌즈를 삭제하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자 지정 렌즈를 선택합니다.
3. 삭제할 사용자 지정 렌즈를 선택하고 삭제를 선택합니다.
4. 삭제를 선택합니다.

렌즈가 적용된 기존 워크로드에 사용자 지정 렌즈가 삭제되었다는 알림이 전송되지만 계속 사용할 수 있습니다. 새 워크로드에는 더 이상 사용자 지정 렌즈를 적용할 수 없습니다.

> **면책 조항**
>
> 사용자 지정 렌즈를 다른 AWS 계정에 공유하면 AWS가 사용자 지정 렌즈를 다른 계정에서 사용할 수 있도록 승인하는 것으로 간주됩니다. 사용자가 자체 AWS 계정에서 사용자 지정 렌즈를 삭제하거나 AWS 계정를 해지하더라도 이러한 다른 계정에서는 공유된 사용자 지정 렌즈에 계속 액세스하여 사용할 수 있습니다.

AWS WA Tool의 렌즈 형식 사양

렌즈는 특정 JSON 형식을 사용하여 정의됩니다. 사용자 지정 렌즈를 생성하기 시작하면 템플릿 JSON 파일을 다운로드할 수 있습니다. 이 파일은 원칙의 기본 구조, 질문, 모범 사례, 개선 계획을 정의하므로 사용자 지정 렌즈의 기반으로 사용할 수 있습니다.

렌즈 섹션

이 섹션에서는 사용자 지정 렌즈 자체의 속성을 정의합니다. 다음은 속성의 이름과 설명입니다.

- `schemaVersion`: 사용할 사용자 지정 렌즈 스키마의 버전입니다. 템플릿에 의해 설정되므로 변경하지 마세요.
- `name`: 렌즈의 이름입니다. 이름은 최대 128자까지 지정할 수 있습니다.
- `description`: 렌즈에 대한 텍스트 설명입니다. 이 텍스트는 워크로드 생성 중에 추가할 렌즈를 선택하거나 나중에 기존 워크로드에 적용할 렌즈를 선택할 때 표시됩니다. 설명은 최대 2048자까지 작성할 수 있습니다.

```
   "schemaVersion": "2021-11-01",
   "name": "Company Policy ABC",
   "description": "This lens provides a set of specific questions to assess compliance
with company policy ABC-2021 as revised on 2021/09/01.",
```

원칙 섹션

이 섹션에서는 사용자 지정 렌즈와 관련된 원칙을 정의합니다. 질문을 AWS Well-Architected Framework의 원칙에 매핑하거나, 자체 원칙을 정의하거나, 두 작업을 모두 수행할 수 있습니다.

사용자 지정 렌즈 하나에는 최대 10개의 원칙을 정의할 수 있습니다.

- id: 원칙의 ID입니다. ID에는 3~128자까지 사용 가능하며 영숫자 및 밑줄('_') 문자만 포함할 수 있습니다. 원칙에 사용되는 ID는 고유해야 합니다.

  질문을 Framework의 원칙에 매핑할 때는 다음 ID를 사용하세요.

  - operationalExcellence
  - security
  - reliability
  - performance
  - costOptimization
  - sustainability
- name: 원칙의 이름입니다. 이름은 최대 128자까지 지정할 수 있습니다.

```
    "pillars": [
       {
           "id": "company_Privacy",
           "name": "Privacy Excellence",
           .
           .
           .
       },
       {
           "id": "company_Security",
           "name": "Security",
           .
           .
           .
       }
    ]
```

질문 섹션

이 섹션에서는 원칙과 관련된 질문을 정의합니다.

사용자 지정 렌즈에서는 원칙에 최대 20개의 질문을 정의할 수 있습니다.

- `id`: 질문의 ID입니다. ID에는 3~128자까지 사용 가능하며 영숫자 및 밑줄('_') 문자만 포함할 수 있습니다. 질문에 사용되는 ID는 고유해야 합니다.
- `title`: 질문의 제목입니다. 제목은 최대 128자까지 지정할 수 있습니다.
- `description`: 질문을 더 자세히 설명합니다. 설명은 최대 2048자까지 작성할 수 있습니다.
- `helpfulResource displayText`: 선택 사항입니다. 질문에 대한 유용한 정보를 제공하는 텍스트입니다. 텍스트는 최대 2048자까지 작성할 수 있습니다. `helpfulResource url`을 지정하는 경우 이 텍스트도 지정해야 합니다.
- `helpfulResource url`: 선택 사항입니다. 질문을 더 자세히 설명하는 URL 리소스입니다. URL은 `http://` 또는 `https://`로 시작해야 합니다.

> **Note**
>
> 사용자 지정 렌즈 워크로드를 Jira와 동기화할 때 질문에는 질문의 "id"와 "title"이 모두 표시됩니다.
>
> Jira 티켓에 사용된 형식은 `[ QuestionID ] QuestionTitle`입니다.

```
"questions": [
    {
        "id": "privacy01",
        "title": "How do you ensure HR conversations are private?",
        "description": "Career and benefits discussions should occur on secure channels
 only and be audited regularly for compliance.",
        "helpfulResource": {
            "displayText": "This is helpful text for the first question",
            "url": "https://example.com/poptquest01_help.html"
        },
        .
        .
        .
    },
    {
        "id": "privacy02",
```

```
        "title": "Is your team following the company privacy policy?",
        "description": "Our company requires customers to opt-in to data use and does
 not disclose customer data to third parties either individually or in aggregate.",
        "helpfulResource": {
            "displayText": "This is helpful text for the second question",
            "url": "https://example.com/poptquest02_help.html"
        },
        .
        .
        .
    }
]
```

선택 항목 섹션

이 섹션에서는 질문과 관련된 선택 항목을 정의합니다.

사용자 지정 렌즈에서는 질문에 최대 15개의 선택 항목을 정의할 수 있습니다.

- `id`: 선택 항목의 ID입니다. ID에는 3~128자까지 사용 가능하며 영숫자 및 밑줄('_') 문자만 포함할 수 있습니다. 질문의 각 선택 항목에 대해 고유한 ID를 지정해야 합니다. 접미사가 _no인 선택 항목을 추가하면 질문에 대한 `None of these` 선택 항목으로 작동합니다.
- `title`: 선택 항목의 제목입니다. 제목은 최대 128자까지 지정할 수 있습니다.
- `helpfulResource displayText`: 선택 사항입니다. 선택 항목에 대한 유용한 정보를 제공하는 텍스트입니다. 텍스트는 최대 2048자까지 작성할 수 있습니다. `helpfulResource url`이 지정된 경우 텍스트를 포함해야 합니다.
- `helpfulResource url`: 선택 사항입니다. 선택 항목을 더 자세히 설명하는 URL 리소스입니다. URL은 `http://` 또는 `https://`로 시작해야 합니다.
- `improvementPlan displayText`: 선택 항목을 개선할 수 있는 방법을 설명하는 텍스트입니다. 텍스트는 최대 2048자까지 작성할 수 있습니다. `None of these` 선택 항목을 제외한 각 선택 항목에는 `improvementPlan`이 필요합니다.
- `improvementPlan url`: 선택 사항입니다. 개선에 도움이 될 수 있는 URL 리소스입니다. URL은 `http://` 또는 `https://`로 시작해야 합니다.
- `additionalResources type`: 선택 사항입니다. 추가 리소스 유형입니다. 이때 값은 `HELPFUL_RESOURCE` 또는 `IMPROVEMENT_PLAN`이 될 수 있습니다.
- `additionalResources content`: 선택 사항입니다. 추가 리소스의 `displayText` 및 `url` 값을 지정합니다. 선택 항목에 최대 5개의 유용한 추가 리소스와 최대 5개의 추가 개선 계획 항목을 지정할 수 있습니다.

- `displayText`: 선택 사항입니다. 유용한 리소스 또는 개선 계획을 설명하는 텍스트입니다. 텍스트는 최대 2048자까지 작성할 수 있습니다. `url`이 지정된 경우 텍스트를 포함해야 합니다.
- `url`: 선택 사항입니다. 유용한 리소스 또는 개선 계획을 위한 URL 리소스입니다. URL은 `http://` 또는 `https://`로 시작해야 합니다.

> **Note**
>
> 사용자 지정 렌즈 워크로드를 Jira와 동기화할 때 선택 항목에는 질문 및 선택 항목의 "id"와 선택 항목의 "title"이 표시됩니다.
> 사용된 형식은 `[ QuestionID | ChoiceID ] ChoiceTitle`입니다.

```
   "choices": [
        {
            "id": "choice_1",
            "title": "Option 1",
            "helpfulResource": {
                "displayText": "This is helpful text for the first choice",
                "url": "https://example.com/popt01_help.html"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt01_iplan.html"
            }
        },
        {
            "id": "choice_2",
            "title": "Option 2",
            "helpfulResource": {
                "displayText": "This is helpful text for the second choice",
                "url": "https://example.com/hr_manual_CORP_1.pdf"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt02_iplan_01.html"
            },
            "additionalResources":[
               {
```

```
                "type": "HELPFUL_RESOURCE",
                "content": [
                  {
                    "displayText": "This is the second set of helpful text for this
choice.",
                    "url": "https://example.com/hr_manual_country.html"
                  },
                  {
                    "displayText": "This is the third set of helpful text for this
choice.",
                    "url": "https://example.com/hr_manual_city.html"
                  }
                ]
              },
              {
                "type": "IMPROVEMENT_PLAN",
                "content": [
                  {
                    "displayText": "This is additional text that will be shown for
improvement of this choice.",
                    "url": "https://example.com/popt02_iplan_02.html"
                  },
                  {
                    "displayText": "This is the third piece of improvement plan
text.",
                    "url": "https://example.com/popt02_iplan_03.html"
                  }
                  {
                    "displayText": "This is the fourth piece of improvement plan
text.",
                    "url": "https://example.com/popt02_iplan_04.html"
                  }
                ]
              }
            ]
        },
        {
            "id": "option_no",
            "title": "None of these",
            "helpfulResource": {
              "displayText": "Choose this if your workload does not follow these best
practices.",
              "url": "https://example.com/popt02_iplan_none.html"
            }
```

```
        }
```

위험 규칙 섹션

이 섹션에서는 선택한 선택 항목이 위험 수준을 결정하는 방법을 정의합니다.

각 위험 수준에 하나씩, 질문당 최대 3개의 위험 규칙을 정의할 수 있습니다.

- `condition`: 질문의 위험 수준에 매핑되는 선택 항목의 부울 표현식으로, 해당 사항이 없는 경우 `default` 값이 지정됩니다.

  각 질문에는 `default` 위험 규칙이 있어야 합니다.
- `risk`: 조건과 관련된 위험을 나타냅니다. 유효한 값은 `HIGH_RISK`, `MEDIUM_RISK`, `NO_RISK`입니다.

위험 규칙의 순서는 중요합니다. 첫 번째 `condition`은 `true`로 평가되며 질문에 대한 위험 수준을 설정합니다. 위험 규칙을 구현하는 일반적인 패턴은 위험이 가장 적은(일반적으로 가장 세분화된) 규칙에서 시작하여 가장 위험한(가장 구체적이지 않은) 규칙 순서로 적용하는 것입니다.

예시:

```
"riskRules": [
      {
        "condition": "choice_1 && choice_2 && choice_3",
        "risk": "NO_RISK"
      },
      {
        "condition": "((choice_1 || choice_2) && choice_3) || (!choice_1 &&
choice_3)",
        "risk": "MEDIUM_RISK"
      },
      {
        "condition": "default",
        "risk": "HIGH_RISK"
      }
]
```

질문에 세 가지 선택 항목(choice_1,choice_2, choice_3)이 있는 경우 이러한 위험 규칙의 결과는 다음과 같습니다.

- 세 가지 선택 항목을 모두 선택해도 위험은 없습니다.
- choice_1 또는 choice_2 중 하나가 선택된 상태에서 choice_3이 선택된 경우 위험 수준은 중간입니다.
- choice_1이 선택되지 않은 상태에서 choice_3이 선택된 경우 역시 위험 수준이 중간입니다.
- 위 조건 중 어느 것에도 해당하지 않으면 높은 위험입니다.

AWS WA Tool의 렌즈 업그레이드

AWS Well-Architected Framework 렌즈 및 기타 AWS 제공 렌즈는 새로운 서비스가 도입되고 클라우드 기반 시스템의 기존 모범 사례가 개선되며 새로운 모범 사례가 추가됨에 따라 업데이트됩니다. 새로운 버전의 렌즈를 사용할 수 있게 되면 최신 모범 사례를 반영하도록 AWS WA Tool이 업그레이드됩니다. 정의된 모든 새 워크로드는 새 버전의 렌즈를 사용합니다.

워크로드에 적용한 사용자 지정 렌즈 또는 검토 템플릿에 새 메이저 버전이 게시된 경우에도 렌즈 업그레이드가 이루어집니다.

렌즈 업그레이드는 다음과 같은 조합으로 구성될 수 있습니다.

- 새로운 질문 또는 모범 사례 추가
- 이전의 질문 또는 더 이상 권장되지 않는 사례 제거
- 기존 질문 또는 모범 사례 업데이트
- 원칙 추가 또는 제거

기존 질문에 대한 답변은 그대로 유지됩니다.

> **Note**
>
> 렌즈 업그레이드는 취소할 수 없습니다. 워크로드를 최신 렌즈 버전으로 업그레이드한 후에는 이전 버전의 렌즈로 돌아갈 수 없습니다.

AWS WA Tool에서 업그레이드할 렌즈 결정

알림 페이지를 보면 최신 렌즈 버전을 사용하지 않는 워크로드를 찾을 수 있습니다.

각 워크로드의 알림 페이지에 표시되는 정보는 다음과 같습니다.

리소스

워크로드 또는 검토 템플릿의 이름입니다.

리소스 유형

리소스의 유형입니다. 워크로드 또는 검토 템플릿 중 하나일 수 있습니다.

연결된 리소스

렌즈의 이름입니다.

알림 유형

업그레이드 알림 유형

- 최신 버전이 아님 – 해당 워크로드에서 사용하고 있는 렌즈 버전이 더 이상 최신이 아닙니다. 더 나은 지침을 위해 최신 렌즈 버전으로 업그레이드하세요.
- 사용되지 않음 – 해당 워크로드에서 사용하고 있는 렌즈 버전이 더 이상 모범 사례를 반영하지 않습니다. 최신 렌즈 버전으로 업그레이드하세요.
- 삭제됨 – 워크로드가 소유자가 삭제한 렌즈를 사용하고 있습니다.

사용 중인 버전

현재 워크로드에 사용되는 렌즈 버전입니다.

현재 사용 가능한 버전

렌즈 버전을 업그레이드할 수 있으며, 렌즈가 삭제된 경우에는 없음입니다.

워크로드에 연결된 렌즈를 업그레이드하려면, 워크로드를 선택하고 렌즈 버전 업그레이드를 선택합니다.

AWS WA Tool에서 렌즈 업그레이드

워크로드 및 검토 템플릿에 맞게 렌즈를 업그레이드할 수 있습니다.

> **Note**
>
> 렌즈 업그레이드는 취소할 수 없습니다. 워크로드 또는 검토 템플릿을 최신 렌즈 버전으로 업그레이드한 후에는 이전 버전의 렌즈로 돌아갈 수 없습니다.

워크로드에 맞게 렌즈 업그레이드

1. 알림 페이지에서 업그레이드할 워크로드를 선택하고 렌즈 버전 업그레이드를 선택합니다. 각 원칙의 변경 사항에 대한 정보가 표시됩니다.

   > **Note**
   >
   > 워크로드 개요 탭에서 사용 가능한 업그레이드 보기 선택할 수도 있습니다.

2. 렌즈를 워크로드에 맞게 업그레이드하기 전에 마일스톤이 생성되어 향후 참조를 위한 기존 워크로드의 상태가 저장됩니다. 마일스톤 이름 필드에 고유한 마일스톤 이름을 입력합니다.
3. 이러한 변경 사항을 이해하고 이를 수락함 옆에 있는 확인 상자를 선택하고 저장을 선택합니다.

렌즈가 업그레이드되면 마일스톤 탭에서 이전 버전의 렌즈를 볼 수 있습니다.

검토 템플릿에 맞게 렌즈 업그레이드

1. 검토 템플릿에 맞게 렌즈를 업그레이드하려면
2. 알림 페이지에서 업그레이드할 검토 템플릿을 선택하고 렌즈 버전 업그레이드를 선택합니다. 각 원칙의 변경 사항에 대한 정보가 표시됩니다.

   > **Note**
   >
   > 검토 템플릿 개요 탭에서 사용 가능한 업그레이드 보기를 선택할 수도 있습니다.

3. 이러한 변경 사항을 이해하고 이를 수락함 옆에 있는 확인 상자를 선택하고 템플릿 답변 업그레이드 및 수정을 선택하여 검토 템플릿의 모범 사례 질문에 대한 답변을 조정하거나, 업그레이드를 선택하여 템플릿 답변 조정 없이 렌즈를 업그레이드하세요.

AWS WA Tool에 대한 Lens Catalog

Lens Catalog는 최신 기술과 업계 중심 모범 사례를 제공하는 AWS Well-Architected Tool 내 공식 생성 AWS 렌즈 모음입니다. 이러한 렌즈는 모든 사용자가 사용할 수 있으며 사용하기 위해 추가 설치가 필요하지 않습니다.

다음 표에는 현재 Lens Catalog에 나와 있는 모든 AWS 공식 렌즈가 설명되어 있습니다.

렌즈 이름	설명
AWS Well-Architected 프레임워크	기본적으로 모든 워크로드에 적용됩니다. 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적이며 지속 가능한 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례 모음입니다.
커넥티드 모빌리티	기술을 운송 시스템에 통합하고 전반적인 모빌리티 경험을 향상시키는 모범 사례입니다.
컨테이너 구축	컨테이너 설계 및 구축 프로세스에 대한 모범 사례를 제공합니다.
데이터 분석	AWS가 실제 사례 연구에서 수집한 통찰력을 포함하며, 개선을 위한 권장 사항과 함께 Well-Architected 분석 워크로드의 주요 설계 요소를 배울 수 있습니다.
DevOps	모든 규모의 조직이 최신 기술과 DevOps 모범 사례를 사용하여 상당한 비즈니스 가치를 제공할 수 있는 고속의 보안 중심 문화를 조성하기 위해 따를 수 있는 구조화된 접근 방식을 설명합니다.
금융 서비스 산업	AWS에서 금융 서비스 산업 워크로드를 설계하는 모범 사례입니다.
생성형 AI	AWS에서 생성형 AI 워크로드를 설계하는 모범 사례입니다.
정부	AWS에서 정부 서비스를 설계하고 제공하는 모범 사례입니다.
의료 산업 렌즈	AWS 클라우드에서 의료 워크로드를 설계, 배포, 관리하는 방법에 대한 모범 사례 및 지침입니다.
IoT	AWS의 사물 인터넷(IoT) 애플리케이션 관리에 대한 모범 사례입니다.

렌즈 이름	설명
합병 및 인수	인수합병 중에 클라우드로 워크로드 통합 및 마이그레이션을 위한 모범 사례입니다.
기계 학습	AWS의 기계 학습 리소스 및 워크로드 관리에 대한 모범 사례입니다.
마이그레이션	AWS 클라우드로 마이그레이션하는 방법에 대한 모범 사례입니다.
SaaS	AWS 클라우드의 서비스형 소프트웨어(SaaS) 워크로드를 구상하고, 배포하고, 설계하는 데 중점을 둡니다.
SAP	AWS 클라우드의 SAP 워크로드에 대한 설계 원칙 및 모범 사례입니다.
서버리스 애플리케이션	AWS에서 서버리스 워크로드를 구축하는 것에 대한 모범 사례입니다. RESTful 마이크로서비스, 모바일 앱 백엔드, 스트림 처리, 웹 애플리케이션과 같은 시나리오에 적용됩니다.

AWS WA Tool에서 템플릿 검토

Well-Architected Framework에 대한 미리 채워진 답변과 사용자 지정 렌즈 모범 사례 질문이 포함된 검토 템플릿을 AWS WA Tool에서 생성할 수 있습니다. Well-Architected 검토 템플릿을 사용하면 Well-Architected 검토를 수행할 때 여러 워크로드에서 공통적으로 발생하는 모범 사례에 대해 동일한 답변을 수동으로 입력할 필요가 없으며, 팀과 워크로드 전반에서 모범 사례의 일관성과 표준화를 촉진하는 데 도움이 됩니다.

검토 템플릿을 생성하여 일반적인 모범 사례 질문에 답하거나 노트를 생성하여 다른 IAM 사용자나 계정 또는 같은 AWS 리전의 조직 또는 조직 단위에 공유할 수 있습니다. 검토 템플릿에서 워크로드를 정의하면 일반적인 모범 사례를 확장하고 워크로드 전반의 중복을 줄이는 데 도움이 됩니다.

AWS WA Tool에서 검토 템플릿 생성

검토 템플릿을 생성하려면

1. 왼쪽 탐색 창에서 검토 템플릿을 선택합니다.
2. 템플릿 생성을 선택합니다.
3. 템플릿 세부 정보 지정 페이지에서 검토 템플릿의 이름 및 설명을 입력합니다.
4. (선택 사항) 템플릿 노트 및 태그 섹션에서 검토 템플릿과 연결할 템플릿 노트 또는 태그를 추가합니다. 추가된 모든 노트는 검토 템플릿을 사용하는 모든 워크로드에 적용되지만 태그는 검토 템플릿에만 적용됩니다.

   태그에 대한 자세한 내용은 AWS WA Tool 리소스에 태그 지정 섹션을 참조하세요.
5. 다음을 선택합니다.
6. 렌즈 적용 페이지에서 검토 템플릿에 적용할 렌즈를 선택합니다. 적용할 수 있는 최대 렌즈 수는 20개입니다.

   렌즈는 사용자 지정 렌즈, Lens Catalog 또는 둘 다에서 선택할 수 있습니다.

   > **Note**
   >
   > 나에게 공유된 렌즈는 검토 템플릿에 적용할 수 없습니다.

7. 템플릿 생성을 선택합니다.

방금 생성한 검토 템플릿에 대한 질문에 답변을 시작하려면

1. 템플릿 개요 탭으로 이동해 질문에 대한 답변 시작하기 정보 알림의 질문에 답변하기 드롭다운에서 렌즈를 선택합니다.

   > **Note**
   >
   > 렌즈 섹션으로 이동하여 렌즈를 선택하고 질문에 답변하기를 선택할 수도 있습니다.

2. 검토 템플릿에 적용된 각 렌즈에 대해 해당하는 질문에 답변하고, 답변을 완료하면 저장 및 종료를 선택합니다.

검토 템플릿을 생성한 후에는 이 템플릿에서 새 워크로드를 정의할 수 있습니다.

검토 템플릿의 개요 탭에는 템플릿 세부 정보 섹션에서 답변한 질문의 총 개수와 렌즈 섹션의 각 렌즈에 대해 답변한 질문의 총 개수가 반영되어야 합니다.

AWS WA Tool에서 검토 템플릿 편집

검토 템플릿을 편집하려면

1. 왼쪽 탐색 창에서 검토 템플릿을 선택합니다.
2. 편집하려는 검토 템플릿의 이름을 선택합니다.
3. 검토 템플릿의 이름, 설명 또는 템플릿 노트를 업데이트하려면 개요 탭의 템플릿 세부 정보 섹션에서 편집을 선택합니다.
   a. 이름, 설명 또는 템플릿 노트를 수정합니다.
   b. 템플릿 저장을 선택하여 검토 템플릿에 변경 사항을 업데이트합니다.
4. 검토 템플릿에 적용할 렌즈를 업데이트하려면 개요 탭의 렌즈 섹션에서 적용 렌즈 편집을 선택합니다.
   a. 추가 또는 제거하려는 렌즈의 확인란을 선택하거나 선택 취소합니다.

      렌즈는 사용자 지정 렌즈, Lens Catalog 또는 둘 다에서 선택하거나 선택 취소할 수 있습니다.

   b. 템플릿 저장을 선택하여 변경 사항을 저장합니다.
5. 렌즈의 모범 사례 질문에 대한 답변을 업데이트하려면 개요 탭의 렌즈 섹션에서 렌즈 이름을 선택합니다.
   a. 렌즈 개요 섹션에서 질문에 답변하기를 선택합니다.

> **Note**
>
> 원하는 경우 왼쪽 탐색 창의 검토 템플릿 드롭다운에서 렌즈 이름을 선택하여 렌즈 개요 섹션으로 이동할 수도 있습니다.

b. 변경하려는 모범 사례 답변 옆의 확인란을 선택하거나 선택 해제합니다.

c. 변경 내용을 저장하려면 저장을 선택합니다.

AWS WA Tool에서 검토 템플릿 공유

검토 템플릿은 사용자 또는 계정에 공유하거나 전체 조직 또는 조직 단위에 공유할 수 있습니다.

검토 템플릿을 공유하려면

1. 왼쪽 탐색 창에서 검토 템플릿을 선택합니다.
2. 공유하려는 검토 템플릿의 이름을 선택합니다.
3. 공유 탭을 선택합니다.
4. 사용자 또는 계정에 공유하려면 생성을 선택하고 IAM 사용자 또는 계정에 공유를 선택합니다. 초대 전송 상자에서 사용자 또는 계정 ID를 지정하고 생성을 선택합니다.
5. 조직 또는 조직 단위에 공유하려면 생성을 선택하고 Organizations와 공유를 선택합니다. 전체 조직에 공유하려면 전체 조직에 권한 부여를 선택합니다. 조직 단위에 공유하려면 개별 조직 단위 권한 부여를 선택하고 상자에서 조직 단위를 지정한 다음 생성을 선택합니다.

> **Important**
>
> 조직 또는 조직 단위(OU)에 프로필을 공유하기 전에 AWS Organizations 액세스를 활성화해야 합니다.

AWS WA Tool의 템플릿에서 워크로드 정의

내가 생성한 검토 템플릿 또는 나에게 공유된 검토 템플릿에서 워크로드를 정의할 수 있습니다. 삭제된 검토 템플릿에서는 새 워크로드를 정의할 수 없으며, 검토 템플릿에 오래된 버전의 렌즈가 포함되어 있는 경우, 검토 템플릿에서 새 워크로드를 정의하려면 먼저 검토 템플릿을 업그레이드해야 합니다. 검토

템플릿 업그레이드 방법에 대한 자세한 내용은 the section called “렌즈 업그레이드” 섹션을 참조하세요.

> **Note**
>
> 검토 템플릿에서 워크로드를 정의하려면 워크로드를 생성할 수 있는 IAM 권한인 `wellarchitected:CreateWorkload`가 활성화되어 있어야 합니다. 또한 `wellarchitected:GetReviewTemplate`, `wellarchitected:GetReviewTemplateAnswer`, `wellarchitected:ListReviewTemplateAnswers`, `wellarchitected:GetReviewTemplateLensReview`와 같은 검토 템플릿 권한도 있어야 합니다. IAM 권한에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서를 참조하세요.

검토 템플릿에서 워크로드를 정의하려면

1. 왼쪽 탐색 창에서 검토 템플릿을 선택합니다.
2. 워크로드를 정의하려는 검토 템플릿의 이름을 선택합니다.
3. 템플릿에서 워크로드 정의를 선택합니다.

   > **Note**
   >
   > 워크로드 페이지의 워크로드 정의 드롭다운에서 검토 템플릿에서 정의를 선택할 수도 있습니다.

4. 검토 템플릿 선택 단계에서 검토 템플릿 카드를 선택하고 다음을 선택합니다.
5. 속성 지정 단계에서 워크로드 속성의 필수 필드를 채우고 다음을 선택합니다. 자세한 내용은 the section called “워크로드 정의” 섹션을 참조하세요.
6. (선택 사항) 프로필 적용 단계에서 기존 프로필을 선택하거나, 프로필 이름을 검색하거나, 프로필 생성을 선택하여 프로필을 생성해 워크로드에 프로필을 연결합니다. Next(다음)를 선택합니다.

   Well-Architected 프로필과 검토 템플릿을 함께 사용할 수 있습니다. 검토 템플릿에 미리 입력된 질문에 대한 답변은 워크로드 내에서 그대로 유지되며 프로필에 따라 질문의 우선순위가 정해집니다.
7. (선택 사항) 렌즈 적용 단계에서 검토 템플릿에 아직 적용되지 않은 추가 렌즈를 사용자 지정 렌즈 또는 Lens Catalog에서 적용하도록 선택할 수 있습니다.

8. 워크로드 정의를 선택합니다.

AWS WA Tool에서 검토 템플릿 삭제

검토 템플릿을 삭제하려면

1. 왼쪽 탐색 창에서 검토 템플릿을 선택합니다.
2. 검토 템플릿 섹션에서 삭제하려는 검토 템플릿을 선택하고 작업 드롭다운에서 삭제를 선택합니다.

> **Note**
>
> 템플릿 이름을 선택하고 검토 템플릿 개요 탭에서 삭제를 선택할 수도 있습니다.

3. 검토 템플릿 삭제 대화 상자에서 필드에 검토 템플릿 이름을 입력하여 삭제를 확인합니다.
4. Delete(삭제)를 선택합니다.

삭제된 검토 템플릿에서는 새 워크로드를 생성할 수 없습니다. 삭제한 검토 템플릿을 다른 IAM 사용자, 계정 또는 조직에 공유한 경우 해당 검토 템플릿에서 워크로드를 생성할 수 없습니다.

AWS WA Tool에서 프로파일 사용

프로필을 생성하여 비즈니스 컨텍스트를 제공하고 Well-Architected 검토를 수행할 때 달성하고자 하는 목표를 식별할 수 있습니다. AWS Well-Architected Tool은 프로필에서 수집한 정보를 사용하여 워크로드 검토 중에 비즈니스와 관련된 우선순위가 지정된 질문 목록에 집중할 수 있습니다. 워크로드에 프로필을 연결하면 개선 계획을 통해 해결해야 할 위험의 우선순위를 확인하는 데도 도움이 됩니다.

프로필 페이지에서 프로필을 생성하여 새 워크로드에 연결하거나 기존 워크로드에 프로필을 추가할 수 있습니다.

프로필 생성

프로필을 생성하려면

1. 왼쪽 탐색 창에서 프로필을 선택합니다.
2. 프로필 생성을 선택합니다.
3. 프로필 속성 섹션에서 프로필의 이름과 설명을 입력합니다.
4. 워크로드 검토 및 개선 계획에서 비즈니스에 우선순위가 지정된 정보를 구체화하려면 프로필 질문 섹션에서 비즈니스와 가장 관련이 있는 답변을 선택하세요.
5. (선택 사항) 태그 섹션에서 프로필에 연결할 태그를 추가합니다.

   태그에 대한 자세한 내용은 AWS WA Tool 리소스에 태그 지정 섹션을 참조하세요.
6. 저장을 선택합니다. 프로필이 성공적으로 생성되면 성공 메시지가 나타납니다.

프로필이 생성되면 프로필 개요가 표시됩니다. 개요에는 이름, 설명, ARN, 생성 및 업데이트 날짜, 프로필 질문에 대한 답변 등 프로필과 관련된 데이터가 표시됩니다. 프로필 개요 페이지에서 프로필을 편집, 삭제 또는 공유할 수 있습니다.

AWS WA Tool에서 프로필 편집

프로필을 편집하려면

1. 왼쪽 탐색 창에서 프로필을 선택하거나 워크로드의 프로필 섹션에서 프로필 보기를 선택합니다.
2. 업데이트할 프로필의 이름을 선택합니다.
3. 프로필 개요 페이지에서 편집을 선택합니다.

4. 프로필 질문을 필요에 따라 업데이트합니다.
5. Save(저장)를 선택합니다.

AWS WA Tool에서 프로필 공유

프로필은 사용자 또는 계정에 공유하거나 전체 조직 또는 조직 단위에 공유할 수 있습니다.

프로필을 공유하려면

1. 왼쪽 탐색 창에서 프로필을 선택합니다.
2. 공유할 프로필 이름을 선택합니다.
3. 공유 탭을 선택합니다.
4. 사용자 또는 계정에 공유하려면 생성을 선택하고 IAM 사용자 또는 계정에 대한 공유 생성을 선택합니다. 초대 전송 상자에서 사용자 또는 계정 ID를 지정하고 생성을 선택합니다.
5. 조직 또는 조직 단위에 공유하려면 생성을 선택하고 Organizations에 대한 공유 생성을 선택합니다. 전체 조직에 공유하려면 전체 조직에 권한 부여를 선택합니다. 조직 단위에 공유하려면 개별 조직 단위에 권한 부여를 선택하고 상자에서 조직 단위를 지정한 다음 생성을 선택합니다.

> **Important**
>
> 조직 또는 조직 단위(OU)에 프로필을 공유하기 전에 AWS Organizations 액세스를 활성화해야 합니다.

AWS WA Tool에서 워크로드에 프로필 추가

기존 워크로드에 프로필을 추가하거나, 워크로드를 정의할 때 프로필을 추가하여 워크로드 검토 프로세스의 속도를 높일 수 있습니다. AWS WA Tool은 프로필에서 수집한 정보를 사용하여 비즈니스와 관련된 워크로드 검토 질문의 우선순위를 정합니다.

워크로드를 정의할 때 프로필을 추가하는 방법에 대한 자세한 내용은 the section called “워크로드 정의” 섹션을 참조하세요.

기존 워크로드에 프로필을 추가하려면

1. 왼쪽 탐색 창에서 워크로드를 선택하고 프로필과 연결할 워크로드의 이름을 선택합니다.

> **Note**
>
> 하나의 프로필만 워크로드에 연결할 수 있습니다.

2. 프로필 섹션에서 프로필 추가를 선택합니다.
3. 사용 가능한 프로필 목록에서 워크로드에 적용할 프로필을 선택하거나 프로필 생성을 선택합니다. 자세한 내용은 the section called “프로필 생성” 단원을 참조하십시오.
4. Save(저장)를 선택합니다.

워크로드 개요에는 답변이 달린 우선순위 질문 수와 우선순위가 지정된 위험 수가 연결된 프로필의 정보를 기반으로 표시됩니다. 워크로드 검토에서 우선순위가 지정된 질문을 해결하려면 계속 검토를 선택합니다. 자세한 내용은 the section called “워크로드 문서화” 단원을 참조하십시오.

프로필 섹션에는 워크로드와 연결된 프로필의 이름, 설명, ARN, 버전 및 마지막 업데이트 날짜가 표시됩니다.

AWS WA Tool에서 워크로드의 프로필 제거

워크로드에서 프로필을 제거하면 워크로드가 프로필과 연결되어 있기 이전의 버전으로 되돌아가고, 워크로드 검토 질문 및 위험은 더 이상 우선순위가 지정되지 않습니다.

워크로드에서 프로필을 제거하려면

1. 워크로드의 프로필 섹션에서 제거를 선택합니다.
2. 제거를 확인하려면 텍스트 입력 필드에 프로필 이름을 입력합니다.
3. 제거를 선택합니다.

워크로드에서 프로필이 성공적으로 제거되었다는 알림이 표시됩니다. 프로필을 제거하면 워크로드가 프로필과 연결되어 있기 이전의 버전으로 되돌아가고, 워크로드 검토 질문 및 위험은 더 이상 우선순위가 지정되지 않습니다.

AWS WA Tool에서 프로필 삭제

프로필을 만든 경우 AWS WA Tool에서 사용할 수 있는 프로필 목록에서 프로필을 삭제할 수 있습니다.

프로필 페이지에서 프로필을 삭제해도 연결된 워크로드에서 프로필이 제거되지는 않습니다. 삭제되기 전에 공유되고 워크로드와 연결되어 있던 프로필을 계속 사용할 수 있지만 삭제된 프로필에 새 워크로드를 연결할 수는 없습니다. the section called “프로필 알림”는 삭제된 프로필을 사용하여 워크로드 소유자에게 전송됩니다.

> **면책 조항**
>
> 프로필을 다른 AWS 계정에 공유하면 AWS가 프로필을 다른 계정에서 사용할 수 있도록 승인하는 것으로 간주됩니다. 사용자가 자체 AWS 계정에서 프로필을 삭제하거나 AWS 계정를 해지하더라도 이러한 다른 계정에서는 공유된 프로필에 계속 액세스하여 사용할 수 있습니다.

프로필 목록에서 프로필을 삭제하려면

1. 왼쪽 탐색 창에서 프로필을 선택합니다.
2. 제거할 프로필 이름을 선택합니다.
3. Delete(삭제)를 선택합니다.
4. 제거를 확인하려면 텍스트 입력 필드에 프로필 이름을 입력합니다.
5. Delete(삭제)를 선택합니다.

프로필 목록에는 프로필을 유지하고 워크로드에서는 프로필을 제거하려는 경우 the section called “워크로드에서 프로필 제거” 섹션을 참조하세요.

AWS Well-Architected Tool Connector for Jira

AWS Well-Architected Tool Connector for Jira를 사용하여 Jira 계정을 AWS Well-Architected Tool과 연결하고 워크로드의 개선 항목을 Jira 프로젝트와 동기화하여 개선 사항을 구현할 때 폐쇄 루프 메커니즘을 생성할 수 있습니다.

커넥터는 자동 및 수동 동기화를 모두 제공합니다. 자세한 내용은 커넥터 구성을 참조하세요.

계정 수준 및 워크로드 수준에서 커넥터를 설정할 수 있으며 워크로드당 계정 수준 설정을 재정의할 수 있습니다. 워크로드 수준에서 워크로드가 완전히 동기화되지 않도록 제외할 수도 있습니다.

개선 항목을 기본 WA Jira 프로젝트와 동기화하도록 선택하거나 동기화할 기존 프로젝트 키를 지정할 수 있습니다. 워크로드 수준에서 필요한 경우 각 워크로드를 고유한 Jira 프로젝트에 동기화할 수 있습니다.

> **Note**
>
> 커넥터는 Jira에서 스크럼 및 칸반 프로젝트만 지원합니다.

개선 항목이 Jira와 동기화되면 다음과 같이 구성됩니다.

- 프로젝트: WA(또는 지정한 기존 프로젝트)
- 에픽: 워크로드
- 작업: 질문
- 하위 작업: 모범 사례
- 레이블: 기반

설정 페이지에서 Jira 계정 동기화를 설정한 후 Jira 커넥터를 구성하고 개선 항목을 Jira 계정에 동기화할 수 있습니다.

커넥터 설정

커넥터를 설치하려면

> **Note**
>
> 다음 단계는 모두가 AWS 계정이 아닌 Jira 계정에서 수행됩니다.

1. Jira 계정에 로그인합니다.
2. 상단 탐색 모음에서 앱을 선택한 다음 추가 앱 탐색을 선택합니다.
3. Jira용 앱 및 통합 검색 페이지에서 AWS Well-Architected를 입력합니다. 그런 다음 AWS Well-Architected Tool Connector for Jira를 선택합니다.
4. 앱 페이지에서 앱 받기를 선택합니다.
5. Jira에 추가 창에서 지금 가져오기를 선택합니다.
6. 앱을 설치한 후 설정을 완료하려면 구성을 선택합니다.
7. AWS Well-Architected Tool 구성 페이지에서 새 AWS 계정 연결을 선택합니다.
8. AccessKeyId와 비밀 키를 입력합니다. 선택 사항: 세션 토큰을 입력합니다. 그런 다음 연결을 선택합니다.

   > **Note**
   >
   > 계정에 `wellarchitected:ConfigureIntegration` 권한이 있는지 확인합니다. Jira에 AWS 계정을 추가하려면 이 권한이 필요합니다.
   > 여러 AWS 계정을 AWS WA Tool에 연결할 수 있습니다.

   > **Note**
   >
   > 보안 모범 사례로 단기 IAM 자격 증명을 사용하는 것이 좋습니다. AWS 계정에 대한 AccessKeyId 및 보안 암호 키 생성에 대한 자세한 내용은 액세스 키 관리(콘솔)를 참조하고, 단기 자격 증명 사용에 대한 자세한 내용은 임시 자격 증명 요청을 참조하세요.
9. 리전에서 연결하려는 AWS 리전을 선택합니다. 그런 다음 연결을 선택합니다.

Jira 프로젝트 설정

사용자 지정 프로젝트를 사용할 때는 프로젝트 설정에 다음과 같은 문제 유형이 있어야 합니다.

- 스크럼: 에픽, 스토리, 하위 작업
- 칸반: 에픽, 작업, 하위 작업

문제 유형 관리에 대한 자세한 내용은 Atlassian Support | 문제 유형 추가, 편집 및 삭제를 참조하세요.

AWS Well-Architected Tool에서 커넥터의 연결 상태를 확인하려면

1. AWS 계정 콘솔에 로그인하고 AWS Well-Architected Tool로 이동합니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. Jira 계정 동기화 섹션의 Jira 앱 연결 상태에서 구성된 상태를 확인합니다.

이제 커넥터가 설정되고 구성할 준비가 되었습니다. 계정 및 워크로드 수준에서 Jira 동기화 설정을 구성하려면 커넥터 구성을 참조하세요.

커넥터 구성

AWS Well-Architected Tool Connector for Jira를 사용하면 계정 수준, 워크로드 수준 또는 둘 다에서 Jira 동기화를 구성할 수 있습니다. 계정 수준 설정과 관계없이 워크로드 수준 Jira 설정을 구성하거나 특정 워크로드에서 계정 수준 설정을 재정의하여 워크로드의 동기화 동작을 지정할 수 있습니다. 워크로드를 정의할 때 Jira 설정을 구성할 수도 있습니다.

커넥터는 자동 동기화와 수동 동기화의 두 가지 동기화 방법을 제공합니다. 두 동기화 방법 모두에서 AWS WA Tool에서 수행된 변경 사항은 Jira 프로젝트에 반영되고 Jira에서 수행된 변경 사항은 AWS WA Tool에 다시 동기화됩니다.

> **Important**
>
> 자동 동기화를 사용하면 Jira의 변경 사항에 따라 AWS WA Tool이 워크로드를 수정하는 데 동의하는 것입니다.
> Jira와 동기화하지 않으려는 민감한 정보가 있는 경우 워크로드의 참고 필드에 이 정보를 입력하지 마세요.

- 자동 동기화: 커넥터는 모범 사례 선택 또는 선택 취소, 질문 완료를 포함하여 질문이 업데이트될 때마다 Jira 프로젝트와 워크로드를 자동으로 업데이트합니다.
- 수동 동기화: Jira와 AWS WA Tool간에 개선 항목을 동기화하려면 워크로드 대시보드에서 Jira와 동기화를 선택해야 합니다. 동기화하려는 특정 요소와 질문을 선택할 수도 있습니다. 자세한 내용은 워크로드 동기화를 참조하세요.

계정 수준에서 커넥터를 구성하려면

1. 왼쪽 탐색 창에서 설정을 선택합니다.
2. Jira 계정 동기화 창에서 편집을 선택합니다.
3. 동기화 유형에서 다음 중 하나를 선택합니다.
   a. 변경 시 워크로드를 자동으로 동기화하려면 자동을 선택합니다.
   b. 워크로드를 동기화할 시기를 수동으로 선택하려면 수동을 선택합니다.
4. 기본적으로 커넥터는 WA Jira 프로젝트를 생성합니다. 자체 Jira 프로젝트 키를 지정하려면 다음을 수행합니다.
   a. 기본 Jira 프로젝트 키 재정의를 선택합니다.
   b. Jira 프로젝트 키를 입력합니다.

   > **Note**
   > 워크로드 수준에서 프로젝트를 변경하지 않는 한 지정된 Jira 프로젝트 키는 모든 워크로드에 사용됩니다.

5. 설정 저장을 선택합니다.

워크로드 수준에서 커넥터를 구성하려면

1. 왼쪽 탐색 창에서 워크로드를 선택하고 구성할 워크로드의 이름을 선택합니다.
2. 속성을 선택합니다.
3. Jira 창에서 편집을 선택합니다.
4. 워크로드의 Jira 설정을 구성하려면 계정 수준 설정 재정의를 선택합니다.

> **Note**
>
> 워크로드별 설정을 적용하려면 계정 수준 설정 재정의를 선택해야 합니다.

5. 동기화 재정의에서 다음 중 하나를 선택합니다.

   a. Jira 동기화에서 워크로드를 제외하려면 워크로드 동기화 안 함을 선택합니다.

   b. 워크로드를 동기화할 시기를 수동으로 선택하려면 워크로드 동기화 - 수동을 선택합니다.

   c. 워크로드 변경 사항을 자동으로 동기화하려면 워크로드 동기화 - 자동을 선택합니다.

6. (선택 사항) Jira 프로젝트 키에 워크로드를 동기화할 프로젝트 키를 입력합니다. 이 프로젝트 키는 계정 수준 프로젝트 키와 다를 수 있습니다.

   프로젝트 키를 지정하지 않으면 커넥터가 WA Jira 프로젝트를 생성합니다.

7. Save(저장)를 선택합니다.

수동 동기화 수행에 대한 자세한 내용은 워크로드 동기화를 참조하세요.

워크로드 동기화

자동 동기화의 경우 워크로드를 업데이트할 때(예: 질문을 완료하거나 새 모범 사례를 선택할 때) 커넥터가 개선 항목을 자동으로 동기화합니다.

수동 동기화와 자동 동기화 모두에서 Jira의 모든 변경 사항(예: 질문 완료 또는 모범 사례)은 AWS Well-Architected Tool에 다시 동기화됩니다.

워크로드를 수동으로 동기화하려면

1. 워크로드를 Jira와 동기화할 준비가 되면 왼쪽 탐색 창에서 워크로드를 선택합니다. 그런 다음 동기화할 워크로드를 선택합니다.
2. 워크로드 개요에서 Jira와 동기화를 선택합니다.
3. 동기화할 렌즈를 선택합니다.
4. Jira와 동기화에 대한 질문에서 Jira 프로젝트와 동기화할 질문 또는 전체 요소를 선택합니다.

   - 제거하려는 질문은 질문 제목 옆에 있는 X 아이콘을 선택합니다.

5. 동기화를 선택합니다.

커넥터 제거

AWS Well-Architected Tool Connector for Jira를 완전히 제거하려면 다음 작업을 수행합니다.

- 계정 수준 동기화 설정을 재정의하는 모든 워크로드에서 Jira 동기화를 끕니다.
- 계정 수준에서 Jira 동기화 해제
- Jira에서 AWS 계정의 연결 해제
- Jira 계정에서 커넥터 제거

계정 수준에서 커넥터를 끄려면

> **Note**
>
> 다음 단계는 AWS 계정에서 수행됩니다.

1. 왼쪽 탐색 창에서 설정을 선택합니다.
2. Jira 계정 동기화 섹션에서 편집을 선택합니다.
3. Jira 계정 동기화 켜기 옵션을 선택 해제합니다.
4. 설정 저장을 선택합니다.

AWS 계정 연결을 해제하려면

> **Note**
>
> 다음 단계는 모두가 AWS 계정이 아닌 Jira 계정에서 수행됩니다.

1. Jira 계정에 로그인합니다.
2. 상단 탐색 모음에서 앱을 선택한 다음 앱 관리를 선택합니다.
3. AWS Well-Architected Tool Connector for Jira옆의 드롭다운 화살표를 선택한 다음 구성을 선택합니다.
4. AWS Well-Architected Tool 구성 창의 작업에서 X를 선택하여 AWS 계정의 연결을 해제합니다.

커넥터를 제거하려면

> **Note**
>
> 다음 단계는 모두가 AWS 계정이 아닌 Jira 계정에서 수행됩니다.
> 커넥터를 제거하기 전에 커넥터 구성에서 연결된 모든 AWS 계정이 연결 해제되었는지 확인하는 것이 좋습니다.

1. Jira 계정에 로그인합니다.
2. 상단 탐색 모음에서 앱을 선택한 다음 앱 관리를 선택합니다.
3. AWS Well-Architected Tool Connector for Jira 옆의 드롭다운 화살표를 선택합니다.
4. 제거를 선택한 다음 앱 제거를 선택합니다.

마일스톤

마일스톤은 특정 시점의 워크로드 상태를 기록합니다.

워크로드에 연결된 모든 질문을 처음 완료한 후 마일스톤을 저장합니다. 워크로드를 개선 계획의 항목에 따라 변경할 때는 마일스톤을 추가로 저장하여 진행 상황을 측정할 수 있습니다.

워크로드를 개선할 때마다 마일스톤을 저장한 것이 모범 사례입니다.

마일스톤 저장

마일스톤은 현재 워크로드 상태를 기록합니다. 워크로드 소유자는 언제든 마일스톤을 저장할 수 있습니다.

마일스톤을 저장하는 방법

1. 워크로드 세부 정보 페이지에서 마일스톤 저장을 선택합니다.
2. 마일스톤 이름 상자에 마일스톤 이름을 입력합니다.

> **Note**
>
> 이름은 3~100자 이내로 작성해야 합니다. 문자 3개 이상이 공백이어서는 안 됩니다. 워크로드와 연결되는 마일스톤 이름은 고유해야 합니다. 고유성 여부를 확인할 때 공백과 대문자는 무시합니다.

3. 저장을 선택하여 마일스톤을 저장합니다.

마일스톤이 저장된 이후에는 기록된 워크로드 데이터를 변경할 수 없습니다. 워크로드를 삭제하면 연결된 마일스톤까지 삭제됩니다.

마일스톤 보기

워크로드에 연결된 마일스톤은 다음과 같은 방법으로 확인할 수 있습니다.

- 워크로드 세부 정보 페이지에서 마일스톤을 선택하고 확인할 마일스톤을 차례대로 선택합니다.
- 대시보드 페이지에서 워크로드를 선택한 후 (마일스톤 섹션에서 확인할 마일스톤을 선택합니다.

마일스톤 보고서 생성

마일스톤 보고서를 생성할 수 있습니다. 워크로드 질문에 대한 응답, 노트, 마일스톤이 저장될 때의 위험도 높음 및 중간이 보고서에 포함됩니다.

보고서를 생성하면 AWS Well-Architected Tool에 대한 액세스 권한이 없는 다른 사용자들과 마일스톤에 대한 세부 정보를 공유할 수 있습니다.

마일스톤 보고서를 생성하는 방법

1. 다음 중 한 가지 방법으로 마일스톤을 선택합니다.
   - 워크로드 세부 정보 페이지에서 마일스톤을 선택하고 원하는 마일스톤을 선택합니다.
   - 대시보드 페이지에서 마일스톤을 보고할 워크로드를 선택합니다. 마일스톤 섹션에서 마일스톤을 선택합니다.
2. 보고서 생성을 선택하여 보고서를 생성합니다.

   PDF 파일이 생성되어 다운로드하거나 직접 볼 수 있습니다.

공유 초대

공유 초대란 다른 AWS 계정이 소유한 워크로드, 사용자 지정 렌즈 또는 검토 템플릿에 대한 공유 요청입니다. 워크로드 또는 렌즈는 AWS 계정의 모든 사용자, 개별 사용자 또는 둘 모두에게 공유할 수 있습니다.

- 워크로드 초대를 수락하면 워크로드 및 대시보드 페이지에 워크로드가 추가됩니다.
- 사용자 지정 렌즈 초대를 수락하면 해당 렌즈가 사용자 지정 렌즈 페이지에 추가됩니다.
- 프로필 초대를 수락하면 프로필이 프로필 페이지에 추가됩니다.
- 검토 템플릿 초대를 수락하면 템플릿이 검토 템플릿 페이지에 추가됩니다.

초대를 거부하면 목록에서 제거됩니다.

> **Note**
>
> 워크로드, 사용자 지정 렌즈, 프로필, 검토 템플릿은 동일한 AWS 리전 내에서만 공유할 수 있습니다.

워크로드 또는 사용자 지정 렌즈 소유자는 공유 액세스 권한이 있는 사용자를 제어합니다.

왼쪽 탐색 창에서 사용할 수 있는 공유 초대 페이지는 보류 중인 워크로드 및 사용자 지정 렌즈 초대에 대한 정보를 제공합니다.

각 워크로드 초대마다 표시되는 정보는 다음과 같습니다.

명칭

공유할 워크로드, 사용자 지정 렌즈 또는 검토 템플릿의 이름입니다.

리소스 유형

초대의 유형(워크로드, 사용자 지정 렌즈, 프로필 또는 검토 템플릿)입니다.

소유자

워크로드를 소유하고 있는 AWS 계정 ID입니다.

권한

워크로드에 부여되는 권한입니다.

- 읽기 전용

  워크로드, 사용자 지정 렌즈, 프로필 또는 검토 템플릿에 대한 읽기 전용 액세스를 제공합니다.

- 기고자

  답변 및 해당 노트에 대한 업데이트 액세스 및 나머지 워크로드에 대한 읽기 전용 액세스를 제공합니다. 이 권한은 워크로드에 대해서만 사용할 수 있습니다.

권한 세부 정보

권한에 대한 자세한 설명입니다.

공유 초대 수락

공유 초대를 수락하려면

1. 수락할 공유 초대를 선택합니다.
2. 수락을 선택합니다.

워크로드 초대를 수락하면 워크로드 및 대시보드 페이지에 워크로드가 추가됩니다. 사용자 지정 렌즈 초대의 경우, 사용자 지정 렌즈가 사용자 지정 렌즈 페이지에 추가됩니다. 프로필 초대의 경우, 프로필이 프로필 페이지에 추가됩니다. 검토 템플릿 초대의 경우, 템플릿이 검토 템플릿 페이지에 추가됩니다.

7일 이내에 초대를 수락할 수 있습니다. 7일 이내에 수락하지 않은 초대는 자동으로 만료됩니다.

사용자와 사용자의 AWS 계정가 모두 워크로드 초대를 수락한 경우 사용자에게 주어진 워크로드 초대에 따라 사용자의 권한이 결정됩니다.

공유 초대 거부

공유 초대를 거부하려면

1. 거부할 워크로드 또는 사용자 지정 렌즈 초대를 선택합니다.
2. 거부를 선택합니다.

초대가 목록에서 제거됩니다.

알림

알림 페이지에는 연결된 렌즈와 프로필이 있는 워크로드 및 검토 템플릿의 버전 차이가 표시됩니다. 알림 페이지에서 워크로드에 맞는 렌즈 또는 프로필의 최신 버전으로 업그레이드할 수 있습니다.

렌즈 알림

새로운 버전의 렌즈가 사용 가능해지면 워크로드 또는 검토 템플릿 페이지 상단에 배너가 나타나 알려줍니다. 오래된 렌즈를 사용하는 특정 워크로드나 검토 템플릿을 확인하는 경우 새로운 렌즈 버전을 사용할 수 있음을 표시하는 배너도 나타납니다.

사용 가능한 업그레이드 보기를 선택하고 업그레이드할 수 있는 워크로드 또는 검토 템플릿 목록을 확인합니다.

워크로드 또는 검토 템플릿에 맞게 렌즈를 업그레이드하는 방법은 the section called “렌즈 업그레이드” 섹션을 참조하세요.

공유된 렌즈의 소유자가 렌즈를 삭제하면, 삭제된 렌즈와 연결된 워크로드가 있는 경우 기존 워크로드에서 렌즈를 계속 사용할 수 있지만 새 워크로드에 추가할 수는 없다는 알림을 받게 됩니다.

프로필 알림

프로필 알림에는 두 가지 유형이 있습니다.

- 프로필 업그레이드
- 프로필 삭제

워크로드와 관련된 프로필이 편집되면(자세한 내용은 the section called “프로필 편집” 참조), 프로필의 새 버전이 있다는 알림이 프로필 알림에 표시됩니다.

공유된 프로필의 소유자가 프로필을 삭제하면, 삭제된 프로필과 연결된 워크로드가 있는 경우 기존 워크로드에서 프로필을 계속 사용할 수 있지만 새 워크로드에 추가할 수는 없다는 알림을 받게 됩니다.

프로필 버전을 업그레이드하려면

1. 왼쪽 탐색 창에서 알림을 선택합니다.
2. 프로필 알림 탭의 목록에서 워크로드 이름을 선택하거나 검색 창을 사용하여 워크로드 이름으로 검색합니다.

3. 프로필 버전 업그레이드를 선택합니다.
4. 승인 섹션에서 이러한 변경 사항을 이해하고 이를 수락함 확인 상자를 선택합니다.
5. (선택 사항) 마일스톤을 저장하기로 선택한 경우 마일스톤 저장 상자를 선택하고 마일스톤 이름을 입력합니다.
6. 저장을 선택합니다.

프로필이 업그레이드되면 최신 버전 번호와 업데이트 날짜가 워크로드의 프로필 섹션에 표시됩니다.

자세한 내용은 프로파일 섹션을 참조하세요.

대시보드

왼쪽 탐색 창의 대시보드에서는 워크로드 및 이와 연결된 중간 위험 및 고위험 문제에 액세스할 수 있습니다. 나에게 공유된 워크로드도 포함할 수 있습니다. 대시보드는 네 가지 섹션으로 구성됩니다.

- 요약 — 총 워크로드 수, 중간 위험 및 고위험이 있는 워크로드 수, 모든 워크로드에 존재하는 중간 위험 및 고위험 문제의 총 개수를 보여줍니다.
- 원칙당 Well-Architected Framework 문제 — 모든 워크로드에 대한 원칙별 고위험 및 중간 위험 문제를 그래프로 보여줍니다.
- 워크로드당 Well-Architected Framework 문제 — 각 워크로드에 대한 원칙별 고위험 및 중간 위험 문제를 보여줍니다.
- 개선 계획 항목별 Well-Architected Framework 문제 — 모든 워크로드에 대한 개선 계획 항목을 보여줍니다.

요약

이 섹션에는 워크로드의 총 개수와 Well-Architected Framework 렌즈 및 기타 모든 렌즈에서 고위험 및 중간 위험 문제가 있는 워크로드 수가 표시됩니다. 내 AWS 계정에서 소유하거나 공유한 모든 워크로드에 있는 고위험 및 중간 위험 문제의 총 개수가 표시됩니다.

나와 공유된 워크로드 포함을 선택하면 요약 통계, 통합 보고서 및 기타 대시보드 섹션에 내 워크로드 및 나에게 공유된 워크로드가 모두 반영됩니다.

보고서 생성을 선택하면 통합 보고서가 PDF 파일로 생성됩니다.

보고서 이름은 `wellarchitected_consolidatedreport_`*`account-ID`*`.pdf` 형식으로 지정됩니다.

원칙당 Well-Architected Framework 문제

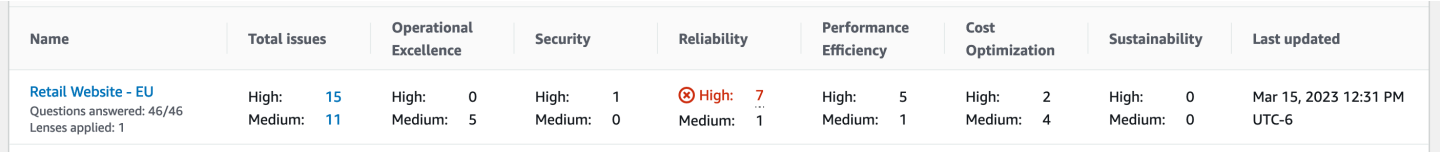
원칙당 Well-Architected Framework 문제 섹션에는 모든 워크로드에 대한 원칙별 고위험 및 중간 위험 문제 수가 그래픽으로 표시됩니다.

대시보드의 나머지 섹션을 사용하여 한 세부 수준에서 다음 세부 수준으로 이동할 수 있습니다.

> **Note**
>
> 이 섹션에는 Well-Architected Framework 렌즈의 문제만 포함되어 있습니다.

워크로드당 Well-Architected Framework 문제

워크로드당 Well-Architected Framework 문제 섹션에는 각 워크로드에 대한 정보가 표시됩니다.



Name	Total issues	Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability	Last updated
Retail Website - EU Questions answered: 46/46 Lenses applied: 1	High: 15 Medium: 11	High: 0 Medium: 5	High: 1 Medium: 0	High: 7 Medium: 1	High: 5 Medium: 1	High: 2 Medium: 4	High: 0 Medium: 0	Mar 15, 2023 12:31 PM UTC-6

각 워크로드마다 표시되는 정보는 다음과 같습니다.

명칭

워크로드 이름입니다 답변이 완료된 질문 수와 워크로드에 적용된 렌즈 개수도 표시됩니다.

워크로드 이름을 선택하여 워크로드 세부 정보 페이지로 이동해 마일스톤, 개선 계획 및 공유를 확인하세요.

총 문제 수

Well-Architected Framework 렌즈에서 파악한 워크로드의 총 문제 수입니다.

고위험 또는 중간 위험 문제의 수를 선택하면 해당 문제에 대한 권장 개선 계획을 확인할 수 있습니다.

운영 우수성

운영 우수성 원칙의 워크로드에서 식별된 고위험 문제(HRI) 및 중간 위험 문제(MRI)의 수입니다.

보안

보안 원칙에 대해 식별된 HRI 및 MRI의 수입니다.

신뢰성

신뢰성 원칙에 대해 식별된 HRI 및 MRI의 수입니다.

성능 효율성

성능 효율성 원칙에 대해 식별된 HRI 및 MRI의 수입니다.

비용 최적화

비용 최적화 원칙에 대해 식별된 HRI 및 MRI의 수입니다.

지속 가능성

지속 가능성 원칙에 대해 식별된 HRI 및 MRI의 수입니다.

최종 업데이트 날짜

워크로드가 마지막으로 업데이트된 날짜와 시간입니다.

각 워크로드에 대해 고위험 문제(HRI) 수가 가장 많은 원칙이 강조 표시됩니다.

> **Note**
>
> 이 섹션에는 Well-Architected Framework 렌즈의 문제만 포함되어 있습니다.

개선 계획 항목별 Well-Architected Framework 문제

개선 계획 항목별 Well-Architected Framework 문제 섹션에서는 모든 워크로드에 대한 개선 계획 항목을 보여줍니다. 원칙과 심각도를 기준으로 항목을 필터링할 수 있습니다.

각 개선 계획 항목마다 다음 정보가 표시됩니다.

개선 항목

개선 계획 항목의 이름입니다.

개선 계획 항목과 관련된 모범 사례를 표시할 이름을 선택합니다.

원칙

개선 항목과 관련된 원칙입니다.

Risk

관련 문제의 위험도가 높은지 중간인지를 나타냅니다.

적용 가능한 워크로드

이 개선 계획이 적용되는 워크로드 수입니다.

개선 계획 항목을 선택하면 적용 가능한 워크로드를 확인할 수 있습니다.

> **Note**
>
> 이 섹션에는 Well-Architected Framework 렌즈의 개선 계획 항목만 포함되어 있습니다.

AWS Well-Architected Tool에서의 보안

AWS에서 클라우드 보안은 가장 중요합니다. AWS 고객은 보안에 가장 보안에 민감한 조직의 요구 사항에 부합하도록 빌드된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 사용자의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 AWS 규정 준수 프로그램의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. AWS Well-Architected Tool에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램의 범위에 속하는 AWS 서비스를 참조하세요.
- 클라우드의 보안 – 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS WA Tool 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 AWS WA Tool을(를) 구성하는 방법을 보여줍니다. 또한 AWS WA Tool 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스 사용 방법을 알아봅니다.

주제

AWS Well-Architected Tool의 데이터 보호

AWS 공동 책임 모델은 AWS Well-Architected Tool의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center 또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정하세요. AWS 활동 캡처에 CloudTrail 추적을 사용하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용하세요.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-3 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 AWS WA Tool 또는 기타 AWS 서비스에서 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

AWS WA Tool에 의해 저장된 모든 데이터는 유휴 시 암호화됩니다.

전송 중 암호화

AWS WA Tool에서 송수신되는 모든 데이터는 전송 중에 암호화됩니다.

AWS에서 사용자 데이터를 사용하는 방법

AWS Well-Architected 팀은 고객에게 AWS WA Tool 서비스를 제공하고 개선하기 위해 AWS Well-Architected Tool에서 집계된 데이터를 수집합니다. 고객의 워크로드 및 아키텍처 개선을 위한 노력을 지원하기 위해 개별 고객 데이터를 AWS 계정 팀과 공유해야 할 수도 있습니다. AWS Well-Architected 팀은 각 질문에 대해 워크로드 속성 및 선택한 선택 항목에만 액세스할 수 있습니다. AWS는 AWS 외부의 AWS WA Tool 데이터를 공유하지 않습니다.

AWS Well-Architected 팀이 액세스할 수 있는 워크로드 속성은 다음과 같습니다.

- 워크로드 이름
- 검토 소유자
- 환경
- 리전
- 계정 ID
- 산업 유형

AWS Well-Architected 팀은 다음 항목에 액세스할 수 없습니다.

- 워크로드 설명
- 아키텍처 설계
- 사용자가 입력한 모든 노트

AWS Well-Architected Tool의 Identity and Access Management(IAM)

AWS Identity and Access Management(IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 통제할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 어떤 사용자가 AWS WA Tool 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

대상

AWS Identity and Access Management(IAM)을 사용하는 방법은 AWS WA Tool에서 수행하는 작업에 따라 달라집니다.

서비스 사용자 - AWS WA Tool 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증과 권한을 관리자가 제공합니다. 더 많은 AWS WA Tool 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. AWS WA Tool의 기능에 액세스할 수 없는 경우 AWS Well-Architected Tool ID 및 액세스 문제 해결을 참조하세요.

서비스 관리자 - 회사에서 AWS WA Tool 리소스를 책임지고 있는 담당자라면 AWS WA Tool에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 AWS WA Tool 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 AWS WA Tool에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 AWS Well-Architected Tool에서 IAM을 사용하는 방식을 참조하세요.

IAM 관리자 - IAM 관리자라면 AWS WA Tool에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 AWS WA Tool 자격 증명 기반 정책 예제를 보려면 AWS Well-Architected Tool ID 기반 정책 예제을 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 사용하여 AWS에 로그인하는 방식입니다. AWS 계정 루트 사용자이나 IAM 사용자로, 또는 IAM 역할을 수임하여 인증(AWS에 로그인)받아야 합니다.

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 AWS에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증, Google 또는 Facebook

보안 인증이 페더레이션 ID의 예제입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 연동을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임합니다.

사용자 유형에 따라AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. AWS에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법을 참조하세요.

AWS에 프로그래밍 방식으로 액세스하는 경우, AWS에서는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK) 및 명령줄 인터페이스(CLI)를 제공합니다. AWS 도구를 사용하지 않는 경우, 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용 AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS은(는) 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의 AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

AWS 계정을(를) 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 ID로 시작합니다. 이 ID는 AWS 계정루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구합니다.

페더레이션 ID는 엔터프라이즈 사용자 디렉터리, 웹 ID 공급자, AWS Directory Service, Identity Center 디렉터리의 사용자 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하는 모든 사용자입니다. 페더레이션 ID는 AWS 계정에 액세스할 때 역할을 수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 AWS 계정 및 애플리케이션에서 사용하기 위해 고유한

ID 소스의 사용자 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가지고 있는 AWS 계정 내 ID입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가지고 있는 AWS 계정 계정 내 ID입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. AWS Management Console에서 일시적으로 IAM 역할을 수임하려면 사용자에서 IAM 역할로 전환(콘솔)하면 됩니다. AWS CLI 또는 AWS API 작업을 직접적으로 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.

- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 AWS 서비스을(를) 사용하면 리소스에 정책을 직접 연결할 수 있습니다(역할을 프록시로서 사용하는 대신) . 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부 AWS 서비스는 다른 AWS 서비스의 특성을 사용합니다. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 위탁자의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 – 서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 링크 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon EC2에서 실행 중인 애플리케이션 – IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS역할을 할당하고 해당 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 생성하고 AWS ID 또는 리소스에 연결하여 AWS에서 내 액세스를 제어합니다. 정책은 ID 또는 리소스와 연결될 때 해당 권한을 정의하는 AWS의 객체입니다. AWS는 보안 주체(사용자, 루트 사용자

또는 역할 세션)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 AWS에 JSON 문서로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWSJSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console, AWS CLI 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 AWS 계정에 속한 다수의 사용자, 그룹 및 역할에 독립적으로 추가할 수 있는 정책입니다. 관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함되어 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 AWS 서비스가 포함될 수 있습니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3, AWS WAF 및 Amazon VPC는 ACL을 지원하는 대표적인 서비스입니다. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS는 비교적 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCP) – SCP는 AWS Organizations에서 조직 또는 조직 단위(OU)에 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations는 기업이 소유하는 여러 개의 AWS 계정을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 특성을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 AWS 계정 루트 사용자을 비롯하여 멤버 계정의 엔티티에 대한 권한을 제한합니다. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 관계없이 AWS 계정 루트 사용자를 포함한 ID에 대한 유효 권한에 영향을 줄 수 있습니다. RCP를 지원하는 AWS 서비스 목록을 포함하여 Organizations 및 RCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련될 때 AWS가 요청을 허용할지 여부를 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS Well-Architected Tool에서 IAM을 사용하는 방식

IAM을 사용하여 AWS WA Tool에 대한 액세스를 관리하기 전에 AWS WA Tool와 함께 사용할 수 있는 IAM 기능을 알아보세요.

AWS Well-Architected Tool를 통해 사용할 수 있는 IAM 기능

IAM 기능	AWS WA Tool 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요
서비스 연결 역할	아니요

AWS WA Tool 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 IAM으로 작동하는 AWS 서비스를 참조하세요.

AWS WA Tool ID 기반 정책

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 작업의 이름은 연결된 AWSAPI 작업의 이름과 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS WA Tool 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 AWS 서비스가 포함될 수 있습니다.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 서로 다른 AWS 계정에 있는 경우, 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에도 리소스 액세스 권한을 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

AWS WA Tool 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 작업의 이름은 연결된 AWSAPI 작업의 이름과 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS WA Tool의 정책 작업은 작업 앞에 wellarchitected: 접두사를 사용합니다. 예를 들어, 엔터티가 워크로드를 정의할 수 있도록 하려면 관리자가 wellarchitected:CreateWorkload 작업을 허용하는 정책을 연결해야 합니다. 마찬가지로, 엔터티가 워크로드를 삭제하지 못하도록 관리자가 wellarchitected:DeleteWorkload 작업을 거부하는 정책을 연결할 수 있습니다. 정책 명령문에는 Action 또는 NotAction 요소가 포함되어야 합니다. AWS WA Tool는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 집합을 정의합니다.

AWS WA Tool 작업 목록을 보려면 Service Authorization Reference의 Actions Defined by AWS Well-Architected Tool를 참조하세요.

정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS WA Tool 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조의 AWS Well-Architected Tool에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Well-Architected Tool가 정의한 작업을 참조하세요.

AWS WA Tool 워크로드 리소스에는 다음과 같은 ARN이 있습니다.

```
arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}
```

ARN 형식에 대한 자세한 내용은 Amazon 리소스 이름(ARN) 및 AWS 서비스 네임스페이스를 참조하세요.

ARN은 워크로드에 대한 워크로드 속성 페이지에서 찾을 수 있습니다. 예를 들어, 특정 워크로드를 지정하려면 다음과 같이 하십시오.

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/11112222333344445555666677778888"
```

특정 계정에 속하는 모든 워크로드를 지정하려면 와일드카드(*)를 사용합니다.

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/*"
```

워크로드를 생성 및 나열하기 위한 작업과 같은 일부 AWS WA Tool 작업은 특정 리소스에서 수행할 수 없습니다. 이러한 경우, 와일드카드(*)를 사용해야 합니다.

```
"Resource": "*"
```

AWS WA Tool 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조의 AWS Well-Architected Tool에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Well-Architected Tool가 정의한 작업을 참조하세요.

AWS WA Tool 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우, AWS는 논리적 `OR` 작업을 사용하여 조건을 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

AWS WA Tool은 서비스별 조건 키(`wellarchitected:JiraProjectKey`) 1개를 제공하고 일부 글로벌 조건 키 사용을 지원합니다. 모든 AWS 전역 조건 키를 보려면 서비스 권한 부여 참조의 AWS 전역 조건 컨텍스트 키를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우, AWS는 논리적 `OR` 작업을 사용하여 조건을 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

AWS WA Tool의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS WA Tool 태그 기반 인증

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔티티(사용자 또는 역할) 및 많은 AWS리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

AWS WA Tool에서 임시 보안 인증 정보 사용

임시 자격 증명 지원: 예

일부 AWS 서비스는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 보안 인증으로 작동하는 AWS 서비스를 비롯한 추가 정보는 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스를 참조하세요.

사용자 이름과 암호를 제외한 다른 방법을 사용하여 AWS Management Console에 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어, 회사의 Single Sign-On(SSO) 링크를 사용하여 AWS에 액세스하면 해당 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 만들 수 있습니다 그런 다음 이러한 임시 자격 증명을 사용하여 AWS에 액세스할 수 있습니다. AWS에서는 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

AWS WA Tool의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 위탁자로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 위탁자의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 경우에만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS WA Tool의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

AWS WA Tool에 대한 서비스 연결 역할

서비스 링크 역할 지원: 아니요

서비스 연결 역할은 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 링크 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 `Yes`이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS Well-Architected Tool ID 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS WA Tool 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS CLI또는 AWSAPI를 사용해 태스크를 수행할 수 없습니다. IAM 관리자는 지정된 리소스에서 특정 API 태스크를 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례

- AWS WA Tool 콘솔 사용
- 사용자가 자신이 권한을 볼 수 있도록 허용
- 워크로드에 대한 전체 액세스 권한 부여
- 워크로드에 읽기 전용 액세스 권한 부여
- 단일 워크로드 액세스
- AWS Well-Architected Tool Connector for Jira에 서비스별 조건 키 사용

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS WA Tool 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS CloudFormation와 같이, 특정 AWS 서비스를 통해 사용되는 경우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 – AWS 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우, 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

AWS WA Tool 콘솔 사용

AWS Well-Architected Tool 콘솔에 액세스하려면 최소 권한 세트가 있어야 합니다. 이러한 권한은 AWS 계정에서 AWS WA Tool 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

해당 개체가 AWS WA Tool 콘솔을 여전히 사용할 수 있도록 하려면 다음과 같은 AWS 관리형 정책도 개체에 연결합니다.

```
WellArchitectedConsoleReadOnlyAccess
```

워크로드를 생성, 변경 및 삭제할 수 있는 기능을 허용하려면 엔터티에 다음과 같은 AWS 관리형 정책을 연결합니다.

```
WellArchitectedConsoleFullAccess
```

자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

AWS CLI 또는 AWSAPI만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요가 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자가 자신이 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 태스크를 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

워크로드에 대한 전체 액세스 권한 부여

이 예제에서는 AWS 계정의 사용자에게 워크로드에 대한 전체 액세스 권한을 부여하려고 합니다. 모든 액세스는 사용자에게 모든 AWS WA Tool 작업을 허용합니다. 이 액세스는 워크로드 정의, 워크로드 삭제, 워크로드 보기 및 워크로드 업데이트에 필요합니다.

JSON

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:*"
     ],
     "Resource": "*"
     }
   ]
```

```
}
```

워크로드에 읽기 전용 액세스 권한 부여

이 예제에서는 AWS 계정의 사용자에게 워크로드에 대한 읽기 전용 액세스 권한을 부여하려고 합니다. 읽기 전용 액세스가 있으면 사용자가 AWS WA Tool에서 워크로드를 볼 수 있습니다.

JSON

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "*"
     }
   ]
}
```

단일 워크로드 액세스

이 예제에서는 AWS 계정의 사용자에게 us-west-2 리전의 워크로드 중 하나인 99999999999955555555555566666666에 대한 읽기 전용 액세스 권한을 부여하려고 합니다. 계정 ID는 777788889999입니다.

JSON

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
```

```
      ],
      "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555666666666"
      }
    ]
}
```

AWS Well-Architected Tool Connector for Jira에 서비스별 조건 키 사용

이 예제에서는 서비스별 조건 키 `wellarchitected:JiraProjectKey`를 사용하여 계정의 워크로드에 연결할 수 있는 Jira 프로젝트를 제어하는 방법을 보여줍니다.

다음에서는 조건 키의 관련 용도를 설명합니다.

- **`CreateWorkload`:** `wellarchitected:JiraProjectKey`를 `CreateWorkload`에 적용할 때 사용자가 생성한 워크로드에 연결할 수 있는 사용자 지정 Jira 프로젝트를 정의할 수 있습니다. 예를 들어 사용자가 프로젝트 ABC로 새 워크로드를 생성하려고 하지만 정책이 프로젝트 PQR만 지정하는 경우 작업이 거부됩니다.
- **`UpdateWorkload`:** `wellarchitected:JiraProjectKey`를 `UpdateWorkload`에 적용할 때 이 특정 워크로드 또는 모든 워크로드에 연결할 수 있는 사용자 지정 Jira 프로젝트를 정의할 수 있습니다. 예를 들어, 사용자가 프로젝트 ABC로 기존 워크로드를 업데이트하려고 하지만 정책에서 프로젝트 PQR을 지정하는 경우 작업이 거부됩니다. 또한 사용자에게 프로젝트 PQR에 연결된 워크로드가 있고 프로젝트 ABC에 연결할 워크로드를 업데이트하려고 하면 작업이 거부됩니다.
- **`UpdateGlobalSettings`:** `wellarchitected:JiraProjectKey`를 `UpdateGlobalSettings`에 적용할 때 AWS 계정에 연결할 수 있는 사용자 지정 Jira 프로젝트를 정의할 수 있습니다. 계정 수준 설정은 계정 수준 Jira 설정을 재정의하지 않는 계정의 워크로드를 보호합니다. 예를 들어 사용자가 `UpdateGlobalSettings`에 액세스할 수 있는 경우 계정의 워크로드를 정책에 지정되지 않은 프로젝트에 연결할 수 없습니다.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
```

```
    "wellarchitected:UpdateGlobalSettings",
    "wellarchitected:CreateWorkload"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
   }
  },
  {
   "Sid": "VisualEditor1",
   "Effect": "Allow",
   "Action": [
    "wellarchitected:UpdateWorkload"
   ],
   "Resource": "arn:aws:wellarchitected:us-east-1:111122223333:workload/example-
workload",
   "Condition": {
    "StringEqualsIfExists": {
     "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
   }
  }
 ]
}
```

AWS Well-Architected Tool의 AWS 관리형 정책

AWS 관리형 정책은 AWS에 의해 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. 만약 AWS가 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 위탁자 ID(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새 AWS 서비스을(를) 시작하거나 새 API 작업을 기존 서비스에 이용하는 경우, AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: WellArchitectedConsoleFullAccess

`WellArchitectedConsoleFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 AWS Well-Architected Tool에 대한 모든 액세스 권한을 부여합니다.

권한 세부 정보

JSON

```
{
   "Version": "2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:*"
     ],
     "Resource": "*"
     }
   ]
}
```

AWS 관리형 정책: WellArchitectedConsoleReadOnlyAccess

`WellArchitectedConsoleReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 AWS Well-Architected Tool에 대한 읽기 전용 액세스 권한을 부여합니다.

권한 세부 정보

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "wellarchitected:Get*",
                "wellarchitected:List*",
                "wellarchitected:ExportLens"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSWellArchitectedOrganizationsServiceRolePolicy

`AWSWellArchitectedOrganizationsServiceRolePolicy` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 조직과의 AWS Well-Architected Tool 통합을 지원하는 데 필요한 AWS Organizations 관리 권한을 부여합니다. 이러한 권한을 통해 조직 관리 계정에서 리소스를 AWS WA Tool에 공유할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations:ListAWSServiceAccessForOrganization` – 보안 주체가 AWS WA Tool에서 AWS 서비스 액세스가 가능한지 확인할 수 있습니다.
- `organizations:DescribeAccount` – 보안 주체가 조직의 계정에 대한 정보를 검색할 수 있습니다.
- `organizations:DescribeOrganization` – 보안 주체가 조직 구성에 대한 정보를 검색할 수 있습니다.
- `organizations:ListAccounts` – 보안 주체가 조직에 속한 계정 목록을 검색할 수 있습니다.
- `organizations:ListAccountsForParent` – 보안 주체가 조직의 지정된 루트 노드에서 조직에 속한 계정 목록을 검색할 수 있습니다.
- `organizations:ListChildren` – 보안 주체가 조직의 주어진 루트 노드에서 조직에 속한 계정 및 조직 단위(OU)의 목록을 검색할 수 있습니다.
- `organizations:ListParents` – 보안 주체가 OU에서 지정한 직계 상위 항목 또는 조직 내 계정 목록을 검색할 수 있습니다.
- `organizations:ListRoots` – 보안 주체가 조직 내 모든 루트 노드 목록을 검색할 수 있습니다.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSWellArchitectedDiscoveryServiceRolePolicy

`AWSWellArchitectedDiscoveryServiceRolePolicy` 정책을 IAM ID에 연결할 수 있습니다.

이 정책을 통해 AWS Well-Architected Tool이 AWS WA Tool 리소스와 관련된 AWS 서비스 및 리소스에 액세스할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `trustedadvisor:DescribeChecks` – 사용 가능한 Trusted Advisor 검사 목록을 표시합니다.
- `trustedadvisor:DescribeCheckItems` – Trusted Advisor에서 플래그를 지정한 상태 및 리소스를 포함한 Trusted Advisor 검사 데이터를 가져옵니다.
- `servicecatalog:GetApplication` – AppRegistry 애플리케이션의 세부 정보를 가져옵니다.
- `servicecatalog:ListAssociatedResources` – AppRegistry 애플리케이션과 관련된 리소스를 나열합니다.

- `cloudformation:DescribeStacks` – AWS CloudFormation 스택의 세부 정보를 가져옵니다.
- `cloudformation:ListStackResources` – AWS CloudFormation 스택과 관련된 리소스를 나열합니다.
- `resource-groups:ListGroupResources` – ResourceGroup의 리소스를 나열합니다.
- `tag:GetResources` – ListGroupResources에 필요합니다.
- `servicecatalog:CreateAttributeGroup` – 필요한 경우 서비스 관리형 속성 그룹을 생성합니다.
- `servicecatalog:AssociateAttributeGroup` – 서비스 관리형 속성 그룹을 AppRegistry 애플리케이션과 연결합니다.
- `servicecatalog:UpdateAttributeGroup` – 서비스 관리형 속성 그룹을 업데이트합니다.
- `servicecatalog:DisassociateAttributeGroup` – 서비스 관리형 속성 그룹과 AppRegistry 애플리케이션의 연결을 끊습니다.
- `servicecatalog:DeleteAttributeGroup` – 필요한 경우 서비스 관리형 속성 그룹을 삭제합니다.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeChecks",
    "trustedadvisor:DescribeCheckItems"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources",
    "resource-groups:ListGroupResources",
    "tag:GetResources"
```

```
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:ListAssociatedResources",
     "servicecatalog:GetApplication",
     "servicecatalog:CreateAttributeGroup"
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:AssociateAttributeGroup",
     "servicecatalog:DisassociateAttributeGroup"
    ],
    "Resource": [
     "arn:*:servicecatalog:*:*:/applications/*",
     "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:UpdateAttributeGroup",
     "servicecatalog:DeleteAttributeGroup"
    ],
    "Resource": [
     "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
   }
  ]
}
```

AWS 관리형 정책으로 AWS WA Tool 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후부터 AWS WA Tool의 AWS 관리형 정책 업데이트에 관한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS WA Tool 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWS WA Tool에서 관리형 정책 변경	`WellArchitectedConsoleReadOnlyAccess` 에 `"wellarchitected:Export*"` 가 추가되었습니다.	2023년 6월 22일
AWS WA Tool에서 서비스 역할 정책 추가	AWS Well-Architected Tool에서 AWS WA Tool 리소스와 관련된 AWS 서비스 및 리소스에 액세스할 수 있도록 `AWSWellArchitectedDiscoveryServiceRolePolicy` 가 추가되었습니다.	2023년 5월 3일
AWS WA Tool에서 권한 추가	AWS WA Tool에서 AWS WA Tool에 대한 AWS 서비스 액세스가 활성화되었는지 확인할 수 있는 `ListAWSServiceAccessForOrganization` 권한을 부여하는 새 작업을 추가했습니다.	2022년 7월 22일
AWS WA Tool에서 변경 사항 추적 시작	AWS WA Tool에서 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2022년 7월 22일

AWS Well-Architected Tool ID 및 액세스 문제 해결

다음 정보를 사용하여 AWS WA Tool 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- AWS WA Tool에서 작업을 수행할 권한이 없음

AWS WA Tool에서 작업을 수행할 권한이 없음

AWS Management Console에서 작업을 수행할 권한이 없다는 메시지가 나타나는 경우 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음의 예제 오류는 *mateojackson* 사용자가 콘솔을 사용해 DeleteWorkload 작업을 수행하려고 하지만 권한이 없는 경우 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: wellarchitected:DeleteWorkload on resource: 11112222333344445555666677778888
```

이 예시에서는 wellarchitected:DeleteWorkload 작업을 사용해 11112222333344445555666677778888 리소스에 액세스할 수 있도록 정책을 업데이트 해달라고 관리자에게 요청합니다.

AWS Well-Architected Tool의 인시던트 대응

AWS Well-Architected Tool의 인시던트 대응은 AWS 책임입니다. AWS에는 인시던트 대응에 적용되는 문서화된 공식 정책 및 프로그램이 있습니다.

널리 영향을 미치는 AWS 운영 문제는 AWS Service Health Dashboard에 게시됩니다.

AWS Health Dashboard를 통해 개별 계정에도 운영 문제가 게시됩니다. AWS Health Dashboard 사용 방법에 대한 자세한 내용을 알아보려면 AWS Health 사용 설명서를 참조하세요.

AWS Well-Architected Tool 규정 준수 확인

AWS 서비스(이)가 특정 규정 준수 프로그램의 범위에 포함되는지 알아보려면 규정 준수 프로그램 제공 범위 내 AWS 서비스를 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반적인 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact(을)를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact에서 보고서 다운로드를 참조하세요.

AWS 서비스 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다.AWS에서는 규정 준수를 지원할 다음과 같은 리소스를 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모든 AWS 서비스에 HIPAA 자격이 있는 것은 아닙니다.
- AWS 규정 준수 리소스 - 고객 조직이 속한 산업 및 위치에 적용될 수 있는 워크북 및 가이드 컬렉션입니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에서는 AWS 서비스를 보호하기 위한 모범 사례를 요약하고 여러 프레임워크(미국 표준 기술 연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제 표준화기구(ISO) 등)에서 보안 컨트롤에 대한 지침을 매핑합니다.
- AWS Config 개발자 가이드의 규칙을 사용하여 리소스 평가 – AWS Config 서비스는 내부 사례, 산업 지침 및 규제에 대한 리소스 구성의 준수 상태를 평가합니다.
- AWS Security Hub – 이 AWS 서비스(은)는 AWS 내 보안 상태에 대한 포괄적인 보기를 제공합니다. Security Hub는 보안 컨트롤을 사용하여 AWS리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty - 이 AWS 서비스는 의심스럽고 악의적인 활동이 있는지 환경을 모니터링하여 AWS 계정, 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이 AWS 서비스은(는) AWS 사용을 지속해서 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 간소화할 수 있도록 지원합니다.

AWS Well-Architected Tool의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전에서는 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 대기 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS Well-Architected Tool에서 인프라 보안

관리형 서비스인 AWS Well-Architected Tool은 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 직접 호출을 사용하여 네트워크를 통해 AWS WA Tool에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS Well-Architected Tool의 구성 및 취약성 분석

구성 및 IT 컨트롤은 AWS와 고객 간의 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. AWS에서는 교차 서비스 가장으로 인해 혼동된 대리자 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

`aws:SourceArn`이 리소스에 다른 서비스를 제공하는 권한을 제한하려면 리소스 정책에서 `aws:SourceAccount` 및 AWS Well-Architected Tool 글로벌 조건 컨텍스트 키를 사용하는 것이 좋

습니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 aws:SourceArn을 사용하세요. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 aws:SourceAccount을(를) 사용합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 aws:SourceArn 전역 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모르거나 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드 문자(*)를 포함한 aws:SourceArn 글로벌 조건 컨텍스트 키를 사용합니다. 예를 들어 arn:aws:wellarchitected:*:*123456789012*:*입니다.

만약 aws:SourceArn 값에 Amazon S3 버킷 ARN과 같은 계정 ID가 포함되어 있지 않은 경우, 권한을 제한하려면 두 글로벌 조건 컨텍스트 키를 모두 사용해야 합니다.

aws:SourceArn의 값은 워크로드 또는 렌즈여야 합니다.

다음 예는 AWS WA Tool에서 aws:SourceArn 및 aws:SourceAccount 글로벌 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "wellarchitected.amazonaws.com"
    },
    "Action": "wellarchitected:CreateWorkload",
    "Resource": [
    "arn:aws:wellarchitected:us-east-1:111122223333:ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
```

```
}
```

AWS WA Tool 리소스 공유

소유한 리소스를 공유하려면 다음 작업을 수행하세요.

- AWS Organizations 내에서 리소스 공유 활성화 (선택 사항)
- 워크로드 공유
- 사용자 지정 렌즈 공유
- 프로필 공유
- 검토 템플릿 공유

> **참고**
>
> - 리소스를 공유하면 리소스를 생성한 AWS 계정가 아닌 다른 보안 주체도 해당 리소스를 사용할 수 있습니다. 리소스를 공유해도 해당 리소스를 생성한 계정의 리소스에 적용되는 권한은 변경되지 않습니다.
> - AWS WA Tool은 리전 서비스입니다. 내가 리소스를 공유한 보안 주체는 해당 리소스가 생성된 AWS 리전에서만 리소스 공유에 액세스할 수 있습니다.
> - 2019년 3월 20일 이후에 도입된 리전에서 리소스를 공유하려면 사용자 및 공유를 받은 AWS 계정 모두 AWS Management Console에서 리전을 사용하도록 설정해야 합니다. 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS Organizations 내에서 리소스 공유 활성화

AWS Organizations에서 계정을 관리하는 경우 이를 활용하여 리소스를 더 쉽게 공유할 수 있습니다. Organizations 사용 여부와 관계없이, 사용자는 개별 계정과 리소스를 공유할 수 있습니다. 그러나 계정이 조직에 있는 경우 각 계정을 열거할 필요 없이 개별 계정과 공유하거나 조직 또는 OU의 모든 계정과 공유할 수 있습니다.

조직 내에서 리소스를 공유하려면 먼저 AWS WA Tool 콘솔이나 AWS Command Line Interface(AWS CLI)를 사용하여 AWS Organizations에 대한 공유를 활성화해야 합니다. 조직의 리소스를 공유하는 경우 AWS WA Tool에서는 보안 주체에게 초대를 보내지 않습니다. 조직의 보안 주체는 초대를 교환하지 않고도 공유 리소스에 액세스할 수 있습니다.

조직 내에서 리소스 공유를 활성화하면 AWS WA Tool은 `AWSServiceRoleForWellArchitected`라는 서비스 연결 역할을 생성합니다. 이 역할은 AWS WA Tool 서비스만 수임할 수 있으며, AWS 관리형 정책 `AWSWellArchitectedOrganizationsServiceRolePolicy`를 사용하여 서비스가 속한 조직에 대한 정보를 검색할 수 있는 AWS WA Tool 권한을 부여합니다.

전체 조직 또는 OU와 리소스를 더 이상 공유할 필요가 없는 경우 리소스 공유를 비활성화할 수 있습니다.

요구 사항

- 조직의 관리 계정에 보안 주체로 로그인한 상태에서만 이 단계를 수행할 수 있습니다.
- 조직에서 모든 기능이 활성화되어 있어야 합니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.

> **Important**
>
> AWS WA Tool 콘솔을 사용하여 AWS Organizations와의 공유를 활성화해야 합니다. 이렇게 하면 `AWSServiceRoleForWellArchitected` 서비스 연결 역할이 생성됩니다. AWS Organizations 콘솔 또는 enable-aws-service-access AWS CLI 명령을 사용하여 AWS Organizations를 통한 신뢰할 수 있는 액세스를 활성화하면 `AWSServiceRoleForWellArchitected` 서비스 연결 역할이 생성되지 않으며 조직 내에서 리소스를 공유할 수 없습니다.

조직 내 리소스 공유를 활성화하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.

   조직의 관리 계정에 보안 주체로 로그인한 상태여야 합니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. AWS Organizations 지원 활성화를 선택합니다.
4. 설정 저장을 선택합니다.

조직 내 리소스 공유를 활성화하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.

   조직의 관리 계정에 보안 주체로 로그인한 상태여야 합니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. AWS Organizations 지원 활성화를 선택 해제합니다.
4. 설정 저장을 선택합니다.

AWS WA Tool 리소스에 태그 지정

AWS WA Tool 리소스 관리를 돕기 위해 태그 형식으로 각 리소스에 고유한 메타데이터를 할당할 수 있습니다. 이 주제에서는 태그를 설명하고 태그를 생성하는 방법을 보여줍니다.

내용

태그 기본 사항

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다.

태그를 사용하면 AWS 리소스를 용도, 소유자, 환경과 같은 다양한 기준으로 분류할 수 있습니다. 동일한 유형의 리소스가 많은 경우 할당한 태그에 따라 특정 리소스를 빠르게 식별할 수 있습니다. 예를 들어 AWS WA Tool 서비스에 태그 집합을 정의하면 각 서비스의 소유자 및 스택 수준을 추적하는 데 도움이 됩니다. 각 리소스 유형에 대해 일관된 태그 키 집합을 고안하는 것이 좋습니다.

태그가 리소스에 자동으로 할당되는 것은 아닙니다. 태그를 추가한 후에는 언제든지 태그 키와 값을 편집하거나 리소스에서 태그를 제거할 수 있습니다. 리소스를 삭제하면 리소스 태그도 삭제됩니다.

태그는 AWS WA Tool에는 의미가 없으며 엄격하게 문자열로 해석됩니다. 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 Null로 설정할 수는 없습니다. 해당 리소스에 대해 키가 기존 태그와 동일한 태그를 추가하는 경우 새 값이 이전 값을 덮어씁니다.

AWS Management Console, AWS CLI, AWS WA Tool API를 사용하여 태그 관련 작업을 수행할 수 있습니다.

AWS Identity and Access Management(IAM)를 사용하는 경우 AWS 계정에서 태그를 생성, 편집 또는 삭제할 수 있는 권한이 있는 사용자를 제어할 수 있습니다.

리소스에 태그 지정

새로운 또는 기존 AWS WA Tool 리소스에 태그를 지정할 수 있습니다.

AWS WA Tool 콘솔을 사용 중인 경우 새로 생성된 리소스 또는 기존 리소스에 태그를 언제든지 적용할 수 있습니다. 기존 워크로드의 경우 속성 탭을 통해 태그를 적용할 수 있습니다. 기존 사용자 지정 렌즈, 프로필 및 검토 템플릿의 경우 개요 탭을 통해 태그를 적용할 수 있습니다.

AWS WA Tool API, AWS CLI 또는 AWS SDK를 사용 중인 경우 관련 API 작업의 `tags` 파라미터를 사용하여 새 리소스에 태그를 적용하거나 `TagResource` API 작업을 사용하여 기존 리소스에 태그를 적용할 수 있습니다. 자세한 내용은 TagResource를 참조하세요.

일부 리소스 생성 작업에서는 리소스 생성 시 리소스에 태그를 지정할 수 있습니다. 리소스 생성 중에 태그를 적용할 수 없는 경우 리소스 생성 프로세스는 실패합니다. 이로써 생성 중에 태그를 지정하려는 리소스는 지정된 태그와 함께 생성되거나 전혀 생성되지 않습니다. 생성 시 리소스에 태그를 지정하면 리소스 생성 후 사용자 지정 태그 지정 스크립트를 실행할 필요가 없습니다.

다음 표는 태그를 지정할 수 있는 AWS WA Tool 리소스와 생성 시 태그를 지정할 수 있는 리소스를 설명합니다.

AWS WA Tool 리소스 태그 지정 지원

Resource	태그 지원	태그 전달 지원	생성 시 태그 지정 지원(AWS WA Tool API, AWS CLI, AWS SDK)
AWS WA Tool 워크로드	예	아니요	예
AWS WA Tool 사용자 지정 렌즈	예	아니요	예
AWS WA Tool 프로필	예	아니요	예
AWS WA Tool 검토 템플릿	예	아니요	예

태그 제한

태그에 적용되는 기본 제한은 다음과 같습니다.

- 리소스당 최대 태그 수 – 50개
- 각 리소스에 대해 각 태그 키는 고유하며 하나의 값만 가질 수 있습니다.
- 최대 키 길이 - UTF-8 형식의 유니코드 문자 128자
- 최대 값 길이 - UTF-8 형식의 유니코드 문자 256자
- 태그 지정 스키마를 여러 AWS 서비스와 리소스에서 사용하는 경우 다른 서비스에서 허용되는 문자에 제한이 있을 수 있음에 유의하세요. 일반적으로 허용되는 문자는 UTF-8로 표시할 수 있는 문자, 숫자 및 공백과 특수 문자 + - = . _ : / @입니다.
- 태그 키와 값은 대소문자를 구분합니다.
- AWS 용도로 예약된 키 또는 값에는 `aws:`, `AWS:` 또는 이러한 접두사의 대문자 또는 소문자 조합을 사용하지 않습니다. 이 접두사가 지정된 태그 키나 값은 편집하거나 삭제할 수 없습니다. 이 접두사가 포함된 태그는 리소스당 태그 수 제한에 포함되지 않습니다.

콘솔을 사용한 태그 작업

AWS WA Tool 콘솔을 사용하면 새 리소스 또는 기존 리소스에 연결된 태그를 관리할 수 있습니다.

생성 중 개별 리소스에서 태그 추가

AWS WA Tool 리소스를 생성할 때 태그를 해당 리소스에 추가할 수 있습니다.

개별 리소스에 대한 태그 추가 및 삭제

AWS WA Tool을 사용하면 워크로드의 경우 속성 탭에서, 그리고 사용자 지정 렌즈, 프로필 및 검토 템플릿의 경우 개요 탭에서 리소스와 관련된 태그를 직접 추가하거나 삭제할 수 있습니다.

워크로드에 태그를 추가하거나 삭제하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 탐색 모음에서 사용할 리전을 선택합니다.
3. 탐색 창에서 워크로드를 선택합니다.
4. 수정할 워크로드를 선택하고 속성을 선택합니다.
5. 태그 섹션에서 태그 관리를 선택합니다.
6. 필요에 따라 태그를 추가하거나 삭제합니다.

    - 태그를 추가하려면 새 태그 추가를 선택한 다음 키와 값 필드를 입력합니다.

- 태그를 삭제하려면 제거를 선택합니다.

7. 추가, 수정 또는 삭제하려는 각 태그에 대해 이 과정을 반복합니다. 저장을 선택하여 변경 사항을 저장합니다.

사용자 지정 렌즈에 태그를 추가하거나 삭제하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 탐색 모음에서 사용할 리전을 선택합니다.
3. 탐색 창에서 사용자 지정 렌즈를 선택합니다.
4. 수정할 사용자 지정 렌즈 이름을 선택합니다.
5. 개요 탭의 태그 섹션에서 태그 관리를 선택합니다.
6. 필요에 따라 태그를 추가하거나 삭제합니다.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키와 값 필드를 입력합니다.
   - 태그를 삭제하려면 제거를 선택합니다.
7. 추가, 수정 또는 삭제하려는 각 태그에 대해 이 과정을 반복합니다. 저장을 선택하여 변경 사항을 저장합니다.

프로필에서 태그를 추가하거나 삭제하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 탐색 모음에서 사용할 리전을 선택합니다.
3. 탐색 창에서 프로필을 선택합니다.
4. 수정할 프로필의 이름을 선택합니다.
5. 개요 탭의 태그 섹션에서 태그 관리를 선택합니다.
6. 필요에 따라 태그를 추가하거나 삭제합니다.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키와 값 필드를 입력합니다.
   - 태그를 삭제하려면 제거를 선택합니다.
7. 추가, 수정 또는 삭제하려는 각 태그에 대해 이 과정을 반복합니다. 저장을 선택하여 변경 사항을 저장합니다.

검토 템플릿에 태그를 추가하거나 삭제하려면

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/wellarchitected/에서 AWS Well-Architected Tool 콘솔을 엽니다.
2. 탐색 모음에서 사용할 리전을 선택합니다.
3. 탐색 창에서 검토 템플릿을 선택합니다.
4. 수정할 검토 템플릿의 이름을 선택합니다.
5. 개요 탭의 태그 섹션에서 태그 관리를 선택합니다.
6. 필요에 따라 태그를 추가하거나 삭제합니다.
   - 태그를 추가하려면 새 태그 추가를 선택한 다음 키와 값 필드를 입력합니다.
   - 태그를 삭제하려면 제거를 선택합니다.
7. 추가, 수정 또는 삭제하려는 각 태그에 대해 이 과정을 반복합니다. 저장을 선택하여 변경 사항을 저장합니다.

API를 사용한 태그 작업

다음 AWS WA Tool API 작업을 사용하여 리소스에 대한 태그를 추가, 업데이트, 나열 및 삭제합니다.

AWS WA Tool 리소스 태그 지정 지원

작업	API 작업
하나 이상의 태그를 추가하거나 덮어씁니다.	TagResource
하나 이상의 태그를 삭제합니다.	UntagResource
리소스에 대한 태그를 나열합니다.	ListTagsForResource

일부 리소스 생성 작업에서는 리소스를 생성할 때 태그를 지정할 수 있습니다. 다음 태스크는 생성 시 태그 지정을 지원합니다.

작업	API 작업
워크로드 생성	CreateWorkload
새 렌즈 가져오기	ImportLens

작업	API 작업
프로필 생성	CreateProfile
검토 템플릿 생성	CreateReviewTemplate

AWS CloudTrail을 사용하여 AWS WA Tool API 호출 로깅

AWS Well-Architected Tool는 AWS WA Tool에서 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail와 통합됩니다. CloudTrail은 AWS WA Tool에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS WA Tool 콘솔로부터의 직접 호출과 AWS WA Tool API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 AWS WA Tool 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 AWS WA Tool에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

CloudTrail의 AWS WA Tool 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. AWS WA Tool에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 정보는 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS WA Tool에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 추가적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 트레일 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에서 Amazon SNS 알림 구성
- 여러 리전으로부터 CloudTrail 로그 파일 받기 및 여러 계정으로부터 CloudTrail 로그 파일 받기

모든 AWS WA Tool 작업이 CloudTrail에서 로깅되고 AWS Well-Architected Tool에서 정의한 작업에서 문서화됩니다. 예를 들어 `CreateWorkload`, `DeleteWorkload` 및 `CreateWorkloadShare` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 이루어진 보안 인증 정보가 일반 사용자인지 루트 사용자인지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지.

자세한 설명은 CloudTrail userIdentity 요소를 참조하십시오.

AWS WA Tool 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 `CreateWorkload` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예시입니다.

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
         "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
         "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

EventBridge

Well-Architected 리소스에 대한 작업이 수행되면 AWS Well-Architected Tool가 Amazon EventBridge로 이벤트를 전송합니다. EventBridge 및 이러한 이벤트를 사용하여 리소스에 변경 사항이 생길 때 알림과 같은 작업을 수행하는 규칙을 작성할 수 있습니다. 자세한 내용은 Amazon EventBridge란 무엇인가요?를 참조하세요.

> **Note**
>
> 이벤트는 최선의 작업을 기반으로 전달됩니다.

다음 작업을 수행하면 EventBridge 이벤트가 발생합니다.

- 워크로드 관련 작업
  - 워크로드 생성 또는 삭제
  - 마일스톤 생성
  - 워크로드 속성 업데이트
  - 워크로드 공유 또는 공유 해제
  - 공유 초대 상태 업데이트
  - 태그 추가 및 삭제
  - 답변 업데이트
  - 검토 노트 업데이트
  - 워크로드에 렌즈 추가 또는 삭제
- 렌즈 관련 작업
  - 사용자 지정 렌즈 가져오기 또는 내보내기
  - 사용자 지정 렌즈 게시
  - 사용자 지정 렌즈 삭제
  - 사용자 지정 렌즈 공유 또는 공유 해제
  - 공유 초대 상태 업데이트
  - 워크로드에 렌즈 추가 또는 삭제

AWS WA Tool의 샘플 이벤트

이 단원에는 AWS Well-Architected Tool의 예제 이벤트가 포함되어 있습니다.

워크로드의 답변 업데이트


```
{
  "version":"0",
  "id":"00de336a-83cc-b80b-f0e6-f44c88a96050",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.wellarchitected",
  "account":"123456789012",
  "time":"2022-02-17T08:01:25Z",
  "region":"us-west-2",
  "resources":[],
  "detail":{
     "eventVersion":"1.08",
     "userIdentity":{
        "type":"AssumedRole",
        "principalId":"AROA4JUSXMN5ZR6S7LZNP:sample-user",
        "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "sessionContext":{
           "sessionIssuer":{
              "type":"Role",
              "principalId":"AROA4JUSXMN5ZR6S7LZNP",
              "arn":"arn:aws:iam::123456789012:role/Admin",
              "accountId":"123456789012",
              "userName":"Admin"
           },
           "webIdFederationData":{},
           "attributes":{
              "creationDate":"2022-02-17T07:21:54Z",
              "mfaAuthenticated":"false"
           }
        }
     },
     "eventTime":"2022-02-17T08:01:25Z",
     "eventSource":"wellarchitected.amazonaws.com",
     "eventName":"UpdateAnswer",
     "awsRegion":"us-west-2",
```

```
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "Status":"Acknowledged",
         "SelectedChoices":"***",
         "ChoiceUpdates":"***",
         "QuestionId":"priorities",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0",
         "IsApplicable":true,
         "LensAlias":"wellarchitected",
         "Reason":"NONE",
         "Notes":"***"
      },
      "responseElements":{
         "Answer":"***",
         "LensAlias":"wellarchitected",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0"
      },
      "requestID":"7bae1153-26a8-4dc0-9307-68b17b107619",
      "eventID":"8339c258-4ddd-48aa-ab21-3f82ce9d79cd",
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

사용자 지정 렌즈 게시

```
{
   "version":"0",
   "id":"4054a34b-60a9-53c1-3146-c1a384dba41b",
   "detail-type":"AWS API Call via CloudTrail",
   "source":"aws.wellarchitected",
   "account":"123456789012",
   "time":"2022-02-17T08:58:34Z",
   "region":"us-west-2",
   "resources":[],
```

```
   "detail":{
      "eventVersion":"1.08",
      "userIdentity":{
         "type":"AssumedRole",
         "principalId":"AROA4JUSXMN5ZR6S7LZNP:example-user",
         "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
         "accountId":"123456789012",
         "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
         "sessionContext":{
            "sessionIssuer":{
               "type":"Role",
               "principalId":"AROA4JUSXMN5ZR6S7LZNP",
               "arn":"arn:aws:iam::123456789012:role/Admin",
               "accountId":"123456789012",
               "userName":"Admin"
            },
            "webIdFederationData":{},
            "attributes":{
               "creationDate":"2022-02-17T07:21:54Z",
               "mfaAuthenticated":"false"
            }
         }
      },
      "eventTime":"2022-02-17T08:58:34Z",
      "eventSource":"wellarchitected.amazonaws.com",
      "eventName":"CreateLensVersion",
      "awsRegion":"us-west-2",
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "IsMajorVersion":true,
         "LensVersion":"***",
         "ClientRequestToken":"03f46163-e95c-4455-8479-266373aa09c7",
         "LensAlias":"***"
      },
      "responseElements":{
         "LensArn":"arn:aws:wellarchitected:us-
west-2:123456789012:lens/6261deecb9def44f9aecc938ca25d94e",
         "LensVersion":"***"
      },
      "requestID":"167b7051-980d-42ee-9967-0b4b3163e948",
      "eventID":"c7ef2b47-419d-45b7-8982-fbade9b558c7",
```

```
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

문서 이력

다음 표에서는 AWS Well-Architected Tool의 본 릴리스 관련 설명서를 소개합니다.

- API 버전: 최신
- 최종 문서 업데이트: 2025년 4월 17일

변경 사항	설명	날짜
새 렌즈	이 릴리스에서는 Lens Catalog에 새 렌즈 하나를 추가했습니다.	2025년 4월 17일
새 렌즈 및 업데이트된 렌즈	이번 릴리스에서는 Lens Catalog에 새 렌즈 하나를 추가하고 다른 렌즈 하나를 업데이트했습니다.	2024년 6월 27일
Jira	이 릴리스에서는 AWS Well-Architected Tool Connector for Jira를 추가했습니다.	2024년 4월 16일
새 렌즈	이번 릴리스에서는 Lens Catalog에 새 렌즈를 추가했습니다.	2024년 3월 26일
업데이트된 기능	이번 릴리스에서는 AWS WA Tool에 Lens Catalog 기능이 추가되었습니다.	2023년 11월 26일
업데이트된 기능	이번 릴리스에는 AWS WA Tool에 검토 템플릿 기능이 추가되었습니다.	2023년 10월 3일
WellArchitectedConsoleReadOnlyAccess 관리형 정책 업데이트	`WellArchitectedConsoleReadOnlyAccess` 에 `"wellarchitected:E`	2023년 6월 22일

	xportLens" 가 추가되었습니다.	
업데이트된 기능	이번 릴리스에는 AWS WA Tool에 프로필 기능이 추가되었습니다.	2023년 6월 13일
업데이트된 기능	이번 릴리스에서는 AWS Trusted Advisor 및 AWS Service Catalog AppRegistry 통합이 강화되고 AWS 관리형 정책에 AWSWellArchitectedDiscoveryServiceRolePolicy 가 추가됩니다.	2023년 5월 3일
내용 업데이트	자세한 위험 및 개선 계획 정보를 포함하도록 대시보드 페이지가 업데이트되었습니다. 통합 워크로드 보고서를 생성하는 기능도 추가되었습니다.	2023년 3월 30일
내용 업데이트	WellArchitectedConsoleReadOnlyAccess 정책 이름을 수정했습니다.	2023년 1월 19일
AWS WA Tool에 대한 IAM 지침 업데이트	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 내용은 IAM의 보안 모범 사례를 참조하세요.	2023년 1월 4일
업데이트된 기능	이번 릴리스에서는 도구에서 FTR 렌즈가 삭제되었습니다.	2022년 12월 14일
업데이트된 기능	이번 릴리스에는 AWS Trusted Advisor 및 AWS Service Catalog AppRegistry 통합이 추가됩니다.	2022년 11월 7일

내용 업데이트	choices에 대한 사용자 지정 렌즈 JSON 예제의 문제를 수정했습니다.	2022년 9월 29일
내용 업데이트	사용자 지정 렌즈 JSON 사양의 choices 섹션이 업데이트되었습니다.	2022년 8월 2일
업데이트된 기능	이번 릴리스에는 AWS 관리형 정책에 대한 추적 변경 내용이 추가되고 AWSWellArchitectedOrganizationsServiceRolePolicy 에 ListAWSServiceAccessForOrganization 권한을 부여하는 새 작업이 추가되었습니다.	2022년 7월 22일
조직 공유 추가	이번 릴리스에는 조직 및 조직 단위(OU)에 워크로드와 사용자 지정 렌즈를 공유하는 기능이 추가되었습니다.	2022년 6월 30일
업데이트된 기능	이번 릴리스에는 사용자 지정 렌즈의 선택 항목에 대한 추가 리소스를 지정하고, 사용자 지정 렌즈를 게시하기 전에 미리 보고, 사용자 지정 렌즈에 태그를 추가하는 기능이 추가되었습니다.	2022년 6월 21일
업데이트된 기능	이번 릴리스에는 AWS re:Post에서 AWS Well-Architected 커뮤니티에 액세스할 수 있는 기능이 추가되었습니다.	2022년 5월 31일

업데이트된 기능	이번 릴리스에는 튜토리얼에 지속 가능성 원칙과 마이너 업데이트가 추가되었습니다.	2022년 3월 31일
EventBridge 지원 추가	이제 Well-Architected 리소스에 변경 사항이 생길 때 AWS WA Tool에서 Amazon EventBridge에 이벤트를 전송합니다.	2022년 3월 3일
업데이트된 기능	이제 개별 모범 사례를 해당 사항 없음으로 표시할 수 있습니다.	2021년 7월 14일
리소스 태그 지정 사용 가능	이번 릴리스에는 워크로드에 태그를 추가하는 기능이 추가되었습니다.	2021년 3월 3일
API 사용 가능	이번 릴리스에는 AWS WA Tool API와 AWS CloudTrail 로깅 정보가 추가되었습니다.	2020년 12월 16일
업데이트된 기능	이번 릴리스에는 FTR 및 SaaS 렌즈가 도구에 추가되었습니다.	2020년 12월 3일
데이터 보호 업데이트	데이터 보호 정보가 업데이트되었습니다.	2020년 11월 5일
내용 업데이트	새 렌즈를 사용하도록 워크로드를 업그레이드한 후에는 이전 버전으로 돌아갈 수 없다는 점을 명확히 했습니다.	2020년 7월 8일
내용 업데이트	2019년 3월 20일 이후에 도입된 AWS 리전 공유를 명확히 했습니다.	2020년 6월 24일

업데이트된 기능	워크로드 공유 초대가 거부되면 워크로드 공유에 대한 액세스가 즉시 제거됩니다. 공유가 수락되면 공유 액세스가 부여됩니다.	2020년 6월 17일
내용 업데이트	HRI(고위험 문제) 및 MRI(중간 위험 문제)에 대한 정의가 추가되었습니다.	2020년 6월 12일
내용 업데이트	AWS에서 사용자 데이터를 사용하는 방법에 대한 섹션이 추가되었습니다.	2020년 5월 21일
업데이트된 기능	이 릴리스에서는 워크로드에 검토 소유자를 추가합니다.	2020년 4월 1일
업데이트된 기능	이 릴리스에서는 워크로드에 아키텍처 다이어그램 링크를 추가합니다.	2020년 3월 10일
내용 업데이트	워크로드 공유는 AWS 리전별로 다르다는 것을 명확히 했습니다.	2020년 1월 10일
업데이트된 기능	이 릴리스에서는 워크로드 공유를 추가합니다.	2020년 1월 9일
내용 업데이트	보안 섹션을 최신 지침으로 업데이트했습니다.	2019년 12월 6일
업데이트된 기능	이 릴리스에서는 워크로드를 정의할 때 업종 필드가 선택 사항입니다.	2019년 8월 19일
업데이트된 기능	이 릴리스에서는 개선 계획 항목을 워크로드 보고서에 추가합니다.	2019년 7월 29일

업데이트된 기능	이 릴리스는 DeleteWorkload 작업을 정책에 추가합니다.	2019년 7월 18일
내용 업데이트	이 안내서의 내용은 가벼운 수정과 함께 업데이트되었습니다.	2019년 6월 19일
내용 업데이트	이 안내서의 내용은 가벼운 수정과 함께 업데이트되었습니다.	2019년 5월 30일
업데이트된 기능	이 릴리스는 워크로드 검토에 사용되는 프레임워크 버전 업그레이드를 지원합니다.	2019년 5월 1일
업데이트된 기능	이번 릴리스에는 워크로드를 정의할 때 AWS 리전 외의 리전을 지정할 수 있는 기능이 추가되었습니다.	2019년 2월 14일
AWS Well-Architected Tool 정식 출시	이번 릴리스에는 AWS Well-Architected Tool이 도입되었습니다.	2018년 11월 29일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하십시오.