AMS 고급 계정 온보딩 정보

AMS 고급 온보딩 가이드

버전 February 11, 2026

AMS 고급 온보딩 가이드: AMS 고급 계정 온보딩 정보

Table of Contents

AWS Managed Services 온보딩 소개

AWS Managed Services(AMS)에 오신 것을 환영합니다. AMS는 AWS 인프라를 지속적으로 관리하는 엔터프라이즈 서비스입니다. 이 가이드는 AMS에 대한 새 계정을 설정하고, AMS에 대한 네트워킹 및 액세스를 설정하고, 온보딩 설정을 검증하는 방법을 포함하여 AMS 사용을 시작하는 데 도움이 되도록 설계되었습니다.

AMS 서비스를 새 AWS 계정에 온보딩하는 데 필요한 작업을 준비하고 수행하는 IT 관리자를 위한 것입니다. AMS 서비스를 온보딩하려면 Active Directory 신뢰를 설정하고 다른 네트워킹 수준 작업을 완료하기 위한 특별한 권한이 필요합니다. 다중 계정 랜딩 존 계정 또는 단일 계정 랜딩 존 계정의 사용 여부를 결정하는 데 도움이 필요하면 단일 MALZ 또는 다중 MALZs.

> **Important**
>
> 이 가이드는이 소개 후 두 부분으로 나뉩니다. 하나는 다중 계정 랜딩 존 계정용이고 다른 하나는 단일 계정 랜딩 존 계정용입니다. 온보딩은 둘 다 상당히 다릅니다. 상황에 적용되는 가이드의 섹션 옆으로 이동하세요.

주제

AMS에 대해 알아보기

AMS를 더 잘 이해하려면 다음 AMS 사용 설명서 섹션을 참조하세요.

- AWS Managed Services란 무엇입니까?는 AMS 서비스를 도입하고 일반적인 AMS 관리형 네트워크 아키텍처뿐만 아니라 주요 기능, 운영 및 인터페이스를 설명합니다. 또한이 장에서는 AMS 관리

형 리소스에 액세스하는 방법과 Bastion을 사용하는 방법을 포함하여 액세스 관리에 대한 정보를 제공합니다.

- 주요 용어는 AMS 용어에 대한 정의와 설명을 제공합니다.
- AMS 기본값 이해는 기본 환경 구성 요소, IAM 및 EC2, 프록시, 모니터링되는 지표, 로깅, 엔드포인트 보안(EPS), 백업 및 패치 적용에 대한 기본값을 포함하여 AMS가 사용하는 기본값을 제공합니다.
- 변경 관리는 변경 요청(RFCs) 및 변경 유형(CTs)의 작동 방식에 대한 세부 정보를 제공하고 AMS RFCs 사용 예제를 포함합니다.
- AWS 콘솔, AMS CLI에 액세스하고, AMS 변경 관리 시스템, AMS SKMS, 보안, 서비스 요청, 인시던트, 모니터링, 로그, EPS, 백업 및 패치 관리를 사용하는 방법에 대한 몇 가지 추가 장이 있습니다.

AMS 다중 계정 랜딩 존 아키텍처에 대한 자세한 내용은 다중 계정 랜딩 존 네트워크 아키텍처를 참조하세요.

AMS 단일 계정 랜딩 존 아키텍처에 대한 자세한 내용은 단일 계정 랜딩 존 네트워크 아키텍처를 참조하세요.

AMS 키 용어

- AMS Advanced: AMS Advanced 설명서의 "서비스 설명" 섹션에 설명된 서비스입니다. 서비스 설명을 참조하세요.
- AMS 고급 계정: AWS AMS 고급 온보딩 요구 사항의 모든 요구 사항을 항상 충족하는 계정입니다. AMS Advanced 혜택, 사례 연구 및 영업 담당자에게 연락하는 방법에 대한 자세한 내용은 AWS Managed Services를 참조하세요.
- AMS Accelerate Accounts: AWS AMS Accelerate 온보딩 요구 사항의 모든 요구 사항을 항상 충족하는 계정입니다. AMS Accelerate 시작하기를 참조하세요.
- AWS Managed Services: AMS 및 또는 AMS Accelerate.
- AWS Managed Services 계정: AMS 계정 및 또는 AMS Accelerate 계정.
- 중요 권장 사항: 리소스 또는에 대한 잠재적 위험 또는 중단을 방지하기 위해 조치가 필요함을 알리는 서비스 요청을 AWS 통해에서 발급한 권장 사항입니다 AWS 서비스. 지정된 날짜까지 중요 권장 사항을 따르지 않기로 결정한 경우 결정으로 인한 모든 손해에 대한 책임은 전적으로 사용자에게 있습니다.
- 고객 요청 구성: 다음에서 식별되지 않은 모든 소프트웨어, 서비스 또는 기타 구성:
  - Accelerate: 지원되는 구성 또는 AMS Accelerate, 서비스 설명.

  - AMS Advanced: 지원되는 구성 또는 AMS Advanced, 서비스 설명.
- 인시던트 통신: AMS는 AMS Accelerate용 지원 센터와 AMS용 AMS 콘솔에서 생성된 인시던트를 통해 인시던트를 사용자에게 전달하거나 사용자가 AMS로 인시던트를 요청합니다. AMS Accelerate 콘솔은 대시보드의 인시던트 및 서비스 요청 요약과 자세한 내용은 지원 센터 링크를 제공합니다.
- 관리형 환경: AMS Advanced 계정 및 또는 AMS에서 운영하는 AMS Accelerate 계정.

  AMS Advanced의 경우 여기에는 다중 계정 랜딩 존(MALZ) 및 단일 계정 랜딩 존(SALZ) 계정이 포함됩니다.
- 결제 시작 날짜:가 AWS Managed Services 온보딩 이메일에서 요청한 정보를 AWS 수신한 다음 영업일입니다. AWS Managed Services 온보딩 이메일은 계정에서 AWS Managed Services를 활성화하는 데 필요한 정보를 수집 AWS 하기 위해에서 사용자에게 보내는 이메일을 말합니다.

  이후에 등록한 계정의 경우 청구 시작일은 AWS Managed Services가 등록된 계정에 대한 AWS Managed Services 활성화 알림을 보낸 다음 날입니다. AWS Managed Services 활성화 알림은 다음과 같은 경우에 발생합니다.

  1. 호환되는 AWS 계정에 대한 액세스 권한을 부여하고 AWS Managed Services에 전달합니다.
  2. AWS Managed Services는 AWS Managed Services 계정을 설계하고 빌드합니다.
- 서비스 종료: 서비스 요청을 통해 AWS 최소 30일 전에 알림을 제공하여 어떤 이유로든 AWS Managed Services 모든 AWS Managed Services 계정 또는 지정된 AWS Managed Services 계정에 대해 AWS Managed Services를 종료할 수 있습니다. 서비스 종료 날짜에 다음 중 하나를 수행합니다.

  1. AWS 모든 AWS Managed Services 계정 또는 해당하는 경우 지정된 AWS Managed Services 계정의 제어를 사용자에게 인계하거나
  2. 양 당사자는 해당하는 경우 모든 AWS Managed Services 계정 또는 지정된 AWS Managed Services 계정에서 AWS 액세스 권한을 부여하는 AWS Identity and Access Management 역할을 제거합니다.
- 서비스 종료 날짜: 서비스 종료 날짜는 30일의 필수 종료 알림 기간이 끝나는 달의 마지막 날입니다. 필수 종료 알림 기간이 해당 월의 20일 이후인 경우 서비스 종료 날짜는 다음 달의 마지막 날입니다. 다음은 종료 날짜에 대한 예제 시나리오입니다.
  - 해지 알림이 4월 12일에 제공된 경우 30일 알림은 5월 12일에 종료됩니다. 서비스 종료 날짜는 5월 31일입니다.
  - 종료 알림이 4월 29일에 제공된 경우 30일 알림은 5월 29일에 종료됩니다. 서비스 종료 날짜는 6월 30일입니다.
- AWS Managed Services:makes를 제공하면 서비스 시작 날짜부터 각 AWS Managed Services 계정에 대한 AWS Managed Services에 액세스하고 사용할 수 있습니다. AWS

- 지정된 AWS Managed Services 계정에 대한 종료: 서비스 요청(“AMS 계정 종료 요청”)을 통해 AWS 알림을 제공하여 어떤 이유로든 지정된 AWS Managed Services 계정에 AWS Managed Services 대한 AWS Managed Services를 종료할 수 있습니다.

인시던트 관리 용어:

- 이벤트: AMS 환경의 변경 사항입니다.
- 알림: 지원되는의 이벤트가 임계값을 AWS 서비스 초과하고 경보를 트리거할 때마다 알림이 생성되고 연락처 목록으로 알림이 전송됩니다. 또한 인시던트 목록에 인시던트가 생성됩니다.
- 인시던트: AWS Managed Services 또는 사용자가 보고한 대로 영향을 미치는 AMS 환경 또는 AWS Managed Services의 예상치 못한 중단 또는 성능 저하입니다.
- 문제: 하나 이상의 인시던트에 대한 공유된 근본 원인입니다.
- 인시던트 해결 또는 인시던트 해결:
  - AMS가 해당 인시던트와 관련하여 사용할 수 없는 모든 AMS 서비스 또는 리소스를 사용 가능한 상태로 복원한 경우
  - AMS가 사용할 수 없는 스택 또는 리소스를 사용 가능한 상태로 복원할 수 없다고 판단한 경우
  - AMS가 사용자가 승인한 인프라 복원을 시작했습니다.
- 인시던트 대응 시간: 인시던트를 생성할 때와 AMS가 콘솔, 이메일, 서비스 센터 또는 전화를 통해 초기 응답을 제공할 때의 시간 차이입니다.
- 인시던트 해결 시간: AMS 또는 사용자가 인시던트를 생성하는 시점과 인시던트가 해결되는 시점 간의 시간 차이입니다.
- 인시던트 우선 순위: AMS 또는 사용자가 인시던트의 우선 순위를 낮음, 중간 또는 높음으로 지정하는 방법입니다.
  - 낮음: AMS 서비스의 중요하지 않은 문제입니다.
  - 중간: 관리형 환경 내의 AWS 서비스를 사용할 수 있지만 의도한 대로 작동하지 않습니다(해당 서비스 설명에 따라).
  - 높음: (1) AMS 콘솔 또는 관리형 환경 내의 하나 이상의 AMS APIs를 사용할 수 없거나, (2) 관리형 환경 내의 하나 이상의 AMS 스택 또는 리소스를 사용할 수 없고 사용 불가능으로 인해 애플리케이션이 기능을 수행할 수 없습니다.

  AMS는 위 지침에 따라 인시던트를 다시 분류할 수 있습니다.
- 인프라 복원: 인시던트 해결이 불가능한 경우 달리 지정하지 않는 한 영향을 받는 스택의 템플릿을 기반으로 기존 스택을 재배포하고 마지막으로 알려진 복원 지점을 기반으로 데이터 복원을 시작합니다.

인프라 용어:

- 관리형 프로덕션 환경: 고객의 프로덕션 애플리케이션이 있는 고객 계정입니다.
- 관리형 비프로덕션 환경: 개발 및 테스트용 애플리케이션과 같은 비프로덕션 애플리케이션만 포함하는 고객 계정입니다.
- AMS 스택: AMS에서 단일 단위로 관리하는 하나 이상의 AWS 리소스 그룹입니다.
- 변경 불가능한 인프라: Amazon EC2 Auto Scaling 그룹(ASGs)에 일반적으로 사용되는 인프라 유지 관리 모델로, 업데이트된 인프라 구성 요소(AMI)는 현재 위치에서 업데이트되지 않고 모든 배포 AWS에 대해 대체됩니다. 변경 불가능한 인프라의 장점은 모든 구성 요소가 항상 동일한 기반에서 생성되므로 동기 상태를 유지하는 것입니다. 변형성은 AMI 구축을 위한 도구 또는 워크플로와 무관합니다.
- 변경 가능한 인프라: Amazon EC2 Auto Scaling 그룹이 아니며 단일 인스턴스 또는 몇 개의 인스턴스만 포함하는 스택에 일반적으로 사용되는 인프라 유지 관리 모델입니다. 이 모델은 수명 주기가 시작될 때 시스템이 배포된 다음 시간이 지남에 따라 업데이트가 해당 시스템에 계층화되는 기존의 하드웨어 기반 시스템 배포를 가장 잘 나타냅니다. 시스템에 대한 모든 업데이트는 인스턴스에 개별적으로 적용되며 애플리케이션 또는 시스템 재시작으로 인해 시스템 가동 중지(스택 구성에 따라 다름)가 발생할 수 있습니다.
- 보안 그룹: 인바운드 및 아웃바운드 트래픽을 제어하는 인스턴스의 가상 방화벽입니다. 보안 그룹은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 따라서 VPC의 서브넷에 있는 각 인스턴스에는 서로 다른 보안 그룹 세트가 할당될 수 있습니다.
- 서비스 수준 계약(SLAs): 예상 서비스 수준을 정의하는 사용자와의 AMS 계약의 일부입니다.
- SLA 사용 불가 및 사용 불가:
  - 오류가 발생하는 API 요청입니다.
  - 사용자가 제출한 콘솔 요청으로 5xx HTTP 응답이 발생합니다(서버가 요청을 수행할 수 없음).
  - AMS 관리형 인프라에서 스택 또는 리소스를 구성하는 모든 AWS 서비스 오퍼링은 서비스 상태 대시보드에 표시된 대로 “서비스 중단” 상태입니다.
  - AMS 제외로 인해 직접 또는 간접적으로 발생하는 사용 불가는 서비스 크레딧 자격을 결정하는 데 고려되지 않습니다. 서비스를 사용할 수 없는 기준을 충족하지 않는 한 서비스를 사용할 수 있는 것으로 간주됩니다.
- 서비스 수준 목표(SLOs): AMS 서비스에 대한 특정 서비스 목표를 정의하는 AMS 계약의 일부입니다.

패치 용어:

- 필수 패치: 환경 또는 계정의 보안 상태를 손상시킬 수 있는 문제를 해결하기 위한 중요한 보안 업데이트입니다. “중요 보안 업데이트”는 AMS 지원 운영 체제의 공급업체가 “중요”로 평가한 보안 업데이트입니다.
- 발표된 패치와 릴리스된 패치: 패치는 일반적으로 일정에 따라 발표되고 릴리스됩니다. 발생한 패치는 패치의 필요성이 발견되면 발표되며, 일반적으로 패치가 릴리스된 직후 발표됩니다.
- 패치 추가 기능: AWS Systems Manager (SSM) 기능을 활용하는 AMS 인스턴스에 대한 태그 기반 패치를 제공하므로 인스턴스에 태그를 지정하고 구성한 기준 및 창을 사용하여 해당 인스턴스에 패치를 적용할 수 있습니다.
- 패치 방법:
  - 현재 위치 패치: 기존 인스턴스를 변경하여 수행되는 패치입니다.
  - AMI 대체 패치: 기존 EC2 Auto Scaling 그룹 시작 구성의 AMI 참조 파라미터를 변경하여 수행되는 패치입니다.
- 패치 공급자(OS 공급업체, 타사): 패치는 애플리케이션의 공급업체 또는 관리 기관에서 제공합니다.
- 패치 유형:
  - CSU(Critical Security Update): 지원되는 운영 체제의 공급업체가 "Critical"로 평가한 보안 업데이트입니다.
  - 중요 업데이트(IU): 지원되는 운영 체제의 공급업체가 “중요”로 평가한 보안 업데이트 또는 “중요”로 평가한 비보안 업데이트입니다.
  - 기타 업데이트(OU): CSU 또는 IU가 아닌 지원되는 운영 체제의 공급업체에 의한 업데이트입니다.
- 지원되는 패치: AMS는 운영 체제 수준 패치를 지원합니다. 보안 취약성 또는 기타 버그를 수정하거나 성능을 개선하기 위해 공급업체에서 업그레이드를 릴리스합니다. 현재 지원되는 OSs 목록은 지원 구성을 참조하세요.

보안 용어:

- 탐지 제어: 보안, 운영 또는 고객 제어와 일치하지 않는 구성에 대해 고객 관리형 환경 및 워크로드를 지속적으로 감독하고 소유자에게 알리거나 리소스를 사전에 수정 또는 종료하여 조치를 취하는 AMS 생성 또는 활성화된 모니터 라이브러리입니다.

서비스 요청 조건:

- 서비스 요청: AMS가 사용자를 대신하여 수행할 작업에 대한 사용자의 요청입니다.
- 알림 알림: AMS 알림이 트리거될 때 AMS가 서비스 요청 목록 페이지에 게시한 알림입니다. 계정에 대해 구성된 연락처도 구성된 방법(예: 이메일)에 의해 알림을 받습니다. 인스턴스/리소스에 연락처

태그가 있고 태그 기반 알림에 대해 클라우드 서비스 제공 관리자(CSDM)에 동의를 제공한 경우 태그의 연락처 정보(키 값)에도 자동 AMS 알림에 대한 알림이 전송됩니다.

- 서비스 알림: 서비스 요청 목록 페이지에 게시되는 AMS의 알림입니다.

기타 용어:

- AWS Managed Services 인터페이스: AMS: AWS Managed Services 고급 콘솔, AMS CM API 및 지원 API. AMS Accelerate의 경우: 지원 콘솔 및 지원 API.
- 고객 만족도(CSAT): AMS CSAT는 모든 사례 또는 서신에 대한 사례 대응 등급, 분기별 설문 조사 등을 포함한 심층 분석을 통해 정보를 제공합니다.
- DevOps: DevOps는 모든 단계에서 자동화 및 모니터링을 강력하게 지원하는 개발 방법론입니다. DevOps는 자동화의 토대를 통해 전통적으로 분리된 개발 및 운영 기능을 결합하여 개발 주기 단축, 배포 빈도 증가 및 보다 신뢰할 수 있는 릴리스를 목표로 합니다. 개발자가 운영을 관리할 수 있고 운영에서 개발을 알리면 문제와 문제가 더 빠르게 발견 및 해결되고 비즈니스 목표가 더 쉽게 달성됩니다.
- ITIL: Information Technology Infrastructure Library(ITIL이라고 함)는 IT 서비스의 수명 주기를 표준화하도록 설계된 ITSM 프레임워크입니다. ITIL은 서비스 전략, 서비스 설계, 서비스 전환, 서비스 운영, 서비스 개선 등 IT 서비스 수명 주기를 다루는 5단계로 구성됩니다.
- IT 서비스 관리(ITSM): IT 서비스를 비즈니스 요구 사항에 맞게 조정하는 일련의 사례입니다.
- 관리형 모니터링 서비스(MMS): AMS는 자체 모니터링 시스템인 관리형 모니터링 서비스(MMS)를 운영합니다.이 시스템은 AWS 상태 이벤트를 사용하고 Amazon CloudWatch 데이터 및 다른의 데이터를 집계 AWS 서비스하여 Amazon Simple Notification Service(Amazon SNS) 주제를 통해 생성된 모든 경보를 AMS 운영자(온라인 24x7)에게 알립니다.
- 네임스페이스: IAM 정책을 생성하거나 Amazon 리소스 이름(ARNs)으로 작업할 때 네임스페이스 AWS 서비스 를 사용하여를 식별합니다. 작업 및 리소스를 식별할 때 네임스페이스를 사용합니다.

AMS 모드

이를 통해 비즈니스 성과를 달성하기 위해 원하는 유연성과 규범적 거버넌스 조합을 기반으로 애플리케이션을 호스팅하는 데 적합한 AWS Managed Services(AMS) 모드를 선택할 수 있습니다.

이 정보의 대상은 다음과 같습니다.

- 랜딩 존의 전략 및 거버넌스를 담당하는 고객 팀. 이 정보는 팀이 내부 및 외부 고객에게 제공하려는 AMS 모드를 사용하여 AMS 관리형 랜딩 존의 기반을 마련하는 데 도움이 됩니다.

- 비즈니스 및 애플리케이션 소유자는 애플리케이션을 AMS로 마이그레이션하는 작업을 담당했습니다. 이 정보는 애플리케이션을 마이그레이션/호스팅하는 데 적합한 AMS 모드를 사용하여 애플리케이션 마이그레이션을 계획하는 데 도움이 됩니다. 참고로 소프트웨어 개발 수명 주기(SDLC) 수명 주기의 여러 단계에서 동일한 애플리케이션을 둘 이상의 AMS 모드에서 호스팅할 수 있습니다.
- AMS 파트너는 AMS를 구축하고 AMS로 마이그레이션하기 위한 다양한 옵션에 대해 고객을 안내하는 작업을 담당했습니다.

이 정보는 AMS를 활용하여 클라우드로의 여정을 가속화하기로 이미 결정했다고 가정합니다. 클라우드 마이그레이션 여정의 두 지점에서이 백서를 참조하세요. 첫째, AMS 관리형 플랫폼 설정의 기초 단계에서 참조하세요. 둘째, 클라우드 채택 여정의 기반에서 마이그레이션 단계로 전환할 때 AMS로의 온보딩이 완료되고 애플리케이션 거버넌스 및 운영에 집중하고 있는 직후입니다.

AMS 모드 및 애플리케이션 또는 워크로드

새 애플리케이션 계정을 요청하거나 기존 애플리케이션 계정에서 애플리케이션을 호스팅하여 올바른 모드를 선택할 때 애플리케이션의 운영 및 거버넌스 요구 사항을 고려합니다. 각 애플리케이션 또는 워크로드에 적합한 AMS 모드 선택은 다음 요인에 따라 달라집니다.

- 환경에서 제공할 SDLC 수명 주기 함수의 유형(예: 조정되지 않은 변경 사항이 있는 샌드박스, 자주 변경되는 UAT, 최소한의 변경 사항이 있고 규제가 엄격한 프로덕션)
- 필요한 거버넌스 정책(OU 수준에서 SCPs를 통해 적용됨)
- 운영 모델(운영 책임을 소유하거나 AMS에 아웃소싱하려는 경우)
- 클라우드 운영 시간, 운영 비용 등 원하는 비즈니스 성과입니다.

> **Note**
>
> AMS 서비스당 모드 유형에 대한 설명은 AMS의 모드 및 계정 유형을 참조하세요.
> 다양한 모드의 실제 사용 사례는 AMS 모드의 실제 사용 사례를 참조하세요.

다음 표에는 애플리케이션 소유자가 가장 적합한 AMS 모드를 결정하는 데 도움이 되는 주요 고려 사항이 요약되어 있습니다. 애플리케이션 소유자는 특정 애플리케이션에 적용되는 모드를 완전히 이해하려면 애플리케이션 마이그레이션 전에 평가 단계를 포함해야 합니다. 예: 클라우드 네이티브 서비스 또는 서버리스 아키텍처를 기반으로 하는 애플리케이션의 경우 가장 좋은 옵션은 개발자 모드에서 빌드 및 반복을 시작하고 AMS 관리형 - SSP 모드를 사용하여 최종 코드형 인프라를 배포하는 것입니다. 이 경우 자동 배포를 위해 생성된 CloudFormation 템플릿이 AMS에서 제시한 수집 지침을 충족하는지

확인하기 위해 라이트 리팩터링이 필요할 수 있습니다. 또한 모든 IAM 권한은 최소 권한 모델을 따르도록 AMS Security의 승인을 받아야 합니다.

애플리케이션을 호스팅하도록 선택한 AMS 모드를 사용하면 원하는 클라우드 운영 모델을 구축할 수 있습니다.

> **Note**
>
> 애플리케이션을 호스팅하기 위해 선택한 다양한 AMS 모드를 기반으로 단일 AMS 관리형 랜딩 존에 둘 이상의 클라우드 운영 모델이 존재할 수 있습니다.

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
운영 준비 상태						
로깅, 모니터링 및 이벤트 관리	모든 관리형 인프라를 담당하는 AMS			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	고객 책임
연속성 관리	고객이 선택한 백업 계획을 실행할 AMS 책임			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
인스턴스 수준 액세스 관리	온프레미스 도메인과의 단방향 AD 신뢰를 통해 AMS 관리됩니다. 관리형 인프라가 AMS 도메인에 조인해야 함			해당 사항 없음	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
보안 관리 및 계정 수준 액세스 관리	모든 관리형 계정에 대한 AMS 책임			모든 관리형 계정을 담당하는 AMS	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
패치 관리	모든 관리형 계정에 대한 AMS 책임			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
변경 관리	모든 관리형 계정에 대한 AMS 책임			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
프로비저닝 관리	AMS에서 제공되는 프로비저닝 옵션에 대한 권장 및 표준화	AMS 규범적 표준에 따라 AWS Service Catalog용 AWS 서비스 API를 직접 사용할 수 있는 유연성	AMS 규범적 표준에 따라 AWS 서비스 API를 직접 사용할 수 있는 유연성	SSP 서비스에 AWS 서비스 APIs를 직접 사용할 수 있는 유연성	프로비저닝에 AWS 서비스 API를 직접 사용할 수 있는 유연성	
인시던트 관리 및 감사	모든 관리형 계정에 대한 AMS 책임				AMS Change Management System 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
GuardRails 및 공유 인프라(네트워크) 및 보안 프레임워크	AMS Core 계정의 권장 및 표준화 활용					유연한 맞춤형 AMS Core 계정 활용
애플리케이션 준비 상태						
애플리케이션 리팩터링	라이트 리팩터링 필요				라이트 리팩터링 필요(AMS Standard CM을 사용하여 프로비저닝된 경우)	리팩터링 필요 없음
AWS 서비스 지원	AMS에서 지원하는 것으로 제한됨					제한되지 않음
비즈니스 고려 사항						
운영 준비 시간	3~6개월			6개월 + 고객 애플리케이션 운영 역량에 따라 다름		고객 인프라 및 애플리케이션 운영 역량에 따라 6~18개월
비용	$$$$			$$$	$$	$

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
애플리케이션 예제	3 티어 스택이 있는 Webserver, 규정 준수 및 규제 요구 사항이 있는 앱			API Gateway를 사용하는 Webserver, ECS/EKS를 활용하는 컨테이너화된 애플리케이션	Lambda, Glue, Athena 등을 사용하는 Data Lake 애플리케이션에서 반복/최적화	샌드박스, 타사 관리형 애플리케이션과 같은 분산형 계정/애플리케이션

*OOD(Operations On Demand)에는 표준 CM 모드를 사용하는 고객이 전용 리소싱을 통해 변경 사항을 관리할 수 있는 기능이 있습니다. 자세한 내용은 오퍼링의 온디맨드 운영 카탈로그를 참조하고 클라우드 서비스 제공 관리자(CSDM)에게 문의하세요.

> **Note**
>
> SSP 모드와 개발자 모드 간의 가격 비교는 동일한 AWS 서비스가 프로비저닝된다고 가정합니다.

AMS 모드와 비즈니스 및 IT 목표 비교

그림과 같이 애플리케이션에 대해 고도로 제어되고 표준화된 거버넌스 모델을 찾고 있다면 AMS 관리형 표준 변경, AWS Service Catalog 또는 직접 변경 모드가 가장 적합합니다. 운영 준비 없이 애플리케이션 혁신에 중점을 둔 맞춤형 거버넌스 모델이 필요한 경우 고객 관리형 모드를 선택합니다. 고객 관리형 모드를 사용하면 인시던트 관리, 구성 관리, 프로비저닝 관리, 보안 관리, 패치 관리 등과 같은 운영 기능을 지원하는 인력, 프로세스 및 도구를 구축할 책임이 있으므로 애플리케이션을 운영하는 데 시간이 더 오래 걸릴 수 있습니다.

AMS 계정 후 규범적 지침

조직이 분산 운영 및 DevOps 관행을 채택함에 따라 Well Architected의 원칙을 충족하기 위해 워크로드를 배포하기 전에 모든 계정에 적용해야 하는 핵심 운영 기능 세트가 있습니다.

이 링크는 Word 문서가 포함된 ZIP 파일과 스크립트 및 예제가 포함된 ZIP 파일을 다운로드합니다. 자동 계정 설정은 새 애플리케이션 계정의 설정을 자동화하거나 부트스트랩하는 스크립트 세트입니다.

새 계정이 판매되고 워크로드가 배포되기 전에 운영, 보안 및 관리 관점에서 계정을 준비하기 위해 기본 백업 계획, 패치 기간 및 암호화(기타)를 설정합니다. 애플리케이션 계정 설정의 민첩성, 일관성 및 응답성을 개선하는 데 도움이 되도록 다음 샘플 "사용 방법"이 참조용으로 제공됩니다.

자동 계정 설정.

수행하는 작업, 수행하지 않는 작업

AMS는 AWS 인프라를 배포하는 표준화된 접근 방식을 제공하고 필요한 지속적인 운영 관리를 제공합니다. 역할, 책임 및 지원되는 서비스에 대한 전체 설명은 서비스 설명을 참조하세요.

> **Note**
>
> AMS가 추가 AWS 서비스를 제공하도록 요청하려면 서비스 요청을 제출합니다. 자세한 내용은 서비스 요청하기를 참조하세요.

- 수행하는 작업:

  온보딩을 완료하면 AMS 환경을 사용하여 변경(RFCs), 인시던트 및 서비스 요청에 대한 요청을 받을 수 있습니다. AMS 서비스와의 상호 작용은 애플리케이션 스택의 수명 주기를 중심으로 이루어집니다. 새 스택은 미리 구성된 템플릿 목록에서 정렬되고, 특정 Virtual Private Cloud(VPC) 서브넷으로 시작되며, 변경 요청(RFCs, 이벤트 및 인시던트가 연중무휴 모니터링됩니다.

  활성 애플리케이션 스택은 패치 적용을 포함하여 AMS에서 모니터링 및 유지 관리되며 변경이 필요하거나 스택이 폐기되지 않는 한 스택 수명 동안 추가 작업이 필요하지 않습니다. 스택의 상태 및 기능에 영향을 미치는 AMS에서 감지한 인시던트는 알림을 생성하며 해결하거나 확인하기 위해 조치가 필요할 수도 있고 필요하지 않을 수도 있습니다. 서비스 요청을 제출하여 방법 질문 및 기타 문의를 할 수 있습니다.

  또한 AMS를 사용하면 AMS에서 관리하지 않는 호환되는 AWS 서비스를 활성화할 수 있습니다. AWS-AMS 호환 서비스에 대한 자세한 내용은 셀프 서비스 프로비저닝 모드를 참조하세요.

- 하지 말아야 할 일:

  AMS는 다양한 수동 및 자동 옵션을 제공하여 애플리케이션 배포를 간소화하지만 애플리케이션의 개발, 테스트, 업데이트 및 관리는 사용자의 책임입니다. AMS는 애플리케이션에 영향을 미치는 인프라 문제에 대한 문제 해결 지원을 제공하지만 AMS는 애플리케이션 구성에 액세스하거나 검증할 수 없습니다.

AMS 송신 트래픽 관리

기본적으로 AMS 프라이빗 및 고객 애플리케이션 서브넷의 대상 CIDR이 0.0.0.0/0인 라우팅에는 NAT(네트워크 주소 변환) 게이트웨이가 대상으로 사용됩니다. AMS 서비스인 TrendMicro 및 패치는 AMS가 서비스를 제공할 수 있고 TrendMicro 및 운영 체제가 업데이트를 받을 수 있도록 인터넷에 대한 외부 액세스 권한이 있어야 하는 구성 요소입니다.

AMS는 다음과 같은 경우에 한해 고객 관리형 송신 디바이스를 통해 송신 트래픽을 인터넷으로 전환하도록 지원합니다.

- 암시적(예: 투명) 프록시 역할을 합니다.

  and

- AMS HTTP 및 HTTPS 종속성(이 섹션에 나열됨)을 허용하여 AMS 관리형 인프라를 지속적으로 패치하고 유지 관리할 수 있습니다.

다음은 몇 가지 예시입니다.

- 전송 게이트웨이(TGW)에는 다중 계정 랜딩 존 네트워킹 계정의 AWS Direct Connect 연결을 통해 고객 관리형 온프레미스 방화벽을 가리키는 기본 경로가 있습니다.
- TGW에는 AWS PrivateLink를 활용하는 다중 계정 랜딩 존 송신 VPC의 AWS 엔드포인트를 가리키는 기본 경로가 있으며, 다른 AWS 계정의 고객 관리형 프록시를 가리킵니다.
- TGW에는 다른 AWS 계정의 고객 관리형 방화벽을 가리키는 기본 경로가 있으며, site-to-site VPN 연결은 다중 계정 랜딩 존 TGW에 대한 연결로 사용됩니다.

AMS는 해당 AMS HTTP 및 HTTPS 종속성을 식별했으며 이러한 종속성을 지속적으로 개발하고 구체화합니다. egressMgmt.zip을 참조하세요. ZIP에는 JSON 파일과 함께 README가 포함되어 있습니다.

> **Note**
>
> - 이 정보는 포괄적이지 않습니다. 일부 필수 외부 사이트는 여기에 나열되지 않습니다.
> - 거부 목록 또는 차단 전략에서이 목록을 사용하지 마십시오.
> - 이 목록은 송신 필터링 규칙 세트의 시작점으로 사용되며, 보고 도구를 사용하여 실제 트래픽이 목록에서 정확히 벗어나는 위치를 결정합니다.

송신 트래픽 필터링에 대한 정보를 요청하려면 CSDM에 ams-csdm@amazon.com으로 이메일을 보내세요.

AMS의 IAM 사용자 역할

IAM 역할은 자격 AWS 증명이 할 수 있는 것과 없는 것을 결정하는 권한 정책이 있는 자격 증명이라는 점에서 IAM 사용자와 유사합니다 AWS. 그러나 역할은 한 사람하고만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다.

현재 표준 AMS 계정의 경우 AMS 기본 사용자 역할 `Customer_ReadOnly_Role`1개가 있고 관리형 Active Directory가 있는 AMS 계정`customer_managed_ad_user_role`의 경우 추가 역할 1개가 있습니다.

역할 정책은 CloudWatch 및 Amazon S3 로그 작업, AMS 콘솔 액세스, 대부분의 읽기 전용 제한, 계정 S3 콘솔에 대한 AWS 서비스제한된 액세스 및 AMS 변경 유형 액세스에 대한 권한을 설정합니다.

또한 `Customer_ReadOnly_Role`에는 인스턴스를 예약할 수 있는 변경 가능한 예약 인스턴스 권한이 있습니다. 일부 비용 절감 값이 있으므로 특정 수의 Amazon EC2 인스턴스가 장기간 필요할 경우 해당 APIs. 자세한 내용은 Amazon EC2 예약 인스턴스를 참조하세요.

> **Note**
>
> 기존 정책을 재사용하지 않는 한, IAM 사용자에 대한 사용자 지정 IAM 정책을 생성하기 위한 AMS 서비스 수준 목표(SLO)는 영업일 기준 4일입니다. 기존 IAM 사용자 역할을 수정하거나 새 역할을 추가하려면 각각 IAM: 개체 업데이트 또는 IAM: 개체 RFC 생성을 제출합니다.

Amazon IAM 역할에 익숙하지 않은 경우 IAM 역할에서 중요한 정보를 참조하세요.

다중 계정 랜딩 존(MALZ): AMS 다중 계정 랜딩 존 기본 사용자 지정되지 않은 사용자 역할 정책을 보려면 다음 단원MALZ: 기본 IAM 사용자 역할을 참조하십시오.

MALZ: 기본 IAM 사용자 역할

기본 다중 계정 AMS 다중 계정 랜딩 존 사용자 역할에 대한 JSON 정책 설명입니다.

> **Note**
>
> 사용자 역할은 사용자 지정할 수 있으며 계정별로 다를 수 있습니다. 역할을 찾는 방법에 대한 지침이 제공됩니다.

다음은 기본 MALZ 사용자 역할의 예입니다. 필요한 정책이 설정되어 있는지 확인하려면 AWS 명령을 실행`get-role`하거나 AWS 관리 -> IAM 콘솔에 로그인하고 탐색 창에서 역할을 선택합니다.

코어 OU 계정 역할

코어 계정은 MALZ 관리형 인프라 계정입니다. AMS 다중 계정 랜딩 존 코어 계정에는 관리 계정과 네트워킹 계정이 포함됩니다.

코어 OU 계정: 공통 역할 및 정책

Role	정책 또는 정책
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(퍼블릭 AWS 관리형 정책).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess(퍼블릭 AWS 관리형 정책).
AWSManagedServicesChangeManagementRole(코어 계정 버전)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

코어 OU 계정: 관리 계정 역할 및 정책

Role	정책 또는 정책
AWSManagedServicesBillingRole	AMSBillingPolicy(AMSBillingPolicy).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(퍼블릭 AWS 관리형 정책).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess(퍼블릭 AWS 관리형 정책).
AWSManagedServicesChangeManagementRole(관리 계정 버전)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

코어 OU 계정: 네트워킹 계정 역할 및 정책

Role	정책 또는 정책
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(퍼블릭 AWS 관리형 정책).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess(퍼블릭 AWS 관리형 정책).
AWSManagedServicesChangeManagementRole(네트워킹 계정 버전)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Role	정책 또는 정책
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

애플리케이션 계정 역할

애플리케이션 계정 역할은 애플리케이션별 계정에 적용됩니다.

애플리케이션 계정: 역할 및 정책

Role	정책 또는 정책
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(퍼블릭 AWS 관리형 정책).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess(퍼블릭 AWS 관리형 정책). 이 정책은 모든 지원 작업 및 리소스에 대한 액세스를 제공합니다. 자세한 내용은 AWS Support 시작하기를 참조하세요.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportAccess 예제 이 정책은 모든 지원 작업 및 리소스에 대한 액세스를 제공합니다.
	AWSCertificateManagerFullAccess 정보, (퍼블릭 AWS 관리형 정책)
	AWSWAFFullAccess information, (퍼블릭 AWS 관리형 정책). 이 정책은 AWS WAF 리소스에 대한 전체 액세스 권한을 부여합니다.
	AMSSecretsManagerSharedPolicy

Role	정책 또는 정책
AWSManagedServicesChangeManagementRole(애플리케이션 계정 버전)	ReadOnlyAccess
	AWSSupportAccess(퍼블릭 AWS 관리형 정책). 이 정책은 모든 지원 작업 및 리소스에 대한 액세스를 제공합니다. 자세한 내용은 AWS Support 시작하기를 참조하세요.
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Policy
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccess
	AMSS3Policy
	AMSReservedInstancesPolicy

정책 예제

사용되는 대부분의 정책에 대한 예제가 제공됩니다. 활성 AWS 계정이 있는 경우 ReadOnlyAccess 정책(모든 AWS 서비스에 대한 읽기 전용 액세스를 제공하는 페이지)을 보려면이 링크를 사용할 수 ReadOnlyAccess. 또한 여기에 요약된 버전이 포함되어 있습니다.

AMSBillingPolicy

AMSBillingPolicy

회계 부서에서 새 결제 역할을 사용하여 관리 계정의 결제 정보 또는 계정 설정을 보고 변경할 수 있습니다. 대체 연락처와 같은 정보에 액세스하거나, 계정 리소스 사용량을 보거나, 결제 탭을 유지하거나, 결제 방법을 수정하려면이 역할을 사용합니다. 이 새 역할은 AWS Billing IAM 작업 웹 페이지에 나열된 모든 권한으로 구성됩니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
```

```
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

모든 AMS 변경 유형과 요청된 변경 유형의 기록을 볼 수 있는 권한.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

배포 | 관리형 랜딩 존 | 관리 계정 | 애플리케이션 계정 생성(VPC 사용) 변경 유형을 요청할 수 있는 권한.

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

배포 | 관리형 랜딩 존 | 네트워킹 계정 | 애플리케이션 라우팅 테이블 변경 유형 생성을 요청할 수 있는 권한.

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy (관리용 | 기타 | 기타 CTs)

관리 | 기타 | 기타 | 생성 및 관리 | 기타 | 기타 | 변경 유형 업데이트를 요청할 수 있는 권한.

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

를 통해 AMS가 공유하는 보안 암호/해시를 볼 수 있는 권한 AWS Secrets Manager (예: 감사를 위한 인프라에 대한 암호).

AMS와 공유할 보안 암호/해시를 생성할 수 있는 권한(예: 배포해야 하는 제품의 라이선스 키).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
```

```
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

AMSChangeManagementPolicy

모든 AMS 변경 유형 및 요청된 변경 유형의 기록을 요청하고 볼 수 있는 권한.

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

Amazon EC2 예약 인스턴스를 관리할 수 있는 권한. 요금 정보는 Amazon EC2 예약 인스턴스를 참조하세요.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
```

```
    "*"
  ]
 }]
}
```

AMSS3Policy

`AMSS3Policy`

기존 Amazon S3 버킷에서 파일을 생성하고 삭제할 수 있는 권한.

> **Note**
>
> 이러한 권한은 배포 | 고급 스택 구성 요소 | S3 스토리지 | 변경 유형 생성으로 수행해야 하는 S3 버킷을 생성할 수 있는 권한을 부여하지 않습니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSSupportAccess

`AWSSupportAccess`

에 대한 전체 액세스 권한 지원. 자세한 내용은 시작하기를 참조하세요 지원. Premium Support에 대한 자세한 내용은 섹션을 참조하세요지원.

JSON

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

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions` (퍼블릭 AWS관리형 정책)

구독, 구독 취소 및 AWS Marketplace 구독 보기 권한.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

에 대한 전체 액세스 권한 AWS Certificate Manager. 자세한 내용은 AWS Certificate Manager 단원을 참조하십시오.

AWSCertificateManagerFullAccess information, (퍼블릭 AWS 관리형 정책).

JSON

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

AWSWAFFullAccess

AWSWAFFullAccess

에 대한 전체 액세스 권한 AWS WAF. 자세한 내용은 AWS WAF - 웹 애플리케이션 방화벽을 참조하세요.

AWSWAFFullAccess information, (퍼블릭 AWS 관리형 정책). 이 정책은 AWS WAF 리소스에 대한 전체 액세스 권한을 부여합니다.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

ReadOnlyAccess

`ReadOnlyAccess`

AWS 콘솔의 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스. 가 새 서비스를 AWS 시작하면 AMS는 ReadOnlyAccess 정책을 업데이트하여 새 서비스에 대한 읽기 전용 권한을 추가합니다. 이렇게 업데이트된 권한은 정책이 추가되는 모든 보안 주체 엔터티에게 적용됩니다.

이렇게 해도 EC2 호스트 또는 데이터베이스 호스트에 로그인할 수 있는 기능은 부여되지 않습니다.

활성가 있는 경우이 링크 ReadOnlyAccess를 사용하여 전체 ReadOnlyAccess 정책을 볼 AWS 계정 수 있습니다. 전체 ReadOnlyAccess 정책은 모든에 대한 읽기 전용 액세스를 제공하는 한 매우 깁니다 AWS 서비스. 다음은 ReadOnlyAccess 정책의 부분 발췌문입니다.

단일 계정 랜딩 존(SALZ): AMS 단일 계정 랜딩 존 기본 사용자 지정되지 않은 사용자 역할 정책을 보려면 다음 단원SALZ: 기본 IAM 사용자 역할을 참조하십시오.

SALZ: 기본 IAM 사용자 역할

기본 AMS 단일 계정 랜딩 존 사용자 역할에 대한 JSON 정책 설명입니다.

> **Note**
>
> SALZ 기본 사용자 역할은 사용자 지정할 수 있으며 계정별로 다를 수 있습니다. 역할을 찾는 방법에 대한 지침이 제공됩니다.

다음은 기본 SALZ 사용자 역할의 예입니다. 정책이 설정되어 있는지 확인하려면 `get-role` 명령을 실행합니다. 또는 https://console.aws.amazon.com/iam/ AWS Identity and Access Management 콘솔에 로그인한 다음 역할을 선택합니다.

고객 읽기 전용 역할은 여러 정책의 조합입니다. 역할 분석(JSON)은 다음과 같습니다.

관리형 서비스 감사 정책:

관리형 서비스 IAM ReadOnly 정책

관리형 서비스 사용자 정책

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

```
    {
      "Sid": "AllowCustomerToListTheLogBucketLogs",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "aws/*",
            "app/*",
            "encrypted",
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
```

```
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
```

```
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
```

```
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
    },
    {
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
      ]
    },
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
```

```
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
```

```
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Customer Secrets Manager 공유 정책

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
```

```
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Customer Marketplace 구독 정책

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
```

```
}
```

기본 액세스 방화벽 규칙

다음은 인스턴스에 액세스하는 데 필요한 기본 방화벽 규칙입니다.

> **Note**
>
> AD 단방향 신뢰 설정에 필요한 방화벽 규칙 및 포트에 대한 자세한 내용은 AWS Artifact 콘솔 -> 보고서 탭으로 이동하여 AMS 보안 가이드를 참조하고 AWS Managed Services를 검색하세요.

Linux 스택 인스턴스 포트

이러한 규칙은 AMS Linux 스택으로 인증하는 데 필요합니다.

Linux 인스턴스 포트 규칙 시작: Linux 스택 인스턴스 종료: CORP 도메인 컨트롤러

포트	프로토콜	서비스	Direction
389	TCP	LDAP	Ingress
389	UDP	LDAP	Ingress
88	TCP	Kerberos	Ingress
88	UDP	Kerberos	Ingress

Windows 스택 인스턴스 포트

이러한 규칙은 AMS Windows 스택으로 인증하는 데 필요합니다.

FROM: Windows 스택 인스턴스 TO: CORP 도메인 컨트롤러

포트	프로토콜	서비스	Direction
88	TCP | UDP	Kerberos	수신 및 송신

포트	프로토콜	서비스	Direction
135	TCP | UDP	DCE/RPC 로케이터 서비스	수신 및 송신
389	TCP | UDP	LDAP	수신 및 송신
3268	TCP | UDP	msft-gc, Microsoft Global Catalog(Active Directory 포리스트의 데이터가 포함된 LDAP 서비스)	수신 및 송신
445	TCP	Microsoft-DS Active Directory, Windows 공유	수신 및 송신
49,152~65,535	TCP	IANA에 등록할 수 없는 동적 또는 프라이빗 포트입니다. 이 범위는 프라이빗 또는 사용자 지정 서비스 또는 임시 용도와 임시 포트의 자동 할당에 사용됩니다.	수신 및 송신

AWS Managed Services의 서비스 관리

주제

AMS 서비스가 작동하는 방식입니다.

AWS Managed Services의 계정 거버넌스

이 섹션에서는 AMS 계정 거버넌스를 다룹니다.

AMS 전반에 걸쳐 자문 지원을 제공하고 관리형 환경의 사용 사례 및 기술 아키텍처를 자세히 이해하는 클라우드 서비스 제공 관리자(CSDM)로 지정됩니다. CSDMs 계정 관리자, 기술 계정 관리자, AWS Managed Services 클라우드 아키텍트(CAs) 및 해당하는 경우 AWS 솔루션 아키텍트(SAs)와 협력하여 소프트웨어 개발 및 운영 프로세스 전반에 걸쳐 새 프로젝트를 시작하고 모범 사례 권장 사항을 제공하는 데 도움을 줍니다. CSDM은 AMS의 기본 연락 지점입니다. CSDM의 주요 책임은 다음과 같습니다.

- 고객과 월별 서비스 검토 회의를 조직하고 주도합니다.
- 보안, 환경의 소프트웨어 업데이트 및 최적화 기회에 대한 세부 정보를 제공합니다.
- AMS에 대한 기능 요청을 포함하여 요구 사항을 충족합니다.
- 결제 및 서비스 보고 요청에 응답하고 이를 해결합니다.
- 재무 및 용량 최적화 권장 사항에 대한 인사이트를 제공합니다.

AWS Managed Services에서 서비스 시작

서비스 시작: AWS Managed Services 계정의 서비스 시작 날짜는 AWS가 해당 AWS Managed Services 계정의 온보딩 요구 사항에 명시된 활동이 완료되었음을 알리는 첫 번째 달의 첫 번째 날입니

다. 단, AWS가 해당 월의 20일 이후에 알림을 보내는 경우 서비스 시작 날짜는 해당 알림 날짜 다음 달의 두 번째 날입니다.

서비스 시작

- R은 작업을 달성하기 위해 작업을 수행하는 책임 당사자를 나타냅니다.
- 나는 종종 작업 또는 결과물 완료 시에만 진행 상황에 대한 정보를 받는 당사자인 정보를 의미합니다.

서비스 시작

단계 #	단계 제목	설명	Custome	AMS
1.	고객 AWS 계정 인계	고객이 새 AWS 계정을 생성하고 이를 AWS Managed Services로 인계합니다.	R	정보
2.	AWS Managed Services 계정 - 디자인	AWS Managed Services 계정 설계 완료	정보	R
3.	AWS Managed Services 계정 - 빌드	AWS Managed Services 계정은 2단계의 설계에 따라 빌드됩니다.	정보	R

고객 관계 관리(CRM)

AWS Managed Services(AMS)는 고객 관계 관리(CRM) 프로세스를 제공하여 잘 정의된 관계가 설정되고 유지되도록 합니다. 이 관계의 기반은 비즈니스 요구 사항에 대한 AMS의 인사이트를 기반으로 합니다. CRM 프로세스를 통해 다음을 정확하고 포괄적으로 이해할 수 있습니다.

- 비즈니스 요구 사항 및 이러한 요구 사항을 충족하는 방법
- 기능 및 제약 조건
- AMS 및 다양한 책임과 의무

CRM 프로세스를 통해 AMS는 일관된 방법을 사용하여 서비스를 제공하고 AMS와의 관계에 대한 거버넌스를 제공할 수 있습니다. CRM 프로세스에는 다음이 포함됩니다.

- 주요 이해관계자 식별
- 거버넌스 팀 구성
- 나와 함께 서비스 검토 회의 수행 및 문서화
- 에스컬레이션 절차를 통해 공식 서비스 불만 제기 절차 제공
- 만족도 및 피드백 프로세스 구현 및 모니터링
- 계약 관리

CRM 프로세스

CRM 프로세스에는 다음과 같은 활동이 포함됩니다.

- 비즈니스 프로세스 및 요구 사항 식별 및 이해. AMS와의 계약은 이해관계자를 식별합니다.
- 요구 사항 및 요구 사항에 맞게 제공할 서비스를 정의합니다.
- 서비스 검토 회의에서 회의를 통해 AMS 서비스 범위, SLA, 계약 및 비즈니스 요구 사항의 변경 사항에 대해 논의합니다. 성과, 업적, 문제 및 행동 계획을 논의하기 위해 임시 회의가 열릴 수 있습니다.
- 고객 만족도 설문 조사와 회의에서 제공된 피드백을 사용하여 만족도를 모니터링합니다.
- 내부적으로 측정된 월별 성능 보고서에 대한 성능 보고.
- 서비스를 함께 검토하여 개선 기회를 결정합니다. 여기에는 제공된 AMS 서비스의 수준 및 품질과 관련하여 사용자와 자주 소통하는 것이 포함됩니다.

CRM 회의

AMS 클라우드 서비스 제공 관리자(CSDMs 정기적으로 회의를 개최하여 서비스 트랙(운영, 보안 및 제품 혁신) 및 경영진 트랙(SLA 보고서, 만족도 측정 및 비즈니스 요구 사항 변경)에 대해 논의합니다.

회의	용도	Mode	Participants
주간 상태 검토 (선택 사항)	미해결 문제 또는 인시던트, 패치, 보안 이벤트, 문제 레코드 12주 운영 추세 +/- 6) 애플리케이션 운영자 문제 주말 일정	현장 고객 location/ Telecom/Chime	AMS: CSDM 및 클라우드 아키텍트(CA) 고객이 할당한 팀원(예: 클라우드/인프라, 애플리케

회의	용도	Mode	Participants
			이션 지원, 아키텍처 팀 등)
월별 비즈니스 검토	서비스 수준 성능 검토(보고서, 분석 및 추세) 재무 분석 제품 로드맵 CSAT	현장 고객 location/ Telecom/Chime	AMS: CSDM, 클라우드 아키텍트(CA), AMS 계정 팀, AMS 기술 제품 관리자(TPM)(선택 사항), AMS OPS 관리자(선택 사항) 사용자: Application Operator 담당자
분기별 비즈니스 검토	점수표 및 서비스 수준 계약(SLA) 성능 및 추세(6개월) 향후 3/6/9/12개월 계획/마이그레이션 위험 및 위험 완화 주요 개선 이니셔티브 제품 로드맵 항목 미래 방향 조정 기회 재무 비용 절감 이니셔티브 비즈니스 최적화	현장 고객 위치	AMS: CSDM, 클라우드 아키텍트, AMS 계정 팀, AMS 서비스 디렉터, AMS 운영 관리자 사용자: 애플리케이션 운영자 담당자, 서비스 담당자, 서비스 디렉터

CRM 회의 계약

AMS CSDM은 다음을 포함하여 회의를 문서화할 책임이 있습니다.

- 작업 항목, 문제 및 참석자 목록을 포함한 의제 생성.
- 각 회의에서 검토한 작업 항목 목록을 생성하여 항목이 일정에 따라 완료되고 해결되었는지 확인합니다.
- 회의 후 영업일 기준 1일 이내에 이메일을 통해 회의록과 작업 항목 목록을 회의 참석자에게 배포합니다.
- 회의록을 적절한 문서 리포지토리에 저장합니다.

CSDM이 없는 경우 회의를 주도하는 AMS 담당자가 회의록을 생성하고 배포합니다.

> **Note**
>
> CSDM은 사용자와 협력하여 계정 거버넌스를 설정합니다.

CRM 월별 보고서

AMS CSDM은 월별 서비스 성능 프레젠테이션을 준비하고 전송합니다. 프레젠테이션에는 다음에 대한 정보가 포함되어 있습니다.

- 보고서 날짜
- 요약 및 인사이트:
  - 주요 콜 아웃: 총 및 활성 스택 수, 스택 패치 상태, 계정 온보딩 상태(온보딩만 해당), 고객별 문제 요약
  - 성능: 인시던트 해결, 알림, 패치 적용, 변경 요청(RFCs), 서비스 요청, 콘솔 및 API 가용성에 대한 통계
  - 문제, 과제, 우려 사항 및 위험: 고객별 문제 상태
  - 예정된 항목: 고객별 온보딩 또는 인시던트 해결 계획
- 관리형 리소스: 스택의 그래프 및 파이형 차트
- AMS 지표: 모니터링 및 이벤트 지표, 인시던트 지표, AMS SLA 준수 지표, 서비스 요청 지표, 변경 관리 지표, 스토리지 지표, 연속성 지표, Trusted Advisor 지표 및 비용 요약(여러 가지 방법 제시). 기능 요청. 연락처 정보.

> **Note**
>
> 설명된 정보 외에도 CSDM은 운영 활동에 대한 AMS의 하청업체 사용을 포함하여 범위 또는 조건의 중요한 변경 사항을 알립니다.
> AMS는 CSDM이 월별 보고서에 포함하는 패치 및 백업에 대한 보고서를 생성합니다. 보고서 생성 시스템의 일부로 AMS는 사용자가 액세스할 수 없는 일부 인프라를 계정에 추가합니다.
>
> - 원시 데이터가 보고된 S3 버킷
> - 데이터를 쿼리하기 위한 쿼리 정의가 있는 Athena 인스턴스
> - S3 버킷에서 원시 데이터를 읽기 위한 Glue 크롤러

AWS Managed Services의 비용 최적화

AWS Managed Services는 월별 비즈니스 검토(MBRs) 중에 매월 상세한 비용 사용률 및 절감 보고서를 제공합니다.

AMS는 표준 프로세스 및 메커니즘 세트를 따라 관리형 계정의 비용 절감 방법을 식별하고 AWS 지출을 최적화하기 위해 변경 사항을 계획하고 롤아웃하는 데 도움이 됩니다.

> **Note**
>
> AMS는 비용 최적화에 도움이 되는 비디오를 개발하고 있습니다. 첫 번째 단계는 비용 최적화 모범 사례의 PDF 및 Excel 스프레드시트를 제공하는 것입니다. 이러한 리소스에 액세스하려면 비용 최적화 ZIP 파일에 대한 빠른 안내서를 엽니다.

비용 최적화 프레임워크

AMS는 AWS 비용을 최적화하기 위해 3단계 접근 방식을 따릅니다.

1. 관리형 환경에서 비용 최적화 방법 식별
2. 비용 최적화 계획을 제시하세요.
3. 측정 가능한 방식으로 비용 최적화 달성 지원

관리형 환경에서 비용 최적화 방법 식별

AMS는 Cost Explorer 및 Trusted Advisor와 같은 AWS 네이티브 도구를 활용하는 동시에 아키텍처 최적화, EC2 인스턴스 및 AWS 계정 중심 최적화 전반에서 20개 이상의 비용 절감 패턴을 활용하여 맞춤형 비용 절감 권장 사항을 구축합니다.

최적화 권장 사항 중 일부는 다음과 같습니다.

아키텍처 최적화 권장 사항:

- 최적의 S3 스토리지 클래스 사용: Amazon S3는 데이터 액세스, 복원력 및 비용에 따라 다양한 워크로드 요구 사항을 충족하는 다양한 스토리지 클래스를 제공합니다. 워크로드 요구 사항에 따른 S3 Intelligent-Tiering 및 S3 스토리지 클래스 분석을 통해 S3 비용을 효율적으로 관리할 수 있습니다.
- 캐싱 아키텍처 사용: 해당하는 경우 캐시 인스턴스를 활용하면 IOPS 요구 사항을 충족하면서 일부 데이터베이스 인스턴스를 교체할 수 있습니다.
- EBS 업그레이드 비용 절감: EBS 볼륨을 gp2에서 gp3로 마이그레이션하면 최대 20%의 비용을 절감할 수 있으며 볼륨 크기에 관계없이 예측 가능한 3,000IOPS 기준 성능과 125MiB/s를 활용할 수 있습니다.
- 탄력성 사용:를 AWS 제공하는 Auto Scaling 기능을 사용하면 비용 최적화를 위한 효과적인 리소스 사용률과 방법을 얻을 수 있습니다. 필요에 따라 인스턴스 조정 정책을 정기적으로 검토하고 업데이트하면 비용을 절감할 수 있습니다.

EC2 인스턴스 중심 권장 사항

- 인스턴스 크기 조정: 인스턴스 크기 조정 및 사용량에 따른 최적의 구성에 중점을 둔 권장 사항입니다. 또한 Amazon EC2 Auto Scaling 기능을 활용하고 해당하는 경우 EC2 인스턴스를 Amazon S3의 AWS Lambda 또는 정적 웹 콘텐츠 등으로 대체하는 것이 좋습니다.
- 인스턴스 예약: AMS Resource Scheduler를 사용하여 시간 일정에 따라 인스턴스를 자동으로 시작 및 중지하면 특히 업무 외 시간에 활용되지 않는 비프로덕션 인스턴스에 대한 비용을 절감하는 데 도움이 됩니다.
- 절감형 플랜 구독: 절감형 플랜은 AWS 사용량을 절약하는 가장 쉬운 방법입니다. EC2 Instance Savings Plans은 Amazon EC2 인스턴스 사용량에 대한 온디맨드 요금에 비해 최대 72%의 절감 효과를 제공합니다. Amazon SageMaker AI Savings Plans은 Amazon SageMaker AI 서비스 사용량을 최대 64% 절감합니다. AMS는 AWS 리소스 사용량에 따라 절감형 플랜에 대한 적절한 권장 사항을 제공합니다.
- 예약 인스턴스(RI) 사용 및 소비 지침: Amazon EC2 예약 인스턴스(RI)는 온디맨드 요금에 비해 상당한 할인(최대 75%)을 제공하고 특정 가용 영역에서 사용할 경우 용량 예약을 제공합니다.

- 스팟 인스턴스 사용: 내결함성 워크로드는 스팟 인스턴스를 활용하고 가격을 최대 90%까지 줄일 수 있습니다.
- 유휴 인스턴스 종료: 유휴 상태이거나 종료할 수 있는 사용률이 낮은 인스턴스를 식별하고 보고합니다.

계정 중심 권장 사항

- 계정 정리: 계정 수준에서 AMS는 사용되지 않는 EBS 볼륨, 중복 CloudTrail 추적, 미사용 리소스가 있는 빈 계정 등을 식별하고 정리를 위한 권장 사항을 제공합니다.
- SLA 권장 사항: 또한 AMS는 Plus 및 Premium 계정을 정기적으로 검토하고 계정에 적합한 SLA 수준을 선택할 것을 권장합니다.
- AMS 자동화 최적화: AMS는 AMS 서비스를 제공하는 데 사용되는 AMS 자동화 및 인프라를 지속적으로 최적화합니다.

고객에게 제시 및 계획 지원

AMS는 주요 고객 이해관계자와 함께 월별 비즈니스 검토(MBRs)를 수행하고 잠재적 비용 절감과 함께 식별된 비용 절감 방법, 메커니즘 및 권장 사항을 제시합니다. 또한 필요한 변경 사항을 계획하기 위해 고객과 협력합니다.

권장 사항 구현 지원 및 비용 영향 측정

AMS는 비용 영향 및 최적화 변경을 달성하고 측정하는 데 도움이 됩니다.

권장 변경 사항의 애플리케이션 영향, 위험 및 성공 기준을 평가하고 AMS 콘솔을 통해 적절한 변경 요청(RFCs)을 제기합니다. AMS는 사용자와 협업하고 관리형 계정에서 비용 최적화와 관련된 변경 사항을 구현합니다. AMS는 비용 영향을 측정하고 월별 비즈니스 검토(MBRs)에 실현된 절감액을 포함합니다.

비용 최적화 책임 매트릭스

AMS 비용 최적화에 대한 책임.

비용 최적화 RACI

활동	Customer	AMS
비용 절감 권장 사항	정보	R

활동	Customer	AMS
컴파일 및 보고서 준비		
비용 절감 보고서 제시	C	R
비용 절감과 관련된 변경 계획	R	C
변경 영향 및 위험 평가	R	C
변경 사항 구현 RFCs 증가	R	C
RFCs 검토 및 변경 사항 구현	C	R
애플리케이션 테스트 및 변경 구현 검증	R	C

활동	Customer	AMS
변경 후 비용에 미치는 영향 측정 및 고객에게 제시	정보	R

AWS Managed Services의 서비스 시간

Feature	AMS 고급
	프리미엄 티어
서비스 요청	24/7
인시던트 관리(P2-P3)	24/7
백업 및 복구	24/7
패치 관리	24/7
모니터링 및 알림	24/7
자동 변경 요청(RFC)	24/7
자동이 아닌 변경 요청(RFC)	24/7
클라우드 서비스 제공 관리자(CSDM)	월요일~금요일: 08:00~17:00, 현지 업무 시간

AWS Managed Services에 대한 도움말 보기

AMS는 하루 24시간, 주 7일, 1년 365일(계정에 적용된 AMS 서비스 수준 계약에 따라) Incident Management, Service Request Management 및 Change Management를 지원합니다.

관리형 환경에 영향을 미치는 AWS 또는 AMS 서비스 성능 문제를 보고하려면 AMS 콘솔을 사용하여 인시던트 보고서를 제출합니다. 자세한 내용은 인시던트 보고를 참조하세요. AMS 인시던트 관리에 대한 일반적인 정보는 인시던트 대응을 참조하세요.

정보나 조언을 요청하거나 AMS에서 추가 서비스를 요청하려면 AMS 콘솔을 사용하여 서비스 요청을 제출합니다. 자세한 내용은 서비스 요청 생성을 참조하세요. AMS 서비스 요청에 대한 일반 정보는 서비스 요청 관리를 참조하세요.

변경 관리 모드

AWS Managed Services(AMS)는 변경 관리 모드를 사용하여 AMS Advanced의 변경 사항을 보호합니다. 변경 관리 모드는 환경에 대한 높은 운영 표준을 유지하고 위험을 제어하고 부정적인 영향을 방지하는 데 도움이 됩니다. AMS Advanced에는 다양한 수준의 제어 및 위험을 제공하는 다양한 모드가 있습니다. 고객 관리형 모드를 제외한 모든 모드는 AMS에서 관리합니다. 사용 가능한 변경 관리 모드는 다음과 같습니다.

- RFC 모드(이전 표준 CM 모드): "변경 요청"(RFC) 시스템 및 AMS 사용자 지정 변경 유형(CTs)을 제공합니다.
- 직접 변경 모드: RFC 모드와 동일하며 AWS APIs 및 콘솔을 사용하여 AMS 관리형 리소스 생성
- AMS의 AWS Service Catalog: Direct Change 모드와 유사하지만 AMS 변경 관리 시스템(RFCs)을 사용하는 대신 AWS Service Catalog를 사용하여 AMS가 관리하는 리소스를 생성합니다.
- 개발자 모드: 직접 변경 모드와 동일 AWS APIs 및 콘솔을 사용하여 생성한 리소스만 AMS 관리형이 아니므로 해당 리소스의 관리는 사용자의 책임입니다.
- 셀프 서비스 프로비저닝(SSP) 모드: AMS 변경 관리 시스템에 액세스할 수 없다는 점을 제외하면 개발자 모드와 동일합니다(RFCs 없음).
- 고객 관리형 모드: AMS는 다중 계정 랜딩 존 랜딩 존을 제공하지만 모든 리소스 관리는 사용자의 책임입니다.

변경 관리(CM) API를 사용하는 AWS Managed Services(AMS) 변경 관리 시스템은 다중 계정 랜딩 존(MALZ) 및 단일 계정 랜딩 존(SALZ) 계정 모두에 대한 변경 요청(RFCs)을 생성하고 관리하는 작업을 제공합니다.

변경 요청(RFC)은 관리형 환경을 변경하기 위해 AMS 인터페이스를 통해 사용자 또는 AMS가 생성하는 요청이며 특정 작업에 대한 변경 유형(CT) ID를 포함합니다.

AMS 변경 관리(CM) API는 변경 요청(RFCs)을 생성하고 관리하는 작업을 제공합니다. RFCs. AMS 연산자는 RFCs으로 표시할 수 있습니다.

태그 또는 기타 이름에 사용할 수 없는 AMS 예약 접두사 목록은 예약 접두사를 참조하세요.

스키마 및 예제를 포함하여 각 변경 유형에 대한 자세한 내용은 AMS 변경 유형 참조를 참조하세요.

> **Note**
>
> 모든 변경 관리 API 호출은 AWS CloudTrail에 기록됩니다. 자세한 내용은 로그 액세스를 참조하세요.

모드 개요

이 정보를 사용하면 비즈니스 성과를 달성하기 위해 원하는 유연성과 규범적 거버넌스 조합을 기반으로 애플리케이션을 호스팅하는 데 적합한 AWS Managed Services(AMS) 모드를 선택하는 데 도움이 됩니다.

이 정보의 대상은 다음과 같습니다.

- 랜딩 존의 전략 및 거버넌스를 담당하는 고객 팀. 이 정보는 팀이 내부 및 외부 고객에게 제공하려는 AMS 모드를 사용하여 AMS 관리형 랜딩 존의 기반을 마련하는 데 도움이 됩니다.
- 비즈니스 및 애플리케이션 소유자는 애플리케이션을 AMS로 마이그레이션하는 작업을 담당했습니다. 이 정보는 애플리케이션을 마이그레이션/호스팅하는 데 적합한 AMS 모드를 사용하여 애플리케이션 마이그레이션을 계획하는 데 도움이 됩니다. 참고로 소프트웨어 개발 수명 주기(SDLC) 수명 주기의 여러 단계에서 동일한 애플리케이션을 둘 이상의 AMS 모드에서 호스팅할 수 있습니다.
- AMS 파트너는 AMS를 구축하고 AMS로 마이그레이션하기 위한 다양한 옵션에 대해 고객을 안내하는 작업을 담당했습니다.

이 정보는 AMS 관리형 플랫폼 설정의 기초 단계와 AMS로의 온보딩이 완료되고 애플리케이션 거버넌스 및 운영에 집중한 직후 클라우드 채택 여정의 기초에서 마이그레이션 단계로 전환할 때 가장 유용합니다.

AMS의 모드 및 계정 유형

AWS Managed Services(AMS) 모드는 각 모드의 특정 거버넌스 프레임워크에 따라 AMS 서비스와 상호 작용하는 방법으로 정의할 수 있습니다. 랜딩 존 차이, 다중 계정 랜딩 존 또는 MALZ 및 단일 계정 랜딩 존 또는 SALZ가 기록됩니다.

> **Note**
>
> 애플리케이션 배포 및 올바른 AMS 모드 선택에 대한 자세한 내용은 AMS 모드 및 애플리케이션 또는 워크로드를 참조하세요.

다양한 모드의 실제 사용 사례는 AMS 모드의 실제 사용 사례를 참조하세요.

다음 표에는 AMS 서비스당 모드에 대한 설명이 나와 있습니다.

AMS 기능	RFC 모드(이전 표준 CM 모드)/OOD*	직접 변경 모드	AWS Service Catalog	셀프 서비스 프로비저닝/개발자 모드	고객 관리형
랜딩 존 구성	MALZ 및 SALZ	MALZ 및 SALZ	MALZ 및 SALZ		
변경 관리	변경 일정, 수동 변경 사항 검토 및 변경 레코드	IAM 또는 보안 그룹과 같은 고위험 변경의 경우 RFC 모드와 동일	없음		
로깅, 모니터링, 가드레일 및 이벤트 관리	예(지원되는 리소스)			아니요	
연속성 관리	예(지원되는 리소스)			해당 사항 없음/아니요	아니요
보안 관리	인스턴스 수준 보안 제어 및 계정 수준 제어			계정 수준 제어	AWS 조직 수준 제어
패치 관리	예			해당 사항 없음/아니요	아니요
인시던트 및 문제 관리	AMS 지원 리소스에 대한 응답 및 해결 SLA			결과 리소스에 대한 응답 SLA	아니요
보고	예			아니요	

AMS 기능	RFC 모드(이전 표준 CM 모드)/OOD*	직접 변경 모드	AWS Service Catalog	셀프 서비스 프로비저닝/개발자 모드	고객 관리형
서비스 요청 관리	예			지원 요청만	아니요

*OOD(Operations On Demand)에는 RFC 모드를 사용하는 고객이 전용 리소싱을 통해 변경 사항을 관리할 수 있는 기능이 있습니다. 자세한 내용은 오퍼링의 온디맨드 운영 카탈로그를 참조하고 클라우드 서비스 제공 관리자(CSDM)에게 문의하세요.

> **Note**
>
> AMS의 셀프 서비스 프로비저닝 모드 및는 모두 네이티브 AWS 서비스에 기반을 둔 복잡한 아키텍처가 있는 애플리케이션에 적합한 것으로 보일 AMS 고급 개발자 모드 수 있습니다. 워크로드를 설계할 때 비즈니스 컨텍스트에 따라 운영 우수성과 민첩성을 절충합니다. 이는 애플리케이션에 대해 SSP 모드 또는 개발자 모드를 선택할 때 고려할 수 있는 좋은 방법입니다. 선택 사항은 애플리케이션의 SDLC 단계에 따라 변경될 수도 있습니다. 예: 애플리케이션이 프로덕션 준비가 되면이 모드에서 AMS 가드레일이 더 엄격하기 때문에 SSP 모드가 더 적절한 옵션일 수 있습니다. 가드레일은 애플리케이션 OU 수준에서 IAM 업데이트 및 SCPs에 대한 RFC 기반 변경 제어와 같은 예방적 제어의 형태로 적용됩니다. 이러한 비즈니스 의사결정에 따라 엔지니어링 우선 순위가 달라질 수 있습니다. 거버넌스 및 운영 지원을 희생하면서 "pre-prod" 단계에서 애플리케이션 소유자의 유연성을 높이도록 최적화할 수 있습니다.

MALZ 아키텍처 및 관련 AMS 모드

AMS 다중 계정 랜딩 존(MALZ)은 기본 조직 단위(OU): 고객 관리형 OU, 관리형 OU 또는 개발 OU에 따라 애플리케이션 계정(또는 리소스 계정)을 자동으로 프로비저닝할 수 있는 옵션을 제공합니다. 이러한 각 OUs로 생성된 애플리케이션 계정에 프로비저닝된 인프라에는 해당 기본 OUs에서 제공하는 특정 AMS 모드가 적용됩니다. 동일한 애플리케이션 계정에서 두 개 이상의 모드를 혼합하여 찾는 것이 일반적입니다. 예를 들어 RFC 모드와 SSP 모드는 트리거 함수를 위한 API Gateway 및 Lambda와 수집 및 오케스트레이션을 위한 EC2, S3 및 SQS로 구성된 파이프라인 아키텍처를 호스팅하는 AMS 관리형 계정에 공존할 수 있습니다. 이 경우 SSP 모드가 Lambda 및 API Gateway에 적용됩니다.

그림 1은 AMS의 기본 OUs 통해 다양한 모드가 제공되는 방법을 보여줍니다. AMS에서 새 애플리케이션 계정을 요청할 때는 계정의 OU를 선택해야 합니다.

MALZ 아키텍처 및 관련 AMS 모드

AMS는 서비스 제어 정책(SCPs)을 사용하여 계정을 논리적으로 관리하는 방법으로 AWS 모범 사례를 기반으로 하는 기본 OUs를 활용합니다. 이는 각 AMS 모드에서 거버넌스 프레임워크를 적용하는 방법입니다. 기본 OUs에 적용되는 모든 거버넌스 및 보안 가드레일(SCPs 형식)도 사용자 지정/하위 OUs에 자동으로 적용됩니다. 하위 OU에 대해 추가 SCPs를 요청할 수 있습니다. OUs 애플리케이션 계정이 모드와 동일하지 않다는 점을 이해하는 것이 중요합니다. 모드는 계정 내에 프로비저닝된 인프라에 적용되며 AMS와 고객 간의 운영 책임을 정의합니다.

그림 1: MALZ 아키텍처 및 관련 AMS 모드

> **Note**
>
> “제한적”이란 이러한 OUs에 대한 사용자 지정 정책을 요청할 수 있으며, 운영 우수성을 제공하는 AMS의 기능을 방해하지 않도록 case-by-case AMS의 승인을 받았음을 의미합니다. AMS 가드레일의 자세한 목록은 사용 설명서의 AMS 가드레일을 참조하세요.

AMS 모드 및 애플리케이션 또는 워크로드

새 애플리케이션 계정을 요청하거나 기존 애플리케이션 계정에서 애플리케이션을 호스팅하여 올바른 모드를 선택할 때 애플리케이션의 운영 및 거버넌스 요구 사항을 고려합니다. 각 애플리케이션 또는 워크로드에 적합한 AMS 모드 선택은 다음 요인에 따라 달라집니다.

- 환경이 제공할 SDLC 수명 주기 함수의 유형(예: 조정되지 않은 변경 사항이 있는 샌드박스, 자주 변경되는 UAT, 최소한의 변경 사항이 있고 규제가 엄격한 프로덕션)
- 필요한 거버넌스 정책(OU 수준에서 SCPs를 통해 적용됨)
- 운영 모델(운영 책임을 소유하거나 AMS에 아웃소싱하려는 경우)
- 클라우드 운영 시간, 운영 비용 등 원하는 비즈니스 성과입니다.

> **Note**
>
> AMS 서비스당 모드 유형에 대한 설명은 AMS의 모드 및 계정 유형을 참조하세요.
> 다양한 모드의 실제 사용 사례는 AMS 모드의 실제 사용 사례를 참조하세요.

다음 표에는 애플리케이션 소유자가 가장 적합한 AMS 모드를 결정하는 데 도움이 되는 주요 고려 사항이 요약되어 있습니다. 애플리케이션 소유자는 특정 애플리케이션에 적용되는 모드를 완전히 이해하려면 애플리케이션 마이그레이션 전에 평가 단계를 포함해야 합니다. 예: 클라우드 네이티브 서비스 또는 서버리스 아키텍처 기반 애플리케이션의 경우 가장 좋은 옵션은 개발자 모드에서 빌드 및 반복을 시작하고 AMS 관리형 - SSP 모드를 사용하여 최종 코드형 인프라를 배포하는 것입니다. 이 경우 자동 배포를 위해 생성된 CloudFormation 템플릿이 AMS에서 제시한 수집 지침을 충족하는지 확인하기 위해 라이트 리팩터링이 필요할 수 있습니다. 또한 모든 IAM 권한은 최소 권한 모델을 따르도록 AMS Security의 승인을 받아야 합니다.

애플리케이션을 호스팅하도록 선택한 AMS 모드를 사용하면 원하는 클라우드 운영 모델을 구축할 수 있습니다.

> **Note**
>
> 애플리케이션을 호스팅하기 위해 선택한 다양한 AMS 모드를 기반으로 단일 AMS 관리형 랜딩 존에 둘 이상의 클라우드 운영 모델이 존재할 수 있습니다.

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
운영 준비 상태						
로깅, 모니터링 및 이벤트 관리	모든 관리형 인프라를 담당하는 AMS			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	고객 책임
연속성 관리	고객이 선택한 백업 계획을 실행할 AMS 책임			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
					로비저닝된 리소스를 담당하는 고객	
인스턴스 수준 액세스 관리	온프레미스 도메인과의 단방향 AD 신뢰를 통해 AMS 관리됩니다. 관리형 인프라가 AMS 도메인에 조인해야 함			해당 사항 없음	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
보안 관리 및 계정 수준 액세스 관리	모든 관리형 계정에 대한 AMS 책임			모든 관리형 계정을 담당하는 AMS	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
패치 관리	모든 관리형 계정에 대한 AMS 책임			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
변경 관리	모든 관리형 계정에 대한 AMS 책임			셀프 서비스 프로비저닝 서비스(SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
프로비저닝 관리	AMS에서 제공되는 프로비저닝 옵션에 대한 권장 및 표준화	AMS 규범적 표준에 따라 AWS Service Catalog용 AWS 서비스 API를 직접 사용할 수 있는 유연성	AMS 규범적 표준에 따라 AWS 서비스 API를 직접 사용할 수 있는 유연성	SSP 서비스에 AWS 서비스 APIs 수 있는 유연성	프로비저닝에 AWS 서비스 API를 직접 사용할 수 있는 유연성	
인시던트 관리 및 감사	모든 관리형 계정에 대한 AMS 책임				AMS Change Management System 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
GuardRails 및 공유 인프라(네트워크) 및 보안 프레임워크	AMS Core 계정의 권장 및 표준화 활용					유연한 맞춤형 AMS Core 계정 활용
애플리케이션 준비 상태						
애플리케이션 리팩터링	라이트 리팩터링 필요				라이트 리팩터링 필요(AMS Standard CM을 사용하여 프로비저닝된 경우)	리팩터링 필요 없음
AWS 서비스 지원	AMS에서 지원하는 것으로 제한됨					제한되지 않음
비즈니스 고려 사항						
운영 준비 시간	3~6개월			6개월 + 고객 애플리케이션 운영 역량에 따라 다름		고객 인프라 및 애플리케이션 운영 역량에 따라 6~18개월
비용	$$$$			$$$	$$	$

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
애플리케이션 예제	3 티어 스택이 있는 Webserver, 규정 준수 및 규제 요구 사항이 있는 앱			API Gateway를 사용하는 Webserver, ECS/EKS를 활용하는 컨테이너화된 애플리케이션	Lambda, Glue, Athena 등을 사용하는 Data Lake 애플리케이션에서 반복/최적화	샌드박스, 타사 관리형 애플리케이션과 같은 분산형 계정/애플리케이션

*OOD(Operations On Demand)에는 표준 CM 모드를 사용하는 고객이 전용 리소싱을 통해 변경 사항을 관리할 수 있는 기능이 있습니다. 자세한 내용은 오퍼링의 온디맨드 운영 카탈로그를 참조하고 클라우드 서비스 제공 관리자(CSDM)에게 문의하세요.

> **Note**
>
> SSP 모드와 개발자 모드 간의 가격 비교는 동일한 AWS 서비스가 프로비저닝된다고 가정합니다.

AMS 모드와 비즈니스 및 IT 목표 비교

표시된 것처럼 애플리케이션에 대해 고도로 제어되고 표준화된 거버넌스 모델을 찾고 있다면 AMS 관리형 표준 변경, AWS Service Catalog 또는 직접 변경 모드가 가장 적합합니다. 운영 준비 없이 애플리케이션 혁신에 중점을 둔 맞춤형 거버넌스 모델이 필요한 경우 고객 관리형 모드를 선택합니다. 고객 관리형 모드를 사용하면 인시던트 관리, 구성 관리, 프로비저닝 관리, 보안 관리, 패치 관리 등과 같은 운영 기능을 지원하는 인력, 프로세스 및 도구를 구축할 책임이 있으므로 애플리케이션을 운영하는 데 시간이 더 오래 걸릴 수 있습니다.

AMS 모드의 실제 사용 사례

이를 검토하여 AMS 모드를 사용하는 방법을 결정합니다.

- 사용 사례 1, 시간에 민감한 데이터 센터 종료와 함께 비용을 절감하기 위한 비즈니스 요구 사항: 데이터 센터 종료와 같은 매력적인 비즈니스 이벤트가 있는 기업은 클라우드에서 온프레미스 애플리케이션을 다시 호스팅하는 데 관심이 있습니다. 대부분의 온프레미스 인벤토리는 운영 체제 버전이 혼합된 Windows 및 Linux 서버로 구성됩니다. 이를 통해 고객은 클라우드로 전환하여 애플리케이션의 기술 및 보안 태세를 개선하는 비용 절감을 활용하고자 합니다. 고객은 빠르게 움직이고 싶지만 아직 사내 클라우드 운영 전문 지식이 구축되어 있지 않습니다. 고객은 리팩터링의 균형을 찾아야 합니다. 리팩터링이 너무 많으면 촉박한 타임라인에 비해 위험할 수 있습니다. 그러나 OS 버전 업데이트 및 데이터베이스 최적화와 같은 일부 리팩터링을 통해 애플리케이션은 다음 수준의 성능을 달성할 수 있습니다. 이 예제에서 고객은 AMS 관리형 RFC 모드를 선택하여 대부분의 애플리케이션을 다시 호스팅할 수 있습니다. AMS는 인프라 운영을 제공하는 동시에 고객 운영 팀에 클라우드에서 안전하게 운영하는 모범 사례를 안내합니다.

  AMS 관리형 AWS Service Catalog 및 AMS 관리형 Direct Change 모드는 고객에게 동일한 비즈니스 성과와 목표를 달성하면서 유연성을 높입니다. 또한 고객은 AMS Operations On Demand(OOD) 오퍼링을 사용하여 전용 AMS 운영 엔지니어가 변경 요청(RFCs.

  차별화되지 않은 인프라 운영 작업(패치, 백업, 계정 관리 등)을 AMS로 오프로드하는 동안 고객은 애플리케이션을 최적화하는 데 계속 집중하고 클라우드 운영에서 내부 팀을 확장할 수 있습니다. AMS는 고객에게 비용 절감에 대한 월별 보고서를 제공하고 리소스 최적화에 대한 권장 사항을 제시합니다. 이 사용 사례에서는 Windows 2003 및 2008과 같은 레거시 OS 버전에서 호스팅된 end-of-life 애플리케이션이 있고 고객이 리팩터링하지 않기로 결정한 경우 해당 애플리케이션을 AMS로 마이그레이션하고 고객 관리형 모드를 활용하는 계정에서 호스팅할 수도 있습니다.
- 사용 사례 2, 보안 AMS 경계 내에서 Lambda, Glue, Athena로 데이터 레이크 구축: 기업은 AMS의 여러 애플리케이션에 대한 보고 요구 사항을 충족하기 위해 Data Lake를 설정하려고 합니다. 고객은 S3 버킷을 사용하여 데이터 세트를 저장하고 AWS Athena를 사용하여 각 보고서의 데이터 세트를 쿼리하려고 합니다. S3와 AWS Athena는 별도의 AMS 관리형 계정에 배포됩니다. S3가 있는 계정에는 데이터 수집 파이프라인을 빌드하기 위한 Glue, Lambda 및 Step Functions와 같은 다른 서비스도 있습니다. 이 경우 Glue, Lambda, Athena 및 Step Functions는 셀프 서비스 프로비저닝(SSP) 서비스로 간주됩니다. 또한 고객은 임시 도구/스크립팅 서버 역할을 하는 계정에 EC2 인스턴스를 배포했습니다. 고객은 먼저 AMS 관리형 계정에서 SSP 서비스를 활성화하도록 AMS에 요청합니다. AMS는 역할이 고객의 연동 솔루션에 온보딩되면 고객이 수임할 수 있는 각 서비스에 대해 IAM 역할을 프로비저닝합니다. 간편한 관리를 위해 고객은 별도의 IAM 역할에 대한 정책을 하나의 사용자 지정 역할로 결합하여 AWS 서비스 간에 작업할 때 역할을 전환할 필요성을 줄일 수도 있습니다. 계정에서 역할이 활성화되면 고객은 요구 사항에 따라 서비스를 구성할 수 있습니다. 그러나 고객은 AMS 변경 관리 시스템과 협력하여 사용 사례에 따라 추가 권한을 요청해야 합니다.

예를 들어 Glue 크롤러에 액세스하려면 Glue에 추가 권한이 필요합니다. Lambda에 대한 이벤트 소스를 생성하려면 추가 권한도 필요합니다. 고객은 AMS와 협력하여 Athena가 S3 버킷을 쿼리할 수 있도록 교차 계정 액세스를 허용하도록 IAM 역할을 업데이트합니다. Lambda가 Step Functions 서비스를 호출하고 Glue가 모든 S3 버킷을 읽고 쓸 수 있도록 AMS 변경 관리를 통해 서비스 역할 또는 서비스 연결 역할을 업데이트해야 합니다. AMS는 고객과 협력하여 최소 권한 액세스 모델을 따르고 요청된 IAM 변경 사항이 지나치게 허용적이지 않고 불필요한 위험에 노출되지 않도록 합니다. 고객의 데이터 레이크 팀은 고객의 아키텍처와 관련된 서비스에 필요한 모든 IAM 권한을 계획하고 AMS에 이를 활성화하도록 요청합니다. 이는 모든 IAM 변경 사항이 수동으로 처리되고 AMS 보안 팀의 검토를 받기 때문입니다. 이러한 요청을 처리하는 데 걸리는 시간은 애플리케이션 배포 일정에서 고려해야 합니다.

SSP 서비스가 계정에서 작동하므로 고객은 AMS 인시던트 관리 및 서비스 요청을 통해 지원을 요청하고 문제를 보고할 수 있습니다. 그러나 AMS는 Lambda에 대한 성능 및 동시성 지표 또는 Glue에 대한 작업 지표를 적극적으로 모니터링하지 않습니다. SSP 서비스에 대해 적절한 로깅 및 모니터링이 활성화되었는지 확인하는 것은 고객의 책임입니다. 계정의 EC2 인스턴스 및 S3 버킷은 AMS에서 완전히 관리됩니다.

- 사용 사례 3, AMS에서 CICD 배포 파이프라인의 빠르고 유연한 설정: 고객이 AMS의 모든 애플리케이션 계정에 코드 파이프라인을 배포하기 위해 Jenkins 기반 CICD 파이프라인을 설정하려고 합니다. 고객은 AMS 관리형 Direct Change 모드(DCM) 또는 AMS 관리형 개발자 모드에서이 CICD 파이프라인을 호스팅하는 것이 가장 적합할 수 있습니다. 이는 아티팩트 리포지토리를 호스팅하는 CloudFormation 및 S3 버킷에 액세스할 수 있는 원하는 IAM 권한과 함께 EC2에 필요한 사용자 지정 구성으로 Jenkins 서버를 유연하게 설정할 수 있기 때문입니다. AMS 관리형 RFC 모드에서도이 작업을 수행할 수 있지만 고객 팀은 IAM 역할에 대해 여러 개의 수동 RFCs를 생성하여 AMS에서 수동으로 검토하는 최소 허용 권한 세트를 반복해야 합니다. DCM을 사용하면 AMS 관리형 RFCs 대한 수동 RFC를 여러 개 생성할 필요 없이 AWS에서 운영 목표를 달성하여 AMS에서 수동으로 검토하는 최소 허용 권한 세트를 반복할 수 있습니다. AMS 프로세스와 도구를 늘리려면 고객 측 교육뿐만 아니라 시간이 걸립니다. 개발자 모드에서 고객은 "개발자 역할"로 시작하여 네이티브 AWS APIs. 이 파이프라인을 설정하는 가장 빠르고 유연한 방법은 AMS Managed-Developer 모드를 사용하는 것입니다. 개발자 모드는 운영 통합을 손상시키면서 가장 빠르고 쉬운 방법을 제공하는 반면, DCM은 덜 유연하지만 RFC 모드와 동일한 수준의 운영 지원을 제공합니다.
- 사용 사례 4, AMS 기반 내의 맞춤형 운영 모델: 고객이 기한 기반 데이터 센터 종료를 보고 있으며, 애플리케이션 운영 및 인프라 운영을 포함한 타사 MSP가 엔터프라이즈 애플리케이션 중 하나를 완전히 관리합니다. AMS에서 운영할 수 있도록 고객이 일정에이 애플리케이션을 리팩터링할 시간이 없다고 가정하면 고객 관리형 모드가 적절한 옵션입니다. 고객은 AMS 관리형 랜딩 존의 자동 및 빠른 설정을 활용할 수 있습니다. 중앙 집중식 네트워킹 계정을 통해 계정 벤딩 및 연결을 제어하는 중앙 집중식 계정 관리를 활용할 수 있습니다. 또한 AMS Payer 계정을 통해 모든 고객 관리형 계정에

대한 요금을 통합하여 결제를 간소화합니다. 고객은 AMS 관리형 계정에 사용되는 표준 액세스 관리와 별도로 MSP를 사용하여 맞춤형 액세스 관리 모델을 유연하게 설정할 수 있습니다. 이렇게 하면 고객 관리형 모드를 사용하여 온프레미스 환경을 비우는 비즈니스 요구 사항을 충족하면서 AMS 관리형 환경을 설정할 수 있습니다. 이 경우 고객이 클라우드로 마이그레이션하는 Windows 기반 애플리케이션도 보유하고 있고 이를 고객 관리형 계정으로 이동하기로 선택한 경우 고객은 클라우드 운영 모델을 생성할 책임이 있습니다. 이는 기존 IT 프로세스를 혁신하고 인력을 교육하는 고객의 능력에 따라 복잡하고 비용이 많이 들고 시간이 많이 걸릴 수 있습니다. 고객은 이러한 워크로드를 AMS 관리형 계정으로 "리프트 앤 시프트"하여 시간과 비용을 절약하고 인프라 작업을 AMS로 오프로드할 수 있습니다.

> **Note**
>
> 고객은 RFC 또는 SSP 모드의 거버넌스 프레임워크와 개발자 모드 간에 애플리케이션 계정을 이동해야 할 때가 있습니다. 예를 들어 고객은 초기 리프트 앤 시프트 마이그레이션의 일부로 AMS 관리형 모드에서 애플리케이션을 호스팅할 수 있지만, 초과 근무 시 애플리케이션을 다시 작성하여 클라우드 네이티브 AWS 서비스에 최적화하려고 합니다. 사전 프로덕션 계정의 모드를 AMS 관리형 RFC에서 AMS 관리형 개발자 모드로 변경하여 인프라를 프로비저닝할 수 있는 유연성과 민첩성을 제공할 수 있습니다. 그러나 "개발자 역할"을 사용하여 인프라 프로비저닝을 변경한 후에는 동일한 인프라를 AMS 관리형 RFC 모드로 다시 이동할 수 없습니다. 이는 AMS가 AMS 변경 관리 시스템 외부에서 프로비저닝된 인프라의 운영을 보장할 수 없기 때문입니다. 고객은 AMS 관리형 RFC 모드를 제공하는 새 애플리케이션 계정을 생성한 다음 AMS 관리형 계정으로 수집된 CloudFormation 템플릿 또는 사용자 지정 AMIs를 통해 "최적화된" 인프라 구성을 다시 배포해야 할 수 있습니다. 이는 프로덕션 준비 구성을 배포하는 깔끔한 방법입니다. 배포되면 애플리케이션은 규범적 AMS 거버넌스 및 운영의 적용을 받습니다. 고객 관리형 모드와 AMS 관리형 모드 간 전환 모드에도 동일하게 적용됩니다.

RFC 모드

RFC 모드는 AMS Advanced 운영 계획 고객의 기본 모드입니다. 여기에는 변경 또는 RFCs에 대한 요청이 있는 변경 관리 시스템과 계정에 필요한 추가 또는 변경을 요청하는 데 사용할 변경 유형 카탈로그가 포함됩니다. 이 변경 관리 시스템은 계정을 변경할 수 있는 사용자를 제한하는 데 있어 보안 수준을 제공합니다.

AMS 고급 변경 유형에 대한 자세한 내용은 AMS 변경 유형이란 무엇입니까?를 참조하세요.

AMS Advanced 온보딩에 대한 자세한 내용은 AWS Managed Services 온보딩 소개를 참조하세요.

변경 유형 예제 연습은 AMS 고급 변경 유형 참조 분류별 변경 유형 섹션의 관련 변경 유형에 대한 "추가 정보" 섹션을 참조하세요.

> **Note**
>
> RFC 모드는 이전에 "변경 관리 모드" 또는 "표준 CM 모드"라고 불렸습니다.

주제

- RFCs 대해 알아보기
- 변경 유형이란 무엇입니까?
- AMS의 RFC 오류 문제 해결

RFCs 대해 알아보기

변경 요청 또는 RFCs는 두 가지 방식으로 작동합니다. 먼저 RFC 자체에 필요한 파라미터가 있습니다. API의 옵션은 다음과 같습니다`CreateRfc`. 둘째, RFC의 작업에 필요한 파라미터(실행 파라미터)가 있습니다. `CreateRfc` 옵션에 대한 자세한 내용은 AMS API 참조의 CreateRfc 섹션을 참조하세요. 이러한 옵션은 일반적으로 RFC 생성 페이지의 추가 구성 영역에 나타납니다.

`CreateRfc` API, `aws amscm create-rfc` CLI 또는 AMS 콘솔 RFC 생성 페이지를 사용하여 RFC를 생성하고 제출할 수 있습니다. RFC 생성에 대한 자습서는 섹션을 참조하세요RFC 생성.

주제

- RFC란 무엇인가요?
- AMS API/CLI 사용 시 인증
- RFC 보안 검토 이해
- RFC 변경 유형 분류 이해
- RFC 작업 및 활동 상태 이해
- RFC 상태 코드 이해
- RFC 업데이트 CTs 및 CloudFormation 템플릿 드리프트 감지 이해
- RFCs 예약
- RFCs 승인 또는 거부
- RFC 제한 실행 기간 요청

- RFCs 생성, 복제, 업데이트, 찾기 및 취소
- RFCs와 함께 AMS 콘솔 사용
- 일반적인 RFC 파라미터에 대해 알아보기
- RFC 일일 이메일에 가입

RFC란 무엇인가요?

변경 요청 또는 RFC는 AMS 관리형 환경을 변경하거나 AMS에 사용자를 대신하여 변경하도록 요청하는 방법입니다. RFC를 생성하려면 AMS 변경 유형 중에서 선택하고 RFC 파라미터(예: 일정)를 선택한 다음 AMS 콘솔 또는 API 명령 CreateRfc 및 SubmitRfc를 사용하여 요청을 제출합니다.

RFC에는 두 가지 사양이 있습니다. 하나는 RFC 자체용이고 다른 하나는 변경 유형(CT) 파라미터용입니다. 명령줄에서 인라인 RFC 명령 또는 JSON 형식의 표준 CreateRfc 템플릿을 사용하여 생성한 CT JSON 스키마 파일(CT 파라미터 기반)과 함께 작성하고 제출할 수 있습니다. CT 이름은 CT에 대한 비공식 설명입니다. CSIO(범주, 하위 범주, 항목, 작업)는 CT에 대한 보다 공식적인 설명입니다. RFC를 생성할 때 CT ID만 지정해야 합니다.

RFCs 검증과 실행이라는 두 가지 주요 단계를 거칩니다.

1. 검증 단계에서 AMS는 RFC 요청의 완전성과 정확성을 검토합니다. 또한 AMS는 보안 기술 표준에 따라 보안 요청을 평가합니다. AMS는 요청된 변경이 유효하고 실행 가능한지 확인합니다.
2. 실행 단계에서 AMS는 계정에서 요청된 변경 사항을 시도합니다.

AMS는 자동화된 프로세스, 수동 프로세스 또는 두 프로세스의 조합을 통해 두 단계를 모두 처리합니다. 수동 프로세스는 AMS 운영 팀에서 처리합니다. 자세한 내용은 자동 및 수동 CTs 단원을 참조하십시오.

AMS는 요청을 처리하기 위한 세 가지 실행 모드를 제공합니다.

- (AMS 권장) 실행 모드: 자동. 이러한 CTs는 비즈니스 성과를 달성하는 가장 빠른 방법인 RFC 검증 및 실행에 자동화를 사용합니다.
- (AMS 권장) 실행 모드: 수동 및 지정: 관리형 자동화. 이러한 CTs RFC 검증 및 실행을 위해 자동화된 프로세스와 수동 프로세스의 조합을 활용합니다. 자동화가 요청된 변경을 실행할 수 없는 경우 RFC는 수동 처리를 위해 (자동 라우팅 또는 대체 RFC를 생성하여) AMS 운영 팀에 전송됩니다. 이러한 CTs를 제출하면 AMS 자동화로 보완된 요청을 보다 구조화하여 처리 및 실행 결과 기간을 개선할 수 있습니다.

- 실행 모드: 수동 및 지정: 검토 필요. ct-1e1xtak34nx76 관리 | 기타 | 기타 | 업데이트(검토 필요) 또는 ct-0xdawir96cy7k 관리 | 기타 | 기타 | 생성(검토 필요)을 통해 요청된 변경 사항. 이러한 CTs 검증 및 실행을 위한 수동 처리에 의존합니다. 이러한 CTs는 변경 요청의 수동 해석에 따라 달라집니다.

AMS는 변경이 성공적으로 완료되거나(성공) 실패하면(실패) 알려줍니다.

> **Note**
>
> RFC 실패 문제 해결에 대한 자세한 내용은 섹션을 참조하세요AMS의 RFC 오류 문제 해결.

다음 그림은 사용자가 제출한 RFC의 워크플로를 보여줍니다.

AMS API/CLI 사용 시 인증

AMS API/CLI를 사용하는 경우 임시 자격 증명으로 인증해야 합니다. 페더레이션 사용자를 위한 임시 보안 자격 증명을 요청하려면 GetFederationToken, AssumeRole, AssumeRoleWithSAML 또는 AssumeRoleWithWebIdentity AWS 보안 토큰 서비스(STS) APIs.

일반적인 선택은 SAML입니다. 설정 후 호출하는 각 작업에 인수를 추가합니다. 예를 들어 `aws --profile saml amscm list-change-type-categories`입니다.

SAML 2.0 프로파일의 바로 가기는를 사용하여 각 API/CLI 시작 시 프로파일 변수를 설정하는 것입니다`set AWS_DEFAULT_PROFILE=saml`(Windows의 경우 , Linux의 경우 `export AWS_DEFAULT_PROFILE=saml`). CLI 환경 변수 설정에 대한 자세한 내용은 AWS 명령줄 인터페이스 구성, 환경 변수를 참조하세요.

RFC 보안 검토 이해

AWS Managed Services(AMS) 변경 관리 승인 프로세스를 통해 계정의 변경 사항에 대한 보안 검토를 수행할 수 있습니다.

AMS는 AMS 기술 표준을 기준으로 모든 변경 요청(RFCs 평가합니다. 기술 표준을 벗어나 계정의 보안 태세를 저하시킬 수 있는 모든 변경 사항은 보안 검토를 거칩니다. 보안 검토 중에 AMS는 관련 위험을 강조 표시하고, 보안 위험이 높거나 매우 높은 경우 승인된 보안 담당자가 RFC를 수락하거나 거부합니다. 또한 모든 변경 사항을 평가하여 AMS의 운영 능력에 부정적인 영향을 미치는지 평가합니다. 잠재적인 부정적인 영향이 발견되면 AMS 내에서 추가 검토 및 승인이 필요합니다.

AMS 기술 표준

AMS 기술 표준은 최소 보안 기준, 구성 및 프로세스를 정의하여 계정의 기본 보안을 설정합니다. AMS와 사용자 모두 이러한 표준을 따라야 합니다.

기술 표준을 벗어나 계정의 보안 태세를 잠재적으로 저하시킬 수 있는 모든 변경 사항은 위험 수락 프로세스를 거칩니다.이 프로세스에서는 AMS에서 관련 위험을 강조 표시하고 권한 있는 보안 담당자가 사용자 측에서 수락하거나 거부합니다. 또한 이러한 모든 변경 사항을 평가하여 AMS의 계정 운영 능력에 부정적인 영향을 미칠지 여부를 평가하고, 영향을 미칠 경우 AMS 내에서 추가 검토 및 승인이 필요한지 여부를 평가합니다.

RFC 고객 보안 위험 관리(CSRM) 프로세스

조직의 누군가가 관리형 환경에 대한 변경을 요청하면 AMS는 변경 사항을 검토하여 해당 요청이 기술 표준을 벗어나 계정의 보안 태세를 저하시킬 수 있는지 확인합니다. 요청이 계정의 보안 태세를 저하시키는 경우 AMS는 보안 팀에 관련 위험을 알리고 변경을 실행합니다. 또는 변경으로 인해 환경에서 보안 위험이 높거나 매우 높은 경우 AMS는 위험 수락(다음 설명됨)의 형태로 보안 팀 연락처로부터 명시적 승인을 구합니다. AMS 고객 위험 수락 프로세스는 다음을 위해 설계되었습니다.

- 위험을 명확하게 식별하고 올바른 소유자에게 알립니다.
- 환경에 대해 식별된 위험 최소화
- 조직의 위험 프로필을 이해하는 지정된 보안 담당자로부터 승인을 받고 문서화합니다.
- 식별된 위험에 대한 지속적인 운영 오버헤드 감소

기술 표준 및 높거나 매우 높은 위험에 액세스하는 방법

https://console.aws.amazon.com/artifact/ AMS 기술 표준 설명서를 보고서로 참조할 수 있도록 했습니다. AMS 기술 표준 설명서를 사용하여 변경 요청(RFC)을 제출하기 전에 승인된 보안 담당자의 위험 수락이 변경에 필요한지 여부를 파악합니다.

기본 AWSManagedServicesChangeManagementRole로 로그인한 후 보고서 탭 검색 창에서 "AWS Managed Services(AMS) 기술 표준" AWS Artifact 을 검색하여 기술 표준 보고서를 찾습니다.

> **Note**
>
> AMS 기술 표준 문서는 단일 계정 랜딩 존의 Customer_ReadOnly_Role에 액세스할 수 있습니다. 다중 계정 랜딩 존에서는 보안 관리자가 사용하는 AWSManagedServicesAdminRole과 애플리케이션 팀이 사용하는 AWSManagedServicesChangeManagementRole을 사용하여 문서

에 액세스할 수 있습니다. 팀에서 사용자 지정 역할을 사용하는 경우 기타 | 기타 RFC를 생성하여 액세스를 요청하면 지정된 사용자 지정 역할이 업데이트됩니다.

RFC 변경 유형 분류 이해

RFC를 제출할 때 사용하는 변경 유형은 두 가지 광범위한 범주로 나뉩니다.

- 배포:이 분류는 리소스를 생성하기 위한 것입니다.
- 관리:이 분류는 리소스를 업데이트하거나 삭제하기 위한 것입니다. 관리 범주에는 인스턴스 액세스, AMIs 암호화 또는 공유, 스택 시작, 중지, 재부팅 또는 삭제를 위한 변경 유형도 포함됩니다.

RFC 작업 및 활동 상태 이해

`RfcActionState` (API) / 활동 상태(콘솔)는 RFC에서 사람의 개입 또는 작업 상태를 이해하는 데 도움이 됩니다. 주로 수동 RFCs에 사용되는 `RfcActionState`는 사용자 또는 AMS 작업에 필요한 작업이 있는 시기를 이해하고 AMS 작업이 RFC에서 활발하게 작업하는 시기를 확인하는 데 도움이 됩니다. 이렇게 하면 수명 주기 동안 RFC에서 수행되는 작업에 대한 투명성이 향상됩니다.

`RfcActionState` (API) / 활동 상태(콘솔) 정의:

- AwsOperatorAssigned: AWS 운영자가 RFC에서 적극적으로 작업하고 있습니다.
- AwsActionPending: AWS의 응답 또는 작업이 예상됩니다.
- CustomerActionPending: 고객의 응답 또는 조치가 필요합니다.
- NoActionPending: AWS 또는 고객의 조치가 필요하지 않습니다.
- NotApplicable:이 상태는 AWS 운영자 또는 고객이 설정할 수 없으며이 기능이 릴리스되기 전에 생성된 RFCs에만 사용됩니다.

RFC 작업 상태는 제출된 변경 유형에 수동 검토가 필요한지 여부와 일정이 ASAP로 설정되어 있는지 여부에 따라 달라집니다.

- 지연된 일정으로 수동 변경 유형을 검토, 승인 및 시작하는 동안 RFC ActionState가 변경됩니다.
  - 예약된 수동 RFC를 제출하면 ActionState가 자동으로 AwsActionPending으로 변경되어 운영자가 RFC를 검토하고 승인해야 함을 나타냅니다.
  - 운영자가 RFC를 적극적으로 검토하기 시작하면 ActionState가 AwsOperatorAssigned로 변경됩니다.

- 운영자가 RFC를 승인하면 RFC 상태가 예약됨으로 변경되고 ActionState가 자동으로 NoActionPending으로 변경됩니다.
- RFC의 예약된 시작 시간에 도달하면 RFC 상태가 InProgress으로 변경되고 ActionState가 자동으로 AwsActionPending으로 변경되어 RFC 검토를 위해 연산자를 할당해야 함을 나타냅니다.
- 운영자가 RFC를 적극적으로 실행하기 시작하면 ActionState를 AwsOperatorAssigned로 변경합니다.
- 완료되면 연산자가 RFC를 닫습니다. 그러면 ActionState가 NoActionPending으로 자동 변경됩니다.

Important

- 작업 상태는 사용자가 설정할 수 없습니다. RFC의 변경 사항에 따라 자동으로 설정되거나 AMS 연산자가 수동으로 설정합니다.
- RFC에 서신을 추가하면 ActionState가 자동으로 AwsActionPending으로 설정됩니다.
- RFC가 생성되면 ActionState가 NoActionPending으로 자동 설정됩니다.
- RFC가 제출되면 ActionState는 자동으로 AwsActionPending으로 설정됩니다.
- RFC가 거부됨, 취소됨 또는 성공 또는 실패 상태로 완료되면 ActionState가 NoActionPending으로 자동 재설정됩니다.
- 작업 상태는 자동 RFCs 모두에서 활성화되지만 수동 RFCs의 경우 대부분 통신이 필요한 RFCs 경우가 많습니다.

RFC 작업 상태 사용 사례 검토

사용 사례: 수동 RFC 프로세스에 대한 가시성

- 수동 RFC를 제출하면 운영자가 RFC를 검토하고 승인해야 함을 나타내`AwsActionPending`기 위해 RFC 작업 상태가 로 자동 변경됩니다. 운영자가 RFC를 적극적으로 검토하기 시작하면 RFC 작업 상태가 로 변경됩니다`AwsOperatorAssigned`.
- 승인 및 예약되었으며 실행을 시작할 준비가 된 수동 RFC를 생각해 보십시오. RFC 상태가 로 변경되면 `InProgress`RFC 작업 상태가 자동으로 로 변경됩니다`AwsActionPending`. 운영자가 RFC를 적극적으로 실행하기 시작`AwsOperatorAssigned`하면 다시 로 변경됩니다.

- 수동 RFC가 완료되면("성공" 또는 "실패"로 닫힘) RFC 작업 상태가 로 변경NoActionPending되어 고객 또는 운영자의 추가 작업이 필요하지 않음을 나타냅니다.

사용 사례: RFC 대응

- 수동 RFC가 인 경우 AMS 운영자Pending Approval가 추가 정보를 필요로 할 수 있습니다. 연산자는 RFC에 서신을 게시하고 RFC 작업 상태를 로 변경합니다CustomerActionPending. 새 RFC 대응 서신을 추가하여 응답하면 RFC 작업 상태가 자동으로 로 변경됩니다AwsActionPending.
- 자동 또는 수동 RFC가 실패하면 RFC 세부 정보에 서신을 추가하여 AMS 운영자에게 RFC가 실패한 이유를 물어볼 수 있습니다. 서신이 추가되면 RFC 작업 상태가 자동으로 로 설정됩니다AwsActionPending. AMS 운영자가 서신을 보기 위해 RFC를 선택하면 RFC 작업 상태가 로 변경됩니다AwsOperatorAssigned. 연산자가 새 RFC 대응 서신을 추가하여 응답하면 RFC 작업 상태가 고객으로부터 다른 응답이 있음을 CustomerActionPending나타내는 로 설정되거나 고객의 응답이 필요하지 않음을 NoActionPending나타내는 로 설정될 수 있습니다.

RFC 상태 코드 이해

RFC 상태 코드는 요청을 추적하는 데 도움이 됩니다. CLI 출력에서 RFC를 실행하는 동안 또는 콘솔에서 RFC 목록 페이지를 새로 고쳐 이러한 상태 코드를 관찰할 수 있습니다.

해당 RFC의 세부 정보 페이지에서 다음과 같은 RFC의 코드를 볼 수도 있습니다.

목록에 제출하지 않은 RFC가 표시될 수 있습니다. AMS 연산자가 내부 전용 CT를 사용하는 경우 RFC에 제출하고 RFC 목록에 표시됩니다. 자세한 내용은 내부 전용 변경 유형 단원을 참조하십시오.

> **Important**
>
> RFC 상태 변경에 대한 알림을 요청할 수 있습니다. 자세한 내용은 RFC 상태 변경 알림을 참조하세요.

RFC 상태 코드

Success	실패
편집: RFC가 생성되었지만 제출되지 않음 PendingApproval / Submitted: RFC가 제출되었으며 시스템에서 승인이 필요한지 여부를 결정하고 필요한 경우 해당 승인을 얻고 있습니다. AWS에서 승인/고객이 승인: RFC가 승인되었습니다. 자동 RFCs는 AWS의 승인을 받고 수동 RFCs는 운영자 및 경우에 따라 고객의 승인을 받습니다. 예약됨: RFC가 구문 및 요구 사항 검사를 통과했으며 실행이 예약됨 InProgress: RFC가 실행 중입니다. 여러 리소스를 프로비저닝하거나 오래 실행되는 UserData가 있는 RFCs는 실행하는 데 시간이 더 오래 걸립니다. 실행됨: RFC가 실행되었습니다. 성공/성공: RFC가 성공적으로 완료되었습니다.	거부됨: RFCs는 일반적으로 검증에 실패하기 때문에 거부됩니다. 예를 들어 사용할 수 없는 리소스, 즉 서브넷이 지정됩니다. 취소됨: RFCs는 일반적으로 구성된 시작 시간이 경과하기 전에 검증을 통과하지 못하기 때문에 취소됩니다. 실패: RFC가 실패했습니다. 실패 이유는 출력의 StatusReason을 참조하세요. AMS 작업은 자동으로 문제 티켓을 생성하고 필요에 따라 사용자와 통신합니다.

> **Note**
>
> 취소되거나 거부된 RFCs는 UpdateRfc를 사용하여 다시 제출할 수 있습니다. 단원을 참조하십시오RFCs 업데이트.

RFC가 필요한 모든 조건을 통과하면(예: 필요한 모든 파라미터가 지정됨) 상태가 로 변경됩니다PendingApproval(자동 CTs도 승인이 필요하며 구문 및 파라미터 검사가 통과하면 자동으로 발생함). 전달되지 않으면 상태가 로 변경됩니다Rejected. 는 거부에 대한 정보를 StatusReason 제공하고, ExecutionOutput 필드는 승인 및 완료에 대한 정보를 제공합니다. 오류 코드는 다음과 같습니다.

- InvalidRfcStateException: RFC가 호출된 작업을 허용하지 않는 상태입니다. 예를 들어 RFC가 제출됨 상태로 전환된 경우 더 이상 수정할 수 없습니다.
- InvalidRfcScheduleException: StartTime, EndTime 또는 TimeoutInMinutes 파라미터가 위반되었습니다.
- InternalServerError: 시스템에 문제가 발생했습니다.
- InvalidArgumentException: 파라미터가 잘못 지정되었습니다. 예를 들어 허용할 수 없는 값이 사용됩니다.
- ResourceNotFoundException: 스택 ID와 같은 값을 찾을 수 없습니다.

변경이 승인되기 전에 예약된 요청된 시작 및 종료 시간(변경 실행 기간이라고도 함)이 발생하면 RFC 상태가 로 변경됩니다`Canceled`. 변경이 승인되면 RFC 상태가 로 변경됩니다`Scheduled`. ASAP RFCs입니다. `ExpectedExecutionDuration`

변경 실행 기간이 도착하기 전에 언제든지 예약된 변경(`CLIRequestedStartTime`에서와 함께 제출됨)을 수정하거나 취소할 수 있습니다. 예약된 변경 사항이 수정된 경우 다시 제출해야 합니다.

변경 시작 시간이 도착하고(예약 또는 ASAP) 승인이 완료되면 상태가 로 변경`InProgress`되며 수정할 수 없습니다. 지정된 변경 실행 기간 내에 변경이 완료되면 상태가 로 변경됩니다`Success`. 변경의 일부가 실패하거나 변경 실행 기간이 종료될 때 변경 사항이 계속 진행 중인 경우 상태가 로 변경됩니다`Failure`.

> **Note**
>
> `InProgress`, `Success`또는 상태 `Failure` 변경 중에는 RFC를 수정하거나 취소할 수 없습니다.

다음 다이어그램은 CreateRFC 호출부터 해결까지의 RFC 상태를 보여줍니다.

RFC 업데이트 CTs 및 CloudFormation 템플릿 드리프트 감지 이해

AMS에 프로비저닝된 리소스는 수정된 CloudFormation 템플릿을 사용합니다. 리소스에 서비스의 AWS 관리 콘솔을 통해 직접 변경된 파라미터가 있는 경우 해당 리소스의 CloudFormation 생성 레코드가 동기화되지 않습니다. 이 경우 AMS 업데이트 변경 유형을 사용하여 AMS의 리소스를 업데이트하려고 하면 AMS는 원래 리소스 구성을 참조하고 잠재적으로 변경된 파라미터를 재설정합니다. 이 재설정은 손상될 수 있으므로 추가 AMS 구성 변경이 감지되면 AMS는 업데이트 변경 유형이 있는 RFCs를 허용하지 않습니다.

업데이트 변경 유형 목록은 콘솔 필터를 사용합니다.

드리프트 문제 해결 FAQs

AMS 드리프트 수정에 대한 질문과 답변. 드리프트 문제 해결을 시작하는 데 사용할 수 있는 두 가지 변경 유형이 있습니다. 하나는 실행 모드=수동 또는 "관리형 자동화"이고 다른 하나는 실행 모드=자동입니다.

드리프트 수정 지원 리소스(ct-3kinq0u4l33zf)

다음은 드리프트 수정 변경 유형(ct-3kinq0u4l33zf)에서 지원하는 리소스입니다. 리소스를 수정하려면 대신 "관리형 자동화"(ct-34sxfo53yuzah) 변경 유형을 사용합니다.

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

드리프트 문제 해결 변경 유형

AMS 드리프트 문제 해결 변경 유형 사용에 대한 질문과 답변입니다.

드리프트 문제 해결 기능에 지원되는 리소스 목록은 섹션을 참조하세요드리프트 수정 지원 리소스 (ct-3kinq0u4l33zf).

> **Important**
>
> 드리프트 수정은 스택 템플릿 및/또는 파라미터를 수정하며, 최신 스택 템플릿 및 파라미터를 사용하도록 로컬 템플릿 리포지토리 또는 이러한 스택을 업데이트하는 자동화를 업데이트해야 합니다. 동기화 없이 이전 템플릿 및/또는 파라미터를 사용하면 기본 리소스가 손상될 수 있습니다.
> 관리형 자동화가 없는 자동화된 CT(ct-3kinq0u4l33zf)는 RFC당 10개의 리소스만 수정할 수 있도록 지원합니다. 나머지 리소스를 10개 배치로 수정하려면 모든 리소스가 수정될 때까지 새 RFCs 생성합니다.

어떤 드리프트 문제 해결 변경 유형을 사용해야 합니까?

다음과 같은 경우 비관리형 자동화, 자동 CT(ct-3kinq0u4l33zf)를 사용하는 것이 좋습니다.

- 자동 CT를 사용하여 기존 스택 리소스에 대한 업데이트를 수행하려고 하면 스택이 이므로 RFC가 거부됩니다`DRIFTED`.
- 과거에 Update CT를 사용했는데 스택이 DRIFTED되어 실패했습니다. 업데이트를 다시 시도할 필요가 없으며 대신 관리형 자동화, 수동, CT를 사용할 수 있습니다.

드리프트 문제 해결 관리형 자동화 없음, 자동화, CT(ct-3kinq0u4l33zf)에서 드리프트된 리소스 유형을 지원하지 않거나 드리프트 문제 해결 관리형 자동화, 자동화, CT가 실패하지 않는 경우에만 관리형 자동화, 수동 CT(ct-34sxfo53yuzah)를 사용하는 것이 좋습니다.

문제 해결 중에 스택에 어떤 변경 사항이 적용되나요?

수정하려면 드리프트된 속성에 따라 스택 템플릿 및/또는 파라미터를 업데이트해야 합니다. 또한 문제 해결은 문제 해결 중에 스택의 스택 정책을 업데이트하고 문제 해결이 완료되면 스택 정책을 이전 값으로 복원합니다.

스택 템플릿 및/또는 파라미터에 대해 수행된 변경 사항을 보려면 어떻게 해야 합니까?

RFC에 대한 응답으로 다음 정보와 함께 변경 요약이 제공됩니다.

- `ChangeSummaryJson`: 드리프트 수정의 일부로 스택 템플릿 및/또는 파라미터의 변경 요약을 포함합니다. 문제 해결은 여러 단계로 수행됩니다. 이 변경 요약은 개별 단계의 변경 사항으로 구성됩니다. 문제 해결이 성공하면 마지막 단계의 변경 사항을 확인합니다. 순서대로 실행되는 단계는 JSON의 ExecutionPlan을 참조하세요. 예를 들어 있는 경우 RestoreReferences 섹션은 항상 끝에 실행되며 수정 후 변경 사항에 대한 JSON을 포함합니다. DryRun 모드에서 문제 해결을 실행하면 스택에 이러한 변경 사항이 적용되지 않습니다.

- `PreRemediationStackTemplateAndConfigurationJson`: 스택에서 수정이 트리거되기 전에 템플릿, 파라미터, 출력, StackPolicyBody를 포함한 CloudFormation 스택의 구성 스냅샷을 포함합니다.

문제 해결이 수행되면 어떻게 해야 하나요?

> **Important**
>
> 수정 스택을 업데이트하는 로컬 템플릿 리포지토리 또는 자동화를 RFC 요약에 제공된 최신 템플릿 및 파라미터로 업데이트해야 합니다. 이전 템플릿 및/또는 파라미터를 사용하면 스택 리소스가 더 이상 파괴적으로 변경될 수 있으므로이 작업을 수행하는 것이 매우 중요합니다.

이 문제 해결 중에 내 애플리케이션이 영향을 받나요?

해결은 CloudFormation 스택 구성에서만 수행되는 오프라인 프로세스입니다. 기본 리소스에 대한 업데이트는 수행되지 않습니다.

문제 해결 후 관리 | 기타 | 기타 RFCs 계속 사용하여 리소스에 대한 업데이트를 수행할 수 있나요?

사용 가능한 자동 CT 업데이트를 사용하여 스택 리소스에 대한 업데이트를 항상 수행하는 것이 좋습니다 CTs. 사용 가능한 업데이트 CTs가 사용 사례를 지원하지 않는 경우 관리 | 기타 | 기타 요청을 사용합니다.

수정으로 스택에 새 리소스가 생성되나요?

수정은 스택에 새 리소스를 생성하지 않습니다. 그러나 수정은 새 출력을 생성하고 스택 템플릿 메타데이터 섹션을 업데이트하여 참조용으로 수정 요약을 저장합니다.

문제 해결은 항상 성공하나요?

수정을 수행하려면 템플릿 구성을 신중하게 분석하고 검증해야 합니다. 이러한 검증이 실패하는 시나리오에서는 수정 프로세스가 중지되고 스택 템플릿 또는 파라미터에 대한 변경 사항이 수행되지 않습니다. 또한 지원되는 리소스 유형에 대해서만 문제 해결을 수행할 수 있습니다.

문제 해결에 실패하면 스택 리소스에 대한 업데이트를 수행하려면 어떻게 해야 합니까?

관리 | 기타 | 기타 | CT 업데이트(ct-0xdawir96cy7k)를 사용하여 변경을 요청할 수 있습니다. AMS는 이러한 시나리오를 모니터링하고 문제 해결 솔루션을 개선하기 위해 노력합니다.

지원되는 리소스 유형과 지원되지 않는 리소스 유형이 모두 있는 스택을 수정할 수 있나요?

예. 그러나 수정은 지원되는 리소스 유형이 스택에서 DRIFTED로 발견된 경우에만 수행됩니다. 지원되지 않는 리소스 유형이 DRIFTED인 경우 수정이 계속되지 않습니다.

비CFN Ingest CTs를 통해 생성된 스택에 대한 문제 해결을 요청할 수 있나요?

예. 스택 생성에 사용되는 변경 유형에 관계없이 스택에서 수정을 수행할 수 있습니다.

수정 전에 스택에 대해 수행할 변경 사항을 알 수 있나요?

예. 두 변경 유형 모두 스택이 수정될 경우 수행할 변경을 요청하는 데 사용할 수 있는 DryRun 옵션을 제공합니다. 그러나 최종 수정 변경 사항은 수정 시 스택에 있는 드리프트에 따라 다를 수 있습니다.

RFCs 예약

예약 기능을 사용하면 RFCs. 예약 기능에서 사용할 수 있는 옵션은 다음과 같습니다.

- 이 변경 사항을 최대한 빨리 실행: AMS는 RFC가 승인되는 즉시 실행합니다. 대부분의 CTs 자동으로 승인됩니다. RFC가 특정 시간에 시작되지 않도록 하려면이 옵션을 사용합니다.
- 이 변경 예약: RFC를 실행할 날짜, 시간 및 시간대를 설정합니다. 자동 변경 유형의 경우 RFC를 제출하려는 후 최소 10분 후에 시작 시간을 요청하는 것이 가장 좋습니다. 관리형 자동화 변경 유형의 경우 RFC를 제출하려는 후 최소 24시간이 지난 시작 시간을 요청해야 합니다. 구성된 시작 시간까지 RFC가 승인되지 않으면 RFC가 거부됩니다.

RFC 일정 설정

RFC를 예약하려면 다음 방법 중 하나를 사용합니다.

이 변경 사항을 최대한 빨리 실행합니다.

- 콘솔: 아무 작업도 수행하지 않습니다. 기본 RFC 일정을 사용합니다.
- API 또는 CLI: RFC 생성 작업에서 `RequestedStartTime` 및 `RequestedEndTime` 옵션을 제거합니다.

ASAP "관리형 자동화" RFCs는 제출 후 30일 이내에 승인되지 않은 경우 자동 거부됩니다.

이 변경을 예약합니다.

- 콘솔: 이 변경 예약 라디오 버튼을 선택합니다. 시작 시간 영역이 열립니다. 수동으로 날짜를 입력하거나 일정 위젯을 사용하여 날짜를 선택합니다. ISO 8601 형식으로 표현된 시간을 UTC로 입력하고 드롭다운 목록을 사용하여 위치를 선택합니다. 기본적으로 AMS는 ISO 8601 형식

YYYYMMDDThhmmssZ 또는 YYYY-MM-DDThh:mm:ssZ를 사용하며, 두 형식 중 하나가 허용됩니다.

> **Note**
>
> 기본 종료 시간은 입력한 시작 시간으로부터 4시간입니다. 예약된 변경의 종료 시간을 4시간 이상으로 설정하려면 API 또는 CLI를 사용하여 변경 사항을 실행합니다.

- API 또는 CLI: RFC 생성 작업에서 `RequestedStartTime` 및 `RequestedEndTime` 파라미터 값을 제출합니다. 구성된를 전달해도 이미 시작된 자동 변경 유형에 대한 실행이 중지되지 `RequestedEndTime` 않습니다. "관리형 자동화" 변경 유형의 경우 AMS 운영 조사가 진행 중인 동안 `RequestedEndTime`에 도달하고 AMS와 통신하는 경우 확장을 요청하거나 RFC를 다시 제출하라는 메시지가 표시될 수 있습니다.

> **Tip**
>
> UTC 시간 읽기의 예는 Time-is 웹 사이트의 UTC를 참조하세요. 오후 2:20에 2016-12-05의 날짜/시간 값에 대한 ISO 8601 형식의 예: 2016-12-05T14:20:00Z 또는 20161205T142000Z.

제공하는 경우...

- 만`RequestedStartTime`, RFC는 예약된 것으로 간주되며 `RequestedEndTime`는 `ExecutionDurationInMinutes` 값을 사용하여 채워집니다.
- 만 `RequestedEndTime`해당됩니다. InvalidArgumentException이 발생합니다.
- `RequestedStartTime` 및 모두 `RequestedEndTime` 지정된 시작 시간 + `ExecutionDurationInMinutes` 값으로를 `RequestedEndTime`덮어씁니다.
- `RequestedStartTime` 또는 도 아닙니다. 이러한 값은 null로 `RequestedEndTime`유지되며 RFC는 ASAP RFC로 처리됩니다.

> **Note**
>
> 예약된 모든 RFCs 대해 지정되지 않은 종료 시간은 지정된의 시간과 제출된 변경 유형의 `ExpectedExecutionDurationInMinutes` 속성을 `RequestedStartTime` 더한 시간으로 작성됩니다. 예를 들어 `ExpectedExecutionDurationInMinutes`가 "60"(분)이고 지정된 `RequestedStartTime`가 `2016-12-05T14:20:00Z` (2016년 12월 5일 오전 4시 20분)

인 경우 실제 종료 시간은 2016년 12월 5일 오전 5시 20분으로 설정됩니다. 특정 변경 유형에 ExpectedExecutionDurationInMinutes 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile saml get-change-type-version --
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

RFC 우선 순위 옵션 사용

execution mode = manual 변경 유형에서 우선 순위 옵션을 사용하여 AMS 작업에 요청의 긴급성을 알립니다.

의 우선 순위 옵션execution mode = manual:

수동 RFC의 우선 순위를 높음, 중간 또는 낮음으로 지정합니다. 높음으로 분류된 RFCs는 RFCs 서비스 수준 목표(SLOs) 및 제출 시간에 따라 중간으로 분류된 RFC 이전에 검토 및 승인됩니다. 우선 순위가 낮거나 우선 순위가 지정되지 않은 RFCs는 제출된 순서대로 처리됩니다.

RFCs 승인 또는 거부

승인 필요(수동) CTs와 함께 제출된 RFCs는 사용자 또는 AMS의 승인을 받아야 합니다. 사전 승인된 CTs 자동으로 처리됩니다. 자세한 내용은 CT 승인 요구 사항 단원을 참조하십시오.

> **Note**
>
> 수동 CTs를 사용하는 경우 ASAP 예약 옵션(콘솔에서 ASAP 선택, API/CLI에서 시작 및 종료 시간 비워 두기)을 사용하는 것이 좋습니다. 이러한 CTs는 AMS 운영자가 RFC를 검사하고 승인 및 실행 전에 사용자와 통신해야 하기 때문입니다. 이러한 RFCs 예약하는 경우 최소 24시간을 허용해야 합니다. 예정된 시작 시간 전에 승인이 이루어지지 않으면 RFC가 자동으로 거부됩니다.

AMS에서 승인 필요 RFC를 성공적으로 제출한 경우 사용자의 명시적 승인을 받아야 합니다. 또는 승인 필요 RFC를 제출하는 경우 AMS의 승인을 받아야 합니다. AMS가 제출한 RFC를 승인해야 하는 경우 승인을 요청하는 이메일 또는 기타 미리 결정된 통신이 전송됩니다. 통신에는 RFC ID가 포함됩니다. 통신이 전송된 후 다음 중 하나를 수행합니다.

- 콘솔 승인 또는 거부: 관련 RFC에 대한 RFC 세부 정보 페이지를 사용합니다.

- API/CLI 승인: ApproveRfc는 변경 사항을 승인됨으로 표시합니다. 필요한 경우 소유자와 운영자 모두 조치를 취해야 합니다. 다음은 CLI 승인 명령의 예입니다. 다음 예제에서는 RFC_ID를 적절한 RFC ID로 바꿉니다.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API/CLI 거부: RejectRfc는 변경 사항을 거부로 표시합니다. 다음은 CLI 거부 명령의 예입니다. 다음 예제에서는 RFC_ID를 적절한 RFC ID로 바꿉니다.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

RFC 제한 실행 기간 요청

이전에는 블랙아웃 일수라고 했지만 특정 기간을 제한하도록 요청할 수 있습니다. 해당 시간 동안에는 변경 사항을 실행할 수 없습니다.

제한된 실행 기간을 설정하려면 UpdateRestrictedExecutionTimes API 작업을 사용하고 UTC로 특정 기간을 설정합니다. 지정한 기간은 지정된 이전 기간을 재정의합니다. 지정된 제한된 실행 시간 동안 RFC를 제출하면 잘못된 RFC 일정 오류와 함께 제출이 실패합니다. 최대 200개의 제한된 기간을 지정할 수 있습니다. 기본적으로 제한된 기간은 설정되지 않습니다. 다음은 요청 명령의 예입니다(SAML 인증이 구성된 경우).

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

RestrictedExecutionTimes 설정을 볼 수도 있습니다. ListRestrictedExecutionTimes 예시

```
aws amscm  --profile saml list-restricted-execution-times
```

지정된 제한된 실행 시간 동안 RFC를 제출하려면 RestrictedExecutionTimesOverrideId를 OverrideRestrictedTimeRanges 값으로 추가한 다음 평소와 같이 RFC를 제출합니다. 중요하거나 긴급한 RFC에만이 방법을 사용하는 것이 가장 좋습니다. 자세한 내용은 SubmitRfc에 대한 API 참조를 참조하세요.

RFCs 생성, 복제, 업데이트, 찾기 및 취소

다음 예제에서는 다양한 RFC 작업을 안내합니다.

주제

RFC 생성

콘솔을 사용하여 RFC 생성

다음은 AMS 콘솔에서 빠른 카드가 열리고 변경 유형 찾아보기가 활성화된 RFC 생성 프로세스의 첫 페이지입니다.

다음은 범주별 선택이 활성화된 AMS 콘솔에서 RFC 생성 프로세스의 첫 번째 페이지입니다.

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.
3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다(변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.

4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 RFC가 성공적으로 생성된 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 RFC 생성

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일을 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> `CreateRfc` 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 따옴표 이스케이프)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

템플릿 생성:

> **Note**
>
> RFC를 생성하는이 예제에서는 Load Balancer(ELB) 스택 변경 유형을 사용합니다.

1. 관련 CT를 찾습니다. 다음 명령은 항목 이름에 "ELB"가 포함된 CT 분류 요약을 검색하고 범주, 항목, 작업 및 ChangeTypeID의 출력을 테이블 형식으로 생성합니다(둘 다 하위 범주는 임Advanced stack components).

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
   [Category,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   ----------------------------------------------------------------------
   |                            CtSummaries                             |
   +-----------+---------------------------+---------------------------+
   | Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
   | Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
   +-----------+---------------------------+---------------------------+
   ```

2. 최신 버전의 CT를 찾습니다.

   ChangeTypeId 및 ChangeTypeVersion:이 연습의 변경 유형 ID는 ct-123h45t6uz7jl (ELB 생성)입니다. 최신 버전을 확인하려면 다음 명령을 실행합니다.

   ```
   aws amscm list-change-type-version-summaries --filter
    Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
   ```

3. 옵션 및 요구 사항을 알아봅니다. 다음 명령은 스키마를 CreateElbParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 실행 파라미터 JSON 파일을 수정하고 저장합니다. 이 예제에서는 파일 이름을 CreateElbParams.json.

   프로비저닝 CT의 경우 StackTemplateId는 스키마에 포함되며 실행 파라미터에 제출해야 합니다.

   TimeoutInMinutes의 경우 RFC가 실패하기 전에 스택을 생성하는 데 허용되는 분 수는이 설정으로 인해 RFC 실행이 지연되지 않지만 충분한 시간을 제공해야 합니다(예: "5"를 지정하지 않음). 오래 실행되는 UserData: EC2 생성 및 ASG 생성CTs의 경우 유효한 값은 "60"~"360"입니다. 다른 모든 프로비저닝 CTs에 허용되는 최대 "60"을 권장합니다.

   스택을 생성할 VPC의 ID를 제공합니다. CLI 명령를 사용하여 VPC ID를 가져올 수 있습니다`aws amsskms list-vpc-summaries`.

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. RFC JSON 템플릿을 CreateElbRfc.json:이라는 현재 폴더의 파일로 출력합니다.

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. CreateElbRfc.json 파일을 수정하고 저장합니다. 별도의 파일에서 실행 파라미터를 생성했으므로 `ExecutionParameters` 줄을 제거합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. RFC를 생성합니다. 다음 명령은 실행 파라미터 파일과 RFC 템플릿 파일을 지정합니다.

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

> **Note**
>
> AMS API/CLI를 사용하여 RFC JSON 파일 또는 CT 실행 파라미터 JSON 파일을 생성하지 않고도 RFC를 생성할 수 있습니다. 이렇게 하려면 `create-rfc` 명령을 사용하고 필요한 RFC 및 실행 파라미터를 명령에 추가합니다. 이를 "인라인 생성"이라고 합니다. 모든 프로비저닝 CTs 리소스에 대한 파라미터가 포함된 `Parameters` 배열이 `execution-parameters` 블록 내에 포함되어 있습니다. 파라미터에는 슬래시(\)로 이스케이프된 따옴표가 있어야 합니다. RFC를 생성하는 다른 문서화된 방법을 "템플릿 생성"이라고 합니다. 여기에서 RFC 파라미터에 대한 JSON 파일과 실행 파라미터에 대한 다른 JSON 파일을 생성하고 `create-rfc` 명령을 사용하여 두 파일을 제출합니다. 이러한 파일은 템플릿 역할을 할 수 있으며 향후 RFCs. 템플릿을 사용하여 RFCs를 생성할 때 명령을 사용하여 다음과 같이 명령을 실행하여 원하는 콘텐츠로 JSON 파일을 생성할 수 있습니다. 명령은 표시된 콘텐츠가 포함된 "parameters.json"이라는 파일을 생성합니다. 이러한 명령을 사용하여 RFC JSON 파일을 생성할 수도 있습니다.

AMS 콘솔RFCs 복제(다시 생성)

AMS 콘솔을 사용하여 기존 RFC를 복제할 수 있습니다.

AMS 콘솔을 사용하여 RFC를 복제하거나 다시 생성하려면 다음 단계를 따르세요.

1. 관련 RFC를 찾습니다. 왼쪽 탐색 창에서 RFCs 클릭합니다.

   RFCs 열립니다.

2. 복제하려는 RFC를 찾을 때까지 페이지를 스크롤합니다. 필터 옵션을 사용하여 목록의 범위를 좁힙니다. 복제할 RFC를 선택합니다.

   RFC 세부 정보 페이지가 열립니다.

3. 복사본 생성을 클릭합니다.

   변경 요청 생성 페이지가 열리고 모든 옵션이 원래 RFC에서 로 설정됩니다.

4. 원하는 대로 변경합니다. 추가 옵션을 설정하려면 기본 옵션을 고급으로 변경합니다. 모든 옵션을 설정한 후 제출을 선택합니다.

   활성 RFC 세부 정보 페이지가 복제된 RFC의 새 RFC ID와 함께 열리고 복제된 RFC가 RFC 대시보드에 나타납니다.

RFCs 업데이트

RFC를 업데이트한 다음 제출하거나 다시 제출하여 거부되었거나 아직 제출되지 않은 RFC를 다시 제출할 수 있습니다. 지정된 RFCsRequestedStartTime가 제출 전에 통과했거나 지정된 TimeoutInMinutes가 RFC를 실행하기에 충분하지 않기 때문에 대부분의 RFC가 거부됩니다 (TimeoutInMinutes는 성공적인 RFC를 연장하지 않으므로 Amazon EC2 또는 장기 실행 UserData가 있는 Amazon EC2 Auto Scaling 그룹의 경우 항상 "60"~"360"으로 설정하는 것이 좋습니다). 이 섹션에서는 CLI 버전의 `UpdateRfc` 명령을 사용하여 새 RFC 파라미터로 RFC를 업데이트하거나 문자열화된 JSON 또는 업데이트된 파라미터 파일을 사용하여 새 파라미터를 업데이트하는 방법을 설명합니다.

이 예제에서는 AMS UpdateRfc API의 CLI 버전 사용에 대해 설명합니다(RFC 업데이트 참조). 일부 리소스(DNS 프라이빗 및 퍼블릭, 로드 밸런서 스택 및 스택 패치 구성)를 업데이트하기 위한 변경 유형이 있지만 RFC를 업데이트할 CT는 없습니다.

한 번에 하나의 UpdateRfc 작업을 제출하는 것이 좋습니다. 예를 들어 DNS 스택에서 여러 업데이트를 제출하면 업데이트가 DNS 업데이트를 동시에 시도하지 못할 수 있습니다.

필수 데이터: `RfcId`: 업데이트 중인 RFC입니다.

선택적 데이터: `ExecutionParameters`:와 같이 필요하지 않은 필드를 업데이트하지 않는 한 수정된 실행 파라미터를 `Description`제출하여 RFC가 거부되거나 취소되는 문제를 해결합니다. 제출된 모든 null이 아닌 값은 원래 RFC에서 해당 값을 덮어씁니다.

1. 거부되거나 취소된 관련 RFC를 찾으려면이 명령을 사용할 수 있습니다(값을 로 대체할 수 있음Canceled).

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. 다음 RFC 파라미터 중 하나를 수정할 수 있습니다.

```
{
    "Description": "string",
    "ExecutionParameters": "string",
    "ExpectedOutcome": "string",
    "ImplementationPlan": "string",
    "RequestedEndTime": "string",
    "RequestedStartTime": "string",
    "RfcId": "string",
    "RollbackPlan": "string",
    "Title": "string",
    "WorstCaseScenario": "string"}
```

설명 필드를 업데이트하는 명령의 예:

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
 --region us-east-1
```

ExecutionParameters VpcId 필드를 업데이트하는 명령의 예:

```
aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
 "RFC_ID" --region us-east-1
```

업데이트가 포함된 실행 파라미터 파일로 RFC를 업데이트하는 예제 명령. EC2 스택 | 생성의 2단계에서 예제 실행 파라미터 파일을 참조하세요.

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. 를 사용하여 RFC를 다시 제출submit-rfc하고 RFC를 처음 생성할 때와 동일한 RFC ID를 사용합니다.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC가 성공하면 명령줄에 확인 메시지나 오류 메시지가 표시되지 않습니다.

4. 요청 상태를 모니터링하고 실행 출력을 보려면 다음 명령을 실행합니다.

```
aws amscm get-rfc --rfc-id RFC_ID
```

RFCs 찾기

콘솔을 사용하여 변경 요청(RFC) 찾기

AMS 콘솔을 사용하여 RFC를 찾으려면 다음 단계를 따릅니다.

> **Note**
> 이 절차는 예약된 RFCs, 즉 ASAP 옵션을 사용하지 않은 RFCs에만 적용됩니다.

1. 왼쪽 탐색 창에서 RFCs 클릭합니다.

   RFCs 열립니다.
2. 목록을 스크롤하거나 필터 옵션을 사용하여 목록을 구체화합니다.

   RFC 목록은 필터 기준에 따라 변경됩니다.
3. 원하는 RFC의 제목 링크를 선택합니다.

   RFC ID를 포함한 정보가 포함된 해당 RFC에 대한 RFC 세부 정보 페이지가 열립니다.
4. 대시보드에 RFCs가 많은 경우 필터 옵션을 사용하여 RFC로 검색할 수 있습니다.

   - 제목: 생성 시 RFC에 제공된 제목 줄 또는 제목(API/CLI)입니다.
   - RFC ID: RFC의 식별자입니다.
   - 활동 상태: RFC 상태를 알고 있는 경우 운영자가 현재 RFC를 보고 있다는 의미의 AwsOperatorAssigned, RFC 실행을 진행하기 전에 AMS 운영자가 무언가를 수행해야 한다는 의미의 AwsActionPending 또는 RFC 실행을 진행하기 전에 조치를 취해야 한다는 의미의 CustomerActionPending 중에서 선택할 수 있습니다.
   - 상태: RFC 상태를 알고 있는 경우 다음 중에서 선택할 수 있습니다.
     - 예약됨: 예약된 RFCs.
     - 취소됨: 취소된 RFCs.

  - 진행 중: RFCs 진행 중입니다.
  - 성공: 성공적으로 실행된 RFCs.
  - 거부됨: 거부된 RFCs.
  - 편집: 편집 중인 RFCs.
  - Failure: 실패한 RFCs.
  - 승인 보류 중: AMS 또는 사용자가 승인할 때까지 진행할 수 없는 RFCs. 일반적으로 이는 RFC를 승인해야 함을 나타냅니다. 서비스 요청 목록에서 이에 대한 서비스 알림을 받게 됩니다.
- 변경 유형: 범주, 하위 범주, 항목 및 작업을 선택하면 변경 유형 ID가 검색됩니다.
- 요청된 시작 시간 또는 요청된 종료 시간:이 필터 옵션을 사용하면 이전 또는 이후를 선택한 다음 날짜 및 선택적으로 시간(hh:mm 및 시간대)을 입력할 수 있습니다. 이 필터는 예약된 RFCs(ASAP RFCs 아님)에서만 성공적으로 작동합니다.
- 상태: 예약됨, 취소됨, 진행 중, 성공, 거부됨, 편집 중 또는 실패.
- 제목: RFC에 제공한 제목(또는 RFC가 API/CLI로 생성된 경우 제목)입니다.
- 변경 유형 ID: RFC와 함께 제출된 변경 유형의 식별자를 사용합니다.

  다음 스크린샷과 같이 검색을 통해 필터를 추가할 수 있습니다.

5. 원하는 RFC의 제목 링크를 클릭합니다.

   RFC ID를 포함한 정보가 포함된 해당 RFC에 대한 RFC 세부 정보 페이지가 열립니다.

CLI를 사용하여 변경 요청(RFC) 찾기

여러 필터를 사용하여 RFC를 찾을 수 있습니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 RFC에서 `CreateRfc` 파라미터를 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 `--`

notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}" RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

RFC ID를 기록하지 않고 나중에 찾아야 하는 경우 AMS 변경 관리(CM) 시스템을 사용하여 이를 검색하고 필터 또는 쿼리로 결과의 범위를 좁힐 수 있습니다.

1. CM API ListRfcSummaries 작업에는 필터가 있습니다. 논리적 AND 작업에서 `Attribute` 및 를 `Value` 결합하거나 , `Condition`및 `Attribute`를 기반으로 결과를 필터링할 수 있습니다`Values`.

   RFC 필터링

속성	유효값	유효한 조건	기본 조건	참고
ActualEndTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값보다 먼저 발생하는 날짜를 나타내야 합니다.
ActualStartTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값보다 먼저 발생하는 날짜를 나타내야 합니다.

속성	유효값	유효한 조건	기본 조건	참고
AutomationStatusId	수동, 자동	같음	같음	자동화 상태는 두 개뿐입니다.
ChangeTypeId	유효한 변경 유형 ID. 예: ct-123h45t6uz7jl	같음	같음	변경 유형 또는 CSIO 찾기
ChangeTypeVersion	유효한 변경 유형 ID. 예: 1.0	같음	같음	변경 유형 또는 CSIO 찾기
CreatedBy	모든 문자열(최대 허용 길이는 2048자)	포함	포함	RFC의 CreatedBy 필드에는 RFC를 생성한 사용자의 ARN이 포함됩니다.
CreatedTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값보다 먼저 발생하는 날짜를 나타내야 합니다.
LastModifiedTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값보다 먼저 발생하는 날짜를 나타내야 합니다.

속성	유효값	유효한 조건	기본 조건	참고
LastSubmittedTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값보다 먼저 발생하는 날짜를 나타내야 합니다.
RequestedEndTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값보다 먼저 발생하는 날짜를 나타내야 합니다.
RequestedStartTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값보다 먼저 발생하는 날짜를 나타내야 합니다.

속성	유효값	유효한 조건	기본 조건	참고
RfcStatusId	취소됨, 편집 중, 실패, InProgress, PendingApproval 중, 거부됨, 예약됨, 성공	같음	같음	AMS 콘솔에서 RFC 목록을 새로 고치거나 GetRfc를 실행합니다.
제목	유효한 RFC 제목	포함	포함	각 개별 필드의 정규식은 지원되지 않습니다. 대/소문자를 구분하지 않는 검색

예시:

SQS와 관련된 모든 RFCs의 IDs를 찾으려면(SQS가 CT의 항목 부분에 포함된 경우) 다음 명령을 사용할 수 있습니다.

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

다음과 같이 반환됩니다.

```
-------------------------------------------------------------------------------
|                          ListRfcSummaries                                   |
+----------+---------------------------------+-------+-------+---------------+
|Deployment| Advanced Stack Components       |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+---------------+
```

에 사용할 수 있는 또 다른 필터`list-rfc-summaries`는 자동 또는 수동 RFCs`AutomationStatusId`를 찾는 입니다.

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

에 사용할 수 있는 또 다른 필터`list-rfc-summaries`는 `Title` (콘솔의 제목)입니다.

```
Attribute=Title,Value=RFC-TITLE
```

RFCs:

- (제목에는 "Windows 2012" 또는 "Amazon Linux"라는 문구가 포함되어 있음) 및
- (RfcStatusId EQUALS "Success" 또는 "InProgress") AND
- (20170101T000000Z <= RequestedStartTime <= 20170103T000000Z) AND (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> 고급를 통해 `Filters`AMS는 향후 릴리스에서 다음 필드를 더 이상 사용하지 않으려고 합니다.

- 값: 값 필드는 필터 필드의 일부입니다. 고급 기능을 지원하는 값 필드를 사용합니다.
- RequestedEndTimeRange: 고급 기능을 지원하는 필터 필드 내에서 RequestedEndTime 사용
- RequestedStartTimeRange: 고급 기능을 지원하는 필터 필드 내에서 RequestedStartTime을 사용합니다.

CLI 쿼리 사용에 대한 자세한 내용은 --query 옵션을 사용하여 출력을 필터링하는 방법 및 쿼리 언어 참조인 JMESPath 사양을 참조하세요.

2. AMS 콘솔을 사용하는 경우:

   RFCs 페이지로 이동합니다. 필요한 경우 RFC 주체를 기준으로 필터링할 수 있습니다. RFC 주체는 RFC를 생성할 `Title` 때 RFC로 입력한 것입니다.

팁

> **Note**
> 이 절차는 예약된 RFCs, 즉 ASAP 옵션을 사용하지 않은 RFCs에만 적용됩니다.

RFCs 취소

콘솔 또는 AMS API/CLI를 사용하여 RFC를 취소할 수 있습니다.

콘솔을 사용하여 RFC를 취소하려면 RFC 목록에서 RFC를 찾아 열고 취소를 클릭합니다.

필수 데이터:

- `Reason`: RFC를 취소하는 이유.
- `RfcId`: 취소하려는 RFC입니다.

1. 일반적으로 RFC를 제출한 직후 취소합니다(RFC ID가 유용해야 함). 그렇지 않으면 예약한 후 지정된 시작 시간 이전이 아니면 취소할 수 없습니다. RFC ID를 찾아야 하는 경우이 명령을 사용할 수 있습니다(수동으로 승인된 RFC를 `PendingApproval` `Value`로 대체할 수 있음).

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. RFC를 취소하는 명령의 예:

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
region us-east-1
```

RFCs와 함께 AMS 콘솔 사용

AMS 콘솔은 RFCs를 생성하고 제출하는 데 도움이 되는 기능을 제공합니다.

RFC 목록 페이지 사용(콘솔)

AMS 콘솔 RFCs 목록 페이지에는 다음 옵션이 제공됩니다.

- 필터를 통한 고급 RFC 검색. 자세한 내용은 RFCs 찾기 단원을 참조하세요.
- RFC가 마지막으로 수정된 시간을 찾습니다. 이 값은 RFC 상태가 마지막으로 변경된 시간을 나타냅니다.
- RFC 주체를 사용하여 RFC 세부 정보 보기. 이 링크를 선택하면 해당 RFC의 세부 정보 페이지가 열립니다.
- RFC 상태 보기. 자세한 정보는 RFC 상태 코드 이해 섹션을 참조하세요.

RFC 빠른 생성 사용(콘솔)

RFC 빠른 생성 카드 또는 목록 테이블을 사용하거나 분류별로 RFCs에 대한 변경 유형을 선택합니다.

자세한 내용은 RFC 생성를 참조하세요.

RFC 서신 및 첨부 파일 추가(콘솔)

예를 들어 "PendingApproval" 상태일 때 RFC가 제출된 후 승인되기 전에 RFC에 서신을 추가할 수 있습니다. RFC가 승인된 후('예약됨' 또는 'InProgress' 상태) 요청에 대한 변경으로 해석될 수 있으므로 서신을 추가할 수 없습니다. RFC가 완료되면("Canceled", "Rejected", "Success" 또는 "Failure" 상태) 대응이 다시 활성화됩니다. 단, RFC가 30일 이상 닫히면 대응이 비활성화됩니다.

> **Note**
>
> 각 서신은 5,000자로 제한됩니다.

첨부 파일에 대한 제한 사항:

- 서신당 첨부 파일은 3개뿐입니다.
- RFC당 50개의 첨부 파일을 제한합니다.
- 각 연결의 크기는 5MB 미만이어야 합니다.
- 일반 텍스트(`.txt`), 쉼표로 구분된 값(`.csv`), JSON(`.json`) 또는 YAML()과 같은 텍스트 파일만 허용됩니다`.yaml`. YAML 형식의 경우 파일 확장명를 사용하여 파일을 첨부해야 합니다`.yaml`.

  > **Note**
  >
  > XML 콘텐츠가 있는 텍스트 파일은 금지됩니다. AMS와 공유할 XML 콘텐츠가 있는 경우 서비스 요청을 사용합니다.

- 파일 이름은 숫자, 문자, 공백, 대시(-), 밑줄(_), 점(.)만 포함하여 255자로 제한됩니다.
- RFC에서 첨부 파일을 업데이트하고 삭제하는 것은 현재 지원되지 않습니다.

RFC에 서신과 첨부 파일을 추가하려면 다음 단계를 따르세요.

1. AMS 콘솔의 RFC 세부 정보 페이지에서 페이지 하단의 서신 섹션을 찾습니다.

   서신을 보내기 전에:

   일부 서신을 보낸 후:

2. 새 서신을 추가하려면 회신 텍스트 상자에 메시지를 입력합니다. 서신과 관련된 파일을 첨부하려면 첨부 파일 추가를 선택한 다음 원하는 파일을 선택합니다.

3. 완료되면 제출을 선택합니다.

   새 서신은 첨부된 파일에 대한 링크와 함께 RFC 세부 정보 페이지의 서신 목록에 표시됩니다.

RFC 이메일 알림 구성(콘솔)

AMS 콘솔 변경 요청 생성 페이지에서는 이메일 주소를 추가하여 RFC 상태 변경 알림을 받을 수 있는 옵션을 제공합니다.

또한 다음과 같은 모든 변경 유형에 알림용 이메일 주소를 추가할 수 있습니다.

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

파라미터 부분이 아닌 요청의 RFC 파라미터 부분에 있는 모든 변경 유형 인라인 또는 템플릿 요청에 유사한 줄(`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`)을 추가합니다.

일반적인 RFC 파라미터에 대해 알아보기

다음은 제출해야 하는 RFC 파라미터와 RFCs

- 변경 유형 정보: ChangeTypeId 및 ChangeTypeVersion. 변경 유형 IDs. https://docs.aws.amazon.com/managedservices/latest/ctref/index.html

  `query` 인수를 사용하여 CLI`list-change-type-classification-summaries`에서를 실행하여 결과의 범위를 좁힙니다. 예를 들어, 결과를 좁혀 `Item` 이름에 "Access"가 포함된 유형을 변경합니다.

  ```
  aws amscm list-change-type-classification-summaries --query
   "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
  ```

  를 실행`get-change-type-version`하고 변경 유형 ID를 지정합니다. 다음 명령은 ct-2tylseo8rxfsc의 CT 버전을 가져옵니다.

  ```
  aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
  ```

- 제목: RFC의 이름입니다.이 이름은 AMS 콘솔 RFC 목록에서 RFC의 주체가 되며 `GetRfc` 명령과 필터를 사용하여 검색할 수 있습니다. `Title`

- 예약: 예약된 RFC를 원하는 경우 `RequestedStartTime` 및 `RequestedEndTime` 파라미터를 포함하거나 이 변경 예약 콘솔 옵션을 사용해야 합니다. ASAP RFC(승인되는 즉시 실행됨)의 경우 CLI를 사용할 때 `RequestedStartTime` 및 `RequestedEndTime` null을 그대로 둡니다. 콘솔을 사용하는 경우 ASAP 옵션을 수락합니다.

  `RequestedStartTime`이 누락된 경우 RFC가 거부됩니다.
- 프로비저닝 CTs: 실행 파라미터 또는 `Parameters`는 리소스를 프로비저닝하는 데 필요한 특정 설정입니다. CT에 따라 크게 달라집니다.
- 비프로비저닝 CTs: CTs 또는 기타 | 기타 또는 스택 삭제와 같이 리소스를 프로비저닝하지 않는 CTs에는 최소한의 실행 파라미터가 있으며 `Parameters` 블록이 없습니다.
- 또한 일부 RFCs에서는를 지정`TimeoutInMinutes`하거나 RFC가 실패하기 전에 스택을 생성하는 데 허용되는 분 수를 지정해야 합니다. 유효한 값은 장기 실행 UserData의 경우 60(분)~360입니다. 이 `TimeoutInMinutes` 초과되기 전에 실행을 완료할 수 없는 경우 RFC가 실패합니다. 그러나이 설정은 RFC 실행을 지연시키지 않습니다.
- S3 버킷 또는 ELB와 같이 인스턴스를 생성하는 RFCs는 일반적으로 최대 7개의 태그(키/값 페어)를 추가할 수 있는 스키마를 제공합니다. 배포 | 고급 스택 구성 요소 | 태그 | 변경 유형 생성(ct-3cx7we852p3af)을 사용하여 RFC를 제출하여 S3 버킷에 태그를 더 추가할 수 있습니다. EC2, EFS, RDS 및 다중 계층(HA 2계층 및 HA 1계층) 스키마는 최대 50개의 태그를 허용합니다. 태그는 스키마의 `ExecutionParameters` 부분에 지정됩니다. 태그를 제공하는 것은 큰 가치가 있을 수 있습니다. 자세한 내용은 Amazon EC2 리소스에 태그 지정 단원을 참조하십시오.

  AMS 콘솔을 사용하는 경우 태그를 추가하려면 추가 구성 영역을 열어야 합니다.

> **Tip**
>
> 많은 CT 스키마에는 스키마 상단에 `Description` 및 `Name` 필드가 있습니다. 이러한 필드는 스택 또는 스택 구성 요소의 이름을 지정하는 데 사용되며 생성 중인 리소스의 이름은 지정되지 않습니다. 일부 스키마는 생성 중인 리소스의 이름을 지정하는 파라미터를 제공하고 일부는 그렇지 않습니다. 예를 들어 EC2 스택 생성을 위한 CT 스키마는 EC2 인스턴스 이름을 지정하는 파라미터를 제공하지 않습니다. 이렇게 하려면 "Name" 키와 이름을 지정할 값을 사용하여 태그를 생성해야 합니다. 이러한 태그를 생성하지 않으면 EC2 인스턴스가 이름 속성 없이 EC2 콘솔에 표시됩니다.

RFC AWS 리전 옵션 사용

AMS API 및 CLI(amscm 및 amsskms) 엔드포인트는에 있습니다us-east-1. SAML(Security Assertion Markup Language)과 연동하면 온보딩 시 AWS 리전을 us-east-1로 설정하는 스크립트가 제공됩니다. SAML을 사용하는 경우 명령을 실행할 때 --region 옵션을 지정할 필요가 없습니다. SAML이 us-east-1을 사용하도록 구성되어 있지만 계정이 해당 AWS 리전에 없는 경우 다른 AWS 명령(예:)을 실행할 때 계정 온보딩 리전을 지정해야 합니다aws s3.

> **Note**
>
> 이 가이드에 제공된 대부분의 명령 예제에는 --region 옵션이 포함되어 있지 않습니다.

RFC 일일 이메일에 가입

RFC 다이제스트 기능을 사용하여 지난 24시간 동안 계정의 RFC 활동을 요약하는 일일 이메일에 가입할 수 있습니다. RFC 다이제스트 기능은 계정의 RFCs. RFC 다이제스트는 응답을 보류 중인 작업을 놓칠 가능성을 줄일 수 있습니다.

RFC 다이제스트 기능을 켜려면 AMS Cloud Service Delivery Manager(CSDM)에 문의하십시오. CSDM에서 구독합니다. RFC 다이제스트 이메일 목록에 포함할 이메일 주소(또는 별칭)를 최대 20개까지 요청할 수 있습니다. 현재 이메일 일정은 09:00 UTC-8에 고정됩니다.

RFC 다이제스트 기능을 끄려면 요청과 함께 CSDM에 문의하세요.

RFC 다이제스트를 설정하지 않고 RFCs에 대한 알림을 원하는 경우 또는 RFCs 다이제스트가 제공하는 것보다 RFC에 대한 자세한 정보를 원하는 경우 변경 관리 시스템을 사용하여 정보를 원하는 모든 개별 RFC에 대해 CloudWatch Events 알림 또는 이메일 알림을 설정합니다. RFC 알림 설정에 대한 자세한 내용은 RFC 상태 변경 알림을 참조하세요.

RFC 다이제스트에 포함된 주제는 다음과 같습니다.

- 고객 승인 대기 중: 승인 대기 중인 PendingApproval 중 상태인 RFCs를 나열합니다.
- 고객 응답 대기 중: RFCs 서신에 대한 응답을 기다리고 있는 RFC를 나열합니다.
- AWS 승인 또는 회신 보류 중: AMS에서 회신 또는 승인을 기다리고 있는 RFCs를 나열합니다.
- 완료됨: 성공, 실패, 취소됨 및 거부됨 상태의 RFCs를 나열합니다.

다음은 RFC 다이제스트의 예입니다.

변경 유형이란 무엇입니까?

변경 유형은 AWS Managed Services(AMS)의 변경 요청(RFC)이 수행하고 변경 작업 자체와 수동 및 자동의 변경 유형을 포함하는 작업을 나타냅니다. AMS에는 다른 Amazon 웹 서비스에서 사용하지 않는 대규모 변경 유형 모음이 있습니다. 리소스 배포, 관리 또는 액세스 권한을 얻기 위해 변경 요청(RFC)을 제출할 때 이러한 변경 유형을 사용합니다.

주제

자동 및 수동 CTs

변경 유형에 대한 제약 조건은 자동 또는 수동인지 여부입니다. 이는 AMS 콘솔에서 실행 모드라고 하는 변경 유형 `AutomationStatusId` 속성입니다.

자동 변경 유형은 예상 결과와 실행 시간이 있으며 일반적으로 1시간 이내에 AMS 자동 시스템을 통해 실행됩니다(대부분 CT가 프로비저닝하는 리소스에 따라 다름). 수동 변경 유형은 흔하지 않지만 AMS 연산자가 실행되기 전에 RFC에서 작업해야 하므로 다르게 처리됩니다. 이는 RFC 제출자와 통신하는 것을 의미하기도 하므로 수동 변경 유형을 완료하려면 다양한 시간이 필요합니다.

예약된 모든 RFCs 대해 지정되지 않은 종료 시간은 지정된의 시간과 제출된 변경 유형의 `ExpectedExecutionDurationInMinutes` 속성을 `RequestedStartTime` 더한 시간으로 작성됩니다. 예를 들어 `ExpectedExecutionDurationInMinutes`가 "60"(분)이고 지정된 `RequestedStartTime`가 `2016-12-05T14:20:00Z` (2016년 12월 5일 오전 4시 20분)인 경우 실제 종료 시간은 2016년 12월 5일 오전 5시 20분으로 설정됩니다. 특정 변경 유형에 `ExpectedExecutionDurationInMinutes` 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> 실행 모드가 수동인 예약된 RFCs 콘솔에서 최소 24시간 후에 실행되도록 설정해야 합니다.

> **Note**
>
> 수동 CTs를 사용하는 경우 ASAP 예약 옵션(콘솔에서 ASAP 선택, API/CLI에서 시작 및 종료 시간 비워 두기)을 사용하는 것이 좋습니다. 이러한 CTs는 AMS 운영자가 RFC를 검사하고 승인 및 실행 전에 사용자와 통신해야 하기 때문입니다. 이러한 RFCs 예약하는 경우 최소 24시간을 허용해야 합니다. 예정된 시작 시간 전에 승인이 이루어지지 않으면 RFC가 자동으로 거부됩니다.

AMS는 4시간 이내에 수동 CT에 응답하는 것을 목표로 하며 가능한 한 빨리 대응하지만 RFC를 실제로 실행하는 데 훨씬 더 오래 걸릴 수 있습니다.

수동이고 AMS 검토가 필요한 CTs 목록은 콘솔의 개발자 리소스 페이지에서 사용할 수 있는 변경 유형 CSV 파일을 참조하세요.

YouTube 동영상: AMS RFCs 하나요?

AMS 콘솔에서 CT의 실행 모드를 찾으려면 변경 유형 찾아보기 검색 옵션을 사용해야 합니다. 결과는 일치하는 변경 유형 또는 변경 유형의 실행 모드를 보여줍니다.

AMS CLI를 사용하여 특정 변경 유형에 `AutomationStatus` 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

모든 AMS 변경 유형에 대한 정보를 제공하는 AMS 변경 유형 참조에서 변경 유형을 조회할 수도 있습니다.

> **Note**
>
> AMS API/CLI는 현재 AWS API/CLI의 일부가 아닙니다. AMS API/CLI에 액세스하려면 AMS 콘솔을 통해 AMS SDK를 다운로드합니다.

CT 승인 요구 사항

AMS CTs에는 항상 AwsApprovalId와 CustomerApprovalId라는 두 가지 승인 조건이 있습니다.이 조건은 RFC에서 실행을 승인하기 위해 AMS 또는 사용자 또는 다른 사람이 필요한지 여부를 나타냅니다.

승인 조건은 실행 모드와 다소 관련이 있습니다. 자세한 내용은 섹션을 참조하세요자동 및 수동 CTs.

CT의 승인 조건을 확인하려면 AMS 변경 유형 참조에서 확인하거나 GetChangeTypeVersion을 실행합니다. 둘 다 CT `AutomationStatusId` 또는 실행 모드도 제공합니다.

AMS 콘솔을 사용하거나 다음 명령을 사용하여 RFCs를 승인할 수 있습니다.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 승인 조건

CT 승인 조건이 인 경우	의 승인이 필요합니다.	및
`AwsApprovalId: Required`	AMS 변경 유형 시스템	아무 조치도 필요하지 않습니다. 이 조건은 자동 CTs의 경우 일반적입니다.
`AwsApprovalId: NotRequiredIfSubmitter`	제출된 RFC가 제출된 계정에 대한 경우 AMS 변경 유형 시스템이며 다른 사람은 없습니다.	아무 조치도 필요하지 않습니다. 이 조건은 AMS 운영자가 항상 검토하므로 수동 CTs의 경우 일반적입니다.
`CustomerApprovalId: NotRequired`	AMS 변경 유형 시스템	RFC가 구문 및 파라미터 검사를 통과하면 자동으로 승인됩니다.

CT 승인 조건이 인 경우	의 승인이 필요합니다.	및
`CustomerApprovalId: Required`	AMS 변경 유형 시스템 및 사용자,	알림이 전송되므로 알림에 응답하거나 ApproveRfc 작업을 실행하여 RFC를 명시적으로 승인해야 합니다.
`CustomerApprovalId: NotRequiredIfSubmitter`	RFC를 제출한 경우 AMS 변경 유형 시스템이며 다른 사람은 없습니다.	RFC가 구문 및 파라미터 검사를 통과하면 자동으로 승인됩니다.
긴급 보안 인시던트 또는 패치	AMS	자동 승인되고 구현됩니다.

유형 버전 변경

변경 유형은 버전이 지정되고 변경 유형에 대한 주요 업데이트가 수행되면 버전이 변경됩니다.

AMS 콘솔을 사용하여 변경 유형을 선택한 후 추가 구성 영역을 열고 변경 유형 버전을 선택할 수 있습니다. API/CLI 명령줄에서 변경 유형 버전을 지정할 수도 있습니다. 다음과 같은 다양한 이유로이 작업을 수행할 수 있습니다.

- 원하는 업데이트 변경 유형의 버전은 현재 업데이트하려는 리소스를 생성하는 데 사용한 변경 생성 유형의 버전과 일치해야 합니다. 예를 들어 ELB 변경 유형 버전 1 생성을 사용하여 생성한 Elastic Load Balancer(ELB) 인스턴스가 있을 수 있습니다. 업데이트하려면 ELB 업데이트 버전 1을 선택합니다.
- 최신 변경 유형과 다른 옵션이 있는 변경 유형 버전을 사용하려고 합니다. AMS 업데이트는 주로 보안상의 이유로 유형을 변경하므로 권장하지 않으며 항상 최신 버전을 선택하는 것이 좋습니다.

변경 유형 생성

변경 유형 생성은 version-to-version 변경 유형 업데이트와 일치합니다. 즉, 리소스를 프로비저닝하는 데 사용하는 변경 유형 버전은 나중에 해당 리소스를 수정하는 데 사용할 업데이트 변경 유형 버전과 일치해야 합니다. 예를 들어 S3 버킷 변경 유형 생성 버전 2.0으로 S3 버킷을 생성하고 나중에 RFC를 제출하여 해당 S3 버킷을 수정하려는 경우 버전 S3.0으로 S3 버킷 업데이트 변경 유형이 있더라도 S3 버킷 업데이트 변경 유형 버전 2.0도 사용해야 합니다.

나중에 변경 유형 업데이트를 사용하여 수정하려는 경우 변경 유형 생성으로 리소스를 프로비저닝할 때 사용하는 변경 유형 ID 및 버전에 대한 레코드를 보관하는 것이 좋습니다.

변경 유형 업데이트

AMS는 변경 유형 생성을 사용하여 생성된 리소스를 업데이트하는 업데이트 변경 유형을 제공합니다. 업데이트 변경 유형은 원래 리소스를 프로비저닝하는 데 사용된 변경 생성 유형과 version-to-version이 일치해야 합니다.

리소스를 쉽게 업데이트할 수 있도록 리소스를 프로비저닝할 때 사용하는 변경 유형 ID 및 버전을 기록해 두는 것이 좋습니다.

YouTube 동영상: 업데이트 CTs 사용하여 AWS Managed Services(AMS) 계정의 리소스를 변경하려면 어떻게 해야 하나요?

내부 전용 변경 유형

내부 전용 변경 유형을 볼 수 있습니다. 따라서 AMS가 수행할 수 있거나 수행할 수 있는 작업을 알 수 있습니다. 사용하려는 내부 전용 변경 유형이 있는 경우 서비스 요청을 제출합니다.

예를 들어 관리 | 모니터링 및 알림 | CloudWatch 경보 억제 | 내부 전용 CT 업데이트가 있습니다. AMS는 이를 사용하여 인프라 업데이트(패칭 등)를 배포하고 업데이트가 잘못 트리거될 수 있는 경보 알림을 끕니다. 이 CT가 제출되면 RFC 목록에 CT의 RFC가 표시됩니다. RFC에 배포된 모든 내부 전용 CT는 RFC 목록에 표시됩니다.

변경 유형 스키마

모든 변경 유형은 리소스의 생성, 수정 또는 액세스 시 입력에 대한 JSON 스키마를 제공합니다. 스키마는 변경 요청(RFC)을 생성할 수 있도록 파라미터와 설명을 제공합니다.

RFC를 성공적으로 실행하면 실행 출력이 생성됩니다. RFCs 프로비저닝의 경우 실행 출력에는 CloudFormation의 스택을 나타내며 CloudFormation 콘솔에서 검색할 수 있는 "stack_id"가 포함됩니다. 실행 출력에는 생성된 인스턴스의 ID 출력이 포함되고 해당 ID를 사용하여 해당 AWS 콘솔에서 인스턴스를 검색할 수 있습니다. 예를 들어 ELB CT 실행 생성 출력에는 CloudFormation에서 검색할 수 있는 "stack_id"가 포함되며 Amazon EC2 콘솔에서 Elastic Load Balancing에 대해 검색할 수 있는 키=ELB 값=<stack-xxxx>가 출력됩니다.

CT 스키마를 살펴보겠습니다. 이것은 상당히 작은 스키마인 CodeDeploy Application Create의 스키마입니다. 일부 스키마에는 매우 큰 `Parameter` 영역이 있습니다.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
```

스키마의 첫 번째 부분은 요청된 변경 유형에 대한 정보를 AMS에 제공합니다.

TimeoutInMinutes 파라미터를 사용하면 변경 유형을 실행하기 위

```
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
to
      allow for execution of the change. This will not prolong
execution,
      but the RFC fails if the change is not completed in the
specified time.
      Valid values are 60 up to 360, for long-running
UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
          "description": "The name of an AWS CodeDeploy
application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
```

한 경계 시간을 표시할 수 있습니다. 장기 실행 UserData의 경우 유효한 값은 60~360입니다.

파라미터 섹션에서는 생성 중인 리소스 또는 요청 중인 작업에 대한 설정을 지정합니다.

"추가 속성" 섹션에서는 필요한 파라미터와 선택 사항인 파라미터를 알 수 있습니다.

```
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

> **Note**
>
> 이 스키마는 최대 7개의 태그를 허용하지만 EC2, EFS, RDS 및 다중 계층 생성 스키마는 최대 50개의 태그를 허용합니다.

변경 유형에 대한 권한 관리

사용자 지정 정책을 사용하여 다른 그룹 또는 사용자가 사용할 수 있는 변경 유형(CTs)을 제한할 수 있습니다.

이에 대한 자세한 내용은 AMS 사용 설명서의 권한 설정을 참조하세요.

변경 유형에서 민감한 정보 수정

AMS 변경 유형 스키마`"metadata":"ams:sensitive":"true"`는 암호와 같은 민감한 정보를 포함하는 파라미터에 사용되는 파라미터 속성을 제공합니다. 이 속성을 설정하면 제공된 입력이 가려집니다. 이 파라미터 속성은 설정할 수 없지만 AMS를 사용하여 변경 유형을 생성하고 입력 시 가려야 하는 파라미터가 있는 경우 이를 요청할 수 있습니다.

쿼리 옵션을 사용하여 변경 유형 찾기

이 예제에서는 AMS 콘솔을 사용하여 제출하려는 RFC에 적합한 변경 유형을 찾는 방법을 보여줍니다.

콘솔 또는 API/CLI를 사용하여 변경 유형 ID(CT) 또는 버전을 찾을 수 있습니다. 검색 또는 분류 선택이라는 두 가지 방법이 있습니다. 두 선택 유형 모두 가장 자주 사용, 가장 최근에 사용 또는 알파벳순을 선택하여 검색을 정렬할 수 있습니다.

YouTube 동영상: AWS Managed Services CLI를 사용하여 RFC를 생성하려면 어떻게 해야 하고 CT 스키마는 어디에서 찾을 수 있습니까?

AMS 콘솔의 RFCs

- 변경 유형별 찾아보기(기본값)를 선택한 상태에서 다음 중 하나를 수행합니다.
  - 빠른 생성 영역을 사용하여 AMS의 가장 인기 CTs 중에서 선택합니다. 레이블을 클릭하면 제목 옵션이 자동으로 채워진 RFC 실행 페이지가 열립니다. 필요에 따라 나머지 옵션을 완료하고 실행을 클릭하여 RFC를 제출합니다.
  - 또는 모든 변경 유형 영역까지 아래로 스크롤하여 옵션 상자에 CT 이름을 입력하기 시작합니다. 정확한 변경 유형 이름이나 전체 변경 유형 이름을 가질 필요는 없습니다. 관련 단어를 입력하여 변경 유형 ID, 분류 또는 실행 모드(자동 또는 수동)별로 CT를 검색할 수도 있습니다.

    기본 카드 보기를 선택하면 입력 시 일치하는 CT 카드가 나타나고 카드를 선택한 다음 RFC 생성을 클릭합니다. 테이블 보기를 선택한 상태에서 관련 CT를 선택하고 RFC 생성을 클릭합니다. 두 방법 모두 RFC 실행 페이지를 엽니다.
- 또는 변경 유형 선택을 탐색하려면 페이지 상단의 범주별 선택을 클릭하여 일련의 드롭다운 옵션 상자를 엽니다.
- 범주, 하위 범주, 항목 및 작업을 선택합니다. 해당 변경 유형에 대한 정보 상자가 페이지 하단에 패널이 나타납니다.
- 준비가 되면 Enter 키를 누르면 일치하는 변경 유형 목록이 나타납니다.
- 목록에서 변경 유형을 선택합니다. 해당 변경 유형에 대한 정보 상자가 페이지 하단에 나타납니다.
- 올바른 변경 유형을 지정한 후 RFC 생성을 선택합니다.

> **Note**
>
> 이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 `--profile` 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`. 와 같이 모든 AMS 명령이 us-east-1에서 부족하므로 `--region` 옵션을 추가해야 할 수도 있습니다`aws amscm ams-cli-command --region=us-east-1`.

> **Note**
>
> AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 `--region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml`경우를 추가해야 할 수도 있습니다.

AMS CM API(ListChangeTypeClassificationSummaries 참조) 또는 CLI를 사용하여 변경 유형을 검색하려면

필터 또는 쿼리를 사용하여 검색할 수 있습니다. ListChangeTypeClassificationSummaries 작업에는 `Category`, `SubcategoryItem`, 및에 대한 필터 옵션이 `Operation`있지만 값은 기존 값과 정확히 일치해야 합니다. CLI를 사용할 때 보다 유연한 결과를 얻으려면 `--query` 옵션을 사용할 수 있습니다.

AMS CM API/CLI를 사용한 유형 필터링 변경

속성	유효값	유효/기본 조건	참고
ChangeTypeId	ChangeTypeId를 나타내는 모든 문자열(예: ct-abc123xyz7890)	같음	변경 유형 IDs는 변경 유형 참조를 참조하세요. 변경 유형 IDs는 변경 유형 찾기 또는 CSIO를 참조하세요.
범주	모든 자유 형식 텍스트	포함	각 개별 필드의 정규식은 지원되지 않습니다. 대/소문자를 구분하지 않는 검색
Subcategory			
Item			
연산			

1. 다음은 변경 유형 분류를 나열하는 몇 가지 예입니다.

   다음 명령은 모든 변경 유형 범주를 나열합니다.

```
aws amscm list-change-type-categories
```

다음 명령은 지정된 범주에 속하는 하위 범주를 나열합니다.

```
aws amscm list-change-type-subcategories --category CATEGORY
```

다음 명령은 지정된 범주 및 하위 범주에 속하는 항목을 나열합니다.

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. 다음은 CLI 쿼리를 사용하여 변경 유형을 검색하는 몇 가지 예입니다.

   다음 명령은 항목 이름에 "S3"가 포함된 CT 분류 요약을 검색하고 범주, 하위 범주, 항목, 작업 및 변경 유형 ID의 출력을 테이블 형식으로 생성합니다.

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-------------------------------------------------------------+
|               ListChangeTypeClassificationSummaries         |
+----------+-------------------------+--+------+--------------+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+----------+-------------------------+--+------+--------------+
```

3. 그런 다음 변경 유형 ID를 사용하여 CT 스키마를 가져오고 파라미터를 검사할 수 있습니다. 다음 명령은 스키마를 CreateS3Params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

   CLI 쿼리 사용에 대한 자세한 내용은 --query 옵션을 사용하여 출력을 필터링하는 방법 및 쿼리 언어 참조인 JMESPath 사양을 참조하세요.

4. 변경 유형 ID가 있으면 변경 유형의 버전을 확인하여 최신 버전인지 확인하는 것이 좋습니다. 이 명령을 사용하여 지정된 변경 유형의 버전을 찾습니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

특정 변경 유형에 AutomationStatus 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

특정 변경 유형에 ExpectedExecutionDurationInMinutes 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

AMS의 RFC 오류 문제 해결

CloudFormation 설명서를 통해 많은 AMS 프로비저닝 RFC 실패를 조사할 수 있습니다. AWS CloudFormation 문제 해결: 오류 문제 해결을 참조하세요.

추가 문제 해결 제안은 다음 섹션에 나와 있습니다.

AMS의 “관리” RFC 오류

AMS "관리" 범주 변경 유형(CTs)을 사용하면 리소스에 대한 액세스를 요청하고 기존 리소스를 관리할 수 있습니다. 이 섹션에서는 몇 가지 일반적인 문제를 설명합니다.

RFC 액세스 오류

- RFC에 지정한 사용자 이름과 FQDN이 올바르고 도메인에 존재하는지 확인합니다. FQDN을 찾는 데 도움이 필요하면 FQDN 찾기를 참조하세요.
- 액세스를 위해 지정한 스택 ID가 EC2-related 스택인지 확인합니다. ELB 및 Amazon Simple Storage Service(S3)와 같은 스택은 액세스 RFCs의 대상이 아니며, 대신 읽기 전용 액세스 역할을 사용하여 이러한 스택 리소스에 액세스합니다. 스택 ID 찾기에 대한 도움말은 스택 IDs.
- 제공한 스택 ID가 올바르고 관련 계정에 속하는지 확인합니다.

다른 액세스 RFC 실패에 대한 도움말은 액세스 관리를 참조하세요.

YouTube 동영상: 거부 및 실패를 방지하기 위해 변경 요청(RFC)을 올바르게 제기하려면 어떻게 해야 하나요?

RFC(수동) CT 예약 오류

대부분의 변경 유형은 ExecutionMode=Automated이지만 일부는 ExecutionMode=Manual이며 RFC 실패를 방지하기 위해 변경 유형을 예약하는 방법에 영향을 미칩니다.

ExecutionMode=ManualRFCs는 AMS 콘솔을 사용하여 RFC를 생성하는 경우 향후 최소 24시간 동안 실행되도록 설정해야 합니다.

AMS는 8시간 이내에 수동 CT에 응답하는 것을 목표로 하며 가능한 한 빨리 대응하지만 RFC가 실제로 실행되는 데 훨씬 더 오래 걸릴 수 있습니다.

수동 업데이트 CTsRFCs 사용

업데이트하려는 스택 유형에 대한 업데이트 변경 유형이 있는 경우 AMS 작업은 스택 업데이트에 대한 관리 | 기타 | 기타 RFCs를 거부합니다.

RFC 스택 삭제 오류

RFC 스택 삭제 실패: 관리 | 표준 스택 | 스택 | CT 삭제를 사용하는 경우 AMS 스택 이름과 함께 스택에 대한 자세한 이벤트가 CloudFormation 콘솔에 표시됩니다. AMS 콘솔에 있는 이름과 비교하여 스택을 식별할 수 있습니다. CloudFormation 콘솔은 장애 원인에 대한 자세한 내용을 제공합니다.

스택을 삭제하기 전에 스택이 생성된 방법을 고려해야 합니다. AMS CT를 사용하여 스택을 생성하고 스택 리소스를 추가하거나 편집하지 않은 경우 문제 없이 스택을 삭제할 수 있습니다. 그러나 스택에 대해 스택 삭제 RFC를 제출하기 전에 스택에서 수동으로 추가된 리소스를 제거하는 것이 좋습니다. 예를 들어 전체 스택 CT(HA 2 티어)를 사용하여 스택을 생성하는 경우 보안 그룹 - SG1이 포함됩니다. 그런 다음 AMS를 사용하여 다른 보안 그룹인 SG2를 생성하고 전체 스택의 일부로 생성된 SG1의 새 SG2를 참조한 다음 스택 삭제 CT를 사용하여 스택을 삭제하면 SG2에서 참조하므로 SG1이 삭제되지 않습니다. SG1 SG2

> **Important**
>
> 스택을 삭제하면 원치 않고 예상치 못한 결과가 발생할 수 있습니다. AMS는 이러한 이유로 고객을 대신하여 스택 또는 스택 리소스를 삭제*하지 않는 것을 선호합니다. 참고로 AMS는 삭제할 적절한 자동 변경 유형을 사용하여 삭제할 수 없는 사용자 대신(제출된 관리 | 기타 | 기타 | 변경 유형 업데이트) 리소스만 삭제합니다. 추가 고려 사항:

- 리소스가 '삭제 방지'에 대해 활성화된 경우 AMS는 관리 | 기타 | 기타 | 변경 유형 업데이트를 제출하고 삭제 방지가 제거된 후 자동 CT를 사용하여 해당 리소스를 삭제할 경우 이를 차단 해제하는 데 도움이 될 수 있습니다.
- 스택에 리소스가 여러 개 있고 스택 리소스의 하위 집합만 삭제하려는 경우 CloudFormation 업데이트 변경 유형을 사용합니다(CloudFormation 수집 스택: 업데이트 참조). 관리 | 기타 | 기타 | 변경 유형 업데이트 및 필요한 경우 AMS 엔지니어가 변경 세트를 만드는 데 도움을 줄 수도 있습니다.
- 드리프트로 인해 CloudFormation Update CT를 사용하는 데 문제가 있는 경우 AMS는 Management | Other | Other | Update를 제출하여 드리프트를 해결하고(AWS CloudFormation Service에서 지원하는 범위까지) 자동 CT, Management/Custom Stack/Stack From CloudFormation Template/Approve Changeset and Update를 사용하여 검증하고 실행할 수 있는 ChangeSet를 제공하는 경우에 도움이 될 수 있습니다. CloudFormation

AMS는 예상치 못하거나 예상치 못한 리소스 삭제가 없도록 위의 제한을 유지합니다.

자세한 내용은 AWS CloudFormation 문제 해결: 스택 삭제 실패를 참조하세요.

RFC 업데이트 DNS 오류

DNS 호스팅 영역을 업데이트하는 여러 RFCs가 실패할 수 있으며, 일부 RFC는 이유 없이 실패할 수 있습니다. DNS 호스팅 영역(프라이빗 또는 퍼블릭)을 업데이트하기 위해 여러 RFCs를 동시에 생성하면 동일한 스택을 동시에 업데이트하려고 하기 때문에 일부 RFCs가 실패할 수 있습니다. AMS 변경 관리는 스택이 이미 다른 RFCs에 의해 업데이트되고 있기 때문에 스택을 업데이트할 수 없는 RFC를 거부하거나 실패합니다. AMS에서는 한 번에 하나의 RFC를 생성하고 RFC가 성공할 때까지 기다린 후 동일한 스택에 대해 새 RFC를 생성하는 것이 좋습니다.

RFC IAM 엔터티 오류

AMS는 요구 사항에 맞게 설계된 AMS 계정에 여러 기본 IAM 역할 및 프로필을 프로비저닝합니다. 그러나 가끔 추가 IAM 리소스를 요청해야 할 수 있습니다.

사용자 지정 IAM 리소스를 요청하는 RFCs를 제출하는 프로세스는 수동 RFCs에 대한 표준 워크플로를 따르지만 승인 프로세스에는 적절한 보안 제어가 마련되어 있는지 확인하기 위한 보안 검토도 포함됩니다. 따라서 프로세스는 일반적으로 다른 수동 RFCs보다 오래 걸립니다. 이러한 RFCs의 주기 시간을 줄이려면 다음 지침을 따르세요.

IAM 검토의 의미와 기술 표준 및 위험 수락 프로세스에 매핑되는 방법에 대한 자세한 내용은 섹션을 참조하세요RFC 보안 검토 이해.

일반적인 IAM 리소스 요청:

- CloudEndure와 같은 주요 클라우드 호환 애플리케이션과 관련된 정책을 요청하는 경우 AMS 사전 승인된 IAM CloudEndure 정책: WIGs Cloud Endure Landing Zone 예제 파일의 압축을 풀고 `customer_cloud_endure_policy.json`

> **Note**
>
> 보다 허용적인 정책을 원하는 경우 CloudArchitect/CSDM과 요구 사항에 대해 논의하고 필요한 경우 정책을 구현하는 RFC를 제출하기 전에 AMS 보안 검토 및 승인을 받습니다.

- 기본적으로 계정의 AMS에서 배포한 리소스를 수정하려면 기존 리소스를 변경하는 대신 해당 리소스의 수정된 사본을 요청하는 것이 좋습니다.
- 인간 사용자에 대한 권한을 요청하는 경우(사용자에게 권한을 연결하는 대신) 역할에 권한을 연결한 다음 사용자에게 해당 역할을 수임할 수 있는 권한을 부여합니다. 이에 대한 자세한 내용은 임시 AMS 고급 콘솔 액세스를 참조하세요.
- 임시 마이그레이션 또는 워크플로에 대한 예외적인 권한이 필요한 경우 요청에서 해당 권한의 종료 날짜를 제공합니다.
- 보안 팀과 요청의 주체에 대해 이미 논의한 경우 CSDM에 최대한 자세히 승인 증거를 제공합니다.

AMS가 IAM RFC를 거부하는 경우 거부에 대한 명확한 이유를 제공합니다. 예를 들어 IAM 정책 생성 요청을 거부하고 정책에 대한 부적절한 내용을 설명할 수 있습니다. 이 경우 식별된 변경을 수행하고 요청을 다시 제출할 수 있습니다. 요청 상태에 대한 추가 설명이 필요한 경우 서비스 요청을 제출하거나 CSDM에 문의하십시오.

다음 목록은 IAM RFCs를 검토할 때 AMS가 완화하려고 하는 일반적인 위험을 설명합니다. IAM RFC에 이러한 위험이 있는 경우 RFC가 거부될 수 있습니다. 예외가 필요한 경우 AMS는 보안 팀에 승인을 요청합니다. 이러한 예외를 찾으려면 CSDM과 조정하십시오.

> **Note**
>
> AMS는 어떤 이유로든 계정 내 IAM 리소스에 대한 변경을 거부할 수 있습니다. RFC 거부와 관련된 우려 사항은 서비스 요청을 통해 AMS Operations에 문의하거나 CSDM에 문의하십시오.

- 자체 권한을 수정하거나 계정 내 다른 리소스의 권한을 수정할 수 있는 권한과 같은 권한 에스컬레이션. 예시:
  - 더 많은 권한을 가진 다른 역할과 `iam:PassRole` 함께를 사용합니다.
  - 역할 또는 사용자로부터 IAM 정책을 연결/분리할 수 있는 권한.
  - 계정의 IAM 정책 수정.
  - 관리 인프라의 맥락에서 API를 호출하는 기능입니다.
- AMS 서비스를 제공하는 데 필요한 리소스 또는 애플리케이션을 수정할 수 있는 권한. 예시:
  - 접속, 관리 호스트 또는 EPS 인프라와 같은 AMS 인프라 수정.
  - 로그 관리 AWS Lambda 함수 또는 로그 스트림 삭제.
  - 기본 CloudTrail 모니터링 애플리케이션의 삭제 또는 수정입니다.
  - 디렉터리 서비스 Active Directory(AD)의 수정입니다.
  - CloudWatch(CW) 경보 비활성화.
  - 랜딩 존의 일부로 계정에 배포된 보안 주체, 정책 및 네임스페이스의 수정입니다.
- 정보 보안을 위태롭게 하는 상태에서 인프라를 생성할 수 있는 권한과 같은 모범 사례를 벗어나는 인프라 배포. 예시:
  - 퍼블릭 또는 암호화되지 않은 S3 버킷 생성 또는 EBS 볼륨의 퍼블릭 공유.
  - 퍼블릭 IP 주소의 프로비저닝입니다.
  - 광범위한 액세스를 허용하도록 보안 그룹을 수정했습니다.
- 인프라 및 계정 내 애플리케이션에 대한 데이터 손실, 무결성 손실, 부적절한 구성 또는 서비스 중단을 초래할 수 있는 권한과 같이 애플리케이션에 영향을 미칠 수 있는 권한이 지나치게 광범위합니다. 예시:
  - `ModifyNetworkInterfaceAttribute` 또는와 같은 APIs를 통해 네트워크 트래픽을 비활성화하거나 리디렉션합니다`UpdateRouteTable`.
  - 관리형 호스트에서 볼륨을 분리하여 관리형 인프라를 비활성화합니다.
- AMS 서비스 설명의 일부가 아니며 AMS에서 지원하지 않는 서비스에 대한 권한.

  AMS 서비스 설명에 나열되지 않은 서비스는 AMS 계정에서 사용할 수 없습니다. 기능 또는 서비스에 대한 지원을 요청하려면 CSDM에 문의하십시오.
- 너무 관대하거나 보수적이거나 잘못된 리소스에 적용되므로 명시된 목표를 충족하지 않는 권한. 예시:
  - 관련 키에 대한 `s3:PutObject` 권한 없이 필수 KMS 암호화가 있는 S3 버킷에 대한 `KMS:Encrypt` 권한 요청입니다.

- 계정에 없는 리소스와 관련된 권한입니다.
- RFCs의 설명이 요청과 일치하지 않는 것으로 보이는 IAM RFC입니다.

“배포” RFC 오류

AMS "배포" 범주 변경 유형(CTs)을 사용하면 다양한 AMS 지원 리소스를 계정에 추가하도록 요청할 수 있습니다.

리소스를 생성하는 대부분의 AMS CTs는 CloudFormation 템플릿을 기반으로 합니다. 고객은 CloudFormation 콘솔을 사용하여 CloudFormation 스택 설명을 기반으로 스택을 나타내는 스택을 빠르게 식별할 CloudFormation수 있습니다. 실패한 스택은 DELETE_COMPLETE 상태일 수 있습니다. CloudFormation 스택을 식별하면 이벤트에 생성에 실패한 특정 리소스와 그 이유가 표시됩니다.

CloudFormation 설명서를 사용하여 문제 해결

대부분의 AMS 프로비저닝 RFCs는 CloudFormation 템플릿을 사용하며이 설명서는 문제 해결에 유용할 수 있습니다. 해당 CloudFormation 템플릿에 대한 설명서를 참조하세요.

- 애플리케이션 로드 밸런서 생성 실패: AWS::ElasticLoadBalancingV2::LoadBalancer(Application Load Balancer)
- Auto Scaling 그룹 생성: AWS::AutoScaling::AutoScalingGroup(Auto Scaling 그룹)
- memcached 캐시 생성: AWS::ElastiCache::CacheCluster(캐시 클러스터)
- Redis 캐시 생성: AWS::ElastiCache::CacheCluster(캐시 클러스터)
- DNS 호스팅 영역 생성(DNS 프라이빗/퍼블릭 생성과 함께 사용): AWS::Route53::HostedZone(R53 호스팅 영역)
- DNS 레코드 세트 생성(DNS 프라이빗/퍼블릭 생성과 함께 사용): AWS::Route53::RecordSet(리소스 레코드 세트)
- EC2 스택 생성: AWS::EC2::Instance(Elastic Compute Cloud)
- EFS(Elastic File System): AWS::EFS::FileSystem(Elastic File System)
- 로드 밸런서 생성: AWS::ElasticLoadBalancing::LoadBalancer(Elastic Load Balancer)
- RDS DB 생성: AWS::RDS::DBInstance(관계형 데이터베이스)
- Amazon S3 생성: AWS::S3::Bucket(Simple Storage Service)
- 대기열 생성: AWS::SQS::Queue(단순 대기열 서비스)

RFC 생성 AMIs 오류

Amazon Machine Image(AMI)는 소프트웨어 구성이 기재된 템플릿입니다(예: 운영 체제, 애플리케이션 서버, 애플리케이션). AMI에서 인스턴스를 바로 시작하실 수 있는데, 이 인스턴스는 AMI의 사본으로, 클라우드에서 실행되는 가상 서버입니다. AMIs는 매우 유용하며 EC2 인스턴스 또는 Auto Scaling 그룹을 생성하는 데 필요하지만 몇 가지 요구 사항을 준수해야 합니다.

- RFC가 성공하려면에 대해 지정하는 인스턴스가 중지 상태여야 `Ec2InstanceId` 합니다. ASG가 중지된 인스턴스를 종료하므로이 파라미터에 Auto Scaling 그룹(ASG) 인스턴스를 사용하지 마십시오.
- AMS Amazon Machine Image(AMI)를 생성하려면 AMS 인스턴스로 시작해야 합니다. 인스턴스를 사용하여 AMI를 생성하려면 먼저 인스턴스가 중지되고 도메인에서 조인 해제되었는지 확인하여 인스턴스를 준비해야 합니다. 자세한 내용은 Sysprep을 사용하여 표준 Amazon Machine Image 생성을 참조하세요.
- 새 AMI에 지정하는 이름은 계정 내에서 고유해야 합니다. 그렇지 않으면 RFC가 실패합니다. 이 작업을 수행하는 방법은 AMI | 생성에 설명되어 있으며, 자세한 내용은 및 AWS AMI 설계를 참조하세요.

> **Note**
>
> AMI 생성 준비에 대한 자세한 내용은 AMI | 생성을 참조하세요.

EC2s 또는 ASGs 오류를 생성하는 RFCs

제한 시간이 있는 EC2 또는 ASG 실패의 경우 AMS는 사용된 AMI가 사용자 지정되었는지 확인할 것을 권장합니다. 그렇다면이 가이드에 포함된 AMI 생성 단계(AMI | 생성 참조)를 참조하여 AMI가 올바르게 생성되었는지 확인하세요. 사용자 지정 AMI를 생성할 때 흔히 발생하는 실수는 가이드의 단계를 따라 Sysprep의 이름을 바꾸거나 호출하는 것이 아닙니다.

RDS 오류를 생성하는 RFCs

Amazon Relational Database Service(RDS) 장애는 RDS를 생성할 때 다양한 엔진을 사용할 수 있으며 각 엔진에는 고유한 요구 사항과 제한이 있기 때문에 여러 가지 이유로 발생할 수 있습니다. AMS RDS 스택을 생성하기 전에 AWS RDS 파라미터 값을 주의 깊게 검토하세요. CreateDBInstance를 참조하세요.

크기 권장 사항을 포함하여 일반적으로 Amazon RDS에 대한 자세한 내용은 Amazon Relational Database Service 설명서를 참조하세요.

Amazon S3s 오류를 생성하는 RFCs

S3 스토리지 버킷을 생성할 때 발생하는 한 가지 일반적인 오류는 버킷에 고유한 이름을 사용하지 않는 것입니다. 이전에 제출한 것과 동일한 이름의 S3 버킷 CT 생성을 제출한 경우 해당 BucketName에 S3 버킷이 이미 존재하기 때문에 실패합니다. 이는 CloudFormation 스택 이벤트에서 버킷 이름이 이미 사용 중임을 보여주는 콘솔에 자세히 설명되어 있습니다.

RFC 검증과 실행 오류 비교

RFC 실패 및 관련 메시지는 선택한 RFC에 대한 AMS 콘솔 RFC 세부 정보 페이지의 출력 메시지에서 다릅니다.

- 검증 실패 이유는 상태 필드에서만 사용할 수 있습니다.
- 실행 실패 이유는 실행 출력 및 상태 필드에서 확인할 수 있습니다.

RFC 오류 메시지

나열된 변경 유형(CTs)에 대해 다음 오류가 발생하면 이러한 솔루션을 사용하여 문제의 원인을 찾고 수정할 수 있습니다.

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

다음 문제 해결 옵션을 참조한 후 추가 지원이 필요한 경우 RFC 서신을 통해 AMS를 참여시킵니다. 자세한 내용은 RFC 서신 및 첨부 파일(콘솔)을 참조하세요.

워크로드 수집(WIGS) 오류

> **Note**
>
> Windows 및 Linux용 검증 도구를 다운로드하여 온프레미스 서버와 AWS의 EC2 인스턴스에서 직접 실행할 수 있습니다. 이는 AMS Advanced Application Developer's Guide Migrating workloads: Linux pre-ingestion validation and Migrating workloads: Windows pre-ingestion validation을 통해 찾을 수 있습니다.

- EC2 인스턴스가 대상 AMS 계정에 있는지 확인합니다. 예를 들어 AMI를 비 AMS 계정에서 AMS 계정으로 공유한 경우 워크로드 수집 RFC를 제출하기 전에 공유 AMI를 사용하여 AMS 계정에 EC2 인스턴스를 생성해야 합니다.
- 인스턴스에 연결된 보안 그룹에 송신 트래픽이 허용되는지 확인합니다. SSM 에이전트는 퍼블릭 엔드포인트에 연결할 수 있어야 합니다.
- 인스턴스에 SSM 에이전트와 연결할 수 있는 적절한 권한이 있는지 확인합니다. 이러한 권한은와 함께 제공되며 EC2 콘솔에서 이를 확인할 `customer-mc-ec2-instance-profile`수 있습니다.

EC2 인스턴스 스택 중지 오류

- 인스턴스가 이미 중지되거나 종료된 상태인지 확인합니다.
- EC2 인스턴스가 온라인 상태이고 `InternalError` 오류가 표시되면 AMS가 조사할 서비스 요청을 제출합니다.
- 변경 유형 관리 | 고급 스택 구성 요소 | EC2 인스턴스 스택 | 중지 ct-3mvt2zkyveqj를 사용하여 Auto Scaling 그룹(ASG) 인스턴스를 중지할 수 없습니다. ASG 인스턴스를 중지해야 하는 경우 서비스 요청을 제출합니다.

EC2 인스턴스 스택 생성 오류

메시지는 CREATION_FAILED 상태 이유인 CloudFormation에서 보낸 `InternalError` 것입니다. 다음 단계에 따라 CloudWatch 스택 이벤트의 스택 실패에 대한 세부 정보를 찾을 수 있습니다.

- AWS Management 콘솔에서 스택이 생성, 업데이트 또는 삭제되는 동안 스택 이벤트 목록을 볼 수 있습니다. 이 목록에서 실패 이벤트를 찾은 다음 해당 이벤트에 대한 상태 사유를 확인할 수 있습니다.

  상태 이유에는 문제를 이해하는 데 도움이 될 수 있는 AWS CloudFormation 또는 특정 서비스의 오류 메시지가 포함될 수 있습니다.
- 스택 이벤트 보기에 대한 자세한 내용은 AWS Management Console에서 AWS CloudFormation 스택 데이터 및 리소스 보기를 참조하세요.

EC2 인스턴스 볼륨 복원 오류

AMS는 EC2 인스턴스 볼륨 복원에 실패할 때 내부 문제 해결 RFC를 생성합니다. 이는 EC2 인스턴스 볼륨 복원이 재해 복구(DR)의 중요한 부분이며 AMS가이 내부 문제 해결 RFC를 자동으로 생성하기 때문입니다.

내부 문제 해결 RFC가 생성되면 RFC에 대한 링크를 제공하는 배너가 표시됩니다. 이 내부 문제 해결 RFC는에 RFC 장애에 대한 더 많은 가시성을 제공하며, 동일한 오류로 이어지는 재시도 RFCs를 제출하거나이 장애에 대해 AMS에 수동으로 연락하는 대신 변경 사항을 추적하고 AMS에서 장애를 처리하고 있음을 알 수 있습니다. 또한 AMS 연산자가 요청을 기다리는 대신 RFC 장애에 대해 사전에 작업하므로 변경 사항에 대한 time-to-recovery(TTR) 지표가 줄어듭니다.

RFC에 대한 도움을 받는 방법

AMS에 문의하여 장애의 근본 원인을 식별할 수 있습니다. AMS 업무 시간은 하루 24시간, 주 7일, 1년 365일입니다.

AMS는 도움을 요청할 수 있는 몇 가지 방법을 제공합니다.

- 열린 RFC 또는 완료되었지만 잘못된 RFC에 대한 지원이 필요한 경우 RFC 양방향 통신문을 통해 AMS를 참여시킵니다. 자세한 내용은 RFC 서신 및 첨부 파일(콘솔)을 참조하세요.
- 관리형 환경에 영향을 미치는 AWS 또는 AMS 서비스 성능 문제를 보고하려면 AMS 콘솔을 사용하여 인시던트 보고서를 제출합니다. 자세한 내용은 인시던트 보고를 참조하세요. AMS 인시던트 관리에 대한 일반적인 정보는 인시던트 대응을 참조하세요.
- 사용자 또는 리소스 또는 애플리케이션이 AMS로 작업하는 방식에 대한 구체적인 질문이 있거나 인시던트를 에스컬레이션하려면 다음 중 하나 이상을 이메일로 보내십시오.
  1. 먼저 서비스 요청 또는 인시던트 보고서 응답이 만족스럽지 않은 경우 CSDM에 ams-csdm@amazon.com으로 이메일을 보냅니다.
  2. 다음으로 에스컬레이션이 필요한 경우 AMS Operations Manager에 이메일을 보낼 수 있습니다 (하지만 CSDM에서이 작업을 수행할 수 있음). ams-opsmanager@amazon.com
  3. 추가 에스컬레이션은 AMS Director에게: ams-director@amazon.com
  4. 마지막으로 언제든지 AMS VP: ams-vp@amazon.com에 연결할 수 있습니다.

AMS의 직접 변경 모드

주제

- 직접 변경 모드 시작하기

- 보안 및 규정 준수
- 직접 변경 모드에서 변경 관리
- Direct Change 모드를 사용하여 스택 생성
- 직접 변경 모드 사용 사례

AWS Managed Services(AMS) Direct Change 모드(DCM)는 AMS Advanced Plus 및 Premium 계정에 대한 기본 AWS 액세스를 제공하여 AWS 리소스를 프로비저닝하고 업데이트함으로써 AMS Advanced 변경 관리를 확장합니다. DCM을 사용하면 네이티브 AWS API(콘솔 또는 CLI/SDK) 또는 AMS Advanced 변경 관리 요청(RFCs)을 사용할 수 있으며, 두 경우 모두 모니터링, 패치, 백업, 인시던트 대응 관리를 포함하여 리소스 및 변경 사항이 AMS에서 완전히 지원됩니다. DCM을 통해 프로비저닝된 리소스는 AMS 서비스 지식 관리 시스템(SKMS)에 등록되고, AMS 관리형 Active Directory 도메인(해당하는 경우)에 조인되며, AMS 관리 에이전트를 실행합니다. 기존 도구(예: CloudFormation, AWS SDK 및 CDK)를 사용하여 AMS 관리형 CloudFormation 스택을 개발하고 배포합니다.

> **Note**
>
> 직접 변경 모드는 AMS 변경 관리 RFCs 제거하지 않습니다. DCM을 사용하여 AMS RFCs 대한 전체 액세스 권한을 가집니다.

Akash의 동영상을 보고 자세히 알아보기(6:30)

직접 변경 모드 시작하기

먼저 사전 조건을 확인한 다음 적격 AMS Advanced 계정에서 변경 요청(RFC)을 제출합니다.

1. DCM과 함께 사용하려는 계정이 요구 사항을 충족하는지 확인합니다.
   - 계정은 AMS Advanced Plus 또는 Premium입니다.
   - 계정에 Service Catalog가 활성화되어 있지 않습니다. 현재 DCM과 Service Catalog 모두에 동시에 계정을 온보딩하는 것은 지원하지 않습니다. 이미 Service Catalog에 온보딩되어 있지만 DCM에 관심이 있는 경우 클라우드 서비스 제공 관리자(CSDM)와 요구 사항에 대해 논의하세요. Service Catalog에서 DCM으로 전환하기로 결정한 경우 Service Catalog를 오프보드하여 이를 수행하려면 아래 변경 요청에 요청을 포함하세요. AMS의 Service Catalog에 대한 자세한 내용은 AMS 및 Service Catalog를 참조하세요.
2. 관리 | 관리형 계정 | 직접 변경 모드 | 변경 유형 활성화(ct-3rd4781c2nnhp)를 사용하여 변경 요청(RFC)을 제출합니다. 예제 연습은 직접 변경 모드 | 활성화를 참조하세요.

CT가 처리되면 미리 정의된 IAM 역할 `AWSManagedServicesCloudFormationAdminRole` 및 `AWSManagedServicesUpdateRole`가 지정된 계정에 프로비저닝됩니다.

3. 내부 페더레이션 프로세스를 사용하여 DCM 액세스가 필요한 사용자에게 적절한 역할을 할당합니다.

> **Note**
>
> 원하는 수의 SAMLIdentityProviders, AWS Services 및 IAM 엔터티(역할, 사용자 등)를 지정하여 역할을 수임할 수 있습니다. `SAMLIdentityProviderARNs`, `IAMEntityARNs`또는 중 하나 이상을 제공해야 합니다`AWSServicePrincipals`. 자세한 내용은 회사의 IAM 부서 또는 AMS 클라우드 아키텍트(CA)에 문의하세요.

직접 변경 모드 IAM 역할 및 정책

계정에서 직접 변경 모드가 활성화되면 다음과 같은 새 IAM 엔터티가 배포됩니다.

`AWSManagedServicesCloudFormationAdminRole`:이 역할은 CloudFormation 콘솔에 대한 액세스 권한을 부여하고, CloudFormation 스택을 생성 및 업데이트하고, 드리프트 보고서를 보고, CloudFormation ChangeSets를 생성 및 실행합니다. 이 역할에 대한 액세스는 SAML 공급자를 통해 관리됩니다.

역할에`AWSManagedServicesCloudFormationAdminRole` 배포되고 연결된 관리형 정책은 다음과 같습니다.

- AMS 고급 다중 계정 랜딩 존(MALZ) 애플리케이션 계정
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
    - 이 정책은에 부여된 권한을 나타냅니다`AWSManagedServicesCloudFormationAdminRole`. 사용자와 파트너는이 정책을 사용하여 계정의 기존 역할에 대한 액세스 권한을 부여하고 해당 역할이 계정의 CloudFormation 스택을 시작하고 업데이트하도록 허용합니다. 다른 IAM 엔터티가 CloudFormation 스택을 시작하도록 허용하려면 추가 AMS 서비스 제어 정책(SCP) 업데이트가 필요할 수 있습니다.
- AMS 고급 단일 계정 랜딩 존(SALZ) 계정
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2

- cdk-legacy-mode-s3-access[인라인 정책]
- AWS ReadOnlyAccess 정책

AWSManagedServicesUpdateRole:이 역할은 다운스트림 AWS 서비스 APIs에 대한 제한된 액세스 권한을 부여합니다. 역할은 변경 및 비변환 API 작업을 제공하는 관리형 정책과 함께 배포되지만, 일반적으로 IAM, KMS,GuardDuty, VPC, AMS 인프라 리소스 및 구성 등과 같은 특정 서비스에 대해 변경 작업(예: Create/Delete/PUT)을 제한합니다.이 역할에 대한 액세스는 SAML 공급자를 통해 관리됩니다.

역할에AWSManagedServicesUpdateRole 배포되고 연결된 관리형 정책은 다음과 같습니다.

- AMS Advanced 다중 계정 랜딩 존 애플리케이션 계정
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy
- AMS Advanced 단일 계정 랜딩 존 계정
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy2

이 외에도 관리형 정책AWSManagedServicesUpdateRole 역할에는 AWS 관리형 정책이 ViewOnlyAccess 연결되어 있습니다.

보안 및 규정 준수

보안 및 규정 준수는 AMS Advanced와 고객 간의 공동 책임입니다. AMS 고급 직접 변경 모드는이 공동 책임을 변경하지 않습니다.

직접 변경 모드의 보안

AMS Advanced는 규범적 랜딩 존, 변경 관리 시스템 및 액세스 관리를 통해 추가 가치를 제공합니다. 직접 변경 모드를 사용하는 경우이 책임 모델은 변경되지 않습니다. 그러나 추가 위험을 알고 있어야 합니다.

직접 변경 모드 "업데이트" 역할(참조직접 변경 모드 IAM 역할 및 정책)은 계정 내에서 AMS 지원 서비스의 인프라 리소스를 변경할 수 있도록 엔터티가 액세스할 수 있는 승격된 권한을 제공합니다. 권한이 높아지면 리소스, 서비스 및 작업에 따라 다양한 위험이 존재합니다. 특히 감독, 실수 또는 내부 프로세스 및 제어 프레임워크 준수 부족으로 인해 잘못된 변경이 이루어지는 상황에서는 더욱 그렇습니다.

AMS 기술 표준에 따라 다음과 같은 위험이 식별되었으며 권장 사항은 다음과 같습니다. AMS 기술 표준에 대한 자세한 내용은를 통해 확인할 수 있습니다 AWS Artifact. 에 액세스하려면 CSDM에 AWS Artifact문의하여 지침을 받거나 시작하기로 AWS Artifact 이동합니다.

AMS-STD-001: 태그 지정

표준	깨졌나요?	위험	권장 사항
모든 AMS 소유 리소스에는 다음과 같은 키-값 페어가 있어야 합니다. 위에 나열된 태그 이외의 모든 AMS 소유 태그에는 upper/lower/mix스 대/소문자AMS*MC*와 같은 접두사가 있어야 합니다.	예. CloudFormation,CloudTrail, EFS, OpenSearch, CloudWatch Logs, SQS, SSM, Tagging api에 대한 중단 - 이러한 서비스는 AMS 네임스페이스에 대한 태깅을 제한하는 `aws:TagsKey` 조건을 지원하지 않습니다. 다음 표 AMS-STD-003에 제공된 표준은 AppId, 환경 및 AppName을 변경할 수 있지만 AMS 소유 리소스의 경우 변경할 수 없다고 명시합니다.	AMS 리소스의 잘못된 태그 지정은 AMS 측 리소스의 보고, 알림 및 패치 적용 작업에 부정적인 영향을 미칠 수 있습니다.	AMS 팀 이외의 모든 사용자의 AMS 기본 태그 지정 요구 사항을 변경하려면 액세스를 재시도해야 합니다.

표준	깨졌나요?	위험	권장 사항
	IAM 권한을 통해 달성할 수 없습니다.		
AMS 소유 스택의 태그는 변경 요청에 따라 삭제해서는 안 됩니다.	예. CloudFormation은 AMS 네임스페이스에 대한 태그를 제한하는 `aws:TagsKey` 조건을 지원하지 않습니다.		
다음 표 AMSAMS-STD-002 태그 이름 지정 규칙을 사용할 수 없습니다.	예. CloudFormation, CloudTrail, Amazon Elastic File System(EFS), OpenSearch, CloudWatch Logs, Amazon Simple Queue Service(SQS), Amazon EC2 Systems Manager(SSM), 태그 지정 API에 대한 중단. 이러한 서비스는 AMS 네임스페이스에 대한 태그 지정을 제한하는 `aws:TagsKey` 조건을 지원하지 않습니다.		

AMS-STD-002: Identity and Access Management(IAM)

표준	깨졌나요?	위험	권장 사항
4.7 변경 관리 프로세스(RFC)를 우회하는 작업은 인스턴스 시작 또는 중지, S3 버킷 또	예. 셀프 서비스 작업의 목적을 통해 AMS RFC 시스템을 우회하	보안 액세스 모델은 AMS의 핵심 기술 패싯이며 콘솔 또는 프로그래밍 방식의 액세	IAM 사용자는 시간 제한을 두고 최소 권한과 need-to-know 따라 권

표준	깨졌나요?	위험	권장 사항
는 RDS 인스턴스 생성 등과 같이 허용되지 않아야 합니다. 개발자 모드 계정 및 셀프 서비스 프로비저닝 모드 서비스(SSPS)는 작업이 할당된 역할의 경계 내에서 수행되는 한 면제됩니다.	는 작업을 수행할 수 있습니다.	스를 위한 IAM 사용자는이 액세스 제어를 우회합니다. IAM 사용자 액세스는 AMS 변경 관리에서 모니터링되지 않습니다. 액세스는 CloudTrail에만 로깅됩니다.	한을 부여받아야 합니다.

AMS-STD-003: 네트워크 보안

표준	깨졌나요?	위험	권장 사항
S2. EC2 인스턴스의 탄력적 IP는 공식 위험 수락 계약 또는 내부 팀의 유효한 사용 사례에서만 사용해야 합니다.	예. 셀프 서비스 작업을 사용하면 탄력적 IP 주소(EIP)를 연결하고 연결을 해제할 수 있습니다.	인스턴스에 탄력적 IP를 추가하면 인스턴스가 인터넷에 노출됩니다. 이렇게 하면 정보 공개 및 무단 활동의 위험이 증가합니다.	보안 그룹을 통해 해당 인스턴스에 대한 불필요한 트래픽을 차단하고 보안 그룹이 인스턴스에 연결되어 있는지 확인하여 비즈니스상의 이유로 필요한 경우에만 트래픽을 허용하도록 합니다.
S14. 동일한 고객에게 속한 계정 간의 VPC 피어링 및 엔드포인트 연결을 허용할 수 있습니다.	예. IAM 정책을 통해 불가능합니다.	AMS 계정에서 나가는 트래픽은 계정 경계를 벗어나면 모니터링되지 않습니다.	소유하고 있는 AMS 계정으로만 피어링하는 것이 좋습니다. 사용 사례에 필요한 경우 보안 그룹 및 라우팅 테이블을 사용하여 관련 연결을 통해 송신할 수 있는 트래픽 범위, 리소스 및 유형을 제한합니다.

표준	깨졌나요?	위험	권장 사항
AMS 기본 AMIs는 동일한 AWS 조직에서 소유하고 있는지 확인할 수 있는 한 AMS 관리형 계정과 비관리형 계정 간에 공유할 수 있습니다.		AMIs 민감한 데이터가 포함될 수 있으며 의도하지 않은 계정에 노출될 수 있습니다.	조직 외부에서 공유하기 전에 조직이 소유한 계정과만 AMIs를 공유하거나 사용 사례 및 계정 정보를 검증합니다.

AMS-STD-007: 로깅

표준	깨졌나요?	위험	권장 사항
19. 모든 로그는 한 AMS 계정에서 동일한 고객의 다른 AMS 계정으로 전달할 수 있습니다.	예. 동일한 조직에 있는 고객 계정의 확인으로 인한 고객 로그의 잠재적 비보안은 IAM 정책을 통해 달성할 수 없습니다.	로그에는 민감한 데이터가 포함될 수 있으며 의도하지 않은 계정에 노출될 수 있습니다.	조직 외부에서 공유하기 전에 AWS 조직에서 관리하는 계정과만 로그를 공유하거나 사용 사례 및 계정 정보를 검증합니다. 이를 여러 가지 방법으로 확인할 수 있습니다. 클라우드 서비스 제공 관리자(CSDM)에게 문의하십시오.
20. 모든 로그는 내부 도구를 사용하여 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만(동일한 계정인지 AWS Organizations 확인하거나 이메일 도메인을 고객의 회사 이름 및 PAYER 연결 계정과 일치시켜) AMS에서 비 AMS 계정으로 전달할 수 있습니다.			

이에 따라 내부 권한 부여 및 인증 팀과 협력하여 Direct Change 모드 역할에 대한 권한을 제어합니다.

직접 변경 모드의 규정 준수

Direct Change 모드는 프로덕션 워크로드와 비프로덕션 워크로드 모두와 호환됩니다. 규정 준수 표준(예: PHI, HIPAA, PCI)을 준수하고 Direct Change 모드 사용이 내부 제어 프레임워크 및 표준을 준수하도록 하는 것은 사용자의 책임입니다.

직접 변경 모드에서 변경 관리

변경 관리는 AMS Advanced가 변경 요청을 구현하는 데 사용하는 프로세스입니다. 변경 요청(RFC)은 관리형 환경을 변경하기 위해 사용자 또는 AMS Advanced 인터페이스를 통해 AMS Advanced가 생성한 요청으로, 특정 작업에 대한 AMS Advanced 변경 유형(CT) ID를 포함합니다. 자세한 내용은 변경 관리를 참조하세요.

> **Note**
>
> 직접 변경 모드는 AMS 변경 관리 RFCs 제거하지 않으며 DCM을 사용하는 AMS RFCs에 대한 전체 액세스 권한을 여전히 가집니다.

AMS Direct Change 모드(DCM)는 AWS 리소스를 프로비저닝하고 업데이트하기 위해 AMS Advanced Plus 및 Premium 계정에 대한 기본 AWS 액세스를 제공하여 AMS Advanced 변경 관리를 확장합니다. IAM 역할을 통해 Direct Change 모드 권한을 부여받은 사용자는 기본 AWS API 액세스를 사용하여 AMS Advanced 계정의 리소스를 프로비저닝하고 변경할 수 있습니다. 사용자는 동일한 IAM 역할을 사용하여 AMS Advanced 변경 관리 RFCs를 계속 사용할 수 있습니다. 두 경우 모두 모니터링, 패치, 백업, 인시던트 대응 관리를 포함하여 AMS에서 리소스와 리소스 변경 사항을 완벽하게 지원합니다. 이러한 계정에서 적절한 역할이 없는 사용자는 AMS Advanced 변경 관리 RFC 프로세스를 사용하여 변경해야 합니다.

변경 관리 사용 사례

보안상의 이유로 AMS Advanced의 일부 변경은 변경 관리 변경 요청(RFC) 프로세스를 통해서만 수행할 수 있습니다. `AWSManagedServicesCloudFormationAdminRole`는 CloudFormation(CFN)을 통해 수행되는 작업으로 제한됩니다. DCM을 통해 스택을 생성하는 방법에 대한 자세한 내용은 Direct Change 모드를 사용하여 스택 생성을 참조하세요. `AWSManagedServicesUpdateRole`는 다음 작업으로 제한됩니다.

관리 | 관리형 계정 | 직접 변경 모드 | 활성화(ct-3rd4781c2nnhp) 변경 유형을 포함한 각 변경 유형에 대한 예제 안내는 분류별 AMS 고급 변경 유형 참조 변경 유형 섹션에서 관련 변경 유형에 대

한 "추가 정보" 섹션을 참조하세요. https://docs.aws.amazon.com/managedservices/latest/ctref/classifications.html

서비스	작업
AWS Key Management Service (AWS KMS)	업데이트
AWS Certificate Manager	생성
AWS Identity and Access Management (IAM)	임의
Site-to-Site VPN	임의
AMS 리소스 스케줄러	
AWS Backup	백업 계획 생성
AMS 워크로드 수집(WIGs)	임의
AMS Advanced MALZ 계정 변경 사항	
Amazon GuardDuty	
AMS 고급 스택 액세스	임의
Amazon Elastic Block Store(EBS) 볼륨	Delete
Amazon Elastic Block Store(EBS) 기본 암호화	기본 암호화 활성화
Amazon Elastic Compute Cloud(Amazon EC2)	호스트 이름 변경
Amazon Machine Image(AMI)	삭제, 공유
Amazon EC2 보안 그룹	임의
AMS 고급 SSPS	
AWS 관리형 Microsoft AD	
AMS Advanced 개발자 모드	
Amazon Simple Storage Service(Amazon S3)	S3 버킷 정책 생성

서비스	작업
AWS Systems Manager	생성

Direct Change 모드를 사용하여 스택 생성

AMS에서 스택을 관리하려면를 사용하여 CloudFormation에서 스택을 시작할 때 다음 두 가지 요구 사항이 있습니다`AWSManagedServicesCloudFormationAdminRole`.

- 템플릿에는가 포함되어야 합니다`AmsStackTransform`.
- 스택 이름은 접두사 뒤에 17자의 영숫자 문자열`stack-`로 시작해야 합니다.

> **Note**
>
> 를 성공적으로 사용하려면 스택 템플릿에 CloudFormation (CFN)가 스택을 생성하거나 업데이트하기 위한 `CAPABILITY_AUTO_EXPAND` 기능이 포함되어 있음을 확인해야 `AmsStackTransform`합니다. 이렇게 하려면를 create-stack 요청의 `CAPABILITY_AUTO_EXPAND` 일부로 전달합니다. 가 템플릿에 포함될 때이 기능이 확인되지 않으면 CFN`AmsStackTransform`은 요청을 거부합니다. CFN 콘솔은 템플릿에 변환이 있는 경우이 기능을 전달하도록 보장하지만 APIs를 통해 CFN과 상호 작용할 때이 기능을 놓칠 수 있습니다.
>
> 다음 CFN API 호출을 사용할 때마다이 기능을 전달해야 합니다.
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

DCM을 사용하여 스택을 생성하거나 업데이트할 때 스택에서 CFN 수집 및 스택 업데이트 CTs의 동일한 검증 및 증강이 수행됩니다. 자세한 내용은 CloudFormation 수집 지침, 모범 사례 및 제한을 참조하세요. 단, AMS 기본 보안 그룹(SGs)은 독립형 EC2 인스턴스 또는 Auto Scaling 그룹(ASGs)의 EC2 인스턴스에 연결되지 않습니다. 독립형 EC2 인스턴스 또는 ASGs를 사용하여 CloudFormation 템플릿을 생성할 때 기본 SGs.

> **Note**
>
> 이제를 사용하여 IAM 역할을 생성하고 관리할 수 있습니
> 다`AWSManagedServicesCloudFormationAdminRole`.

AMS 기본 SGs에는 인스턴스를 성공적으로 시작하고 나중에 AMS 작업 및 사용자에 의해 SSH 또는 RDP를 통해 액세스할 수 있는 수신 및 송신 규칙이 있습니다. AMS 기본 보안 그룹이 너무 허용적이라고 판단되면 사용자와 AMS 작업이 인시던트 발생 시 인스턴스에 액세스할 수 있도록 허용하는 한 보다 제한적인 규칙을 사용하여 자체 SGs를 생성하고 인스턴스에 연결할 수 있습니다.

AMS 기본 보안 그룹은 다음과 같습니다.

- SentinelDefaultSecurityGroupPrivateOnly:이 SSM 파라미터를 통해 CFN 템플릿에서 액세스할 수 있습니다. `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll:이 SSM 파라미터를 통해 CFN 템플릿에서 액세스할 수 있습니다. `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS 변환

CloudFormation 템플릿에 `Transform` 문을 추가합니다. 그러면 시작 시 스택을 검증하고 AMS에 등록하는 CloudFormation 매크로가 추가됩니다.

JSON 예제

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
```

YAML 예제

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

또한 기존 스택의 템플릿을 업데이트할 때 `Transform` 문을 추가합니다.

JSON 예제

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML 예제

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
```

```
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

스택 이름

스택 이름은 접두사 뒤에 17자의 영숫자 문자열`stack-`로 시작해야 합니다. 이는 AMS 스택 IDs.

다음은 호환되는 스택 IDs.

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

직접 변경 모드 사용 사례

다음은 직접 변경 모드의 사용 사례입니다.

를 통한 리소스 프로비저닝 및 관리 CloudFormation

- 기존 CloudFormation 기반 도구 및 프로세스를 통합합니다.

지속적인 리소스 관리 및 업데이트

- 위험이 낮은 작은 원자성 변화.
- 수동 또는 자동 RFC를 통해 실행되는 변경 사항입니다.

- 네이티브 AWS API 액세스가 필요한 도구입니다.
- 마이그레이션 단계에 있는 경우 DCM 역할을 사용할 수 있습니다. 마이그레이션 팀은 DCM에 대한 권한을 활용하여 스택을 생성하거나 수정합니다.
- CI/CD 파이프라인에서 DCM 역할을 사용하여 새 AMIs를 빌드하고 Amazon ECS 작업을 생성하는 등의 작업을 수행할 수 있습니다.

AMS 고급 개발자 모드

주제

AWS Managed Services(AMS) 개발자 모드는 AMS Advanced Plus 및 Premium 계정에서 승격된 권한을 사용하여 AMS Advanced 변경 관리 프로세스 외부에서 AWS 리소스를 프로비저닝하고 업데이트합니다. AMS Advanced Developer 모드는 AMS Advanced Virtual Private Cloud(VPC) 내에서 네이티브 AWS API 호출을 활용하여 이를 수행하므로 관리형 환경에서 인프라와 애플리케이션을 설계하고 구현할 수 있습니다.

개발자 모드가 활성화된 계정을 사용하는 경우 AMS Advanced 변경 관리 프로세스를 통해 또는 AMS Amazon Machine Image(AMI)를 사용하여 프로비저닝된 리소스에 대해 연속성 관리, 패치 관리 및 변경 관리가 제공됩니다. 그러나 이러한 AMS 관리 기능은 AWS APIs 통해 프로비저닝된 리소스에는 제공되지 않습니다.

사용자는 AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝되는 인프라 리소스를 모니터링할 책임이 있습니다. 개발자 모드는 프로덕션 워크로드와 비프로덕션 워크로드 모두와 호환됩니다. 권한이 승격되면 내부 제어를 준수할 책임이 증가합니다.

> **Important**
>
> 개발자 모드를 사용하여 생성한 리소스는 AMS Advanced 변경 관리 프로세스를 사용하여 생성한 경우에만 AMS Advanced에서 관리할 수 있습니다.

개발자 모드는 사용할 수 있는 AMS 고급 모드 중 하나입니다. 자세한 내용은 모드 개요 단원을 참조하십시오.

AMS 고급 개발자 모드 시작하기

AMS Advanced Developer 모드가 있는 다양한 AMS Advanced 계정과 개발자 모드를 성공적으로 구현하는 방법을 알아봅니다.

주제

AMS 개발자 모드를 시작하기 전에

개발자 모드를 구현하기 전에 알아야 할 몇 가지 사항이 있습니다.

AMS Advanced는 변경 요청(RFCs)을 통해 AMS Advanced 변경 관리 프로세스 외부에서 생성된 DevMode 계정의 기존 스택 또는 리소스를 관리할 수 없습니다. 그러나 계정이 DevMode에 있는 동안 AMS Advanced는 RFCs를 사용하여 AMS Advanced 변경 관리 프로세스를 통해 프로비저닝된 리소스를 계속 관리합니다.

DevMode 계정으로 시작하여 나중에 AMS Advanced 관리형 애플리케이션 계정으로 은폐할 수 없습니다.

AMS 개발자 모드의 사전 조건

다음은 개발자 모드를 구현하기 위한 사전 조건입니다.

- 온보딩된 AMS Advanced Plus 또는 Premium 계정이 하나 이상 있는 AMS Advanced 고객이어야 합니다.
- 사용하는 모든 계정은 AMS Advanced Plus 또는 Premium 계정이어야 합니다.

- 다중 계정 랜딩 존(MALZ): `AWSManagedServicesDevelopmentRole` 사전 정의된 AWS Identity and Access Management (IAM) 역할을 사용해야 합니다. 이 역할을 요청합니다. 다음 섹션에서는 개발자 모드 권한을 획득하는 방법을 설명합니다.
- 단일 계정 랜딩 존(SALZ): `customer_developer_role` 사전 정의된 AWS Identity and Access Management (IAM) 역할을 사용해야 합니다. 이 역할을 요청합니다. 다음 섹션에서는 개발자 모드 권한을 획득하는 방법을 설명합니다.

AMS Advanced Developer 모드를 구현하는 방법

적격 AMS Advanced 계정에 사전 정의된 IAM 역할을 프로비저닝하도록 요청하여 개발자 모드를 구현합니다.

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALZ: `customer_developer_role`

그런 다음 페더레이션 네트워크의 관련 사용자에게 역할을 할당합니다.

개발자 모드는 AMS 고급 관리형 리소스에 대한 AMS 고급 변경 관리와 고객이 관리하는 리소스에 대한 고객 관리형 역할 페더레이션이라는 두 가지 변경 벡터를 생성하므로 개발자 모드 사용이 내부 제어 프레임워크 및 표준을 준수하는지 확인하는 것이 좋습니다. AMS Advanced 프로세스는 선언을 계속 준수하지만 고객 프로세스 및 제어 프레임워크를 업데이트해야 할 수 있습니다.

AMS Advanced 계정에서 개발자 모드를 구현하려면

1. 개발자 모드와 함께 사용할 계정이에 나열된 요구 사항을 충족하는지 확인합니다AMS 개발자 모드의 사전 조건.
2. 변경 유형(CT) 관리 | 관리형 계정 | 개발자 모드 | 활성화(관리형 자동화)를 사용하여 변경 요청(RFC)을 제출합니다. 이 CT를 사용하는 방법의 예는 개발자 모드 | 활성화(관리형 자동화)를 참조하세요.

   CT가 처리되면 미리 정의된 IAM 역할(`AWSManagedServicesDevelopmentRole`MALZ의 경우 , SALZ의 `customer_developer_role` 경우)이 요청된 계정에 프로비저닝됩니다.
3. 내부 페더레이션 프로세스를 사용하여 개발자 모드 액세스가 필요한 사용자에게 적절한 역할을 할당합니다.

   AMS Advanced는 리소스의 원치 않거나 승인되지 않은 프로비저닝 또는 변경을 방지하기 위해 액세스를 제한할 것을 권장합니다.

AMS Advanced Developer 모드 권한

사전 정의된 역할(`AWSManagedServicesDevelopmentRole`MALZ의 경우 , SALZ의 `customer_developer_role` 경우)은 AMS Advanced에서 운영하는 공유 서비스 구성 요소(예: 관리 호스트, 도메인 컨트롤러, Trend Micro EPS, 접속 및 지원되지 않는 AWS 서비스)에 대한 액세스를 제한하면서 IAM 역할을 포함하여 AMS Advanced VPC 내에서 애플리케이션 인프라 리소스를 생성할 수 있는 권한을 부여합니다. 또한이 역할은 AWS 서비스 Amazon GuardDuty, AWS Organizations, AWS Directory Service APIs.

역할을 통해 추가 IAM 역할을 생성할 수 있지만 개발자 모드 액세스에 포함된 것과 동일한 권한 경계가에서 생성한 모든 IAM 역할에 적용됩니다`AWSManagedServicesDevelopmentRole`.

개발자 모드의 보안 및 규정 준수

보안 및 규정 준수는 AMS Advanced와 고객 간의 공동 책임입니다. AMS 고급 개발자 모드는 변경 관리 프로세스 외부에서 프로비저닝되거나 변경 관리를 통해 프로비저닝되지만 개발자 모드 권한으로 업데이트된 리소스에 대한 공동 책임을 사용자에게 이전합니다. 공동 책임에 대한 자세한 내용은 AWS Managed Services를 참조하세요.

주의:

- DevMode를 사용하면 사용자와 권한 있는 팀이 AMS 보안의 핵심에서 deny-by-default 원칙을 우회할 수 있습니다. 이점, 셀프 서비스, AMS 대기 시간 단축을 단점과 비교해야 합니다. 누구나 보안 팀의 지식 없이 예기치 않고 파괴적인 조치를 수행할 수 있습니다. 개발 모드 및 직접 변경 모드를 활성화하는 자동 변경 유형이 노출되며, 조직의 권한이 있는 모든 사람이 이러한 CTs 실행하고 이러한 모드를 활성화할 수 있습니다.
- 사용자 기반에서 CT 실행 권한을 관리하는 것은 사용자의 책임입니다.
- AMS는 CT 실행 권한을 관리하지 않습니다.

권장 사항:

- 보호
  - 고객은 권한을 통해이 CT에 대한 액세스를 방지할 수 있습니다. IAM 역할 정책 설명을 사용하여 권한 제한을 참조하세요.
  - ITSM 시스템과 같은 프록시를 구현하여이 CT에 대한 액세스 방지
  - 필요에 따라 정책 및 동작을 방지하는 서비스 제어 정책(SCPs https://docs.aws.amazon.com/managedservices/latest/userguide/scp-library.html

- 감지
  - RFC에서 실행 중인 CTs(개발자 모드 ct-1opjmhuddw194 및 직접 변경 모드 활성화, ct-3rd4781c2nnhp 활성화)를 모니터링하고 그에 따라 응답합니다.
  - 계정에서 IAM 리소스가 있는지 검토 및/또는 감사하여 개발자 모드 또는 직접 변경 모드가 배포된 계정을 식별합니다.
- 응답
  - 필요에 따라 개발자 모드에서 계정 제거

개발자 모드의 보안

AMS Advanced는 규범적 랜딩 존, 변경 관리 시스템 및 액세스 관리를 통해 추가 가치를 제공합니다. 개발자 모드를 사용하는 경우 AMS Advanced의 보안 값은 기본 AMS Advanced 보안 강화 네트워크를 설정하는 표준 AMS Advanced 계정과 동일한 계정 구성을 사용하여 유지됩니다. 네트워크는 역할(AWSManagedServicesDevelopmentRoleMALZ의 경우 , SALZ의 customer_developer_role 경우)에 적용되는 권한 경계로 보호되므로 사용자가 계정을 설정할 때 설정된 파라미터 보호 기능을 해제하지 못하도록 제한됩니다.

예를 들어 역할이 있는 사용자는 Amazon Route 53에 액세스할 수 있지만 AMS Advanced 내부 호스팅 영역은 제한됩니다. 에서 생성한 IAM 역할에도 동일한 권한 경계가 적용되어 계정이 AMS Advanced에 온보딩될 때 설정된 파라미터 보호 기능을 사용자가 분해하지 못하도록 제한AWSManagedServicesDevelopmentRole하는에 대한 권한 경계가 AWSManagedServicesDevelopmentRole적용됩니다.

개발자 모드의 규정 준수

개발자 모드는 프로덕션 워크로드와 비프로덕션 워크로드 모두와 호환됩니다. 규정 준수 표준(예: PHI, HIPAA, PCI)을 준수하고 개발자 모드 사용이 내부 제어 프레임워크 및 표준을 준수하도록 하는 것은 사용자의 책임입니다.

개발자 모드의 변경 관리

변경 관리는 AMS Advanced 서비스가 변경 요청을 구현하는 데 사용하는 프로세스입니다. 변경 요청(RFC)은 관리형 환경을 변경하기 위해 AMS Advanced 인터페이스를 통해 사용자 또는 AMS Advanced가 생성하는 요청이며 특정 작업에 대한 변경 유형(CT) ID를 포함합니다. 자세한 내용은 변경 관리 모드 단원을 참조하십시오.

개발자 모드 권한이 부여된 AMS Advanced 계정에서는 변경 관리가 적용되지 않습니다. IAM 역할(AWSManagedServicesDevelopmentRoleMALZ의 경우 , SALZ의 customer_developer_role

경우)로 개발자 모드 권한을 부여받은 사용자는 기본 AWS API 액세스를 사용하여 AMS Advanced 계정의 리소스를 프로비저닝하고 변경할 수 있습니다. 이러한 계정에서 적절한 역할이 없는 사용자는 AMS Advanced 변경 관리 프로세스를 사용하여 변경해야 합니다.

> **Important**
>
> 개발자 모드를 사용하여 생성한 리소스는 AMS Advanced 변경 관리 프로세스를 사용하여 생성한 경우에만 AMS Advanced에서 관리할 수 있습니다. AMS Advanced 변경 관리 프로세스 외부에서 생성된 리소스에 대해 AMS Advanced에 제출된 변경 요청은 사용자가 처리해야 하므로 AMS Advanced에서 거부합니다.

셀프 서비스 프로비저닝 서비스 API 제한

모든 AMS Advanced 자체 프로비저닝 서비스는 개발자 모드에서 지원됩니다. 자체 프로비저닝된 서비스에 대한 액세스에는 각 사용 설명서 섹션에 설명된 제한 사항이 적용됩니다. 개발자 모드 역할에서 자체 프로비저닝된 서비스를 사용할 수 없는 경우 개발자 모드 변경 유형을 통해 업데이트된 역할을 요청할 수 있습니다.

다음 서비스는 서비스 APIs에 대한 전체 액세스를 제공하지 않습니다.

개발자 모드에서 제한된 자체 프로비저닝 서비스

서비스:	참고
Amazon API Gateway	APIs 호출이 허용됩니다`SetWebACL` .
Application Auto Scaling	확장 가능 대상만 등록 또는 등록 취소하고 조정 정책을 추가 또는 삭제할 수 있습니다.
AWS CloudFormation	접두사가 인 이름이 있는 CloudFormation 스택에는 액세스하거나 수정할 수 없습니다`mc-`.
AWS CloudTrail	`ams-` 및/또는 접두사가 붙은 이름이 있는 CloudTrail 리소스에는 액세스하거나 수정할 수 없습니다`mc-`.
Amazon Cognito(사용자 풀)	소프트웨어 토큰을 연결할 수 없습니다.

서비스:	참고
	사용자 풀, 사용자 가져오기 작업, 리소스 서버 또는 자격 증명 공급자를 생성할 수 없습니다.
AWS Directory Service	Connect 및 WorkSpaces 서비스에는 다음 Directory Service 작업만 필요합니다. 다른 모든 디렉터리 서비스 작업은 개발자 모드 권한 경계 정책에 의해 거부됩니다. • ds:AuthorizeApplication • ds:CreateAlias • ds:CreateIdentityPoolDirectory • ds:DeleteDirectory • ds:DescribeDirectories • ds:GetAuthorizedApplication Details • ds:ListAuthorizedApplications • ds:UnauthorizeApplication 단일 계정 랜딩 존 계정에서 경계 정책은 개발 모드 활성화 계정에 대한 액세스를 유지하기 위해 AMS Advanced에서 사용하는 AMS Advanced 관리형 디렉터리에 대한 액세스를 명시적으로 거부합니다.
Amazon Elastic Compute Cloud	, DhcpOptions , Gateway, 및 문자열이 포함된 Amazon EC2 APIsSubnet에 액세스할 수 없습니다VPCVPN. AMS, ManagementHostASG , 및/또는 접두사가 붙은 태그가 있는 Amazon EC2 리소스mc에는 액세스하거나 수정할 수 없습니다sentinel.

서비스:	참고
Amazon EC2(보고서)	보기 액세스 권한만 부여됩니다(수정할 수 없음). 참고: Amazon EC2 보고서가 이동 중입니다. 보고서 메뉴 항목은 Amazon EC2 콘솔 탐색 메뉴에서 제거됩니다. Amazon EC2 사용 보고서를 제거한 후 보려면 AWS Billing 및 비용 관리 콘솔을 사용합니다.
AWS Identity and Access Management (IAM)	기존 권한 경계를 삭제하거나 IAM 사용자 암호 정책을 수정할 수 없습니다. 올바른 IAM 역할(`AWSManagedServices DevelopmentRole` MALZ의 경우 , `customer_developer_role` SALZ의 경우)을 사용하지 않는 한 IAM 리소스를 생성하거나 수정할 수 없습니다. `ams`, `mccustomer_deny_policy` , 및/또는 접두사가 붙은 IAM 리소스는 수정할 수 없습니다`sentinel`. 새 IAM 리소스(역할, 사용자 또는 그룹)를 생성할 때 권한 경계(MALZ: `AWSManagedServicesDevelopmentRolePermissionsBoundary` , SALZ: `ams-app-infra-permissions-boundary`)를 연결해야 합니다.
AWS Key Management Service (AWS KMS)	AMS 고급 관리형 KMS 키에 액세스하거나 수정할 수 없습니다.
AWS Lambda	접두사가 인 AWS Lambda 함수에는 액세스하거나 수정할 수 없습니다`AMS`.
CloudWatch Logs(CloudWatch 로그)	이름 앞에 `mc`, `lambda`, 및/또는 접두사가 붙은 CloudWatch 로그 스트림`aws`에 액세스할 수 없습니다`AMS`.

서비스:	참고
Amazon Relational Database Service(Amazon RDS)	이름이 접두사인 Amazon Relational Database Service(RDS) 데이터베이스(DBs)에는 액세스하거나 수정할 수 없습니다`mc-`.
AWS Resource Groups	`Get`, `List`및 `Search` 리소스 그룹 API 작업에만 액세스할 수 있습니다.
Amazon Route 53	Route53 AMS 고급 유지 관리 리소스에 액세스하거나 수정할 수 없습니다.
Amazon S3	`ams-*`, , `ams` `ms-a`또는 접두사가 붙은 이름이 있는 Amazon S3 버킷에는 액세스할 수 없습니다`mc-a`.
AWS Security Token Service	허용되는 유일한 보안 토큰 서비스 API는 입니다`DecodeAuthorizationMessage` .
Amazon SNS	이름이 접두사 `AMS-`, `Energon-Topic` 또는 인 SNS 주제에 액세스할 수 없습니다`MMS-Topic` .
AWS Systems Manager 관리자(SSM)	`ams`, `mc`또는 접두사가 붙은 SSM 파라미터는 수정할 수 없습니다`svc`. `ams` 또는 접두사가 붙은 태그가 있는 Amazon EC2 인스턴스`SendCommand` 에는 SSM API를 사용할 수 없습니다`mc`.
AWS 태그 지정	접두사가 인 AWS API 작업 태그 지정에만 액세스할 수 있습니다`Get`.

서비스:	참고
AWS Lake Formation	다음 AWS Lake Formation API 작업은 거부됩니다. • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	Elastic Inference API 작업 만 호출할 수 있습니다`elastic-inference:Connect` . 이 권한은에 `customer_sagemaker_admin_policy` 연결된에 포함됩니다`customer_sagemaker_admin_role` . 이 작업을 통해 Elastic Inference 액셀러레이터에 액세스할 수 있습니다.
AWS Shield	이 서비스 APIs 또는 콘솔에는 액세스할 수 없습니다.
Amazon Simple Workflow Service	이 서비스 APIs 또는 콘솔에는 액세스할 수 없습니다.

AMS 개발자 모드에서 인프라 프로비저닝

개발자 모드 IAM 역할이 없는 사용자는 개발자 모드가 활성화된 계정`AWSManagedServicesDevelopmentRole`에서 AMS Advanced AMIs. 올바른 역할(MALZ: `AWSManagedServicesDevelopmentRole`, SALZ: `customer_developer_role`)을 가진 사용자는 AMS Advanced 변경 관리 시스템 및 AMS Advanced AMIs 사용할 수 있지만 필수는 아닙니다.

> **Note**
>
> AWS AMS Advanced 워크로드 수집을 통해 처리되지 않았거나 AMS Advanced 계정에서 생성되지 않은 AMI에는 AMS Advanced 필수 구성이 포함되지 않습니다.

AMS 개발자 모드의 탐지 제어

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 AWS 아티팩트 시작하기를 참조하세요.

AMS 개발자 모드에서 로깅, 모니터링 및 이벤트 관리

AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에는 로깅, 모니터링 및 이벤트 관리를 사용할 수 없습니다.

AMS 개발자 모드에서의 인시던트 관리

인시던트 대응 시간은 변경되지 않습니다. 인시던트 해결은 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대한 최선의 작업입니다.

> **Note**
>
> AMS 서비스 수준 계약(SLA)은 AMS 변경 관리 시스템(변경 요청 또는 RFCs) 외부에서 생성되거나 업데이트된 리소스, 개발자 모드 포함에는 적용되지 않으므로 개발자 모드에서 업데이트되거나 생성된 리소스는 P3로 자동 저하되며 AMS 지원은 최선의 노력입니다.

AMS 개발자 모드에서 패치 관리

AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에는 패치 관리를 사용할 수 없습니다. 패치 적용 시간:

- 중요한 보안 업데이트의 경우: 변경 관리를 통해 프로비저닝된 후 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대해 공급업체가 릴리스한 후 영업일 기준 10일 이내.
- 중요한 업데이트의 경우: 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대해 공급업체가 릴리스한 후 2개월 이내.

AMS 개발자 모드에서 연속성 관리

AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에는 연속성 관리를 사용할 수 없습니다.

환경 복구 시작 시간은 AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 후 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스의 경우 최대 12시간이 걸릴 수 있습니다.

AMS 개발자 모드의 보안 및 액세스 관리

맬웨어 방지 보호는 AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대한 사용자의 책임입니다. AMS Advanced 변경 관리를 통해 프로비저닝되지 않은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 액세스는 페더레이션 액세스를 제공하는 대신 키 페어에 의해 제어될 수 있습니다.

AMS의 셀프 서비스 프로비저닝 모드

AWS Managed Services(AMS) 셀프 서비스 프로비저닝(SSP) 모드는 AMS 관리형 계정의 기본 AWS 서비스 및 API 기능에 대한 전체 액세스를 제공합니다. 표준화된 범위 축소 AWS Identity and Access Management 역할을 통해 서비스에 액세스합니다. AMS는 서비스 요청 및 인시던트 관리를 제공합니다. 알림, 모니터링, 로깅, 패치, 백업 및 변경 관리는 사용자의 책임입니다. 대부분의 경우 자체 서비스 프로비저닝 서비스(SSPS)는 자체 관리형 또는 서버리스 서비스이므로 패치 적용과 같은 특정 운영 작업을 관리할 필요가 없습니다. AMS 가드레일에 정의된 환경 경계 내에서 이러한 서비스를 사용하면 이점을 얻을 수 있으며, 플랫폼의 기본 보안을 유지하려면 모든 IAM 변경 사항(서비스 연결 역할, 서비스 역할, 교차 계정 역할 또는 정책 업데이트 포함)을 AMS Operations의 승인을 받아야 합니다. 템플릿을 활용하여 CloudFormation 이러한 서비스의 배포를 자동화할 수 있지만 모든 SSP 서비스에서 지원되지는 않습니다.

> **Important**
>
> AWS Managed Services(AMS) 계정에서 SSP 모드를 사용하여 명시된 제한 사항에 따라 AWS 서비스에 액세스하고 서비스를 사용할 수 있습니다.

AMS 계정에는 AMS 관리 없이 사용할 수 AWS 서비스 있는 몇 가지가 있습니다. 셀프 서비스 프로비저닝 모드 서비스 또는 간단히 말해 SSPS, AMS 계정에 추가하는 방법 및 각 서비스에 대한 FAQs는 섹션에 설명되어 있습니다.

셀프 서비스 프로비저닝 서비스는 있는 그대로 제공되며 사용자는 이를 관리할 책임이 있습니다. AMS는 해당 서비스와 연결된 리소스에 대한 알림, 모니터링, 로깅 또는 패치를 제공하지 않습니다. AMS는 AMS 계정에서 서비스를 안전하게 사용할 수 있는 IAM 역할을 제공합니다. AMS SLAs는 적용되지 않습니다.

셀프 서비스를 통해 프로비저닝하는 리소스의 경우 AMS는 인시던트 관리, 탐지 제어 및 가드레일, 보고, 지정된 리소스(Cloud Service Delivery Manager 및 Cloud Architect), 보안 및 액세스, 서비스 요청을 통한 기술 지원을 제공합니다. 또한 해당하는 경우 AMS 변경 관리 시스템 외부에서 프로비저닝되거나 구성된 리소스의 연속성 관리, 패치 관리, 인프라 모니터링 및 변경 관리에 대한 책임을 집니다.

AMS에서 SSP 모드 시작하기

셀프 서비스 프로비저닝은 사용할 수 있는 다중 계정 랜딩 존(MALZ)의 AMS 모드 중 하나입니다. 자세한 내용은 모드 개요 단원을 참조하십시오.

셀프 서비스 프로비저닝 기능을 제공하기 위해 AMS는 권한 경계가 있는 승격된 IAM 역할을 생성하여 직접 AWS 서비스 액세스에서 의도하지 않은 변경을 제한했습니다. 역할이 모든 변경 사항을 방지하는 것은 아니며, 내부 제어 및 규정 준수 정책을 준수하고 사용 AWS 서비스 중인 모든가 필수 인증을 충족하는지 확인해야 합니다. 셀프 서비스 프로비저닝 모드입니다. AWS 규정 준수 요구 사항에 대한 자세한 내용은 AWS 규정 준수를 참조하세요.

다중 계정 랜딩 존 애플리케이션 계정에 셀프 서비스 프로비저닝 서비스를 추가하려면 서비스에 대한 지침에 따라 검토가 필요한 CT 또는 자동 CT인 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형(CT) 추가를 사용합니다.

> **Note**
>
> AMS가 추가 셀프 서비스 프로비저닝 서비스를 제공하도록 요청하려면 서비스 요청을 제출합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon API Gateway 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon API Gateway 기능에 직접 액세스할 수 있습니다. Amazon API Gateway는 어떤 규모에서든 개발자가 API를 손쉽게 생성, 게시, 유지 관리, 모니터링 및 보호할 수 있도록 지원하는 완전관리형 서비스입니다. 를 사용하면 애플리케이션이 Amazon Elastic Compute Cloud(Amazon EC2)에서 실행되는 워크로드,에서 실행되는 코드, AWS Lambda웹 애플리케이션 또는 실시간 통신 애플리케이션과 같은 백엔드 서비스에서 데이터, 비즈니스 로직 또는 기능에 액세스할 수 있는 문 역할을 하는 REST 및 WebSocket APIs를 생성할 AWS Management Console 수 있습니다.

API Gateway는 트래픽 관리, 권한 부여 및 액세스 제어, 모니터링 및 API 버전 관리를 포함하여 최대 수십만 개의 동시 API 호출을 수락하고 처리하는 데 관련된 모든 작업을 처리합니다. API Gateway에는 최소 요금이나 시작 비용이 없습니다. 수신한 API 호출과 전송된 데이터 양에 대해서만 비용을 지불하며, API Gateway 계층형 요금 모델을 사용하면 API 사용량이 확장됨에 따라 비용을 절감할 수 있습니다. 자세한 내용은 Amazon API Gateway를 참조하세요.

FAQ: AMS의 API Gateway

Q: AMS 계정에서 Amazon API Gateway에 대한 액세스를 요청하려면 어떻게 해야 합니까?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct)
변경 유형을 사용하여 RFC를 제출하여 API Gateway에 대한 액세
스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니
다`customer_apigateway_author_rolecustomer_apigateway_cloudwatch_role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon API Gateway를 사용할 때 제한 사항은 무엇인가요?

- API Gateway 구성은 AMS 인프라에 대한 수정을 방지하기 위해 `AMS-` 또는 `MC-` 접두사가 없는 리소스로 제한됩니다.
- `CREATE` Elastic Load Balancer의 무단 생성을 방지하기 위해 VPCLink에 대한 권한이 비활성화됩니다. VPCLinks 필요한 경우 Application Load Balancer | 생성을 참조하세요.

Q: AMS 계정에서 Amazon API Gateway를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

배포하려는 API Gateway 유형에 따라 다릅니다. 독립 실행형 서비스일 수도 있지만 기존 서비스(예: 네트워크 로드 밸런서)에 대한 액세스를 요청할 수도 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Alexa for Business 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Alexa for Business 기능에 직접 액세스할 수 있습니다. Alexa for Business는 조직과 직원이 Alexa를 사용하여 더 많은 작업을 수행할 수 있는 서비스입니다. Alexa for Business를 사용하면 Alexa를 지능형 어시스턴트로 사용하여 회의실, 책상, 심지어 집이나 이동 중에 이미 사용 중인 Alexa 디바이스에서도 생산성을 높일 수 있습니다. IT 및 시설 관리자는 Alexa for Business를 사용하여 직장 내 기존 회의실의 사용률을 측정하고 늘릴 수 있습니다.

자세한 내용은 Alexa for Business를 참조하세요.

AWS Managed Services FAQ의 Alexa for Business

Q: AMS 계정에서 Alexa for Business에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_alexa_console_role`. Alexa for Business에서 제공하는 디바이스 설정 도구에 대한 `customer_alexa_device_setup_user`도 생성됩니다. 그러면이 디바이스 설정 도구를 사용하여 디바이스를 설정할 수 있습니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Alexa for Business 게이트웨이를 사용하면 Alexa for Business를 Cisco Webex 및 Poly Group Series 엔드포인트에 연결하여 음성으로 회의를 제어할 수 있습니다. 게이트웨이 소프트웨어는 온프레미스 하드웨어에서 실행되며 Alexa for Business에서 Cisco 엔드포인트로 회의 지시문을 안전하게 프록시합니다. 게이트웨이가 Alexa for Business와 통신하려면 두 쌍의 AWS 자격 증명이 필요합니다. 제한된 액세스 IAM 사용자 2개를 제공합니다. `customer_alexa_gateway_installer_user` Alexa for Business 게이트웨이`customer_alexa_gateway_execution_user`의 경우 게이트웨이를 설치하기 위한 사용자와 게이트웨이를 작동하기 위한 사용자입니다. 이들은 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(관리형 자동화) 변경 유형(ct-3dpd8mdd9jn1r)이 포함된 RFC를 제출하여 요청할 수 있습니다.

> **Note**
>
> 사용 보고서를 생성하여 Amazon S3로 보내려면 자체 프로비저닝된 서비스 RFC에 Amazon S3 버킷 이름을 지정합니다.

Q: AMS 계정에서 Alexa for Business를 사용하는 데 따르는 제한 사항은 무엇인가요?

제한은 없습니다. Alexa for Business의 전체 기능은 Alexa for Business 자체 프로비저닝 서비스 역할에서 사용할 수 있습니다.

Q: AMS 계정에서 Alexa for Business를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- WPA2 Enterprise Wi-Fi를 사용하여 공유 디바이스를 설정하려는 경우 AWS Private Certificate Authority 가 필요한 디바이스 설정 도구에서이 네트워크 보안 유형을 지정합니다.
- AMS는 네임스페이스 "A4B"로 시작하는 보안 키만 생성합니다. 이는이 네임스페이스에만 제한됩니다.

Q: Alexa for Business 기능에는 별도의 RFCs 필요합니까?

Alexa Voice Service(AVS) 디바이스를 Alexa for Business에 등록하려면 Alexa 내장 디바이스 메이커에 대한 액세스를 제공합니다. 이렇게 하려면 Alexa for Business 콘솔에서 관리 | 기타 | 기타 변경 유형을 사용하여 배포할 수 있는 IAM 역할을 생성해야 합니다. 이를 통해 AVS 디바이스 제조업체는 사용자를 대신하여 Alexa for Business에 디바이스를 등록하고 관리할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon WorkSpaces 애플리케이션 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon WorkSpaces 애플리케이션(WorkSpaces 애플리케이션) 기능에 액세스할 수 있습니다. WorkSpaces 애플리케이션을 사용하면 데스크톱 애플리케이션을 다시 작성 AWS하지 않고도 로 이동할 수 있습니다. WorkSpaces 애플리케이션에 애플리케이션을 설치하고, 시작 구성을 설정하고, 사용자가 애플리케이션을 사용할 수 있도록 할 수 있습니다. WorkSpaces 애플리케이션은 다양한 가상 머신 옵션을 제공하므로 애플리케이션 요구 사항에 가장 적합한 인스턴스 유형을 선택하고 자동 크기 조정 파라미터를 설정하여 최종 사용자의 요구 사항을 쉽게 충족할 수 있습니다. WorkSpaces 애플리케이션을 사용하면 자체 네트워크에서 애플리케이션을 시작할 수 있습니다. 즉, 애플리케이션이 기존 AWS 리소스와 상호 작용할 수 있습니다.

Amazon WorkSpaces 애플리케이션을 사용하면 이미지 빌더를 사용하여 애플리케이션을 빠르고 쉽게 설치, 테스트 및 업데이트할 수 있습니다. Microsoft Windows Server 2012 R2, Windows Server 2016 또는 Windows Server 2019에서 실행되는 모든 애플리케이션이 지원되므로 수정할 필요가 없습니다. 테스트가 완료되면 애플리케이션 시작 구성, 기본 사용자 설정을 설정하고 사용자가 액세스할 수 있도록 이미지를 게시할 수 있습니다.

자세한 내용은 WorkSpaces 애플리케이션을 참조하세요.

AWS Managed Services WorkSpaces 애플리케이션 FAQ

Q: AMS 계정에서 WorkSpaces 애플리케이션에 대한 액세스를 요청하려면 어떻게 해야 합니까?

Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출하여 WorkSpaces 애플리케이션에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_appstream_console_role`.

또한 `customer_appstream_stream_role`는 Active Directory 로그인 자격 증명을 사용하여 사용자를 인증해야 하는 애플리케이션을 스트리밍하도록 배포됩니다.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 WorkSpaces 애플리케이션 사용에 대한 제한 사항은 무엇인가요?

- 다음 기능은 AMS Support 팀에서 구성해야 하며 특정 RFCs 필요합니다. 추가 기능 요청에 대한 지침은 섹션 4에서 확인할 수 있습니다.
  - 인터페이스 VPC 엔드포인트에서 생성 및 스트리밍.
  - 프라이빗 네트워크에서 홈 폴더 및 애플리케이션 설정 지속성을 위한 Amazon S3 엔드포인트를 지원합니다.
  - 모든 플릿 스트리밍 인스턴스에서 사용할 수 있는 IAM 역할을 생성하고 선택합니다.
  - WorkSpaces 애플리케이션 플릿 및 이미지 빌더 Microsoft Active Directory 도메인 조인.
  - WorkSpaces 애플리케이션 사용자 지정 사용 보고서 생성.
  - 사용자 지정 브랜딩은 현재 지원되지 않습니다.

Q: AMS 계정에서 WorkSpaces 애플리케이션을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

WorkSpaces 애플리케이션을 온보딩하기 위해 RFC를 제출하는 동안 WorkSpaces 애플리케이션 사용 보고서에 사용할 Amazon S3 버킷 이름을 포함합니다. 버킷 이름은 WorkSpaces 애플리케이션이 온보딩`customer-appstream-usagereports-policy`될 때 생성되는에 추가됩니다.

Q: 별도의 RFCs 필요한 WorkSpaces 애플리케이션 기능은 무엇입니까?

- WorkSpaces 애플리케이션에 대한 인터페이스 VPC 엔드포인트를 선택하려면 관리 | 기타 | 기타 | 변경 유형 업데이트 RFC를 제출하여 계정에 VPC 엔드포인트를 생성합니다. WorkSpaces 애플리케이션에 대한 사용자 지정 엔드포인트를 생성하는 단계는 WorkSpaces 애플리케이션 사용 설명서의 인터페이스 VPC 엔드포인트에서 생성 및 스트리밍을 참조하세요.

- 관리 | 기타 | 기타 | 변경 유형 생성 RFC를 사용하여 Amazon S3 VPC 엔드포인트를 요청하여 프라이빗 네트워크에서 홈 폴더 및 애플리케이션 설정 지속성에 대한 Amazon S3 엔드포인트 지원을 구성할 수 있습니다. RFC에는 홈 폴더 콘텐츠를 호스팅하는 대상 Amazon S3 버킷 또는 애플리케이션 설정 Amazon S3 버킷이 각각 포함되어야 합니다. 이 RFC는 WorkSpaces 애플리케이션에 Amazon S3 VPC 엔드포인트에 액세스하는 데 필요한 권한을 제공합니다. 스트림에 대한 사용자 지정 엔드포인트를 생성하는 단계는 WorkSpaces 애플리케이션 사용 설명서의 홈 폴더에 Amazon S3 VPC 엔드포인트 사용 및 애플리케이션 설정 지속성을 참조하세요. WorkSpaces
- 모든 플릿 스트리밍 인스턴스에서 사용할 수 있는 IAM 역할을 생성하고 선택하려면 필요한 정책을 사용하여 IAM 역할을 요청하는 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 생성(관리형 자동화) 변경 유형(ct-3dpd8mdd9jn1r) RFC를 제출합니다. IAM 역할 이름은 항상 접두사 "customer_appstream"으로 시작해야 합니다.
- Amazon WorkSpaces 애플리케이션 플릿 및 이미지 빌더는 Active Directory(AD)에서 서비스 계정 생성을 위한 관리 | 기타 | 기타 | 업데이트 변경 유형 RFC를 제출하여 Microsoft Active Directory의 도메인에 조인할 수 있습니다. Microsoft Active Directory에 조인하는 데 필요한 최소 권한은 WorkSpaces 애플리케이션 설명서의 Active Directory 컴퓨터 객체를 생성하고 관리할 수 있는 권한 부여에 정의되어 있습니다.
- 사용자 지정 WorkSpaces 애플리케이션 사용 보고서를 생성하려면 다음을 요청하는 관리 | 기타 | 기타 | 변경 유형 생성 RFC를 제출합니다.
  - "AppStreamUsageReports" CFN 스택 생성
  - 계정에서 "customer_appstream_usagereports_role" 프로비저닝
  - 또한 다음 세부 정보를 제공합니다.
    - CRON 표현식을 제공하여 크롤러 실행을 예약합니다. 기본적으로 매일 23:00 UTC입니다.
    - Athena 쿼리 결과에 사용할 Amazon S3 버킷 ARN입니다. 이 버킷에는 접두사가 있어야 합니다. `aws-athena-query-results`
    - WorkSpaces 애플리케이션용 Amazon S3 버킷 ARN 사용 보고서 로그.

  역할이 프로비저닝된 후 역할을 페더레이션 솔루션에 온보딩하고 로그인한 다음 사용 보고서 역할을 사용하여 사용자 지정 보고서를 생성하기 위해 AWS GlueAWS Glue 및 Athena에 액세스합니다. WorkSpaces 애플리케이션 사용 보고서 사용에 대한 자세한 내용은 WorkSpaces 애플리케이션 설명서의 사용자 지정 보고서 생성 및 WorkSpaces 애플리케이션 사용 데이터 분석을 WorkSpaces.

AMS SSP를 사용하여 AMS 계정에서 Amazon Athena 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Athena(Athena) 기능에 직접 액세스할 수 있습니다. Athena는 표준 SQL을 사용하여 Amazon S3의 데이터를 분석하는

데 도움이 되는 대화형 쿼리 서비스입니다. Athena는 서버리스 서비스이므로 관리할 인프라가 없으며 실행한 쿼리에 대해서만 비용을 지불하면 됩니다. Amazon S3의 데이터를 가리키고 스키마를 정의한 다음 표준 SQL을 사용하여 쿼리를 시작합니다. 대부분의 결과는 몇 초 내에 전달됩니다. Athena를 사용하면 분석을 위해 데이터를 준비하는 데 복잡한 ETL(추extract-transform-load) 작업이 필요하지 않습니다. 따라서 SQL 기술을 보유한 모든 사용자가 대규모 데이터 세트를 빠르게 분석할 수 있습니다. 자세한 내용은 Amazon Athena를 참조하세요.

FAQ: AMS의 Athena

Q: AMS 계정에서 Amazon Athena에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Athena에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_athena_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Athena를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Athena의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Athena를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Athena는 로 생성된 데이터 카탈로그/메타스토어를 사용하므로 AWS Glue 서비스에 대한 주요 종속성이 있습니다 AWS Glue. 따라서 AWS Glue 권한은 성공적인 Athena RFC에 포함됩니다.

역할에는 Amazon S3 버킷`customer_athena_console_role`에 대한 사전 조건이 있습니다. 새 버킷을 생성하려면 자동 CT`ct-1a68ck03fn98r`(배포 | 고급 스택 구성 요소 | S3 스토리지 | 생성)를 사용합니다. 이 자동 CT를 사용하여 Athena용 S3 버킷을 생성하는 경우 버킷 이름은 접두사 로 시작해야 합니다`athena-query-results-*`.

AMS SSP를 사용하여 AMS 계정에서 Amazon Bedrock 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Bedrock 기능에 직접 액세스할 수 있습니다. Amazon Bedrock은 선도적인 AI 스타트업에서 고성능 파운데이션 모델(FMs)을 만들고 통합 API를 통해 사용할 AWS 수 있는 완전관리형 서비스입니다. 다양한 파운데이션 모델 중에서 선택하여 사용 사례에 가장 적합한 모델을 찾을 수 있습니다. 또한 Amazon Bedrock은 보안, 프라이버시 및 책임감 있는 AI를 갖춘 생성형 AI 애플리케이션을 구축할 수 있는 다양한 기능을 제공합니다. Amazon Bedrock을 사용하면 사용 사례에 맞는 최고 수준의 파운데이션 모델을 쉽게 실험 및 평가하고, 미세 조정 및 검색 증강 생성(RAG)과 같은 기술로 데이터를 사용하여 프라이빗으로 사용

자 지정하고, 엔터프라이즈 시스템 및 데이터 소스를 사용하여 작업을 실행하는 에이전트를 구축할 수 있습니다.

Amazon Bedrock의 서버리스 환경을 사용하면 인프라를 관리할 필요 없이 AWS 도구를 사용하여 파운데이션 모델을 빠르고 비공개로 사용자 지정하고 애플리케이션을 쉽고 안전하게 통합 및 배포할 수 있습니다. 자세한 내용은 Amazon Bedrock을 참조하세요.

FAQ: AMS의 Amazon Bedrock

Q: AMS 계정에서 Amazon Bedrock에 대한 액세스를 요청하려면 어떻게 해야 합니까?

Amazon Bedrock에 대한 액세스를 요청하려면 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_bedrock_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Bedrock을 사용할 때 제한 사항은 무엇인가요?

- Amazon Bedrock 지식 기반은 현재 AMS에서 지원되지 않는 Amazon OpenSearch Service Serverless에 대한 종속성으로 인해 SSPS 역할의 일부로 기본적으로 지원되지 않습니다.
- Bedrock Studio는 Amazon DataZone과 같은 지원되지 않는 서비스에 대한 종속성으로 인해 지원되지 않습니다.

Q: AMS 계정에서 Amazon Bedrock을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- AWS Marketplace 권한이 필요한 타사 모델 구독은 기본 역할 (`AWSManagedServicesAdminRole`MALZ의 경우 , SALZ`Customer_ReadOnly_Role`의 경우)로 수행해야 합니다. 이는 기본 역할에 AWS Marketplace 권한이 포함되기 때문입니다.
- 데이터 암호화를 사용하는 경우 콘솔 역할 생성을 요청할 때 AWS KMS 키 ARN을 제공해야 합니다. 또한 사용 중인 Amazon S3 버킷의 이름에 “bedrock”이 있어야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon CloudSearch 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon CloudSearch 기능에 직접 액세스할 수 있습니다. Amazon CloudSearch는 웹 사이트 또는 애플리케이션에 대한 검색 솔루션을 비용 효율적으로 설정, 관리 및 확장하는 데 사용하는 AWS 클라우드의 관리형 서비스입니다. Amazon CloudSearch는 강조 표시, 자동 완성 및 지리 공간 검색과 같은 34개 언어와 인기 있는 검색 기능을 지원합니다. 자세한 내용은 Amazon CloudSearch를 참조하세요.

> **Note**
>
> AWS 는 2024년 7월 25일부터 Amazon CloudSearch에 대한 새로운 고객 액세스를 종료했습니다. Amazon CloudSearch 기존 고객은 서비스를 정상적으로 계속 사용할 수 있습니다. AWS는 계속해서 Amazon CloudSearch의 보안, 가용성 및 성능 개선에 투자하지만 새로운 기능을 도입할 계획은 없습니다.
> Amazon CloudSearch와 Amazon OpenSearch Service의 차이점과 OpenSearch Service로 전환하는 방법을 이해하려면 클라우드 아키텍트(CA)에 문의하여 지침을 받으세요. OpenSearch Service로 전환하는 방법에 대한 자세한 내용은 Amazon CloudSearch에서 Amazon OpenSearch Service 서비스로 전환을 참조하세요.

AWS Managed Services FAQ의 Amazon CloudSearch

Q: AMS 계정에서 Amazon CloudSearch에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon CloudSearch에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_csearch_admin_role`customer_csearch_dev_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon CloudSearch를 사용하는 데 따르는 제한 사항은 무엇인가요?

Amazon CloudSearch의 전체 기능은 AMS 계정에서 사용할 수 있습니다. 모든 AMS 지원 데이터베이스 솔루션은 현재 Amazon CloudSearch에서 지원됩니다. 현재 DynamoDB는 인덱싱할 수 없는 유일한 관리형 AWS 데이터베이스 솔루션입니다.

Q: AMS 계정에서 Amazon CloudSearch를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon CloudSearch는 Amazon S3가 자격 증명 공급자와 협력하여 입력 데이터를 자동으로 분석하고 테이블 필드를 결정하는 데 의존합니다. Amazon S3에 대한 액세스는이 RFC와 함께 제공되지 않으므로 서비스 요청에서 별도로 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon CloudWatch Synthetics 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon CloudWatch Synthetics 기능에 직접 액세스할 수 있습니다. Amazon CloudWatch Synthetics를 사용하여 'canary'를 생성하여 엔드포인트와 APIs 모니터링할 수 있습니다.

카나리아는 일정에 따라 실행되는 Node.js 또는 Python으로 작성된 구성 가능한 스크립트입니다. Node.js 또는 Python을 프레임워크로 사용하는 Lambda 함수를 계정에 생성합니다. canary는 HTTP 프로토콜과 HTTPS 프로토콜 모두에서 작동합니다. 카나리아는 엔드포인트의 가용성과 지연 시간을 확인하고 로드 시간 데이터와 UI 스크린샷을 저장할 수 있습니다. REST API, URL 및 웹사이트 콘텐츠를 모니터링하고 피싱, 코드 주입 및 교차 사이트 스크립팅으로 인한 무단 변경 사항을 검사할 수 있습니다.

카나리아는 고객과 동일한 경로를 따르고 동일한 작업을 수행하므로 애플리케이션에 고객 트래픽이 없는 경우에도 고객 경험을 지속적으로 확인할 수 있습니다. 카나리를 사용하면 고객보다 먼저 문제를 발견할 수 있습니다. 자세한 내용은 Amazon CloudWatch: 합성 모니터링 사용을 참조하세요.

AWS Managed Services FAQ의 Amazon CloudWatch Synthetics

Q: AMS 계정에서 Amazon CloudWatch Synthetics에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon CloudWatch Synthetics에 대한 액세스를 요청합니다. 이 RFC는 계정에 'customer_cw_synthetics_console_role' 및 'customer_cw_synthetics_canary_lambda_role'이라는 IAM 역할을 프로비저닝합니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 'customer_cw_synthetics_console_role' 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon CloudWatch Synthetics를 사용할 때 제한 사항은 무엇인가요?

AMS 계정에서 Amazon CloudWatch Synthetics를 사용하는 데는 제한이 없습니다. AMS 제공 서비스 역할 'customer_cw_synthetics_canary_lambda_role' 외부에서 canary에 대한 역할을 생성하는 것은 금지됩니다.

Q: AMS 계정에서 Amazon CloudWatch Synthetics를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

카나리아는 기본 Amazon CloudWatch Synthetics S3 버킷 "cw-syn-results-*${accountnumber}*-*${default-region}*"을 생성하고 사용합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Cognito 사용자 풀 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Cognito 사용자 풀 기능에 직접 액세스할 수 있습니다. Amazon Cognito 사용자 풀은 수억 명의 사용자로 확장되는 안전한 사용자 디렉터리를 제공합니다. 완전 관리형 서비스인 Amazon Cognito 사용자 풀은 서버 인프

라 구축에 대한 걱정 없이 설정할 수 있습니다. 이 서비스를 사용하면 내부 애플리케이션과 통합하는 데 사용할 수 있는 최종 사용자 풀을 관리할 수 있습니다. 이 서비스는 웹 또는 모바일 애플리케이션을 위한 사용자 지정 데이터베이스 또는 최종 사용자 디렉터리의 대안을 제공합니다. 동시에 Amazon Cognito 사용자 풀은 암호 정책, 다중 인증, 암호 복구 및 서비스 자체 가입과 같은 디렉터리 서비스의 전체 기능 세트를 제공합니다. 또한 애플리케이션이 OpenID, Facebook, Amazon 또는 Google과 같은 다른 인기 있는 퍼블릭 서비스에서 액세스를 페더레이션할 수 있습니다.

Amazon Cognito는 두 가지 주요 제품으로 나뉩니다. Amazon Cognito 사용자 풀 및 Amazon Cognito 자격 증명 공급자. 이 섹션에서는 Amazon S3 또는 DynamoDB와 같은 다른 서비스에 대한 액세스를 제공하는 Amazon Cognito 사용자 풀에 중점을 둡니다. AWS Amazon S3 DynamoDB 이 서비스를 사용하면 Amazon Cognito 사용자 풀 또는 타사 자격 증명 공급자를 사용하여 AWS 서비스에 대한 액세스를 제공할 수 있습니다. 또한 익명 게스트 액세스를 사용하여 AWS 서비스에 대한 액세스를 제공합니다. Amazon Cognito 사용자 풀의 강력한 특성으로 인해 계정의 잠재적 보안 중단을 방지하기 위해 운영 수동 서비스로 case-by-case 수동으로 관리됩니다. 자세한 내용은 Amazon Cognito 사용자 풀을 참조하세요.

AWS Managed Services FAQ의 Amazon Cognito 사용자 풀

일반적인 질문과 답변:

Q: AMS 계정의 Amazon Cognito 사용자 풀에 대한 액세스를 요청하려면 어떻게 해야 합니까?

AMS에서 Amazon Cognito 사용자 풀의 구현은 2단계 프로세스입니다.

1. 관리 제출 | 기타 | 기타 | (ct-1e1xtak34nx76) 변경 유형을 생성하고 AMS 계정에서 Amazon Cognito 사용자 풀 생성을 요청합니다. 다음 정보를 포함합니다.
   - AWS 리전.
   - Cognito 사용자 풀의 이름입니다.
   - Amazon Simple Email Service(Amazon SES)를 사용하여 기본 내부 Cognito 메일 서비스 대신 메시지 및 알림을 보내려는 경우 고객은 계정에서 Amazon SES Service에 대해 이미 검증된 이메일 주소를 제공해야 합니다. 이 주소는 메시지의 "From" 및 "REPLY-TO" 필드에 사용됩니다. 또한 Amazon SES가 활성화된 리전(us-east-1, eu-west-1 또는 us-west-2)을 표시해야 합니다.
   - 가 일회용 암호 및 확인에 SMS 메시지를 사용하려는 경우 고객은 이를 표시해야 합니다.
2. 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 사용자 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_cognito_admin_role`.`customer_cognito_importjob_role` 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다. 이러한 역할을 사용하면 Amazon Cognito 사용자 풀을 관리하고, 풀에서 사용자 및 그룹을 관리하고, 사용자를 위한 가져오기 작업을

생성하고, 알림 및 구독 메시지를 수정하고, 애플리케이션을 사용자 풀에 연결하고, 풀에 페더레이션 서비스를 추가하고, 이미 생성된 풀을 삭제할 수 있습니다.

Q: AMS 계정의 Amazon Cognito 사용자 풀 사용에 대한 제한 사항은 무엇인가요?

Amazon Cognito 사용자 풀을 생성할 수 없습니다. 이 작업을 수행하려면 Amazon SES 및 Amazon Simple Notification Service(SNS)와 같이 Amazon Cognito에서 사용하는 서비스를 활용하기 위한 IAM 역할을 생성해야 합니다.Amazon SNS

Q: AMS 계정에서 Amazon Cognito 사용자 풀을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon SES를 사용하여 사용자 풀에 이메일로 메시지와 알림을 보내려면 계정에서 Amazon SES 서비스를 이미 활성화하고 전송된 이메일의 "FROM" 및 "REPLY-TO" 필드에 사용해야 하는 이메일 주소를 이미 검증해야 합니다. Amazon SES를 사용하여 이메일 주소를 검증하는 방법에 대한 자세한 내용은 Amazon SES에서 이메일 주소 확인을 참조하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon Comprehend 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Comprehend 기능에 직접 액세스할 수 있습니다. Amazon Comprehend는 기계 학습을 사용하여 텍스트에서 인사이트와 관계를 찾는 자연어 처리(NLP) 서비스이므로 기계 학습 경험이 필요하지 않습니다. Amazon Comprehend는 기계 학습을 사용하여 비정형 데이터의 인사이트와 관계를 발견하는 데 도움이 됩니다. 이 서비스는 텍스트의 언어를 식별하고, 주요 문구, 장소, 사람, 브랜드 또는 이벤트를 추출하고, 텍스트가 얼마나 긍정적이거나 부정적인지 이해하고, 토큰화 및 음성 부분을 사용하여 텍스트를 분석하고, 주제별로 텍스트 파일 모음을 자동으로 구성합니다. Amazon Comprehend에서 AutoML 기능을 사용하여 조직의 요구 사항에 맞게 고유하게 조정된 사용자 지정 엔터티 또는 텍스트 분류 모델 세트를 구축할 수도 있습니다. 자세한 내용은 Amazon Comprehend를 참조하세요.

AWS Managed Services FAQ의 Amazon Comprehend

Q: AMS 계정에서 Amazon Comprehend에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Amazon Comprehend 콘솔 및 데이터 액세스 역할은 두 개의 AMS Service RFCs.

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_comprehend_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Comprehend를 사용할 때 제한 사항은 무엇인가요?

Amazon Comprehend 콘솔을 통한 새 IAM 역할 생성 기능은 제한됩니다. 그렇지 않으면 AMS 계정에서 Amazon Comprehend의 전체 기능을 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Comprehend를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon S3 버킷이 AWS KMS 키로 암호화된 경우 Amazon Comprehend를 사용하려면 Amazon S3 및 AWS Key Management Service (AWS KMS)가 필요합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Connect 프로비저닝

> **Note**
>
> 신중한 고려 끝에 2026년 5월 20일부터 Amazon Connect Voice ID에 대한 지원을 종료하기로 결정했습니다. Amazon Connect Voice ID는 2025년 5월 20일부터 더 이상 신규 고객을 받지 않습니다. 2025년 5월 20일 이전에 서비스에 가입한 계정이 있는 기존 고객은 Amazon Connect Voice ID 기능을 계속 사용할 수 있습니다. 2026년 5월 20일 이후에는 Amazon Connect Voice ID를 더 이상 사용할 수 없습니다.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Connect 기능에 직접 액세스할 수 있습니다. Amazon Connect는 기업이 더 저렴한 비용으로 우수한 고객 서비스를 제공할 수 있도록 지원하는 옴니채널 클라우드 고객 센터입니다. Amazon Connect는 고객과 에이전트에게 음성 및 채팅 전반에 걸쳐 원활한 경험을 제공합니다. 여기에는 기술 기반 라우팅, 강력한 실시간 및 기록 분석, easy-to-use 직관적인 관리 도구를 위한 도구 세트가 포함되며, 모두 pay-as-you-go 요금이 적용됩니다.

AMS 다중 계정 랜딩 존 또는 단일 계정 랜딩 존 계정에서 가상 고객 센터 인스턴스의 인스턴스를 하나 이상 생성할 수 있습니다. 에이전트 액세스에 기존 SAML 2.0 자격 증명 공급자를 사용하거나 사용자 수명 주기 관리에 Amazon Connect 기본 지원을 사용할 수 있습니다.

또한 Amazon Connect 콘솔에서 각 Amazon Connect 인스턴스의 수신자 부담/직통 전화번호를 신청할 수 있습니다. easy-to-use 그래픽 사용자 인터페이스를 사용하여 풍부한 고객 응대 흐름을 생성하여 원하는 고객 경험과 라우팅을 달성할 수 있습니다. 고객 응대 흐름은 AWS Lambda 함수를 활용하여 온프레미스 데이터 스토어 및 API와 통합할 수 있습니다. Kinesis Streams 및 Firehose를 사용하여 데이터 스트리밍을 활성화할 수도 있습니다.

통화 녹음, 채팅 트랜스크립트 및 보고서는 AWS KMS 키를 사용하여 암호화된 Amazon S3 버킷에 저장됩니다. 고객 응대 흐름 로그는 CloudWatch 로그 그룹에 저장할 수 있습니다.

자세한 내용은 Amazon Connect를 참조하세요.

AWS Managed Services의 Amazon Connect FAQ

Q: AMS 계정에서 Amazon Connect에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_connect_console_role`.`customer_connect_user_role` 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Connect를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Connect의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Connect를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 표준 AMS RFCs를 사용하여 AWS KMS 키와 Amazon S3 버킷을 생성해야 합니다. 통화 녹음 및 채팅 기록을 저장하려면 Amazon S3 버킷이 필요합니다.
- Active Directory(AD)와 통합하려면 AMS 호스팅 Amazon Connect 인스턴스와 온프레미스 디렉터리 서비스 간의 통합에 AD 커넥터가 필요합니다. AD 커넥터는 '관리 | 기타 | 기타' RFC를 요청하여 계정에서 구성할 수 있습니다.
- 고객 응대 흐름 요구 사항에 따라 다음과 같은 선택적 자체 프로비저닝 서비스를 활성화할 수 있습니다.
  - AWS Lambda: Lambda 함수를 사용하여 고객 응대 흐름을 확장하여 기존 온프레미스 데이터 스토어 또는 APIs. Lambda 자체 프로비저닝 서비스를 사용하여 Lambda 함수를 생성할 수 있습니다.
  - Amazon Kinesis Data Streams: 데이터 스트림을 생성하여 외부 애플리케이션으로 데이터 스트리밍을 활성화할 수 있습니다. 고객 응대 추적 레코드 또는 에이전트 이벤트를 스트리밍할 수 있습니다.
  - Amazon Kinesis Data Firehose: Data Firehose를 생성하여 대용량 고객 응대 추적 레코드를 외부 애플리케이션으로 스트리밍할 수 있습니다.
  - Amazon Lex: Amazon Lex Chatbots를 활용하여 풍부한 고객 경험과 자동화를 위해 Amazon Alexa 서비스를 활용하는 스마트 고객 응대 흐름을 생성할 수 있습니다.
- Q: 아웃바운드 또는 인바운드 통화에 대한 국가 목록을 추가하도록 요청하려면 어떻게 해야 합니까?

  아웃바운드 또는 인바운드 통화 국가 목록을 추가하려면 AMS에 서비스 요청을 제출합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Data Firehose 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Data Firehose 기능에 직접 액세스할 수 있습니다. Firehose는 스트리밍 데이터를 데이터 레이크, 데이터 스토어 및 분석 도구로 안정적으로 로드하는 가장 쉬운 방법입니다. 스트리밍 데이터를 캡처하고 변환하여 Amazon S3, Amazon Redshift, Amazon OpenSearch Service 및 Splunk로 로드할 수 있으므로 현재 이미 사용 중인 기존 비즈니스 인텔리전스 도구 및 대시보드를 사용하여 거의 실시간으로 분석할 수 있습니다. 완전 관리형 서비스로서 데이터 처리량에 대응하여 자동으로 확장되며 지속적인 관리가 필요 없습니다. 또한, 데이터를 로드하기 전에 배치, 압축, 변환 및 암호화하여 대상 스토리지의 사용량을 최소화하고 보안을 강화할 수 있습니다. 자세한 내용은 Amazon Data Firehose란 무엇입니까?를 참조하세요.

AWS Managed Services FAQ의 Firehose

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Data Firehose에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_kinesis_firehose_user_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Firehose를 사용할 때 적용되는 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Data Firehose의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Firehose를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

각 전송 스트림에 대해 새 서비스 연결 IAM 역할을 요청해야 합니다. 필요한 리소스 권한(S3 버킷/KMS 키/Lambda 함수/Kinesis 스트림 포함)으로 역할 정책을 업데이트하여 모든 스트림에 대해 단일 서비스 연결 역할을 재사용할 수도 있습니다.

Firehose를 추가하기 위해 RFC를 제출하면 AMS 운영 엔지니어가 Data Firehose와 연결하려는 리소스(예: S3 AWS KMS, Lambda 및 Kinesis Streams)의 ARNs에 대한 서비스 요청을 통해 연락을 드릴 것입니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon DevOps Guru 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon DevOps Guru 기능에 직접 액세스할 수 있습니다. Amazon DevOps Guru는 개발자와 운영자가 애플리케이션의 성능과 가용성을 쉽게 개선할 수 있는 완전관리형 운영 서비스입니다. DevOps Guru는 운영 문제 식별과 관련

된 관리 작업을 없애므로 애플리케이션을 개선하기 위한 권장 사항을 신속하게 구현할 수 있습니다. 이제 DevOps Guru는 애플리케이션을 개선하는 데 사용할 수 있는 사후 대응 인사이트를 제공합니다. 또한 향후 애플리케이션에 영향을 미칠 수 있는 운영 문제를 방지하는 데 도움이 되는 사전 예방 인사이트를 제공합니다. DevOps Guru는 운영 데이터, 애플리케이션 지표 및 이벤트를 분석하여 정상적인 운영 패턴에서 벗어나는 동작을 식별하기 위해 기계 학습을 적용합니다. DevOps Guru가 운영 문제 또는 위험을 감지하면 알림이 전송됩니다. DevOps Guru는 현재 및 향후 예상되는 운영 문제를 해결하기 위해 각 문제에 대한 지능적인 권장 사항을 제시합니다.

자세한 내용은 Amazon DevOps Guru란 무엇입니까?를 참조하세요.

AWS Managed Services의 Amazon DevOps Guru FAQ

Q: AMS 계정에서 Amazon DevOps Guru에 대한 액세스를 요청하려면 어떻게 해야 하나요?

액세스를 요청하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(관리형 자동화) (ct-3qe6io8t6jtny) 변경 유형을 제출합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_devopsguru_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon DevOps Guru를 사용하는 데 따르는 제한 사항은 무엇인가요?

제한은 없습니다. Amazon DevOps Guru의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon DevOps Guru를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없습니다. DevOps Guru는 Amazon CloudWatch Logs, RDS Insights AWS X-Ray AWS Lambda및 AWS 서비스를 활용합니다 AWS CloudTrail.

AMS SSP를 사용하여 AMS 계정에서 Amazon DocumentDB(MongoDB 호환) 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon DocumentDB(MongoDB 호환) 기능에 직접 액세스할 수 있습니다. Amazon DocumentDB(MongoDB 호환)은 MongoDB 워크로드를 지원하는 빠르고, 확장 가능하며, 가용성이 높은 완전 관리형 도큐먼트 데이터베이스 서비스입니다. Amazon DocumentDB는 미션 크리티컬 MongoDB 워크로드를 대규모로 운영할 때 필요한 성능, 확장성 및 가용성을 제공합니다. Amazon DocumentDB는 MongoDB 클라이언트가 MongoDB 서버에서 기대하는 응답을 에뮬레이션하여 Apache 2.0 오픈 소스 MongoDB 3.6 API를 구현하므로 Amazon DocumentDB에서 기존 MongoDB 드라이버 및 도구를 사용할 수 있습니다. Amazon DocumentDB에서는 스토리지와 컴퓨팅이 분리되어 각 스토리지를 독립적으로 확장할 수 있으며 데이터 크기에 관계없이 지연 시간이 짧은 읽기 전용 복제본을 최대 15개까지 추가하

여 읽기 용량을 초당 수백만 개의 요청으로 늘릴 수 있습니다. Amazon DocumentDB는 99.99% 가용성을 위해 설계되었으며 3개의 AWS 가용 영역(AZs. AWS Database Migration Service (DMS)를 무료로(6개월 동안) 사용하여 가동 중지 없이 온프레미스 또는 Amazon Elastic Compute Cloud(Amazon EC2) MongoDB 데이터베이스를 Amazon DocumentDB로 마이그레이션할 수 있습니다. 자세한 내용은 Amazon DocumentDB(MongoDB 호환)를 참조하세요.

AWS Managed Services Amazon DocumentDB FAQ

Q: AMS 계정에서 Amazon DocumentDB에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Amazon DocumentDB 콘솔 및 데이터 액세스 역할은 콘솔 액세스 및 데이터 액세스라는 두 개의 AMS RFCs를 제출하여 요청할 수 있습니다.

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon DocumentDB에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_documentdb_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon DocumentDB를 사용하는 데 따르는 제한 사항은 무엇인가요?

Amazon DocumentDB에는 Amazon RDS 관련 권한이 필요합니다. AMS는 Amazon RDS를 완전히 관리하므로 Amazon DocumentDB의 IAM 역할에는 Amazon RDS의 작업에 대한 몇 가지 제한이 포함됩니다. 다음과 같은 제한 사항이 있습니다.

- `DeleteDBInstance` 및 `DeleteDBCluster` APIs가 제한되었습니다. 이러한 삭제 APIs 사용하려면 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 업데이트(관리형 자동화) 변경 유형(ct-27tuth19k52b4)을 사용하여 RFC를 제출합니다.
- Amazon RDS 인스턴스에서는 태그를 추가하거나 제거할 수 없습니다.
- Amazon DocumentDB 인스턴스는 퍼블릭으로 설정할 수 없습니다.

Q: AMS 계정에서 Amazon DocumentDB를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon S3 버킷 AWS KMS 이 AWS KMS 키로 암호화된 경우 Amazon DocumentDB를 사용하려면 Amazon S3 및가 필요합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon DynamoDB 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon DynamoDB(DynamoDB) 기능에 직접 액세스할 수 있습니다. Amazon DynamoDB는 모든 규모에서 한

자릿수 밀리초의 성능을 제공하는 키 값 및 문서 데이터베이스입니다. 인터넷 규모 애플리케이션을 위한 보안, 백업 및 복원, 인 메모리 캐싱이 내장된 완전 관리형 다중 리전 다중 활성 데이터베이스입니다. 자세한 내용은 Amazon DynamoDB를 참조하세요.

Amazon DynamoDB Accelerator(DAX)는 캐시를 DynamoDB 테이블에 추가하는 프로세스를 간소화하기 위해 설계된 라이트-스루(write-through) 캐싱 서비스입니다. DAX는 고성능 읽기가 필요한 애플리케이션을 위해 만들어졌습니다.

AWS Managed Services DynamoDB FAQ

Q: AMS 계정에서 DynamoDB 및 DAX에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | 서비스 | AWS 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 DynamoDB 및 DAX에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할 및 정책을 프로비저닝합니다.

- DynamoDB 역할 이름: `customer_dynamodb_role`

  DAX 서비스 역할 이름: `customer_dax_service_role`
- DynamoDB 정책 이름: `customer_dynamodb_policy`

  DAX 서비스 정책: `customer_dax_service_policy`

계정에 프로비저닝된 후에는 페더레이션 솔루션`customer_dynamodb_role`에서를 온보딩해야 합니다.

Q: AMS 계정에서 DynamoDB를 사용하는 데 따르는 제한 사항은 무엇인가요?

DynamoDB Accelerator(DAX)를 포함한 모든 DynamoDB 기능이 지원됩니다.

지정된 테이블에 대한 경보를 생성할 때 경보 이름 앞에 "customer*"를 붙여야 합니다. 예: `customer-employee-table-high-put-latency`.

DynamoDB에 대한 Amazon SNS 주제를 생성할 때 이름이 여야 합니다`dynamodb`.

DynamoDB에서 생성한 Amazon SNS 주제를 삭제하려면 관리 | 기타 | 기타 | 변경 유형 RFC 업데이트를 제출합니다.

Q: AMS 계정에서 DynamoDB를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 DynamoDB를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Elastic Container Registry 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Elastic Container Registry(Amazon ECR) 기능에 직접 액세스할 수 있습니다. Amazon Elastic Container Registry는 개발자가 Docker 컨테이너 이미지를 쉽게 저장, 관리 및 배포할 수 있는 완전 관리형 Docker 컨테이너 레지스트리입니다. Amazon ECR은 Amazon Elastic Container Service(Amazon ECS)와 통합되어 프로덕션 워크플로 개발을 간소화합니다. Amazon ECR을 사용하면 자체 컨테이너 리포지토리를 운영하거나 기본 인프라를 확장할 필요가 없습니다. Amazon ECS는 가용성과 확장성이 뛰어난 아키텍처에서 이미지를 호스팅하므로 애플리케이션용 컨테이너를 안정적으로 배포할 수 있습니다. AWS Identity and Access Management (IAM)과의 통합은 각 리포지토리의 리소스 수준 제어를 제공합니다. Amazon ECR에서는 선결제 요금이나 약정이 없습니다. 리포지토리에 저장한 데이터와 인터넷으로 전송된 데이터의 양에 대해서만 비용을 지불합니다.

자세한 내용은 Amazon Elastic Container Registry를 참조하세요.

AWS Managed Services의 Amazon Elastic Container Registry FAQ

Q: AMS 계정에서 Amazon ECR에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon ECR에 대한 액세스를 요청합니다. 이 RFC는 `customer_ecr_poweruser_instance_profile_policy`각각 `customer_ecr_console_role`, 및 관련 IAM 정책, `customer_ecr_console_policy` 및 `customer_ecr_poweruser_instance_profile`와 같은 IAM 역할을 계정에 프로비저닝합니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon ECR을 사용할 때 제한 사항은 무엇인가요?

AMS 계정에서 Amazon ECR을 사용하기 위한 AMS 네임스페이스에는 제한이 있습니다. 컨테이너 이미지에는 "AMS-" 또는 "Sentinel-" 접두사가 붙지 않을 수 있습니다.

Q: AMS 계정에서 Amazon ECR을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon ECR을 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 EC2 Image Builder 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 EC2 Image Builder 기능에 직접 액세스할 수 있습니다. EC2 Image Builder는 특정 IT 표준을 충족하기 위해 소프트웨어 및 설

정으로 사전 설치 및 사전 구성된 안전하고 up-to-date의 사용자 지정 "골드" 서버 이미지의 생성, 관리 및 배포를 더 쉽게 자동화할 수 있는 완전 관리형 AWS 서비스입니다.

, AWS Management Console AWS CLI 또는 APIs를 사용하여 AWS 계정에서 사용자 지정 이미지를 생성할 수 있습니다. 를 사용하면 Amazon EC2 Image Builder 마법사 AWS Management Console가 다음 단계를 안내합니다.

- 시작 아티팩트 제공
- 소프트웨어 추가 및 제거
- 설정 및 스크립트 사용자 지정
- 선택한 테스트 실행
- AWS 리전에 이미지 배포

빌드하는 이미지는 계정에 생성되며 운영 체제 패치에 대해 지속적으로 구성할 수 있습니다. 자세한 내용은 EC2 Image Builder를 참조하세요.

AWS Managed Services FAQ의 EC2 Image Builder

일반적인 질문과 답변:

Q: AMS 계정에서 EC2 Image Builder에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC를 통해 계정에 다음 IAM 역할이 프로비저닝됩니다 `customer_ec2_imagebuilder_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: EC2 Image Builder의 제한 사항은 무엇입니까?

AMS는 인프라 구성에 대한 서비스 기본값 사용을 지원하지 않습니다. 새 인프라 구성을 생성하거나 기존 인프라 구성을 사용할 수 있습니다.

AMS는 현재 컨테이너 레시피 생성을 지원하지 않습니다.

Q: EC2 Image Builder를 활성화하기 위한 사전 조건 또는 종속성은 무엇입니까?

- EC2 Image Builder 서비스 연결 역할: 서비스 연결 역할을 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API에서 첫 번째 Image Builder 리소스를 생성하면 Image Builder가 서비스 연결 역할을 생성합니다.

- Image Builder를 사용하여 이미지를 빌드하고 테스트를 실행하는 데 사용되는 인스턴스는 Systems Manager 서비스에 액세스할 수 있어야 합니다. SSM 에이전트가 아직 없는 경우 소스 이미지에 설치되고 이미지가 생성되기 전에 제거됩니다.
- AWS IAM: 인스턴스 프로파일과 연결하는 IAM 역할에는 이미지에 포함된 빌드 및 테스트 구성 요소를 실행할 수 있는 권한이 있어야 합니다. 인스턴스 프로파일과 연결된 IAM 역할에 `EC2InstanceProfileForImageBuilder` 및 IAM 역할 정책을 연결해야 합니다`AmazonSSMManagedInstanceCore`. IAM 역할 이름에는 `*imagebuilder*` 키워드가 포함되어야 합니다.
- 로깅을 구성하는 경우 인프라 구성에 지정된 인스턴스 프로파일에 대상 버킷(`arn:aws:s3:::`*`{bucket-name}`*`/*`)에 대한 `s3:PutObject` 권한이 있어야 합니다. 예제:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- 이름이 'imagebuilder'인 SNS 주제를 생성하여 EC2 Image Builder로부터 알림 및 알림을 받습니다.

AMS SSP를 사용하여 AMS 계정 AWS Fargate 의에서 Amazon ECS 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Fargate Amazon ECS 기능에 액세스할 수 있습니다. AWS Fargate 는 Amazon EC2 인스턴스의 Amazon EC2와 함께 컨테이너(의 컨테이너 AWS 참조)를 실행하는 데 사용할 수 있는 기술입니다. 를 AWS Fargate 사용하면 더 이상 컨테이너를 실행하기 위해 가상 머신 클러스터를 프로비저닝, 구성 또는 확장할 필요가 없습니다. 따라서 서버 유형을 선택하거나, 클러스터를 조정할 시점을 결정하거나, 클러스터 패킹을 최적화할 필요가 없습니다.

자세한 내용은 Amazon ECS on AWS Fargate을 참조하세요.

AWS Managed Services FAQ의 Fargate 기반 Amazon ECS

Q: AMS 계정에서 Fargate의 Amazon ECS에 대한 액세스를 요청하려면 어떻게 해야 합니까?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Fargate의 Amazon ECS에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다. `customer_ecs_fargate_console_role` (ECS 정책을 연결할 기존 IAM 역할이 제공되지 않은 경우), `customer_ecs_fargate_events_service_role`, `customer_ecs_task_execution_service_role`, 및 `customer_ecs_codedeploy_service_roleAWSServiceRoleForApplicationAutoScaling_ECSS` 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Fargate에서 Amazon ECS를 사용하는 데 따르는 제한 사항은 무엇인가요?

- 컨테이너 수준 활동은 하이퍼바이저 위에서 발생하며 로깅 기능은 Fargate의 Amazon ECS에 의해 제한되므로 Amazon ECS 작업 모니터링 및 로깅은 사용자의 책임으로 간주됩니다. Fargate의 Amazon ECS 사용자는 Amazon ECS 작업에 대한 로깅을 활성화하는 데 필요한 단계를 수행하는 것이 좋습니다. 자세한 내용은 컨테이너에 대한 awslogs 로그 드라이버 활성화를 참조하세요.
- 컨테이너 수준의 보안 및 멀웨어 보호도 사용자의 책임으로 간주됩니다. Fargate의 Amazon ECS에는 Trend Micro 또는 사전 구성된 네트워크 보안 구성 요소가 포함되지 않습니다.
- 이 서비스는 다중 계정 랜딩 존과 단일 계정 랜딩 존 AMS 계정 모두에 사용할 수 있습니다.
- Route 53 프라이빗 호스팅 영역을 생성하려면 승격된 권한이 필요하므로 Amazon ECS 서비스 검색은 기본적으로 자체 프로비저닝된 역할에서 제한됩니다. 서비스에서 서비스 검색을 활성화하려면 관리 | 기타 | 기타 | 변경 유형 업데이트를 제출합니다. Amazon ECS 서비스에 대한 서비스 검색을 활성화하는 데 필요한 정보를 제공하려면 서비스 검색 설명서를 참조하세요.
- AMS는 현재 Amazon ECS Fargate의 컨테이너에 배포하는 데 사용되는 이미지를 관리하거나 제한하지 않습니다. Amazon ECR, Docker Hub 또는 기타 프라이빗 이미지 리포지토리에서 이미지를 배포할 수 있습니다. 따라서 퍼블릭 이미지나 보안되지 않은 이미지는 계정에 악의적인 활동이 발생할 수 있으므로 배포하지 않는 것이 좋습니다.

Q: AMS 계정에서 Fargate에서 Amazon ECS를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 다음은 Fargate에서 Amazon ECS의 종속성이지만 자체 프로비저닝된 역할로 이러한 서비스를 활성화하는 데 필요한 추가 작업은 없습니다.
  - CloudWatch 로그

  - CloudWatch 이벤트
  - CloudWatch 경보
  - CodeDeploy
  - App Mesh
  - 클라우드 맵
  - Route 53
- 사용 사례에 따라 다음은 Amazon ECS가 의존하는 리소스이며 계정에서 Fargate에서 Amazon ECS를 사용하기 전에 필요할 수 있습니다.
  - Amazon ECS 서비스와 함께 사용할 보안 그룹입니다. 배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성(자동)(ct-3pc215bnwb6p7)을 사용하거나, 보안 그룹에 특수 규칙이 필요한 경우 배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성(관리형 자동화)(ct-1oxx2g2d7hc90)을 사용할 수 있습니다. 참고: Amazon ECS를 사용하여 선택한 보안 그룹은 Amazon ECS 서비스 또는 클러스터가 있는 Amazon ECS 전용으로 생성해야 합니다. 보안 그룹 섹션의 Amazon ECS 설정 및 Amazon Elastic Container Service의 보안에서 자세히 알아볼 수 있습니다.
  - 작업 간 로드 밸런싱을 위한 Application Load Balancer(ALB), Network Load Balancer(NLB), Classic Load Balancer(ELB).
  - ALBs.
  - Amazon ECS 클러스터와 통합할 앱 메시 리소스(예: 가상 라우터, 가상 서비스, 가상 노드).
- 현재 AMS가 표준 AMS 변경 유형 외부에서 생성될 때 지원 보안 그룹의 권한과 관련된 위험을 자동으로 완화할 수 있는 방법은 없습니다. Amazon ECS에서 사용하도록 지정되지 않은 보안 그룹을 사용할 가능성을 제한하려면 Fargate 클러스터와 함께 사용할 특정 보안 그룹을 요청하는 것이 좋습니다.

AMS SSP를 사용하여 AMS 계정 AWS Fargate 의에서 Amazon EKS 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Fargate Amazon EKS 기능에 액세스합니다. AWS Fargate 는 컨테이너에 대한 적절한 크기의 온디맨드 컴퓨팅 용량을 제공하는 기술입니다(컨테이너를 이해하려면 컨테이너란 무엇입니까? 참조). 를 사용하면 더 이상 컨테이너를 실행하기 위해 가상 머신 그룹을 프로비저닝, 구성 또는 확장할 필요가 AWS Fargate 없습니다. 따라서 서버 유형을 선택하거나, 노드 그룹을 조정할 시점을 결정하거나, 클러스터 패킹을 최적화할 필요가 없습니다.

Amazon Elastic Kubernetes Service(Amazon EKS)는 Kubernetes에서 제공하는 확장 가능한 업스트림 모델을 AWS Fargate 사용하여 구축된 컨트롤러 AWS 를 사용하여 Kubernetes를와 통합합니다. 이러한 컨트롤러는 Amazon EKS 관리형 Kubernetes 컨트롤 플레인의 일부로 실행되며 Fargate에서 네이티브 Kubernetes 포드를 예약하는 역할을 합니다. Fargate 컨트롤러에는 여러 개의 변형 및 검증 승인 컨트롤러 외에도 기본 Kubernetes 스케줄러와 함께 실행되는 새 스케줄러가 포함되어 있습니다. Fargate에서 실행하기 위한 조건을 충족하는 포드를 시작하면 클러스터에서 실행되는 Fargate 컨트롤러가 해당 포드를 인식하고 업데이트하고 Fargate에 예약합니다.

자세한 내용은 Amazon EKS on AWS Fargate Now Generally Available 및 Amazon EKS Best Practices Guide for Security("Recommendations", "Review and revoke unnecessary anonymous access" 등 포함)를 참조하세요.

> **Tip**
>
> AMS에는 Amazon EKS와 함께 사용할 수 있는 변경 유형인 배포 | 고급 스택 구성 요소 | ID 및 액세스 관리(IAM) | OpenID Connect 공급자 생성(ct-30ecvfi3tq4k3)이 있습니다. 예제는 Identity and Access Management(IAM) | OpenID Connect Provider 생성을 참조하세요.

AWS Managed Services AWS Fargate 의의 Amazon EKS FAQ

Q: AMS 계정에서 Fargate의 Amazon EKS에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다.

- `customer_eks_fargate_console_role`.

  계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.
- 이러한 서비스 역할은 Fargate의 Amazon EKS에 사용자를 대신하여 다른 AWS 서비스를 호출할 수 있는 권한을 부여합니다.
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

Q: AMS 계정에서 Fargate에서 Amazon EKS를 사용하는 데 따르는 제한 사항은 무엇인가요?

- 관리형 또는 자체 관리형 EC2 노드 그룹 생성은 AMS에서 지원되지 않습니다. EC2 작업자 노드를 사용해야 하는 경우 AMS Cloud Service Delivery Manager(CSDM) 또는 Cloud Architect(CA)에 문의하십시오.
- AMS에는 컨테이너 이미지에 대한 Trend Micro 또는 사전 구성된 네트워크 보안 구성 요소가 포함되지 않습니다. 배포 전에 자체 이미지 스캔 서비스를 관리하여 악성 컨테이너 이미지를 탐지해야 합니다.
- CloudFormation 상호 종속성으로 인해 EKSCTL이 지원되지 않습니다.
- 클러스터를 생성하는 동안 클러스터 컨트롤 플레인 로깅을 비활성화할 수 있는 권한이 있습니다. 자세한 내용을 알아보려면 Amazon EKS 컨트롤 플레인 로깅을 참조하세요. 클러스터 생성 시 모든 중요한 API, 인증 및 감사 로깅을 활성화하는 것이 좋습니다.
- 클러스터 생성 중에 Amazon EKS 클러스터에 대한 클러스터 엔드포인트 액세스는 기본적으로 퍼블릭으로 설정됩니다. 자세한 내용은 Amazon EKS 클러스터 엔드포인트 액세스 제어를 참조하세요. Amazon EKS 엔드포인트를 프라이빗으로 설정하는 것이 좋습니다. 퍼블릭 액세스에 엔드포인트가 필요한 경우 특정 CIDR 범위에 대해서만 퍼블릭으로 설정하는 것이 좋습니다.
- AMS에는 Amazon EKS Fargate의 컨테이너에 배포하는 데 사용되는 이미지를 강제로 적용하고 제한하는 방법이 없습니다. Amazon ECR, Docker Hub 또는 기타 프라이빗 이미지 리포지토리에서 이미지를 배포할 수 있습니다. 따라서 계정에서 악의적인 활동을 수행할 수 있는 퍼블릭 이미지를 배포할 위험이 있습니다.
- 클라우드 개발 키트(CDK) 또는 CloudFormation Ingest를 통한 EKS 클러스터 배포는 AMS에서 지원되지 않습니다.
- 수신 생성을 위해 매니페스트 파일에서 ct-3pc215bnwb6p7 배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성 및 참조를 사용하여 필요한 보안 그룹을 생성해야 합니다. 이는 역할`customer-eks-alb-ingress-controller-role`이 보안 그룹을 생성할 권한이 없기 때문입니다.

Q: AMS 계정에서 Fargate에서 Amazon EKS를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

서비스를 사용하려면 다음 종속성을 구성해야 합니다.

- 서비스에 대해 인증하려면 KUBECTL과 aws-iam-authenticator를 모두 설치해야 합니다. 자세한 내용은 클러스터 인증 관리를 참조하세요.
- Kubernetes는 "서비스 계정"이라는 개념을 사용합니다. EKS의 kubernetes 클러스터 내에서 서비스 계정 기능을 활용하려면 다음 입력과 함께 관리 | 기타 | 기타 | RFC 업데이트가 필요합니다.
  - [필수] Amazon EKS 클러스터 이름
  - [필수] 서비스 계정(SA)이 배포될 Amazon EKS 클러스터 네임스페이스입니다.
  - [필수] Amazon EKS 클러스터 SA 이름입니다.

- [필수] 연결할 IAM 정책 이름 및 권한/문서입니다.
- [필수] 요청 중인 IAM 역할 이름입니다.
- [선택 사항] OpenID Connect 공급자 URL입니다. 자세한 내용은 다음 섹션을 참조하세요.
  - 클러스터의 서비스 계정에 대한 IAM 역할 활성화
  - 서비스 계정에 대한 세분화된 IAM 역할 소개
- 에 대해 Config 규칙을 구성하고 모니터링하는 것이 좋습니다.
  - 퍼블릭 클러스터 엔드포인트
  - 비활성화된 API 로깅

  이러한 Config 규칙을 모니터링하고 수정하는 것은 사용자의 책임입니다.

ALB 수신 컨트롤러를 배포하려면 관리 | 기타 | 기타 업데이트 RFC를 제출하여 ALB 수신 컨트롤러 포드와 함께 사용하는 데 필요한 IAM 역할을 프로비저닝합니다. ALB 수신 컨트롤러와 연결할 IAM 리소스를 생성하려면 다음 입력이 필요합니다(RFC에 포함).

- [필수] Amazon EKS 클러스터 이름
- [선택 사항] OpenID Connect 공급자 URL
- [선택 사항] 애플리케이션 로드 밸런서(ALB) 수신 컨트롤러 서비스가 배포될 Amazon EKS 클러스터 네임스페이스입니다. [기본값: kube-system]
- [선택 사항] Amazon EKS 클러스터 서비스 계정(SA) 이름. [기본값: aws-load-balancer-controller]

클러스터에서 봉투 보안 암호 암호화를 활성화하려면(권장) RFC의 설명 필드에 사용하려는 KMS 키 IDs를 제공하여 서비스를 추가합니다(관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가 (ct-1w8z66n899dct). 봉투 암호화에 대한 자세한 내용은 Amazon EKS에서 AWS KMS를 사용한 보안 암호에 대한 봉투 암호화 추가를 참조하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon EMR 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon EMR 기능에 직접 액세스할 수 있습니다. Amazon EMR은 Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, Presto와 같은 오픈 소스 도구를 사용하여 방대한 양의 데이터를 처리하기 위한 업계 최고의 클라우드 빅 데이터 플랫폼입니다. Amazon EMR을 사용하면 기존 온프레미스 솔루션 비용의 절반 미만과 표준 Apache Spark보다 3배 빠른 속도로 페타바이트 규모의 분석을 실행할 수 있습니다. 단기 실행 작업의 경우 클러스터를 가동 및 가동 중지하고 사용된 인스턴스에 대해 초당 비용을 지

불할 수 있습니다. 장기 실행 워크로드의 경우 수요에 맞게 자동으로 확장되는 고가용성 클러스터를 생성할 수 있습니다.

AMS 다중 계정 랜딩 존 또는 단일 계정 랜딩 존 계정에서 Amazon EMR 클러스터의 인스턴스를 하나 이상 생성하여 임시 및 영구 Amazon EMR 클러스터를 모두 지원할 수 있습니다. Kerberos 인증을 활성화하여 온프레미스 Active Directory 도메인에서 사용자를 인증할 수도 있습니다.

Amazon EMR 클러스터와 함께 여러 데이터 스토어를 활용하여 사용 사례별 하둡 도구 및 라이브러리를 지원할 수 있습니다. Amazon EMR 클러스터는 OnDemand 또는 스팟 인스턴스를 사용하여 생성하고 오토 스케일링을 구성하여 용량을 관리하고 비용을 절감할 수 있습니다.

클러스터 로그 파일은 로깅 및 디버깅을 위해 Amazon S3 버킷에 보관할 수 있습니다. Amazon EMR 클러스터에서 호스팅되는 웹 인터페이스에 액세스하여 hadoop 관리 요구 사항을 지원하거나 고객을 위한 노트북 경험을 지원할 수도 있습니다.

자세한 내용은 Amazon EMR을 참조하세요.

AWS Managed Services의 Amazon EMR FAQ

Q: AMS 계정에서 Amazon EMR에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다.

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

계정에 프로비저닝된 후에는 페더레이션 솔루션에서 customer_emr_console_role을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon EMR을 사용할 때 제한 사항은 무엇인가요?

AWS 콘솔에서 EC2 클러스터에 Amazon EMR을 생성하는 동안 클러스터 생성 - 고급 옵션을 사용하는 것이 좋습니다. Amazon EMR 클러스터는 키가 "for-use-with-amazon-emr-managed-policies"이고 값이 "true"인 태그를 추가하여 생성해야 합니다. 보안 옵션에서 다음 구성을 선택합니다.

- 클러스터의 사용자 지정 역할을 선택합니다.
  - EMR 역할: customer_emr_cluster_service_role

  - EC2 인스턴스 프로파일: customer_emr_cluster_instance_profile
  - Auto Scaling 역할: customer_emr_cluster_autoscaling_role
- EC2 보안 그룹:
  - 마스터: ams-emr-master-security-group
  - 코어 및 작업: ams-emr-worker-security-group
  - 서비스 액세스: ams-emr-serviceaccess-security-group

Q: AMS 계정에서 Amazon EMR을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS는 Amazon EMR 마스터, 작업자 및 서비스 노드에 대한 기본 보안 그룹을 생성합니다.

Amazon EMR 클러스터에 사용할 시작 템플릿 및 보안 그룹에는 "for-use-with-amazon-emr-managed-policies" 태그 키와 "true" 값이 있어야 합니다.

기본 Amazon EMR 클러스터 인스턴스 프로파일을 사용하면 이름이 "emr"을 포함하는 s3 버킷 및 dynamodb 테이블과 같은 리소스에 액세스할 수 있습니다. Amazon EMR에서 사용할 추가 리소스를 사용하도록 추가 IAM 정책을 요청할 수 있습니다. 다음 리소스 ARN은 customer_emr_cluster_instance_profile을 사용하여 Amazon EMR 작업에 사용할 수 있습니다.

- arn:aws:dynamodb:*:*:table/*emr*
- arn:aws:kinesis:*:*:stream/*emr*
- arn:aws:sns:*:*:*emr*arn:aws:sqs:*:*:*emr*
- arn:aws:sqs:*:*:*emr*
- arn:aws:sqs:*:*:AWS-ElasticMapReduce-*
- arn:aws:sdb:*:*:domain:*emr*
- arn:aws:s3:::*emr*

Amazon EMR 클러스터에 kerberos 인증이 필요한 경우:

- 각 각 각기 다른 Amazon EMR 클러스터에 사용할 영역 이름과 온프레미스 Active Directory IP 주소를 제공합니다.
- 인프라 요구 사항:

  다중 계정 랜딩 존(MALZ): RFC를 제출하여 기존 애플리케이션 계정에서 새 관리형 애플리케이션 계정 또는 새 VPC를 생성합니다.

단일 계정 랜딩 존(SALZ): RFC를 제출하여 VPC에 새 서브넷을 생성합니다.

- 온프레미스 Active Directory에서 클러스터 영역에 대한 수신 신뢰를 구성합니다.
- 관리형 AD에서 영역에 대한 DNS 영역을 구성하려면 RFC를 제출합니다.
- 영역 구성:

  MALZ: 관리 제출 | 기타 | 기타 | 업데이트(ct-0xdawir96cy7k) RFC를 업데이트하여 도메인 이름 접미사에 영역 이름을 사용하도록 VPC DHCP 옵션 세트를 업데이트합니다.

  SALZ: 관리 제출 | 기타 | 기타 | 업데이트(ct-0xdawir96cy7k) RFC를 사용하여 도메인 이름 접미사에 특정 영역을 사용할 새 Amazon EMR AMI를 생성합니다.

Amazon EMR 스튜디오를 배포하려면 역할에 Amazon Simple Storage Service 버킷에 대한 사전 조건이 `customer_emr_cluster_service_role` 있습니다. 버킷을 생성하려면 자동 CT`ct-1a68ck03fn98r`(배포 | 고급 스택 구성 요소 | S3 스토리지 | 생성)를 사용합니다. 이 자동 CT를 사용하여 Amazon EMR용 Amazon S3 버킷을 생성하는 경우 버킷 이름은 접두사 로 시작해야 합니다`customer-emr-*`. 또한 Amazon EMR 클러스터와 동일한 AWS 리전에 버킷을 생성해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon EventBridge 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon EventBridge 기능에 직접 액세스할 수 있습니다. Amazon EventBridge: 애플리케이션을 다양한 소스의 데이터와 쉽게 연결할 수 있는 서버리스 이벤트 버스 서비스입니다. EventBridge는 자체 애플리케이션, Software-as-a-Service(SaaS) 애플리케이션 및 AWS 서비스의 실시간 데이터 스트림을 제공하고 해당 데이터를와 같은 대상으로 라우팅합니다 AWS Lambda. 데이터를 전송할 대상을 결정하는 라우팅 규칙을 설정하여 모든 데이터 소스에 실시간으로 대응하는 애플리케이션 아키텍처를 구축할 수 있습니다. EventBridge를 사용하면 느슨하게 결합되고 분산되는 이벤트 기반 아키텍처를 구축할 수 있습니다.

자세한 내용은 Amazon EventBridge를 참조하세요.

AWS Managed Services FAQ의 EventBridge

Q: AMS 계정에서 EventBridge에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 EventBridge에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_eventbridge_rolecustomer_eventbridge_scheduler_execution_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

실행 역할은 EventBridge 스케줄러가 AWS 서비스 사용자를 대신하여 다른와 상호 작용하기 위해 수임하는 IAM 역할`customer_eventbridge_scheduler_execution_role`입니다. 이 역할에 연결된 권한 정책은 EventBridge 스케줄러에 대상을 호출할 수 있는 액세스 권한을 부여합니다.

> **Note**
>
> 기본적으로 EventBridge 스케줄러는 EventBridge에 AWS 소유 키를 사용하여 데이터를 암호화합니다. EventBridge의 고객 관리형 키를 사용하여 데이터를 암호화하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 서비스 프로비저닝을 위한 추가(관리형 자동화) 변경 유형(ct-3qe6io8t6jtny)을 사용하여 RFC를 제출합니다.

Q: AMS 계정에서 EventBridge를 사용할 때 제한 사항은 무엇인가요?

AMS RFCs 제출하고 배치 작업을 트리거하는 서비스 역할, SQS 대기열, CodeBuild, CodePipeline 및 SSM 명령을 생성해야 합니다.

Q: AMS 계정에서 EventBridge를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

EventBridge를 사용하여 Lambda, Amazon SNS AWS Batch, Amazon SQS 또는 Amazon CloudWatch Logs AWS 리소스와 같은 다른 리소스를 트리거하기 전에 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책(관리형 자동화) 변경 유형(ct-3dpd8mdd9jn1r)을 사용하여 RFC로 EventBridge 서비스 역할을 요청해야 합니다. 서비스 역할을 요청할 때 호출할 서비스를 지정합니다. 대상을 호출하는 데 필요한 권한에 대한 자세한 내용은 EventBridge에 리소스 기반 정책 사용을 참조하세요.

EventBridge는 EventBridge AWS 서비스 에서 사용자 AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스와 통합됩니다. CloudTrail을 활성화하고 로그 파일을 S3 버킷에 저장할 수 있어야 합니다. 참고: 모든 AMS 계정에는 CloudTrail이 활성화되어 있으므로 별도의 조치가 필요하지 않습니다.

Q: customer_eventbridge_scheduler_execution_role 역할에는 AWS Key Management Service 키에 대한 사전 조건이 있습니다(암호화에 사용되는 경우 선택 사항). 저장/전송 시 데이터 암호화에 AWS KMS CMKs 채택하려면 어떻게 해야 합니까?

기본적으로 EventBridge 스케줄러는 AWS 소유 키(저장 시 암호화)로 저장되는 이벤트 메타데이터 및 메시지 데이터를 암호화합니다. 또한 EventBridge 스케줄러는 전송 계층 보안(TLS)(전송 중 암호화)을 사용하여 EventBridge 스케줄러와 다른 서비스 간에 전달하는 데이터를 암호화합니다.

특정 사용 사례에서 EventBridge 스케줄러에서 데이터를 보호하는 암호화 키를 제어하고 감사해야 하는 경우 고객 관리형 키를 사용할 수 있습니다.

Amazon EventBridge를 사용하여 AWS KMS 권한을 온보딩하기 전에 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(관리형 자동화) 변경 유형을 사용하여 RFC를 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Forecast 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Forecast(Forecast) 기능에 직접 액세스할 수 있습니다. Amazon Forecast는 기계 학습을 사용하여 매우 정확한 예측을 제공하는 완전관리형 서비스입니다.

> **Note**
>
> AWS 는 2024년 7월 29일부터 Amazon Forecast에 대한 신규 고객 액세스를 종료했습니다. Amazon Forecast 기존 고객은 평소와 같이 서비스를 계속 사용할 수 있습니다.는 Amazon Forecast의 보안, 가용성 및 성능 개선에 AWS 계속 투자하지만 새로운 기능을 도입할 계획 AWS 은 없습니다.
> Amazon Forecast를 사용하려면 CSDM에 문의하여 Amazon Forecast 사용량을 Amazon SageMaker Canvas로 전환하는 방법에 대해 자세히 알아보세요.

Forecast는 Amazon.com 사용된 것과 동일한 기술을 기반으로 기계 학습을 사용하여 시계열 데이터를 추가 변수와 결합하여 예측을 구축합니다. Forecast를 시작하려면 기계 학습 경험이 필요하지 않습니다. 과거 데이터와 예측에 영향을 미칠 수 있다고 생각되는 추가 데이터만 제공하면 됩니다. 예를 들어, 셔츠의 특정 색상에 대한 수요는 계절과 매장 위치에 따라 변경될 수 있습니다. 이 복잡한 관계는 자체적으로 결정하기 어렵지만 기계 학습은 이를 인식하는 데 이상적입니다. 데이터를 제공하면 Forecast는 시계열 데이터만 보는 것보다 최대 50% 더 정확한 예측을 수행할 수 있는 예측 모델을 자동으로 검사하고 의미 있는 것을 식별하며 생성합니다.

자세한 내용은 Amazon Forecast를 참조하세요.

AWS Managed Services FAQ의 Amazon Forecast

Q: AMS 계정에서 Forecast에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 AWS Firewall Manager 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_forecast_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Forecast를 사용하는 데 따르는 제한 사항은 무엇인가요?

기본 S3 버킷 액세스는 이름 지정 패턴이 'customer-forecast-*'인 버킷에만 액세스할 수 있도록 허용합니다. 데이터 버킷에 대한 고유한 이름 지정 규칙이 있는 경우 Cloud Architect(CA)와 버킷 이름 지정 및 관련 액세스 설정에 대해 논의합니다. 예:

- 'AmazonForecast-ExecutionRole-*' 및 관련 적절한 S3 버킷 액세스와 같은 이름을 지정하여 특정 Amazon Forecast 서비스 역할을 정의할 수 있습니다.ExecutionRole S3 IAM 콘솔에서 서비스 역할 - AmazonForecast-ExecutionRole-Admin 및 IAM 정책 - customer_forecast_default_s3_access_policy를 참조하세요.
- 관련 S3 버킷 액세스를 IAM 페더레이션 역할에 연결해야 할 수 있습니다. IAM 콘솔에서 IAM 정책 - customer_forecast_default_s3_access_policy를 참조하세요.

Q: AMS 계정에서 Forecast를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- Forecast를 사용하기 전에 적절한 Amazon S3 버킷(들)을 생성해야 합니다. 특히 기본 S3 버킷 액세스는 'customer-forecast-*'라는 이름 지정 패턴을 사용합니다.
- 'customer-forecast-*' 이외의 S3 버킷에서 이름 지정 패턴을 사용하려면 버킷에 대한 S3 액세스 권한이 있는 새 서비스 역할을 생성해야 합니다.
  1. 'AmazonForecast-ExecutionRole-{suffix}'라는 이름으로 생성할 새 서비스 역할입니다.
  2. customer_forecast_default_s3_access_policy와 유사하고 새 서비스 역할 및 관련 페더레이션 관리자 역할(예: 'customer_forecast_admin_role')과 연결되는 새 IAM 정책 생성

Q: Amazon Forecast를 사용하는 동안 데이터 보안을 강화하려면 어떻게 해야 하나요?

- 저장 데이터 암호화의 경우 AWS KMS 를 사용하여 고객 관리형 CMK를 프로비저닝하여 Amazon S3 서비스의 데이터 스토리지를 보호할 수 있습니다.
  - 프로비저닝 키를 사용하여 버킷에서 기본 암호화를 활성화하고 데이터를 입력하는 동안 AWS KMS 데이터 암호화를 수락하도록 버킷 정책을 설정합니다.
  - Amazon Forecast 서비스 역할 'AmazonForecast-ExecutionRole-*' 및 페더레이션 관리자 역할(예: 'customer_forecast_admin_role')을 AWS KMS 키 사용자로 활성화합니다.
- 전송 중 데이터 암호화의 경우 Amazon S3 버킷 정책에서 객체를 전송하는 데 필요한 HTTPS 프로토콜을 설정할 수 있습니다.
- 액세스 제어에 대한 추가 제한에서 Amazon Forecast 서비스 역할 'AmazonForecast-ExecutionRole-*' 및 관리자 역할(예: 'customer_forecast_admin_role')에 대해 승인된 액세스에 대한 버킷 정책을 활성화합니다.

Q: Amazon Forecast 사용 시 모범 사례는 무엇인가요?

- Amazon Forecast에서 S3 버킷을 사용하는 동안 데이터 분류 관행을 잘 이해하고 관련 데이터 보안 요구 사항을 매핑해야 합니다.
- Amazon S3 버킷 구성의 경우 S3 버킷 정책에서 HTTPS 적용을 활성화하는 것이 좋습니다.
- 'customer-forecast-*'라는 이름의 Amazon S3S3 버킷에 대한 관리자 역할 'customer_forecast_admin_role' 지원 허용 액세스(Get/Delete/Put S3 객체)를 알고 있어야 합니다. 참고: 여러 팀에 대한 세분화된 액세스 제어가 필요한 경우 다음 관행을 따르세요.
  - 관련 Amazon S3 버킷에 대한 최소 권한 액세스를 사용하여 팀 기반 액세스 IAM 자격 증명(역할/사용자)을 정의합니다.
  - 팀/프로젝트 기반 AWS KMS CMKs 생성하면 해당 IAM 자격 증명에 대한 적절한 액세스 권한이 부여됩니다(사용자 액세스 및 'AmazonForecast-ExecutionRole-{team/project}'.
  - 생성된 AWS KMS CMKs를 사용하여 S3 버킷 기본 암호화를 설정합니다.
  - S3 버킷 정책에 HTTPS 프로토콜을 사용하여 S3 API 트래픽을 적용합니다.
  - 관련 IAM 자격 증명(사용자 액세스 및 'AmazonForecast-ExecutionRole-{team/project}'에 대한 승인된 액세스에 대해 S3 버킷 구성을 버킷에 적용합니다.
- 'customer_forecast_admin_role'을 범용으로 사용하려면 이전에 나열된 포인트를 고려하여 S3 버킷을 보호하세요.

Q: Amazon Forecast에 대한 규정 준수 정보는 어디에 있나요?

AWS 서비스 규정 준수 프로그램을 참조하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon FSx 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon FSx 기능에 직접 액세스할 수 있습니다. Amazon FSx는 완전 관리형 타사 파일 시스템을 제공합니다. Amazon FSx는 Windows 기반 스토리지, 고성능 컴퓨팅(HPC), 기계 학습, 전자 설계 자동화(EDA)와 같은 워크로드를 위한 기능 세트와 타사 파일 시스템의 기본 호환성을 제공합니다. Amazon FSx는 하드웨어 프로비저닝, 소프트웨어 구성, 패치 적용 및 백업과 같이 시간이 많이 걸리는 관리 작업을 자동화합니다. Amazon FSx는 파일 시스템을 클라우드 네이티브 AWS 서비스와 통합하여 더 광범위한 워크로드 세트에 훨씬 더 유용합니다.

Amazon FSx는 Windows 기반 애플리케이션용 Amazon FSx for Windows File Server와 컴퓨팅 집약적인 워크로드용 Amazon FSx for Lustre라는 두 가지 파일 시스템 중에서 선택할 수 있습니다. 자세한 내용은 Amazon FSx를 참조하세요.

AWS Managed Services의 Amazon FSx FAQ

Q: AMS 계정에서 Amazon FSx에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon FSx에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_fsx_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon FSx를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. 서비스의 전체 기능을 사용할 수 있습니다.

Q: AMS 계정에서 Amazon FSx를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없습니다. 그러나 다중 AZ와 같은 고급 구성의 경우 DFS 복제 및 DFS 네임스페이스 서비스를 설치하고 관리해야 합니다. 자세한 내용은 다중 AZ 파일 시스템 배포를 참조하세요.

Q: Amazon FSx 파일 시스템을 다중 계정 랜딩 존 Managed AD와 통합하려면 어떻게 해야 하나요?

Amazon FSx 파일 시스템을 생성할 때 MALZ Managed AD를 Windows 인증을 위한 'AWS 관리형 Microsoft Active Directory'로 지정할 수 있습니다. 자세한 내용은 Microsoft Active Directory AWS Directory Service 용에서 Amazon FSx 사용을 참조하세요.

또한 먼저 Managed AD를 애플리케이션 계정과 공유해야 합니다. 관리 | 디렉터리 서비스 | 디렉터리 | 디렉터리 변경 유형 공유(ct-369odosk0pd9w)를 사용하여 RFC를 제출하여이 작업을 수행합니다.

Q: AWS 위임 FSx 관리자 그룹에 속한 사용자는 무엇입니까?

IT 파일 서버 관리자만. 이 그룹에는 모든 파일 공유에 대한 전체 액세스 권한이 있습니다.

Q: FSx 시스템이 프로비저닝될 때 생성되는 기본 파일 공유, 공유를 사용해야 합니까?

아니요. 프로비저닝된 대로 기본 파일 공유, 공유를 사용하지 않는 것이 좋습니다. 최소 권한 원칙을 위반하는 모든 사람에게 전체 액세스 권한을 부여합니다. 대신 비즈니스 요구 사항에 맞는 더 작은 사용자 지정 파일 공유를 생성합니다.

Q: 내 비즈니스의 특정 조직에 대한 사용자 지정 파일 공유를 생성하려면 어떻게 해야 하나요?

사용자 지정 파일 공유 생성에 대한 지침은 파일 공유를 참조하세요. 최소 권한 원칙을 사용하여 각 파일 공유에 대한 액세스를 제한합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon FSx for OpenZFS 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon FSx for OpenZFS 기능에 직접 액세스할 수 있습니다. FSx for OpenZFS는 애플리케이션 코드 또는 데이터 관리 방법을 변경하지 않고도 온프레미스 ZFS 또는 기타 Linux 기반 파일 서버에 있는 데이터를 AWS로 쉽게 이동할 수 있는 완전 관리형 파일 스토리지 서비스입니다. 오픈 소스 OpenZFS 파일 시스템에 구축된 매우 안정적이고 확장 가능하며 성능이 뛰어나고 기능이 풍부한 파일 스토리지를 제공하여 OpenZFS 파일 시스템의 친숙한 기능과 기능에 완전 관리형 AWS 서비스의 민첩성, 확장성 및 단순성을 제공합니다. 클라우드 네이티브 애플리케이션을 구축하는 개발자를 위해 데이터 작업을 위한 풍부한 기능을 갖춘 간단한 고성능 스토리지를 제공합니다.

FSx for OpenZFS 파일 시스템은 업계 표준 NFS 프로토콜(v3, v4.0, v4.1, v4.2)을 사용하여 Linux, Windows 및 macOS 컴퓨팅 인스턴스 및 컨테이너에서 광범위하게 액세스할 수 있습니다. AWS Graviton 프로세서와 최신 AWS 디스크 및 네트워킹 기술(AWS Scalable Reliable Datagram 네트워킹 및 AWS Nitro 시스템 포함)로 구동되는 FSx for OpenZFS는 수백 마이크로초의 지연 시간으로 최대 100만 IOPS를 제공합니다. 즉각적인 point-in-time 스냅샷 및 데이터 복제와 같은 OpenZFS 기능을 완벽하게 지원하는 FSx for OpenZFS를 사용하면 온프레미스 파일 서버를 익숙한 파일 시스템 기능을 제공하고 긴 검증을 수행하고 기존 애플리케이션 또는 도구를 변경하거나 재설계할 필요가 없는 AWS 스토리지로 쉽게 교체할 수 있습니다. 또한 OpenZFS 데이터 관리 기능의 성능과 최신 AWS 기술의 고성능 및 비용 효율성을 결합하여 FSx for OpenZFS를 사용하면 데이터 집약적인 고성능 애플리케이션을 구축하고 실행할 수 있습니다.

완전 관리형 서비스인 FSx for OpenZFS를 사용하면에서 완전 관리형 파일 시스템을 쉽게 시작, 실행 및 확장하여 온프레미스에서 실행하는 파일 서버를 AWS 대체하는 동시에 민첩성을 높이고 비용을 절감할 수 있습니다. FSx for OpenZFS를 사용하면 파일 서버 및 스토리지 볼륨 설정 및 프로비저닝, 데이터 복제, 파일 서버 소프트웨어 설치 및 패치, 하드웨어 장애 감지 및 해결, 백업 수동 수행에 대해 더 이상 걱정할 필요가 없습니다. 또한 AWS Identity and Access Management (IAM), AWS Key Management Service (), Amazon CloudWatch 및 같은 다른 AWS 서비스와의 풍부한 통합AWS KMS을 제공합니다 AWS CloudTrail.

Amazon FSx는 Windows 기반 애플리케이션용 Amazon FSx for Windows File Server와 컴퓨팅 집약적인 워크로드용 Amazon FSx for Lustre라는 두 가지 파일 시스템 중에서 선택할 수 있습니다. 자세한 내용은 Amazon FSx를 참조하세요.

AWS Managed Services FAQ의 Amazon FSx for OpenZFS

Q: AMS 계정에서 FSx for OpenZFS를 사용하기 위해 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon FSx OpenZFS에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_fsx_ontap_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 FSx for OpenZFS를 사용할 때 적용되는 제한 사항은 무엇인가요?

Amazon FSx 탄력적 네트워크 인터페이스(ENIs)의 보안 그룹을 교체하려면 보안 그룹이 AMS 환경의 중요한 경계이므로 관리 | 기타 | 기타 | RFCs 업데이트를 제출해야 합니다. 이것이 유일한 제한입니다.

Q: AMS 계정에서 FSx for OpenZFS를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

사전 조건은 없습니다. 그러나가 AMS SSP를 사용하여 AMS 계정에서 Amazon FSx 프로비저닝 설치되어 있어야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon FSx for NetApp ONTAP 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon FSx for NetApp ONTAP 기능에 직접 액세스할 수 있습니다. Amazon FSx for NetApp ONTAP은 NetApp의 인기 있는 ONTAP 파일 시스템을 기반으로 구축된 매우 안정적이고 확장 가능하며 성능이 뛰어나고 기능이 풍부한 파일 스토리지를 제공하는 완전관리형 서비스입니다. NetApp 파일 시스템의 친숙한 기능, 성능, 기능 및 APIs에 완전 관리형의 민첩성, 확장성 및 단순성을 제공합니다 AWS 서비스.

Amazon FSx for NetApp ONTAP은 AWS 또는 온프레미스에서 실행되는 Linux, Windows 및 macOS 컴퓨팅 인스턴스에서 광범위하게 액세스할 수 있는 기능이 풍부하고 빠르고 유연한 공유 파일 스토리지를 제공합니다. FSx for ONTAP은 밀리초 미만의 지연 시간으로 고성능 SSD 스토리지를 제공하며 버튼 클릭만으로 파일을 스냅샷 처리, 복제 및 복제할 수 있으므로 데이터를 빠르고 쉽게 관리할 수 있습니다. 또한 데이터를 저비용의 탄력적 스토리지로 자동으로 계층화하므로 용량을 프로비저닝하거나 관리할 필요가 없으며 소량의 데이터에 대해서만 SSD 스토리지 비용을 지불하면서 워크로드에 대한 SSD 수준의 성능을 달성할 수 있습니다. 완전 관리형 백업과 교차 리전 재해 복구 지원을 통해 가용성과 내구성이 뛰어난 스토리지를 제공하고 널리 사용되는 데이터 보안 및 바이러스 백신 애플리케이션을 지원하여 데이터를 훨씬 더 쉽게 보호하고 보호할 수 있습니다. 온프레미스에서 NetApp ONTAP을 사용하는 고객의 경우 FSx for ONTAP은 애플리케이션 코드 또는 데이터 관리 방법을 변경할 필요 AWS 없이 파일 기반 애플리케이션을 온프레미스에서 로 마이그레이션, 백업 또는 버스트하는 데 이상적인 솔루션입니다.

완전 관리형 서비스인 Amazon FSx for NetApp ONTAP을 사용하면 클라우드에서 안정적이고 성능이 뛰어나며 안전한 공유 파일 스토리지를 간단하게 시작하고 확장할 수 있습니다. Amazon FSx for

NetApp ONTAP을 사용하면 파일 서버 및 스토리지 볼륨 설정 및 프로비저닝, 데이터 복제, 파일 서버 소프트웨어 설치 및 패치, 하드웨어 장애 감지 및 해결, 장애 조치 및 장애 복구 관리, 백업 수동 수행에 대해 더 이상 걱정할 필요가 없습니다. 또한 AWS Identity and Access Management Amazon WorkSpaces AWS Key Management Service및와 AWS 서비스같은 다른와 풍부한 통합을 제공합니다 AWS CloudTrail.

Amazon FSx는 Windows 기반 애플리케이션용 Amazon FSx for Windows File Server와 컴퓨팅 집약적인 워크로드용 Amazon FSx for Lustre라는 두 가지 파일 시스템 중에서 선택할 수 있습니다. 자세한 내용은 Amazon FSx를 참조하세요.

AWS Managed Services FAQ의 Amazon FSx for NetApp ONTAP

Q: AMS 계정에서 Amazon FSx for NetApp ONTAP에 대한 액세스를 요청하려면 어떻게 해야 합니까?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon FSx for NetApp ONTAP에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_fsx_ontap_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon FSx for NetApp ONTAP을 사용할 때 제한 사항은 무엇인가요?

Amazon FSx for NetApp ONTAP 탄력적 네트워크 인터페이스(ENIs)의 보안 그룹을 교체하려면 보안 그룹이 AMS 환경의 중요한 경계이므로 관리 | 기타 | 기타 | RFCs 업데이트를 제출해야 합니다. 이것이 유일한 제한입니다.

Q: AMS 계정에서 Amazon FSx for NetApp ONTAP을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없습니다. 그러나가 AMS SSP를 사용하여 AMS 계정에서 Amazon FSx 프로비저닝 설치되어 있어야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Inspector Classic 프로비저닝

> **Note**
>
> 지원 종료 공지: 2026년 5월 20일에 AWS 는 Amazon Inspector Classic에 대한 지원을 종료합니다. 2026년 5월 20일 이후에는 Amazon Inspector Classic 콘솔 또는 Amazon Inspector Classic 리소스에 더 이상 액세스할 수 없습니다. Amazon Inspector Classic은 더 이상 새 계정과 지난 6개월 동안 평가를 완료하지 않은 계정에서 사용할 수 없습니다. 다른 모든 계정의 경우 액세스는 2026년 5월 20일까지 유효하며, 그 이후에는 Amazon Inspector Classic 콘솔 또

는 Amazon Inspector Classic 리소스에 더 이상 액세스할 수 없습니다. 자세한 내용은 Amazon Inspector Classic 지원 종료를 참조하세요.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Inspector Classic 기능에 직접 액세스할 수 있습니다. Amazon Inspector Classic은 배포된 애플리케이션의 보안 및 규정 준수를 개선하는 데 도움이 되는 자동화된 보안 평가 서비스입니다 AWS. Amazon Inspector Classic은 애플리케이션의 노출, 취약성 및 모범 사례와의 편차를 자동으로 평가합니다. 평가를 수행한 후 Amazon Inspector Classic은 심각도 수준에 따라 우선순위가 지정된 보안 조사 결과의 세부 목록을 생성합니다. 이러한 결과는 직접 검토하거나 Amazon Inspector Classic 콘솔 또는 API를 통해 사용할 수 있는 세부 평가 보고서의 일부로 검토할 수 있습니다. 자세한 내용은 Amazon Inspector Classic을 참조하세요.

AWS Managed Services FAQ의 Amazon Inspector

Q: AMS 계정에서 Amazon Inspector Classic에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon Inspector Classic에 대한 액세스를 요청합니다. 이 RFC는 계정에 `customer_inspector_admin_role` IAM 역할을 프로비저닝합니다. 역할에는 AWS관리형 AmazonInspectorFullAccess 정책이 포함됩니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Inspector Classic을 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Inspector Classic의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Inspector Classic을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Inspector Classic을 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS에서 새 Amazon Inspector 사용

이제 AMS 계정에서 새 Amazon Inspector를 사용할 수 있습니다.

Amazon Inspector Classic의 경우 `customer-inspector-admin-role-ssm-inspector-agent-policy` 및가 필요`AmazonInspectorFullAccess`했습니다. 그러나 `customer-inspector-admin-role`이제 추가를 포함하는 SSPS 역할가 업데이트되었습니다`policyAmazonInspector2FullAccess`. 이 새 정책은 새 버전의 Amazon Inspector에 대한 API 권한을 허용합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Kendra 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Kendra 기능에 직접 액세스할 수 있습니다. Amazon Kendra는 자연어 처리 및 고급 기계 학습 알고리즘을 사용하여 데이터의 검색 질문에 대한 특정 답변을 반환하는 지능형 검색 서비스입니다. 기존 키워드 기반 검색과 달리 Amazon Kendra는 시맨틱 및 컨텍스트 이해 기능을 사용하여 문서가 검색 쿼리와 관련이 있는지 확인합니다. Amazon Kendra는 질문에 대한 구체적인 답변을 반환하므로 경험이 인간 전문가와의 상호 작용에 가깝습니다. Amazon Kendra는 확장성이 뛰어나고 성능 요구 사항을 충족할 수 있으며, Amazon S3 및 Amazon Lex와 같은 다른 AWS 서비스와 긴밀하게 통합되고, 엔터프라이즈급 보안을 제공합니다. 자세한 내용은 Amazon Kendra;를 참조하세요.

AWS Managed Services FAQ의 Amazon Kendra

Q: AMS 계정에서 Amazon Kendra에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Amazon Inspector Classic에 대한 액세스를 요청하려면 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출합니다. 이 RFC는 계정에 `customer_kendra_console_role` IAM 역할을 프로비저닝합니다. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Kendra를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Kendra의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Kendra를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon Kendra를 시작하기 위한 사전 조건이나 종속성은 없습니다. 그러나 특정 사용 사례에 따라 다른 AWS 서비스에 대한 액세스가 필요할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Kinesis Data Streams 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Kinesis Data Streams(KDS) 기능에 직접 액세스할 수 있습니다. Amazon Kinesis Data Streams는 확장성과 내구성이 뛰어난 실시간 데이터 스트리밍 서비스입니다. KDS는 웹 사이트 클릭스트림, 데이터베이스 이벤트 스트림, 금융 거래, 소셜 미디어 피드, IT 로그, 위치 추적 이벤트와 같은 수십만 개의 소스에서 초당 기가바이트의 데이터를 지속적으로 캡처할 수 있습니다. 수집된 데이터는 밀리초 단위로 실시간 대시보드, 실시간 이상 탐지, 동적 요금 등과 같은 실시간 분석 사용 사례를 가능하게 합니다. 자세한 내용은 Amazon Kinesis Data Streams를 참조하세요.

AWS Managed Services FAQ의 Kinesis Data Streams

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Kinesis Data Streams에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 Amazon Kinesis Data Streams에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_kinesis_data_streaming_user_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Kinesis Data Streams를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Kinesis Data Streams의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Kinesis Data Streams를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Kinesis Data Streams를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Kinesis Video Streams 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon Kinesis Video Streams(KVS) 기능에 액세스할 수 있습니다. Amazon Kinesis Video Streams를 사용하면 분석, 기계 학습(ML), 재생 및 기타 처리를 AWS 위해 연결된 디바이스에서 로 비디오를 안전하게 스트리밍할 수 있습니다. Kinesis Video Streams는 수백만 개의 디바이스에서 스트리밍 비디오 데이터를 수집하는 데 필요한 모든 인프라를 자동으로 프로비저닝하고 탄력적으로 확장합니다. 또한 스트림에 비디오 데이터를 안정적으로 저장, 암호화 및 인덱싱하고 easy-to-use APIs를 통해 데이터에 액세스할 수 있습니다. Kinesis Video Streams를 사용하면 라이브 및 온디맨드 보기를 위해 비디오를 재생하고 Amazon Rekognition Video와의 통합을 통해 컴퓨터 비전 및 비디오 분석을 활용하는 애플리케이션과 Apache MxNet, TensorFlow, OpenCV와 같은 ML 프레임워크용 라이브러리를 빠르게 구축할 수 있습니다. 자세한 내용은 Amazon Kinesis Video Streams 참조하세요.

AWS Managed Services FAQ의 Amazon Kinesis Video Streams

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Kinesis Video Streams해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 Amazon Kinesis Video Streams에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_kinesis_video_streaming_user_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Kinesis Video Streams를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Kinesis Video Streams의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Kinesis Video Streams를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Kinesis Video Streams를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Lex 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Lex 기능에 직접 액세스할 수 있습니다. Amazon Lex는 음성과 텍스트를 사용하여 모든 애플리케이션에 대화형 인터페이스를 구축하는 서비스입니다. Amazon Lex는 음성을 텍스트로 변환하기 위한 자동 음성 인식(ASR)과 텍스트의 의도를 인식하기 위한 자연어 이해(NLU)의 고급 딥 러닝 기능을 제공하여 매우 매력적인 사용자 경험과 생생한 대화형 상호 작용으로 애플리케이션을 구축할 수 있습니다. Amazon Lex를 사용하면 이제 모든 개발자가 Amazon Alexa를 지원하는 것과 동일한 딥 러닝 기술을 사용할 수 있으므로 정교한 자연어, 대화형 봇 또는 챗봇을 빠르고 쉽게 구축할 수 있습니다. 자세한 내용은 Amazon Lex를 참조하세요.

AWS Managed Services의 Amazon Lex FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Lex에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_lex_author_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Lex를 사용할 때 제한 사항은 무엇인가요?

Amazon Lex와 Lambda의 통합은 AMS 인프라의 수정을 방지하기 위해 "AMS-" 접두사가 없는 Lambda 함수로 제한됩니다.

Q: AMS 계정에서 Amazon Lex를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Lex를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon MQ 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon MQ 기능에 직접 액세스할 수 있습니다. Amazon MQ는 클라우드에서 메시지 브로커를 설정하고 운영하는 데 도움이 되는 Apache ActiveMQ용 관리형 메시지 브로커 서비스입니다. 메시지 브로커를 사용하면 서로 다른 소프트웨어 시스템이 서로 다른 프로그래밍 언어를 사용하고 플랫폼에서 정보를 통신하고 교환할 수 있습니다. Amazon MQ는 인기 있는 오픈 소스 메시지 브로커인 ActiveMQ의 프로비저닝, 설정 및 유지 관리를 관리하여 운영 부하를 줄입니다. 현재 애플리케이션을 Amazon MQ에 연결하면 JMS, NMS, AMQP, STOMP, MQTT 및 WebSocket을 포함한 메시징에 업계 표준 APIs 및 프로토콜이 사용됩니다. 표준을 사용하면 대부분의 경우 로 마이그레이션할 때 메시징 코드를 다시 작성할 필요가 없습니다 AWS. 자세한 내용은 Amazon MQ란 무엇입니까?를 참조하세요.

AWS Managed Services의 Amazon MQ FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon MQ에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS 계정에서 Amazon MQ를 사용하는 과정은 2단계로 이루어집니다.

1. Amazon MQ 브로커를 프로비저닝합니다. 이렇게 하려면 Amazon MQ 브로커가 포함된 CFN 템플릿을 배포 | 수집 | CloudFormation 템플릿의 스택 | 변경 유형 생성(ct-36cn2avfrrj9v)이 있는 RFC를 통해 제출하거나, 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)이 있는 RFC를 제출하여 Amazon MQ 브로커가 계정에 프로비저닝되도록 요청합니다.
2. Amazon MQ 콘솔에 액세스합니다. Amazon MQ 브로커가 프로비저닝된 후 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 Amazon MQ 콘솔에 액세스할 수 있습니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_mq_console_role`.

계정에 역할이 프로비저닝된 후 페더레이션 솔루션에 온보딩해야 합니다.

Q: AMS 계정에서 Amazon MQ를 사용하는 데 따르는 제한 사항은 무엇인가요?

Amazon MQ의 전체 기능은 AMS 계정에서 사용할 수 있지만, 필요한 승격된 권한으로 인해 정책을 통해 Amazon MQ 브로커를 프로비저닝할 수 없습니다. 계정에서 Amazon MQ 브로커를 프로비저닝하는 방법에 대한 자세한 내용은 위의 섹션을 참조하세요.

Q: AMS 계정에서 Amazon MQ를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon MQ를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Managed Service for Apache Flink 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon Managed Service for Apache Flink 기능에 액세스할 수 있습니다. Managed Service for Apache Flink는 스트리밍 데이터를 분석하고, 실행 가능한 인사이트를 얻고, 비즈니스 및 고객 요구 사항에 실시간으로 대응하는 가장 쉬운 방법입니다. Amazon Managed Service for Apache Flink는 스트리밍 애플리케이션을 빌드, 관리 및 다른 AWS 서비스와 통합하는 복잡성을 줄여줍니다. SQL 사용자는 템플릿과 대화형 SQL 편집기를 사용하여 스트리밍 데이터를 쉽게 쿼리하거나 전체 스트리밍 애플리케이션을 구축할 수 있습니다. Java 개발자는 오픈 소스 Java 라이브러리 및 AWS 통합을 사용하여 정교한 스트리밍 애플리케이션을 빠르게 구축하여 데이터를 실시간으로 변환하고 분석할 수 있습니다. Amazon Managed Service for Apache Flink는 실시간 애플리케이션을 지속적으로 실행하는 데 필요한 모든 것을 처리하고 수신 데이터의 볼륨과 처리량에 맞게 자동으로 확장합니다. Amazon Managed Service for Apache Flink를 사용하면 스트리밍 애플리케이션이 사용하는 리소스에 대해서만 비용을 지불하면 됩니다. 최소 요금이나 설정 비용은 없습니다. 자세한 내용은 Amazon Managed Service for Apache Flink를 참조하세요.

AWS Managed Services FAQ의 Managed Service for Apache Flink

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Managed Service for Apache Flink에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_kinesis_analytics_application_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Managed Service for Apache Flink를 사용할 때 적용되는 제한 사항은 무엇인가요?

- 구성은 AMS 인프라 수정을 방지하기 위해 'AMS-' 또는 'MC-' 접두사가 없는 리소스로 제한됩니다.
- 새 Kinesis Data Streams 또는 Firehose를 삭제하거나 생성할 수 있는 권한이 정책에서 제거되었습니다. 이를 허용하는 또 다른 정책이 있습니다.

Q: AMS 계정에서 Amazon Kinesis Data Streams를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

몇 가지 종속성이 있습니다.

- Amazon Managed Service for Apache Flink를 사용하려면 Managed Service for Apache Flink로 애플리케이션을 구성하기 전에 Kinesis Data Streams 또는 Firehose를 생성해야 합니다.
- 리소스 기반 정책 권한은 특정 입력 데이터 소스를 나타내야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Managed Streaming for Apache Kafka 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 기능에 액세스할 수 있습니다. Amazon Managed Streaming for Apache Kafka는 완전 관리형 AWS 스트리밍 데이터 서비스이므로 Apache Kafka 클러스터 운영 전문가가 될 필요 없이 Apache Kafka를 사용하여 스트리밍 데이터를 처리하는 애플리케이션을 쉽게 구축하고 실행할 수 있습니다. Amazon MSK는 Apache Kafka 클러스터 및 Apache ZooKeeper 노드의 프로비저닝, 구성 및 유지 관리를 관리합니다. Amazon MSK는 AWS 콘솔에 주요 Apache Kafka 성능 지표도 표시합니다.

Amazon MSK는 VPC 네트워크 격리, 컨트롤 플레인 API 권한 부여를 위한 AWS IAM, 저장 데이터 암호화, 전송 중 TLS 암호화, TLS 기반 인증서 인증,에서 보호되는 SASL/SCRAM 인증 등 Apache Kafka 클러스터에 대한 여러 수준의 보안을 제공합니다 AWS Secrets Manager. 자세한 내용은 Amazon MSK를 참조하세요.

AWS Managed Services의 Amazon MSK FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon MSK에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 정책 및 역할을 프로비저닝합니다.

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: Amazon MSK 사용에 대한 제한 사항은 무엇입니까?

Amazon MSK가 구성한 대상으로 브로커 로그를 전송하려면 `AmazonMSKFullAccess` 정책이 IAM 역할에 연결되어 있는지 확인합니다. 따라서 전체 액세스 권한이 이미 있습니다.

Q: Amazon MSK를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

MSK 클러스터를 생성하기 전에 해당 VPC 내에 VPC와 서브넷이 있어야 합니다. 기본적으로 AMS는 기본 AMS VPC 생성의 일부로 이를 다룹니다.

Amazon MSK의 제한에 대해 알아보려면 Amazon MSK 제한을 참조하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon Managed Service for Prometheus 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Managed Service for Prometheus(AMP) 기능에 직접 액세스할 수 있습니다. Amazon Managed Service for Prometheus는 컨테이너 지표에 대한 서버리스, Prometheus 호환 모니터링 서비스로 컨테이너 환경을 대규모로 더 쉽고 안전하게 모니터링할 수 있도록 합니다. Amazon Managed Service for Prometheus를 사용하면 컨테이너화된 워크로드의 성능을 모니터링하는 데 현재 사용하는 것과 동일한 오픈 소스 Prometheus 데이터 모델과 쿼리 언어를 사용할 수 있으며, 기본 인프라를 관리할 필요 없이 향상된 확장성, 가용성 및 보안도 누릴 수 있습니다.

Amazon Managed Service for Prometheus는 워크로드가 확장 및 축소됨에 따라 운영 지표의 수집, 스토리지 및 쿼리를 자동으로 확장합니다. 보안 AWS 서비스와 통합되어 데이터에 빠르고 안전하게 액세스할 수 있습니다. 자세한 내용은 Amazon Managed Service for Prometheus란 무엇입니까?를 참조하세요.

AWS Managed Services FAQ의 AWS Managed Services for Prometheus

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Managed Service for Prometheus에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer-`

`prometheus-console-role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 `customer-prometheus-console-role` 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Managed Service for Prometheus를 사용할 때 적용되는 제한 사항은 무엇인가요?

모든 기능이 지원됩니다.

Q: AMS 계정에서 Amazon Managed Service for Prometheus를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon Managed Service for Prometheus를 시작하기 위한 사전 조건이나 종속성은 없습니다. 그러나 특정 사용 사례에 따라 다른 AWS 서비스에 대한 액세스가 필요할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Personalize 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Personalize 기능에 액세스합니다. Personalize는 개발자가 애플리케이션을 사용하는 고객을 위한 개별화된 추천을 쉽게 생성할 수 있는 기계 학습 서비스입니다.

기계 학습은 맞춤형 제품 및 콘텐츠 추천, 맞춤형 검색 결과, 대상 마케팅 프로모션을 강화하여 고객 참여를 개선하는 데 점점 더 많이 사용되고 있습니다. 그러나 이러한 정교한 권장 시스템을 만드는 데 필요한 기계 학습 기능을 개발하는 것은 복잡성으로 인해 오늘날 대부분의 조직의 범위를 벗어났습니다. Personalize를 사용하면 이전 기계 학습 경험이 없는 개발자가 Amazon.com 다년간 사용해 온 기계 학습 기술을 사용하여 애플리케이션에 정교한 개인화 기능을 쉽게 구축할 수 있습니다.

Personalize를 사용하면 클릭, 페이지 보기, 가입, 구매 등 애플리케이션의 활동 스트림과 기사, 제품, 비디오 또는 음악과 같이 추천하려는 항목의 인벤토리를 제공할 수 있습니다. Amazon Personalize에 연령 또는 지리적 위치와 같은 사용자의 추가 인구 통계 정보를 제공하도록 선택할 수도 있습니다. Personalize는 데이터를 처리 및 검사하고, 의미 있는 것을 식별하고, 올바른 알고리즘을 선택하고, 데이터에 맞게 사용자 지정된 개인화 모델을 훈련 및 최적화합니다. Amazon Personalize에서 분석한 모든 데이터는 비공개로 안전하게 유지되며 사용자 지정 권장 사항에만 사용됩니다. 간단한 API 직접 호출을 통해 맞춤형 추천 제공을 시작할 수 있습니다. 사용한 만큼만 비용을 지불하고 최소 요금 및 사전 약정이 없습니다.

자세한 내용은 Personalize를 참조하세요.

AWS Managed Services Amazon Personalize FAQ

Q: AMS 계정에서 Personalize에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청하고 AWS Personalize에서 권장 사항을 생성하는 데 사용할 데이터가 포함된 S3 버킷을 지정해야 합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다customer_personalize_console_rolecustomer_personalize_service_role.

- customer_personalize_console_role가 계정에 프로비저닝되면 페더레이션 솔루션의 역할을 온보딩해야 합니다. 이외의 다른 기존 역할에 customer_personalize_console_policy를 연결할 수도 있습니다Customer_ReadOnly_Role.
- customer_personalize_service_role가 계정에 제공되면 새 데이터 세트 그룹을 생성할 때 해당 ARN을 참조할 수 있습니다.

현재 AMS Operations는 계정에이 서비스 역할인 도 배포합니다aws_code_pipeline_service_role_policy.

Q: AMS 계정에서 Personalize를 사용할 때 적용되는 제한 사항은 무엇인가요?

Personalize 구성은 AMS 인프라의 수정을 방지하기 위해 'ams-' 또는 'mc-' 접두사가 없는 리소스로 제한됩니다.

Q: AMS 계정에서 Personalize를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 데이터가 저장되는 S3 버킷이 암호화된 경우 Personalize에서 사용하는 역할이 버킷을 해독하도록 허용할 수 있도록 KMS 키 ID를 제공해야 합니다.

  Personalize는 기본 KMS S3 키를 지원하지 않습니다. KMS를 사용해야 하는 경우 사용자 지정 키를 생성하고 변경 유형 KMS 키 | 생성(관리형 자동화)이 있는 RFC를 열어 다음 정책을 추가합니다.

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
```

```
        }
    ]
}
```

- S3 버킷은 다음 버킷 정책을 사용하여 생성해야 합니다. 변경 유형 S3 스토리지 | 정책 생성이 포함된 RFC를 제출하여이 작업을 수행합니다. 이 정책은 Personalize가 데이터에 액세스할 수 있도록 허용합니다. 해당 버킷에는 Personalize에서 사용할 데이터가 포함됩니다.

  JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
}
```

AMS SSP를 사용하여 AMS 계정에서 Amazon Quick 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 빠른 기능에 액세스할 수 있습니다. Quick은 조직의 모든 사람에게 인사이트를 제공하는 빠른 클라우드 기반 비즈니스 인텔리전스 서비스입니다. 완전 관리형 서비스인 Quick을 사용하면 기계 학습(ML) 인사이트가 포함된 대화형 대시보드를 쉽게 생성하고 게시할 수 있습니다. 자세한 내용은 Amazon Quick을 참조하세요.

AWS Managed Services FAQ의 빠른 정보

일반적인 질문과 답변:

Q: AMS 계정에서 Quick에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_quicksight_console_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Quick을 사용할 때 제한 사항은 무엇인가요?

- AWS IAM 정책 종속성으로 인해 Quick의 리소스 설정에 액세스할 수 없습니다. 그러나 AMS 팀은 서비스 활성화 요청에 대한 응답으로 각 리소스를 활성화합니다.
- 개별 사용자 및 그룹에 대한 리소스 액세스는이 모델에서 지원되지 않습니다.이 기능을 사용하면 사용자가 AMS 인프라를 손상시킬 수 있는 IAM 권한을 변경할 수 있기 때문입니다.
- QuickSight 내에서 IAM 자격 증명을 초대하는 기능은 IAM 객체 변경과 관련된 위험으로 인해 지원되지 않습니다.
- 빠른 서비스는 Enterprise와 Standard라는 두 가지 에디션을 제공합니다. 둘 다 AMS에서 지원되는 SSO(Single Sign-On) 옵션을 제공합니다. 그러나 Enterprise Edition에는 Quick을 Active Directory(AD)와 통합하는 옵션이 있습니다. Quick on AMS는 AMS 계정 구조와 빠른 신뢰 요구 사항 간의 비호환성으로 인해 AD와의 통합을 지원하지 않습니다.

Q: AMS 계정에서 Quick을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- AMS가 Quick을 추가하기 위해이 RFC를 수신하면 추가 정보에 대한 서비스 요청이 전송됩니다. 다음을 제공합니다.
  - 빠른 계정 이름(예: *`CustomerName`*`-quicksight`
  - Quick Edition(Standard 및 Enterprise)
  - 빠른 서비스를 활성화할 AWS 리전입니다(기본값은 AMS AWS 리전).
  - 빠른 계정의 알림 이메일 주소입니다.
  - (선택 사항) 분석할 데이터 파일이 있는 S3 버킷입니다.
  - Quick에 연결하는 VPC 및 서브넷 IDs는 빠른 연결과 계정 내 리소스 간의 프라이빗 연결을 지원하는 VPC 연결을 추가하는 기능을 지원합니다.

AMS 운영자는 사용자를 대신하여 가입 프로세스를 수행하고 두 가지 QuickSight 기능을 구성합니다.

- 데이터 소스에 대한 자동 검색.
- VPC 연결.

> **Note**
>
> 로그인 프로세스 중에 승격된 IAM 및 VPC 권한이 필요하므로 AMS 운영자가 이러한 작업을 수행해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Rekognition 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Rekognition 기능에 직접 액세스할 수 있습니다. Amazon Rekognition을 사용하면 기계 학습 전문 지식이 필요 없는 확장성이 뛰어난 검증된 딥 러닝 기술을 사용하여 애플리케이션에 이미지 및 비디오 분석을 쉽게 추가할 수 있습니다. Amazon Rekognition을 사용하면 이미지 및 비디오에서 객체, 사람, 텍스트, 장면 및 활동을 식별하고 부적절한 콘텐츠를 감지할 수 있습니다. 또한 Amazon Rekognition은 다양한 사용자 확인, 인원 계산 및 공공 안전 사용 사례를 위해 얼굴을 감지, 분석 및 비교하는 데 사용할 수 있는 매우 정확한 얼굴 분석 및 얼굴 검색 기능을 제공합니다.

Amazon Rekognition Custom Labels를 사용하면 비즈니스 요구 사항에 맞는 이미지에서 객체와 장면을 식별할 수 있습니다. 예를 들어 조립 라인에서 특정 기계 부품을 분류하거나 비정상 공장을 감지하는 모델을 구축할 수 있습니다. Amazon Rekognition Custom Labels는 모델 개발의 과중한 작업을 처리하므로 기계 학습 경험이 필요하지 않습니다. 식별하려는 객체 또는 장면의 이미지를 제공하면 서비스가 나머지를 처리합니다.

자세한 내용은 Amazon Rekognition을 참조하세요.

AWS Managed Services FAQ의 Amazon Rekognition

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Rekognition에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_rekognition_console_role & customer_rekognition_service_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Rekognition을 사용할 때 제한 사항은 무엇인가요?

Amazon Rekognition의 전체 기능은 Amazon Rekognition 자체 프로비저닝된 서비스 역할에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Rekognition을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon Rekognition Video 스트림 프로세서 또는 데이터 스트림에 대한 소스 스트리밍 비디오를 Kinesis Data Streams에 데이터를 쓸 대상으로 제공하는 Kinesis Video Streams를 사용하는 경우 RFC를 생성할 `kinesisStreamName` 때 AMS에를 제공합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon SageMaker AI 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon SageMaker AI 기능에 액세스할 수 있습니다. SageMaker AI는 모든 개발자와 데이터 과학자에게 기계 학습 모델을 신속하게 구축, 훈련 및 배포할 수 있는 기능을 제공합니다. Amazon SageMaker AI는 데이터에 레이블을 지정하고 준비하며, 알고리즘을 선택하고, 모델을 훈련하고, 배포를 위해 조정하고 최적화하고, 예측하고, 조치를 취하는 전체 기계 학습 워크플로를 포괄하는 완전관리형 서비스입니다. 모델은 훨씬 적은 노력과 비용으로 더 빠르게 프로덕션에 도달할 수 있습니다. 자세한 내용은 Amazon SageMaker AI를 참조하세요.

AWS Managed Services의 SageMaker AI FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 SageMaker AI에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | (ct-1w8z66n899dct) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 및 `customer_sagemaker_admin_role` 서비스 역할을 프로비저닝합니다`AmazonSageMaker-ExecutionRole-Admin`. 계정에 SageMaker AI가 프로비저닝된 후 페더레이션 솔루션에서 `customer_sagemaker_admin_role` 역할을 온보딩해야 합니다. 서비스 역할은 사용자가 직접 액세스할 수 없습니다. SageMaker AI 서비스는 역할 전달에 설명된 대로 다양한 작업을 수행하는 동안 이를 사용합니다.

Q: AMS 계정에서 SageMaker AI를 사용할 때 제한 사항은 무엇인가요?

- 다음 사용 사례는 AMS Amazon SageMaker AI IAM 역할에서 지원되지 않습니다.
  - SageMaker AI Studio는 현재 지원되지 않습니다.
  - 프라이빗 작업 인력을 관리하기 위한 SageMaker AI Ground Truth는 지원되지 않습니다.이 기능을 사용하려면 Amazon Cognito 리소스에 대한 지나치게 허용적인 액세스가 필요하기 때문입니다. 프라이빗 작업 인력을 관리해야 하는 경우 SageMaker AI 및 Amazon Cognito 권한이 결합된 사용자 지정 IAM 역할을 요청할 수 있습니다. 그렇지 않으면 데이터 레이블 지정에 퍼블릭 작업 인력(Amazon Mechanical Turk 지원) 또는 AWS Marketplace 서비스 공급자를 사용하는 것이 좋습니다.
- SageMaker AI 서비스(aws.sagemaker.{region}.notebook, com.amazonaws.{region}.sagemaker.api & com.amazonaws.{region}.sagemaker.runtime)에 대한 API 호출을 지원하는 VPC 엔드포인트 생성

은 SageMaker AI 관련 서비스로만 권한 범위를 지정할 수 없으므로 지원되지 않습니다. 이 사용 사례를 지원하려면 관리 | 기타 | 기타 RFC를 제출하여 관련 VPC 엔드포인트를 생성합니다.

- SageMaker AI에는 모든 ("*") 리소스에 대한 `DeleteAlarm` 권한이 필요하므로 SageMaker AI 엔드포인트 Auto Scaling은 지원되지 않습니다. 엔드포인트 Auto Scaling을 지원하려면 Management | Other | Other RFC를 제출하여 SageMaker AI 엔드포인트에 대한 Auto Scaling을 설정합니다.

Q: AMS 계정에서 SageMaker AI를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 다음 사용 사례에서는 사용 전에 특별한 구성이 필요합니다.
  - S3 버킷을 사용하여 모델 아티팩트와 데이터를 저장하는 경우 배포 | 고급 스택 구성 요소 | S3 스토리지 | RFC 생성과 함께 필수 키워드("SageMaker", "Sagemaker", "sagemaker" 또는 "aws-glue")가 포함된 라는 S3 버킷을 요청해야 합니다.
  - EFS(Elastic File Store)를 사용할 경우 EFS 스토리지를 동일한 서브넷에 구성하고 보안 그룹에서 허용해야 합니다.
  - 다른 리소스가 SageMaker AI 서비스(노트북, API, 런타임 등)에 직접 액세스해야 하는 경우 다음을 통해 구성을 요청해야 합니다.
    - RFC를 제출하여 엔드포인트에 대한 보안 그룹 생성(배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성(자동)).
    - 관리 제출 | 기타 | 기타 | RFC를 생성하여 관련 VPC 엔드포인트를 설정합니다.

Q:가 직접 액세스할 **`customer_sagemaker_admin_role`** 수 있는 리소스에 대해 지원되는 이름 지정 규칙은 무엇입니까? (다음은 업데이트 및 삭제 권한을 위한 것입니다. 리소스에 지원되는 추가 명명 규칙이 필요한 경우 AMS Cloud Architect에 문의하여 상담을 받으세요.)

- 리소스: `AmazonSageMaker-ExecutionRole-*` 역할 전달
  - 권한: SageMaker AI 자체 프로비저닝된 서비스 역할은 AWS Glue AWS RoboMaker및와 함께 SageMaker AI 서비스 역할(`AmazonSageMaker-ExecutionRole-*`) 사용을 지원합니다 AWS Step Functions.
- 리소스: Secrets Manager의 AWS 보안 암호
  - 권한: `AmazonSageMaker-*` 접두사를 사용하여 보안 암호를 설명, 생성, 가져오기, 업데이트합니다.
  - 권한: `SageMaker` 리소스 태그가 로 설정된 경우 설명, 보안 암호 가져오기`true`.
- 리소스:의 리포지토리 AWS CodeCommit
  - 권한: `AmazonSageMaker-*` 접두사가 있는 리포지토리를 생성/삭제합니다.

  - 권한: 접두사 , *sagemaker*, *SageMaker*가 있는 리포지토리의 Git Pull/Push*Sagemaker*.
- 리소스: Amazon ECR(Amazon Elastic Container Registry) 리포지토리
  - 권한: 권한: 다음 리소스 이름 지정 규칙인를 사용할 때 리포지토리 정책을 설정, 삭제 및 컨테이너 이미지를 업로드합니다*sagemaker*.
- 리소스: Amazon S3 버킷
  - 권한: 리소스에 , *Sagemaker* *sagemaker* 및 접두사가 있는 경우 객체 가져오기, 넣기*SageMaker*, 삭제, 멀티파트 업로드 S3 객체 중단aws-glue.
  - 권한: SageMaker 태그가 로 설정된 경우 S3 객체를 가져옵니다true.
- 리소스: Amazon CloudWatch 로그 그룹
  - 권한: 로그 그룹 또는 스트림 생성, 로그 이벤트 넣기, 나열, 업데이트, 생성, 접두사가 있는 로그 전송 삭제/aws/sagemaker/*.
- 리소스: Amazon CloudWatch 지표
  - 권한: , AWS/SageMaker, , AWS/SageMaker/, aws/SageMaker, 및 접두사가 사용되는 경우 지표 데이터를 넣습니다aws/SageMaker/aws/sagemakeraws/sagemaker//aws/sagemaker/..
- 리소스: Amazon CloudWatch Dashboard
  - 권한: 접두사가 사용될 때 대시보드를 생성/삭제합니다customer_*.
- 리소스: Amazon SNS(Simple Notification Service) 주제
  - 권한: *sagemaker*, *SageMaker*및 접두사가 사용되는 경우 주제를 구독/생성합니다*Sagemaker*.

Q: **AmazonSageMakerFullAccess**와의 차이점은 무엇인가 요**customer_sagemaker_admin_role**?

를 customer_sagemaker_admin_role 사용하는는 다음을 제외하고 AmazonSageMakerFullAccess와 거의 동일한 권한을 customer_sagemaker_admin_policy 제공합니다.

- AWS RoboMaker에 연결할 수 있는 권한, Amazon Cognito 및 AWS Glue 리소스.
- SageMaker AI 엔드포인트 자동 크기 조정. Autoscaling에는 CloudWatch 서비스에 대한 허용적 액세스가 필요하므로 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 업데이트(관리형 자동화) 변경 유형(ct-27tuth19k52b4)을 사용하여 RFC를 제출하여 Autoscaling 권한을 임시 또는 영구적으로 승격해야 합니다.

Q: 유휴 데이터 암호화에 AWS KMS 고객 관리형 키를 채택하려면 어떻게 해야 하나요?

관련 IAM 사용자 또는 역할이 키를 사용할 수 있도록 고객 관리형 키에 키 정책이 올바르게 설정되었는지 확인해야 합니다. 자세한 내용은 AWS KMS 키 정책 문서를 참조하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon Simple Email Service 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Simple Email Service(Amazon SES) 기능에 직접 액세스할 수 있습니다. Amazon Simple Email Service는 디지털 마케터와 애플리케이션 개발자가 마케팅, 알림 및 트랜잭션 이메일을 보낼 수 있도록 설계된 클라우드 기반 이메일 전송 서비스입니다.

SMTP 인터페이스 또는 AWS SDKs 중 하나를 사용하여 Amazon SES를 기존 애플리케이션에 직접 통합할 수 있습니다. 또한 Amazon SES의 이메일 전송 기능을 티켓팅 시스템 및 이메일 클라이언트와 같이 이미 사용 중인 소프트웨어에 통합할 수 있습니다.

자세한 내용은 Amazon Simple Email Service를 참조하세요.

AWS Managed Services의 Amazon SES FAQ

Q: AMS 계정에서 Amazon SES에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon SES에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_ses_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon SES를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- Amazon SES가 버킷에 이벤트를 게시할 수 있도록 S3 버킷 정책을 구성해야 합니다.
- Amazon AWS SES가 계정에 속한 Amazon S3, Amazon SES)을 사용하거나 CMK 키를 구성해야 합니다. Amazon SNS

Q: AMS 계정에서 Amazon SES를 사용할 때 제한 사항은 무엇인가요?

다음 리소스를 생성하려면 RFCs를 생성해야 합니다.

- Kinesis Firehose 스트림에 대한 PutEvents 권한이 있는 SMTP 사용자 및 IAM 서비스 역할입니다.

- Amazon SES 규칙 및 구성 세트의 대상이 해당 AWS 리소스와 함께 작동하려면 AMS 변경 유형을 사용하여 S3 버킷, Firehose 스트림, SNS 주제와 같은 새 리소스를 생성해야 합니다.
- SMTP 자격 증명. 새 SMTP 자격 증명을 요청하려면 변경 유형(관리 | 기타 | 기타 | 생성)을 사용합니다. AMS는 자격 증명을 생성하여 Secrets Manager에 추가합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Simple Workflow Service 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Simple Workflow Service(Amazon SWF) 기능에 직접 액세스할 수 있습니다. Amazon Simple Workflow Service는 개발자가 병렬 또는 순차적 단계가 있는 백그라운드 작업을 빌드, 실행 및 확장하는 데 도움이 됩니다. Amazon SWF를 클라우드에서 완전 관리형 상태 트래커 및 작업 코디네이터로 생각할 수 있습니다. 애플리케이션의 단계를 완료하는 데 500밀리초 이상 걸리거나 처리 상태를 추적해야 하거나 작업이 실패할 경우 복구 또는 재시도해야 하는 경우 Amazon SWF가 도와드릴 수 있습니다. 자세한 내용은 Amazon Simple Workflow Service를 참조하세요.

AWS Managed Services의 Amazon SWF FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon SWF에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_swf_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon SWF를 사용할 때 제한 사항은 무엇인가요?

Lambda `InvokeFunction` 권한은이 서비스에 포함되어 있지만 모든 AMS 고객 역할에 추가된 AMS`customer_deny_policy`는 AMS Lambda 함수 및 AMS 소유 리소스에 대한 액세스를 명시적으로 거부합니다. Amazon SWF 내에서 리소스에 태그를 지정하거나 태그를 해제하려면 관리 | 기타 | 기타 변경 유형을 제출합니다.

Q: AMS 계정에서 Amazon SWF를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon SWF는 AWS Lambda 서비스에 종속되므로이 역할의 일부로 Lambda를 호출할 수 있는 권한이 제공되었으며 Amazon SWF에서 Lambda를 호출하는 데 추가 권한이 필요하지 않습니다. 그렇지 않으면 Amazon SWF를 사용하기 위한 사전 조건이 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Textract 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Textract 기능에 직접 액세스할 수 있습니다. Amazon Textract는 간단한 광학 문자 인식(OCR)을 넘어 양식 및 테이블에서 데이터를 식별, 이해 및 추출하는 스캔한 문서에서 인쇄된 텍스트, 필기 및 기타 데이터를 자동으로 추출하는 완전관리형 기계 학습 서비스입니다. 자세한 내용은 Amazon Textract를 참조하세요.

AWS Managed Services FAQ의 Amazon Textract

일반적인 질문과 답변:

Q: Amazon Textract를 AMS 계정에 설정하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 `customer_textract_console_role`, `customer_textract_human_review_execution_role`및 IAM 역할을 프로비저닝합니다`customer_ec2_textract_instance_profile`. 계정에 프로비저닝된 후에는 페더레이션 솔루션`customer_textract_console_role`의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Textract를 사용할 때 제한 사항은 무엇인가요?

AMS 계정에서 Amazon Textract를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 Amazon Textract를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

RFC 배포 | 고급 스택 구성 요소 |S3 스토리지 | 생성(ct-1a68ck03fn98r)을 제출하여 S3 버킷 생성을 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Transcribe 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Transcribe 기능에 직접 액세스할 수 있습니다. Amazon Transcribe는 오디오 파일에서 타임스탬프가 지정된 텍스트 트랜스크립트를 자동으로 생성하는 완전 관리형이며 지속적으로 훈련된 자동 음성 인식 서비스입니다. Amazon Transcribe를 사용하면 개발자가 애플리케이션에 speech-to-text 변환 기능을 쉽게 추가할 수 있습니다. 컴퓨터가 오디오 데이터를 검색하고 분석하는 것은 사실상 불가능합니다. 따라서 애플리케이션에서 사용하기 전에 녹음된 음성을 텍스트로 변환해야 합니다. 과거에는 고객이 값비싼 계약에 서명해야 하고이 작업을 수행하기 위해 기술 스택에 통합하기 어려운 트랜스크립션 공급자와 협력해야 했습니다. 이러한 공급자 중 다수는 콜센터에서 흔히 사용되는 저충실도 전화 오디오와 같은 다양한 시나리오에 잘 적응하지 못하는 오래된 기술을 사용하므로 정확도가 떨어집니다.

Amazon Transcribe는 자동 음성 인식(ASR)이라는 딥 러닝 프로세스를 사용하여 음성을 텍스트로 빠르고 정확하게 변환합니다. Amazon Transcribe를 사용하여 고객 서비스 호출을 트랜스크립션하고, 자막 및 자막을 자동화하고, 미디어 자산에 대한 메타데이터를 생성하여 완전히 검색 가능한 아카이브를 생성할 수 있습니다. Amazon Transcribe Medical을 사용하여 임상 문서 애플리케이션에 의료 speech-to-text 기능을 추가할 수 있습니다. 자세한 내용은 Amazon Transcribe를 참조하세요.

AWS Managed Services FAQ의 Amazon Transcribe

일반적인 질문과 답변:

Q: Amazon Transcribe를 AMS 계정에 설정하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경
유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_transcribe_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Transcribe를 사용할 때 제한 사항은 무엇인가요?

RA 및에서 달리 지정하지 않는 한 트랜스크립션 작업 시 버킷의 접두사로 'customer-transcribe*'를 사용해야 합니다.

Amazon 트랜스크립션 내에서 IAM 역할을 생성할 수 없습니다.

기본 SSPS의 출력 데이터에 서비스 관리형 S3 버킷을 사용할 수 없습니다(필요한 경우 계정 CA에 문의).

AMS 네임스페이스에 속하지 않는 고객 관리형 KMS 키를 사용하려면 위험 승인을 제출해야 합니다.

Q: AMS 계정에서 Amazon Transcribe를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

S3에는 이름이 'customer-transcribe*'인 버킷에 대한 액세스 권한이 있어야 합니다. S3 버킷이 KMS 키로 암호화된 경우 Amazon Transcribe를 사용하려면 KMS가 필요합니다. 버킷을 암호화할 필요가 없는 경우 "KMStranscribeAllow"를 제거할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon WorkSpaces 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 WorkSpaces 기능에 직접 액세스할 수 있습니다. WorkSpaces를 사용하면 사용자를 위해 WorkSpaces라고 하는 가상 클라우드 기반 Microsoft Windows 또는 Amazon Linux 데스크톱을 프로비저닝할 수 있습니다. WorkSpaces를 사용하면 하드웨어를 구매하고 배포하거나 복잡한 소프트웨어를 설치할 필요가 없습니다. 필요에 따라 신속하게 사용자를 추가 또는 제거할 수 있습니다. 사용자는 지원되는 디바이스의 클라이언트 애플

리케이션을 사용하거나 Windows WorkSpaces의 경우 웹 브라우저를 사용하여 WorkSpaces에 액세스하고 기존 온프레미스 Active Directory(AD) 자격 증명을 사용하여 로그인합니다.

자세한 내용은 Amazon WorkSpaces 참조하세요.

AWS Managed Services FAQ의 WorkSpaces

일반적인 질문과 답변:

Q: AMS 계정에서 WorkSpaces에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_workspaces_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 WorkSpaces 사용에 대한 제한 사항은 무엇인가요?

Workspaces의 전체 기능은 Amazon WorkSpaces 자체 프로비저닝된 서비스 역할에서 사용할 수 있습니다.

Q: AMS 계정에서 WorkSpaces를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- WorkSpaces는 AWS 리전별로 제한되므로 WorkSpaces 인스턴스가 호스팅되는 리전과 동일한 AWS 리전에서 AD 커넥터를 구성해야 합니다.

  고객은 다음 두 가지 방법 중 하나를 사용하여 WorkSpaces를 고객 AD에 연결할 수 있습니다.

  1. AD 커넥터를 사용하여 온프레미스 Active Directory 서비스에 대한 인증 프록시(선호):

     WorkSpaces 인스턴스를 온프레미스 디렉터리 서비스와 통합하기 전에 AMS 계정에서 Active Directory(AD) 커넥터를 구성합니다. AD 커넥터는 기존 AD 사용자(도메인)가 기존 온프레미스 AD 자격 증명을 사용하여 WorkSpaces에 연결할 수 있도록 프록시 역할을 합니다. 이는 WorkSpaces가 리소스 포리스트와 사용자 포리스트 역할을 하는 고객의 온프레미스 도메인에 직접 조인되어 고객 측에서 더 많은 제어가 이루어지기 때문에 선호됩니다.

     자세한 내용은 Amazon WorkSpaces 배포 모범 사례(시나리오 1)를 참조하세요.
  2. AWS Microsoft AD, 공유 서비스 VPC 및 온프레미스에 대한 단방향 신뢰와 함께 AD Connector 사용:

     또한 먼저 AMS 관리형 AD에서 온프레미스 AD로의 단방향 발신 신뢰를 구축하여 온프레미스 디렉터리로 사용자를 인증할 수 있습니다. WorkSpaces는 AD 커넥터를 사용하여 AMS 관리형 AD

를 조인합니다. 그러면 온프레미스 환경과 양방향 신뢰를 설정할 필요 없이 AMS 관리형 AD를 통해 WorkSpaces 액세스 권한이 WorkSpaces 인스턴스에 위임됩니다. 이 시나리오에서 사용자 포리스트는 고객 AD에 있고 리소스 포리스트는 AMS 관리형 AD에 있습니다(AMS 관리형 AD에 대한 변경 사항은 RFC를 통해 요청할 수 있음). WorkSpaces VPC와 AMS 관리형 AD를 실행하는 MALZ 공유 서비스 VPC 간의 연결은 Transit Gateway를 통해 설정됩니다.

자세한 내용은 Amazon WorkSpaces 배포 모범 사례(시나리오 6)를 참조하세요.

> **Note**
>
> AD 커넥터는 사전 필수 AD 구성 세부 정보가 포함된 관리 | 기타 | 기타 | 변경 유형 생성 RFC를 제출하여 구성할 수 있습니다. 자세한 내용은 AD 커넥터 생성을 참조하세요. 메서드 2를 사용하여 AMS 관리형 AD에서 리소스 포리스트를 생성하는 경우 AMS 관리형 AD를 실행하여 AMS 공유 서비스 계정에서 다른 관리 | 기타 | 기타 | 변경 유형 RFC를 제출하세요.

AMS SSP를 사용하여 AMS 계정에서 AMS 코드 서비스 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AMS 코드 서비스 기능에 액세스할 수 있습니다. AMS 코드 서비스는 다음에 자세히 설명된 AWS 코드 관리 서비스의 독점 번들링입니다. AMS Code 서비스와 함께 AMS에 모든 서비스를 배포하도록 선택하거나 AMS에 개별적으로 배포할 수 있습니다.

AMS 코드 서비스에는 다음 서비스가 포함됩니다.

- AWS CodeCommit: 보안 Git 기반 리포지토리를 호스팅하는 완전 관리형 소스 제어 서비스입니다. 이를 통해 팀은 안전하고 확장성이 뛰어난 에코시스템에서 코드에 대해 협업할 수 있습니다. CodeCommit을 사용하면 자체 소스 제어 시스템을 운영하거나 인프라 규모 조정에 대해 걱정할 필요가 없습니다. CodeCommit을 사용하여 소스 코드에서 바이너리에 이르기까지 모든 것을 안전하게 저장할 수 있으며 기존 Git 도구와 원활하게 작동합니다. 자세한 내용은 AWS CodeCommit 섹션을 참조하세요.

  AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요AMS SSP를 사용하여 AMS 계정 AWS CodeCommit 에서 프로비저닝.
- AWS CodeBuild: 소스 코드를 컴파일하고, 테스트를 실행하고, 배포할 준비가 된 소프트웨어 패키지를 생성하는 완전 관리형 지속적 통합 서비스입니다. CodeBuild를 사용하면 자체 빌드 서버를 프로비저닝, 관리 및 조정할 필요가 없습니다. CodeBuild는 지속적으로 규모가 조정되며 여러 빌드를 동시에 처리하기 때문에 빌드가 대기열에서 대기하지 않고 바로 처리됩니다. 사전 패키징된 빌드 환경

을 사용하면 신속하게 시작할 수 있으며 혹은 자체 빌드 도구를 사용하는 사용자 지정 빌드 환경을 만들 수 있습니다. CodeBuild를 사용하면 컴퓨팅 리소스에 대한 분당 사용 요금이 청구됩니다. 자세한 내용은 AWS CodeBuild 섹션을 참조하세요.

AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요AMS SSP를 사용하여 AMS 계정 AWS CodeBuild 에서 프로비저닝.

- AWS CodeDeploy: Amazon EC2 및 온프레미스 서버와 같은 다양한 컴퓨팅 서비스에 대한 소프트웨어 배포를 자동화하는 완전 관리형 배포 서비스입니다. AWS CodeDeploy 를 사용하면 새 기능을 신속하게 릴리스하고, 애플리케이션 배포 중에 가동 중지를 방지하고, 애플리케이션 업데이트의 복잡성을 처리할 수 있습니다. AWS CodeDeploy 를 사용하여 소프트웨어 배포를 자동화할 수 있으므로 오류가 발생하기 쉬운 수동 작업이 필요하지 않습니다. 서비스는 배포 요구 사항에 맞게 확장됩니다. 자세한 내용은 AWS CodeDeploy 섹션을 참조하세요.

  AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요AMS SSP를 사용하여 AMS 계정 AWS CodeDeploy 에서 프로비저닝.

- AWS CodePipeline: 빠르고 안정적인 애플리케이션 및 인프라 업데이트를 위해 릴리스 파이프라인을 자동화하는 데 도움이 되는 완전 관리형 지속적 제공 서비스입니다. CodePipeline은 정의한 릴리스 모델을 기반으로 코드 변경이 있을 때마다 릴리스 프로세스의 구축, 테스트 및 배포 단계를 자동화합니다. 이를 통해 기능과 업데이트를 신속하고 안정적으로 제공할 수 있습니다. GitHub AWS CodePipeline 와 같은 타사 서비스 또는 자체 사용자 지정 플러그인과 쉽게 통합할 수 있습니다. AWS CodePipeline를 사용하면 사용한 만큼만 비용을 지불합니다. 선수금이나 장기 약정을 적용하지 않습니다. 자세한 내용은 AWS CodePipeline 섹션을 참조하세요.

  AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요AMS SSP를 사용하여 AMS 계정 AWS CodePipeline 에서 프로비저닝.

AWS Managed Services FAQ의 AMS 코드 서비스

Q: 내 AMS 계정의 AMS 코드 서비스에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_code_suite_console_role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다. 현재 AMS Operations는 CodeBuild`customer_codebuild_service_role`, CodeDeploy 및 CodePipeline `customer_codedeploy_service_role` `aws_code_pipeline_service_role` 서

비스에 대한 계정에 , , 서비스 역할도 배포합니다. CodeBuild 에 대한 추가 IAM 권한이 `customer_codebuild_service_role` 필요한 경우 AMS 서비스 요청을 제출합니다.

> **Note**
>
> 이러한 서비스를 별도로 추가할 수도 있습니다. 자세한 내용은 AMS SSP를 사용하여 AMS 계정 AWS CodePipeline 에서 프로비저닝각각 AMS SSP를 사용하여 AMS 계정 AWS CodeBuild 에서 프로비저닝, AMS SSP를 사용하여 AMS 계정 AWS CodeDeploy 에서 프로비저닝및 단원을 참조하십시오.

Q: AMS 계정에서 AMS 코드 서비스를 사용할 때 제한 사항은 무엇인가요?

- AWS CodeCommit: SNS 주제를 생성할 수 있는 관련 권한이 주어지면 CodeCommit의 트리거 기능이 비활성화됩니다. CodeCommit에 대한 직접 인증은 제한되므로 사용자는 자격 증명 헬퍼로 인증해야 합니다. kms:Encrypt, kms:Decrypt, kms:ReEncrypt, kms:GenereteDataKey, kms:GenerateDataKeyWithoutPlaintext, kms:DescribeKey 등의 일부 KMS 명령도 제한됩니다.
- CodeBuild: AWS CodeBuild 콘솔 관리자 액세스의 경우 리소스 수준에서 권한이 제한됩니다. 예를 들어 CloudWatch 작업은 특정 리소스로 제한되고 `iam:PassRole` 권한은 제어됩니다.
- CodeDeploy: 현재 CodeDeploy는 Amazon EC2/온프레미스에서만 배포를 지원합니다. CodeDeploy를 통한 ECS 및 Lambda에서의 배포는 지원되지 않습니다.
- CodePipeline: CodePipeline 기능, 단계 및 공급자는 다음으로 제한됩니다.
  - 배포 단계: Amazon S3 및 AWS CodeDeploy
  - 소스 단계: Amazon S3, AWS CodeCommit, 비트 버킷 및 GitHub
  - 빌드 단계: AWS CodeBuild 및 Jenkins
  - 승인 단계: Amazon SNS
  - 테스트 단계: AWS CodeBuild, Jenkins, BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load, Runscope API Monitoring
  - 호출 단계: Step Functions 및 Lambda

> **Note**
>
> AMS Operations는 계정에 `customer_code_pipeline_lambda_policy`를 배포합니다. 이는 Lambda 간접 호출 단계에 대한 Lambda 실행 역할에 연결되어야 합니다. 이 정책을 추가할 Lambda 서비스/실행 역할 이름을 입력합니다. 사용자 지정 Lambda 서비스/실행 역할이 없는 경우 AMS는와 `customer_lambda_basic_execution_role` 함께의 사

본customer_code_pipeline_lambda_execution_role인 라는 새 역할을 생성합니다customer_code_pipeline_lambda_policy.

Q: AMS 계정에서 AMS 코드 서비스를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- CodeCommit: S3 버킷이 AWS KMS 키로 암호화된 경우 S3 AWS KMS 를 사용해야 합니다 AWS CodeCommit.
- CodeBuild: 정의된 AWS CodeBuild 서비스 역할에 추가 IAM 권한이 필요한 경우 AMS 서비스 요청을 통해 요청합니다.
- CodeDeploy: 없음.
- CodePipeline: None. AWS supported services—AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy—는 CodePipeline 시작 전 또는 이와 함께 시작해야 합니다. 그러나 이는 AMS 엔지니어가 수행합니다.

AMS SSP를 사용하여 AMS 계정 AWS Amplify 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Amplify 기능에 직접 액세스할 수 있습니다. AWS Amplify 는 프런트엔드 웹 및 모바일 개발자가 풀스택 애플리케이션을 쉽게 빌드, 연결 및 호스팅할 수 있는 완벽한 솔루션입니다. Amplify는 사용 사례가 발전함에 따라 다양한 AWS 서비스를 활용할 수 있는 유연성을 제공합니다. Amplify는 풀스택 iOS, Android, Flutter, Web 및 React Native 앱을 빌드하는 제품을 제공합니다. 자세한 내용은 AWS Amplify를 참조하세요.

AWS Amplify AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS Amplify 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_amplify_console_role. 계정에 프로비저닝한 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

또한 에는 인프라 변경 권한이 있으므로 위험 수락 AWS Amplify 을 제공해야 합니다. 이렇게 하려면 Cloud Service Delivery Manager(CSDM)로 작업하세요.

Q: AMS 계정 AWS Amplify 에서 사용에 대한 제한 사항은 무엇인가요?

RA 및에서 달리 지정하지 않는 한 Amplify로 작업할 때는를 버킷의 접두사`'amplify*'`로 사용해야 합니다.

Q: AMS 계정 AWS Amplify 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Amplify 에서를 사용하기 위한 사전 조건은 없습니다.

Malz 환경만 해당: Amplify의 기본 온보딩 역할은 "customer_amplify_console_role"입니다. 사용자 지정 역할을 사용하려면 먼저 IAM 엔터티를 배포합니다. 그런 다음 추가 RFC를 생성하여 애플리케이션 계정에 대한 서비스 제어 정책 허용 목록에 사용자 지정 역할을 추가합니다.

AMS SSP를 사용하여 프로비저닝 AWS AppSync

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS AppSync 기능에 액세스할 수 있습니다.는 유연한 API를 생성하여 하나 이상의 데이터 소스에서 데이터에 안전하게 액세스, 조작 및 결합할 수 있도록 함으로써 애플리케이션 개발을 간소화 AWS AppSync 합니다. AWS AppSync 는 애플리케이션이 필요한 데이터를 정확히 가져올 수 있도록 GraphQL을 사용하는 관리형 서비스입니다.

AWS AppSync를 사용하면 NoSQL 데이터 스토어, 관계형 데이터베이스, HTTP APIs 및 사용자 지정 데이터 소스와 같은 다양한 데이터 소스에서 실시간 업데이트가 필요한 애플리케이션을 포함하여 확장 가능한 애플리케이션을 구축할 수 있습니다 AWS Lambda. 모바일 및 웹 앱의 경우는 디바이스가 오프라인 상태가 되면 로컬 데이터 액세스를 제공하고, 다시 온라인 상태가 되면 사용자 지정 가능한 충돌 해결을 통한 데이터 동기화를 AWS AppSync 제공합니다. 자세한 내용은 AWS AppSync를 참조하세요.

AWS AppSync AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS AppSync 에서 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)
를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니
다`customer_appsync_service_role``customer_appsync_author_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션`customer_appsync_author_role`에서를 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS AppSync?

- AppSync에서 데이터 소스를 생성할 때 고객은 이전에 생성한 서비스 역할을 지정해야 하며, 새 역할 생성은 허용되지 않으므로 액세스 거부를 반환합니다.

- AppSync 역할은 AMS 인프라에 대한 수정을 방지하기 위해 'AMS-' 또는 'MC-' 접두사를 포함하는 리소스로 권한을 제한하도록 구성됩니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS AppSync?

서비스는 여러 다른 서비스를 데이터 소스로 사용할 수 있도록 허용합니다. 이러한 서비스를 사용할 수 있는 기본 권한은 서비스 역할(`customer_appsync_service_role`)에 포함되지만 서비스를 사용할 때는 서비스 역할을 수동으로 선택해야 합니다.

AMS SSP를 사용하여 AMS 계정 AWS App Mesh 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS App Mesh 기능에 액세스할 수 있습니다.는 애플리케이션 수준 네트워킹을 AWS App Mesh 제공하여 서비스가 여러 유형의 컴퓨팅 인프라에서 서로 쉽게 통신할 수 있도록 합니다. App Mesh는 서비스가 통신하는 방식을 표준화하여 end-to-end 가시성을 제공하고 애플리케이션의 고가용성을 보장합니다.

AWS App Mesh 를 사용하면 여러 유형의 컴퓨팅 인프라에 구축된 서비스에 대한 일관된 가시성과 네트워크 트래픽 제어를 제공하여 서비스를 쉽게 실행할 수 있습니다. App Mesh를 사용하면 애플리케이션 코드를 업데이트하여 모니터링 데이터가 수집되거나 서비스 간에 트래픽이 라우팅되는 방식을 변경할 필요가 없습니다. App Mesh는 모니터링 데이터를 내보내도록 각 서비스를 구성하고 애플리케이션 전체에서 일관된 통신 제어 로직을 구현합니다. 따라서 오류의 정확한 위치를 빠르게 파악하고 장애가 발생하거나 코드 변경을 배포해야 할 때 네트워크 트래픽을 자동으로 다시 라우팅할 수 있습니다. 자세한 내용은 AWS App Mesh를 참조하세요.

AWS App Mesh AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS App Mesh 에서 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)
를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니
다`customer_app_mesh_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS App Mesh?

의 전체 기능은 AMS 계정에서 AWS App Mesh 사용할 수 있습니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS App Mesh?

AMS 계정 AWS App Mesh 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Audit Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Audit Manager 기능에 액세스합니다. Audit Manager를 사용하면 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 평가하는 방법을 간소화할 수 있습니다. Audit Manager는 증거 수집을 자동화하여 정책, 절차 및 활동이 효과적으로 운영되는지 더욱 쉽게 평가할 수 있도록 합니다. 감사 시기가 되면 Audit Manager는 제어에 대한 이해관계자 검토를 관리하고 수동 작업을 크게 줄이면서 감사 준비 보고서를 작성하는 데 도움이 됩니다. 자세한 내용은 Audit Manager를 참조하세요.

AWS Audit Manager AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Audit Manager 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AWS 서비스 RFC 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화) (ct-3qe6io8t6jtny) 제출을 통해 액세스를 요청할 수 있습니다. 이 RFC는 계정에서 다음 IAM 역할을 프로비저닝합니다`customer-audit-manager-admin-Role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Audit Manager?

AMS 계정 AWS Audit Manager 에서를 사용하는 데는 제한이 없습니다. 에 대한 전체 기능이 AWS Audit Manager 제공됩니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS Audit Manager?

1. 보고서/평가가 상주할 s3 버킷을 AMS에 제공해야 합니다.
2. 서비스로 암호화하려면 사용할 KMS CMK ARN을 AMS에 제공해야 합니다.
3. 주제에 SNS 알림을 보내려면 주제 또는 arn의 이름을 제공해야 합니다.
4. (선택 사항) Audit Manager에서 다중 계정 랜딩 존의 일부로 Organizations를 활성화하고 위임된 관리자 계정을 원하는 경우 추가 사전 요구 사항이 있습니다. RFC(관리 | AWS 서비스 | 호환 서비스| 추가)에 대한 설명 필드에서 위임된 관리자 계정을 Audit Manager 설정의 일부로 사용하고 아래 세부 정보를 제공하려고 한다고 언급합니다.
   - KMS CMK ARN(처음에 Audit Manager를 설정하는 데 사용됨)
   - Audit Manager가이 다중 계정 랜딩 존의 일부로 사용할 수 있는 위임된 관리자 계정 ID(MALZ 애플리케이션 계정일 수 있음)

AMS SSP를 사용하여 AMS 계정 AWS Batch 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Batch 기능에 액세스할 수 있습니다. 개발자, 과학자 및 엔지니어가 수십만 개의 배치 컴퓨팅 작업을 쉽고 효율적으로 실행할 수 AWS Batch 있습니다 AWS.는 제출된 배치 작업의 볼륨 및 특정 리소스 요구 사항에 따라 최적의 수량과 유형의 컴퓨팅 리소스(예: CPU 또는 메모리 최적화 인스턴스)를 AWS Batch 동적으로 프로비저닝합니다. 를 사용하면 작업을 실행하는 데 사용하는 배치 컴퓨팅 소프트웨어 또는 서버 클러스터를 설치하고 관리할 AWS Batch필요가 없으므로 결과를 분석하고 문제를 해결하는 데 집중할 수 있습니다. 자세한 내용은 AWS Batch를 참조하세요.

AWS Batch AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Batch 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

1. 액세스를 요청하려면 RFC 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct)를 AWS Batch제출합니다. 이 RFC는 계정에서 다음과 같은 IAM 역할 및 정책을 프로비저닝합니다.

IAM 역할:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

정책:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. 계정에 프로비저닝한 후에는 페더레이션 솔루션`customer_batch_console_role`의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Batch?

컴퓨팅 환경을 생성할 때 EC2 인스턴스에 "customer_batch" 또는 "customer-batch"로 태그를 지정해야 합니다. 인스턴스에 태그가 지정되지 않은 경우 작업이 완료되면 인스턴스가 일괄적으로 종료되지 않습니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS Batch?

AMS 계정 AWS Batch 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Certificate Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Certificate Manager (ACM) 기능에 액세스합니다. AWS Certificate Manager 는 서비스 및 내부 연결 리소스와 함께 사용할 퍼블릭 및 프라이빗 SSL/TLS(Secure Sockets Layer/Transport Layer Security) 인증서를 프로비저닝, 관리 및 배포할 수 있는 AWS 서비스입니다. SSL/TLS 인증서는 네트워크 통신을 보호하고 인터넷을 통한 웹 사이트 및 프라이빗 네트워크의 리소스의 ID를 설정하는 데 사용됩니다. SSL/TLS 인증서를 구매, 업로드 및 갱신하는 데 시간이 많이 걸리는 수동 프로세스를 AWS Certificate Manager 제거합니다.

를 사용하면 인증서를 요청하고, Elastic Load Balancer, Amazon CloudFront 배포 및 APIs Gateway의 API와 같은 ACM 통합 AWS 리소스에 배포하고,가 인증서 갱신을 AWS Certificate Manager 처리하도록 AWS Certificate Manager할 수 있습니다. 또한 내부 리소스에 대한 프라이빗 인증서를 생성하고 인증서 수명 주기를 중앙에서 관리할 수 있도록 합니다. ACM 통합 서비스와 함께 사용하기 AWS Certificate Manager 위해를 통해 프로비저닝된 퍼블릭 및 프라이빗 인증서는 무료입니다. 애플리케이션을 실행하기 위해 생성한 AWS 리소스에 대해서만 비용을 지불합니다. 를 사용하면의 작업 AWS Private CA 과 발급한 프라이빗 인증서에 대해 매월 AWS Private Certificate Authority요금을 지불합니다. 자세한 내용은 AWS Certificate Manager - AWS 문서를 참조하세요.

AWS Managed Services FAQ의 ACM

일반적인 질문과 답변:

Q: AMS 계정 AWS Certificate Manager 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_acm_create_role`. 이 역할을 사용하여 ACM 인증서를 생성하고 관리할 수 있습니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

`customer_acm_create_role` IAM 역할을 추가하지 않은 경우에도 다음 변경 유형을 사용하여 ACM 인증서를 생성할 수 있습니다.

- ACM | 퍼블릭 인증서 생성
- ACM | 프라이빗 인증서 생성
- 추가 SANs 포함된 ACM 인증서 | 생성

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Certificate Manager?

기존 인증서를 삭제하거나 수정하려면 변경 요청(RFC)을 AMS에 제출해야 합니다. 이러한 작업을 수행하려면 전체 관리자 액세스가 필요합니다(관리 | 고급 스택 구성 요소 | ACM | 인증서 변경 유형 삭제(ct-1q8q56cmwqj9m) 사용). IAM 정책은 태그 이름(mc*, ams* 등)을 기반으로 권한을 제외할 수 없습니다. 인증서에는 비용이 발생하지 않으므로 사용하지 않는 인증서를 삭제하는 것은 시간에 민감하지 않습니다.

Q: Certificate Manager를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

기존 퍼블릭 DNS 이름 및 DNS CNAME 레코드를 생성하기 위한 액세스 권한은 관리형 계정에서 호스팅할 필요가 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Private Certificate Authority 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Private Certificate Authority 기능에 직접 액세스할 수 있습니다. 프라이빗 인증서는 서버, 모바일, IoT 디바이스 및 애플리케이션과 같은 프라이빗 네트워크에서 연결된 리소스 간의 통신을 식별하고 보호하는 데 사용됩니다. AWS Private CA 는 프라이빗 인증서의 수명 주기를 쉽고 안전하게 관리하는 데 도움이 되는 관리형 프라이빗 CA 서비스입니다.는 프라이빗 CA 운영에 대한 선결제 투자 및 지속적인 유지 관리 비용 없이 가용성이 높은 프라이빗 CA 서비스를 AWS Private CA 제공합니다.는 ACM의 인증서 관리 기능을 프라이빗 인증서로 AWS Private CA 확장하여 퍼블릭 및 프라이빗 인증서를 중앙에서 생성하고 관리할 수 있습니다. AWS 관리 콘솔 또는 ACM API를 사용하여 AWS 리소스에 대한 프라이빗 인증서를 쉽게 생성하고 배포할 수 있습니다. EC2 인스턴스, 컨테이너, IoT 디바이스 및 온프레미스 리소스의 경우 프라이빗 인증서를 쉽게 생성 및 추적하고 자체 클라이언트 측 자동화 코드를 사용하여 배포할 수 있습니다. 또한 사용자 지정 인증서 수명, 키 알고리즘 또는 리소스 이름이 필요한 애플리케이션에 대해 프라이빗 인증서를 생성하고 직접 관리할 수 있는 유연성이 있습니다. 자세한 내용은 섹션을 참조하세요AWS Private CA.

AWS Private CA AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Private CA 에서 액세스를 요청하려면 어떻게 해야 하나요?

AWS 서비스 RFC(관리 | AWS 서비스 | 호환 서비스) 제출을 통해 액세스를 요청합니다. 이 RFC를 통해 계정에 다음 IAM 역할이 프로비저닝됩니다`customer_acm_pca_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Private CA?

현재 AWS Resource Access Manager (AWS RAM)는 교차 계정을 공유하는 데 사용할 수 AWS Private CA 없습니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS Private CA?

1. CRL을 생성하려는 경우 저장할 S3 버킷이 필요합니다. AWS Private CA 는 지정한 Amazon S3 버킷에 CRL을 자동으로 저장하고 주기적으로 업데이트합니다. CRL을 설정하려면 먼저 S3 버킷에 아래 버킷 정책이 있어야 합니다. 이 요청을 진행하려면 다음과 같이 ct-0fpjlxa808sh2(관리 | 고급 스택 구성 요소 | S3 스토리지 | 정책 업데이트)를 사용하여 RFC를 생성합니다.

- S3 버킷 이름 또는 ARN을 입력합니다.
- 아래 정책을 RFC에 복사하고를 원하는 S3 버킷 이름으로 `bucket-name` 바꿉니다.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
```

```
    ]
}
```

2. 위의 S3 버킷이 암호화된 경우 서비스 보안 주체 acm-pca.amazonaws.com 복호화 권한이 필요합니다. 이 요청을 진행하려면 다음과 같이 ct-3ovo7px2vsa6n(관리 | 고급 스택 구성 요소 | KMS 키 | 업데이트)을 사용하여 RFC를 생성합니다.

- 정책을 업데이트해야 하는 KMS 키 ARN을 제공합니다.
- 아래 정책을 RFC에 복사하고를 원하는 S3 버킷 이름으로 `bucket-name` 바꿉니다.

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
   }
}
```

3. AWS Private CA CRLs S3 설정 "새 ACLs)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단"을 지원하지 않습니다. 가 ACM Private CA용 CRLs을 안전하게 생성 및 저장하는 방법에 설명된 대로 CRL을 AWS Private CA 작성하도록 허용하려면 S3 계정 및 버킷에서이 설정을 비활성화해야 합니다. 비활성화하려면 ct-0xdawir96cy7k(관리 | 기타 | 기타 | 업데이트)를 사용하여 새 RFC를 생성하고 위험 수락을 연결합니다. https://aws.amazon.com/blogs/security/how-to-securely-create-and-store-your-crl-for-acm-private-ca/ 위험 수락에 대한 질문이 있는 경우 클라우드 아키텍트에 문의하세요.

AMS SSP를 사용하여 AMS 계정에서 AWS CloudEndure 프로비저닝

> **Note**
>
> 가 성공적으로 출시되면 이제 모든 AWS 리전에서 AWS Application Migration Service CloudEndure 마이그레이션 서비스의 수명이 종료됩니다. GovCloud 리전 및 상용 리전으로 AWS Application Migration Service 의 리프트 앤 시프트 마이그레이션에는를 사용하는 것이 좋습니다. 자세한 내용은 란 무엇입니까 AWS Application Migration Service?를 참조하세요. 를 사용하려면 CA에 AWS Application Migration Service문의하여 안내를 받으세요.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CloudEndure 기능에 액세스합니다. AWS CloudEndure 마이그레이션은 물리적, 가상 및 클라우드 기반 인프라에서로 대규모 마이그레이션을 간소화, 가속화 및 자동화합니다 AWS. CloudEndure 재해 복구(DR)는 랜섬웨어 및 서버 손상을 포함한 모든 위협으로부터 가동 중지 시간과 데이터 손실을 방지합니다.

AWS Managed Services FAQ의AWS CloudEndure

Q: AMS 계정에서 CloudEndure에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 사용자를 프로비저닝합니다`customer_cloud_endure_user`. 계정에 프로비저닝된 후에는 사용자의 액세스 키와 보안 키가 AWS Secrets Manager에서 공유됩니다.

이러한 정책은 및 계정에도 프로비저닝됩니다`customer_cloud_endure_policy``customer_cloud_endure_deny_policy`.

또한 애플리케이션 통합을 위한 CloudEndure DR 솔루션에는 인프라 변경 권한이 있으므로 위험 수락을 제공해야 합니다. 이렇게 하려면 클라우드 서비스 제공 관리자(CSDM)와 협력하세요.

Q: AMS 계정에서 CloudEndure를 사용하는 데 따르는 제한 사항은 무엇인가요?

Cloud Endure 복제 및 변환 인스턴스는 지정한 서브넷에서만 시작할 수 있습니다.

Q: AMS 계정에서 CloudEndure를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요? RFC 양방향 서신을 통해 다음을 공유합니다.

- 시작할 복제 및 변환 인스턴스에 대한 VPC 서브넷 세부 정보입니다.
- EBS 볼륨이 암호화된 경우 KMS 키 Amazon 리소스 이름(ARN)입니다.

AMS SSP를 사용하여 AMS 계정 AWS CloudHSM 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS CloudHSM 기능에 직접 액세스할 AWS CloudHSM 수 있습니다. 기업, 계약, 및 AWS 클라우드 내에서 전용 하드웨어 보안 모듈(HSM) 인스턴스를 사용하여 데이터 보안을 위한 규정 준수 요구 사항을 충족합니다. AWS및 AWS Marketplace 파트너, 는 AWS 플랫폼 내에서 민감한 데이터를 보호하기 위한 다양한 솔루션을 제공합니다. 그러나 암호화 키 관리를 위한 계약 또는 규제 명령이 적용되는 일부 애플리케이션 및 데이터의 경우 추가 보호가 필요할 수 있습니다.는 기존 데이터 보호 솔루션을 AWS CloudHSM 보완하고 보안 키 관리를 위해 정부 표준에 따라 설계되고 검증된 HSMs 내에서 암호화 키를 보호할 수 있습니다.를 AWS CloudHSM 사용하면를 안전하게 생성하고, 스토어, 및는 사용자만 키에 액세스할 수 있는 방식으로 데이터 암호화에 사용되는 암호화 키를 관리합니다. 자세한 내용은 AWS CloudHSM를 참조하세요.

AWS CloudHSM AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS CloudHSM 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS 계정에서를 사용하는 과정은 2단계로 이루어집니다.

1. AWS CloudHSM 클러스터를 요청합니다. 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76) 변경 유형을 사용하여 RFC를 제출하여이 작업을 수행합니다. 다음 세부 정보를 포함합니다.
   - AWS 리전.
   - VPC ID/ARN. 제출하는 RFC와 동일한 계정에 있는 VPC ID/VPC ARN을 제공합니다.
   - 클러스터에 대해 최소 두 개의 가용 영역을 지정합니다.
   - HSM 클러스터에 연결할 Amazon EC2 인스턴스 ID입니다.
2. AWS CloudHSM 콘솔에 액세스합니다. 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여이 작업을 수행합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_cloudhsm_console_role`.

계정에 역할이 프로비저닝된 후 페더레이션 솔루션에 온보딩해야 합니다.

Q: AMS 계정 AWS CloudHSM 에서 사용에 대한 제한 사항은 무엇인가요?

AWS CloudHSM 콘솔에 대한 액세스로는 클러스터를 생성, 종료 또는 복원할 수 없습니다. 이러한 작업을 수행하려면 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76) 변경 유형을 제출합니다.

Q: AMS 계정 AWS CloudHSM 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

VPC 내의 클라이언트 Amazon EC2 인스턴스를 통해 포트 2225를 사용하는 TCP 트래픽을 허용하거나 HSM 클러스터에 액세스하려는 온프레미스 서버에 Direct Connect VPN을 사용해야 합니다. AWS CloudHSM 는 보안 그룹 및 네트워크 인터페이스에 Amazon EC2를 사용합니다. 로그 모니터링 또는 감사를 위해 HSM은 모든 로컬 HSM 디바이스 활동에 CloudTrail(AWS API 작업) 및 CloudWatch Logs를 사용합니다.

Q: AWS CloudHSM 클라이언트 및 관련 소프트웨어 라이브러리에는 누가 업데이트를 적용하나요?

라이브러리 및 클라이언트 업데이트를 적용할 책임은 사용자에게 있습니다. CloudHSM 버전 기록 페이지에서 릴리스를 모니터링한 다음 CloudHSM 클라이언트 업그레이드를 사용하여 업데이트를 적용해야 합니다.

> **Note**
>
> HSM 어플라이언스용 소프트웨어 패치는 항상 서비스에서 AWS CloudHSM 자동으로 적용됩니다.

AMS SSP를 사용하여 AMS 계정 AWS CodeBuild 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodeBuild 기능에 액세스할 수 있습니다. AWS CodeBuild 는 소스 코드를 컴파일하고, 테스트를 실행하고, 배포할 준비가 된 소프트웨어 패키지를 생성하는 완전 관리형 지속적 통합 서비스입니다. CodeBuild를 사용하면 자체 빌드 서버를 프로비저닝, 관리 및 조정할 필요가 없습니다. CodeBuild는 지속적으로 규모가 조정되며 여러 빌드를 동시에 처리하기 때문에 빌드가 대기열에서 대기하지 않고 바로 처리됩니다. 사전 패키징된 빌드 환경을 사용하면 신속하게 시작할 수 있으며 혹은 자체 빌드 도구를 사용하는 사용자 지정 빌드 환경을 만들 수 있습니다. CodeBuild를 사용하면 컴퓨팅 리소스에 대한 분당 사용 요금이 청구됩니다. 자세한 내용은 AWS CodeBuild를 참조하세요.

> **Note**
>
> 단일 RFC로 CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 온보딩하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음 , `customer_codebuild_service_role` `customer_codedeploy_service_role`및 세 가지 역할이 모두 계정에 프로비저닝`aws_code_pipeline_service_role`됩니다. 계정에서 프로비저닝한 후 페더레이션 솔루션의 역할을 온보딩해야 합니다.

AWS Managed Services FAQ의 CodeBuild

일반적인 질문과 답변:

Q: AMS 계정 AWS CodeBuild 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS 계정 AWS CodeBuild 에서를 사용하는 과정은 2단계로 이루어집니다.

1. S3 버킷, Amazon CloudWatch 및 로그 그룹과 AWS 조정하도록 빌드 프로세스를 `CodeBuild Service Role` 위한 프로비저닝
2. CodeBuild 콘솔에 대한 액세스 요청

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 AMS 계정에 둘 다 설정하도록 요청할 수 있습니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS CodeBuild 에서 사용에 대한 제한 사항은 무엇인가요?

AWS CodeBuild 콘솔 관리자 액세스의 경우 리소스 수준에서 권한이 제한됩니다. 예를 들어 CloudWatch 작업은 특정 리소스로 제한되고 `iam:PassRole` 권한은 제어됩니다.

Q: AMS 계정에서 CodeBuild를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

정의된 AWS CodeBuild 서비스 역할에 추가 IAM 권한이 필요한 경우 AMS 서비스 요청을 통해 요청합니다.

AMS SSP를 사용하여 AMS 계정 AWS CodeCommit 에서 프로비저닝

> **Note**
>
> AWS 는 2024년 7월 25 AWS CodeCommit일부터 새로운 고객 액세스를 종료했습니다. AWS CodeCommit 기존 고객은 서비스를 정상적으로 계속 사용할 수 있습니다. AWS 는에 대한 보안, 가용성 및 성능 개선에 계속 투자 AWS CodeCommit하지만 새로운 기능을 도입할 계획은 없습니다.
>
> AWS CodeCommit Git 리포지토리를 다른 Git 공급자로 마이그레이션하려면 클라우드 아키텍트(CA)에 문의하여 지침을 받으세요. Git 리포지토리 마이그레이션에 대한 자세한 내용은 AWS CodeCommit 리포지토리를 다른 Git 공급자로 마이그레이션하는 방법을 참조하세요.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodeCommit 기능에 액세스할 수 있습니다. AWS CodeCommit 는 보안 Git 기반 리포지토리를 호스팅하는 완전 관리형 소스 제어 서비스입니다. 이를 통해 팀은 안전하고 확장성이 뛰어난 에코시스템에서 코드에 대해 협업할 수 있습니다. CodeCommit을 사용하면 자체 소스 제어 시스템을 운영하거나 인프라 규모 조정에 대해 걱정할 필요가 없습니다. CodeCommit을 사용하여 소스 코드에서 바이너리에 이르기까지 모든 것을 안전하게 저장할 수 있으며 기존 Git 도구와 원활하게 작동합니다. 자세한 내용은 AWS CodeCommit를 참조하세요.

> **Note**
>
> 단일 RFC로 CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 온보딩하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음 , `customer_codebuild_service_role` `customer_codedeploy_service_role`및 세 가지 역할이 모두 계정에 프로비저닝`aws_code_pipeline_service_role`됩니다. 계정에서 프로비저닝한 후 페더레이션 솔루션의 역할을 온보딩해야 합니다.

AWS Managed Services FAQ의 CodeCommit

Q: AMS 계정에서 CodeCommit에 대한 액세스를 요청하려면 어떻게 해야 합니까?

AWS CodeCommit 콘솔 및 데이터 액세스 역할은 두 개의 AWS 서비스 RFCs

- Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 AWS CodeCommit 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_codecommit_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

  데이터 액세스(예: 훈련 및 개체 목록)에는 S3 데이터 소스(필수), 출력 버킷(필수) 및 KMS(선택 사항)를 지정하는 각 데이터 소스에 대해 별도의 CTs가 필요합니다. 모든 데이터 소스에 액세스 역할이 부여된 한 AWS CodeCommit 작업 생성에는 제한이 없습니다. 데이터 액세스를 요청하려면 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76)을 사용하여 RFC를 제출합니다.

Q: AMS 계정 AWS CodeCommit 에서 사용에 대한 제한 사항은 무엇인가요?

CodeCommit의 트리거 기능은 SNS 주제를 생성할 수 있는 관련 권한으로 인해 비활성화됩니다. CodeCommit에 대한 직접 인증은 제한되므로 사용자는 자격 증명 헬퍼로 인증해

야 합니다. `kms:Encrypt`, , , `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenereteDataKey` `kms:GenerateDataKeyWithoutPlaintext`등의 일부 KMS 명령도 제한됩니 다`kms:DescribeKey`.

Q: AMS 계정 AWS CodeCommit 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

S3 버킷이 KMS 키로 암호화된 경우를 사용하려면 S3 및 KMS가 필요합니다 AWS CodeCommit.

AMS SSP를 사용하여 AMS 계정 AWS CodeDeploy 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodeDeploy 기능에 액세스할 수 있습니다. AWS CodeDeploy 는 Amazon EC2 AWS Fargate AWS Lambda및 온프레미스 서버와 같은 다양한 컴퓨팅 서비스에 대한 소프트웨어 배포를 자동화하는 완전 관리형 배포 서비스입니다. AWS CodeDeploy 는 새 기능을 신속하게 릴리스하고, 애플리케이션 배포 중 가동 중지 시간을 방지하고, 애플리케이션 업데이트의 복잡성을 처리할 수 있도록 지원합니다. AWS CodeDeploy 를 사용하여 소프트웨어 배포를 자동화할 수 있으므로 오류가 발생하기 쉬운 수동 작업이 필요하지 않습니다. 서비스는 배포 요구 사항에 맞게 확장됩니다. 자세한 내용은 AWS CodeDeploy를 참조하세요.

> **Note**
>
> 단일 RFC로 CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 온보딩하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음 , `customer_codebuild_service_role` `customer_codedeploy_service_role`및 세 가지 역할이 모두 계정에 프로비저닝`aws_code_pipeline_service_role`됩니다. 계정에서 프로비저닝한 후 페더레이션 솔루션의 역할을 온보딩해야 합니다.

AWS Managed Services FAQ의 CodeDeploy

Q: AMS 계정에서 CodeDeploy에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 CodeDeploy에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_codedeploy_console_role``customer_codedeploy_service_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 `customer_codedeploy_console_role` 역할을 온보딩해야 합니다.

Q: AMS 계정에서 CodeDeploy를 사용할 때 제한 사항은 무엇인가요?

현재 컴퓨팅 플랫폼은 Amazon EC2/온프레미스로만 지원됩니다. 블루/그린 배포는 지원되지 않습니다.

Q: AMS 계정에서 CodeDeploy를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 CodeDeploy를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS CodePipeline 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodePipeline 기능에 액세스할 수 있습니다. AWS CodePipeline 는 빠르고 안정적인 애플리케이션 및 인프라 업데이트를 위해 릴리스 파이프라인을 자동화하는 데 도움이 되는 완전 관리형 지속적 전송 서비스입니다. CodePipeline은 정의한 릴리스 모델을 기반으로 코드 변경이 있을 때마다 릴리스 프로세스의 구축, 테스트 및 배포 단계를 자동화합니다. 이를 통해 기능과 업데이트를 신속하고 안정적으로 제공할 수 있습니다. GitHub AWS CodePipeline 와 같은 타사 서비스 또는 자체 사용자 지정 플러그인과 쉽게 통합할 수 있습니다. AWS CodePipeline를 사용하면 사용한 만큼만 비용을 지불합니다. 선수금이나 장기 약정을 적용하지 않습니다. 자세한 내용은 AWS CodePipeline를 참조하세요.

> **Note**
>
> 단일 RFC로 CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 온보딩하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음 , `customer_codebuild_service_role` `customer_codedeploy_service_role`및 세 가지 역할이 모두 계정에 프로비저닝`aws_code_pipeline_service_role`됩니다. 계정에서 프로비저닝한 후 페더레이션 솔루션의 역할을 온보딩해야 합니다.
> AMS의 CodePipeline은 최소 권한 모델 및 AMS 변경 관리 프로세스를 우회하는 서비스 역할 및 정책을 생성하기 위해 승격된 권한이 필요하기 때문에 소스 단계에 대한 "Amazon CloudWatch Events"를 지원하지 않습니다.

AWS Managed Services FAQ의 CodePipeline

Q: AMS 계정에서 CodePipeline에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관련 계정`customer_code_pipeline_console_role`에서에 대한 서비스 요청을 제출하여 CodePipeline에 대한 액세스를 요청합니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

현재 AMS Operations는 계정에이 서비스 역할인 도 배포합니다`aws_code_pipeline_service_role_policy`.

Q: AMS 계정에서 CodePipeline을 사용할 때 제한 사항은 무엇인가요?

예. CodePipeline 기능, 단계 및 공급자는 다음으로 제한됩니다.

1. 배포 단계: Amazon S3로 제한 및 AWS CodeDeploy
2. 소스 단계: Amazon S3, AWS CodeCommit BitBucket 및 GitHub로 제한됨
3. 빌드 단계: AWS CodeBuild및 Jenkins로 제한됨
4. 승인 단계: Amazon SNS로 제한됨
5. 테스트 단계: 제한 대상 AWS CodeBuild, Jenkins, BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load 및 Runscope API Monitoring
6. 호출 단계: Step Functions 및 Lambda로 제한됨

> **Note**
>
> AMS 작업은 `customer_code_pipeline_lambda_policy` 계정에 배포되며 Lambda 간접 호출 단계에 대한 Lambda 실행 역할에 연결되어야 합니다. 이 정책을 추가할 Lambda 서비스/실행 역할 이름을 제공하세요. 사용자 지정 Lambda 서비스/실행 역할이 없는 경우 AMS는 라는 새 역할을 생성합니다. `customer_code_pipeline_lambda_execution_role`이 역할은와 `customer_lambda_basic_execution_role` 함께의 사본이 됩니다`customer_code_pipeline_lambda_policy`.

Q: AMS 계정에서 CodePipeline을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AWS 지원되는 서비스는 CodePipeline 시작 전 또는 이와 함께 시작해야 AWS CodeCommit AWS CodeBuild AWS CodeDeploy 합니다.

AMS SSP를 사용하여 AMS 계정 AWS Compute Optimizer 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Compute Optimizer 기능에 액세스할 수 있습니다. AWS Compute Optimizer 는 기계 학습을 사용하여 과거 사용률 지표를 분석하여 비용을 절감하고 성능을 개선하기 위해 워크로드에 최적의 AWS 컴퓨팅 리소스를 권장합니다. 컴퓨팅(Amazon EC2 및 ASGs)을 과도하게 프로비저닝하면 불필요한 인프라 비용이 발

생하고 컴퓨팅을 과소 프로비저닝하면 애플리케이션 성능이 저하될 수 있습니다. Compute Optimizer를 사용하면 사용률 데이터를 기반으로 Amazon EC2 Auto Scaling 그룹에 속하는 인스턴스 유형을 포함하여 최적의 Amazon EC2 인스턴스 유형을 선택할 수 있습니다. 자세한 내용은 AWS Compute Optimizer를 참조하세요.

AWS Managed Services FAQ의 Compute Optimizer

Q: AMS 계정에서 Compute Optimizer에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_compute_optimizer_readonly_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Compute Optimizer를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. AMS 계정에서 AWS Compute Optimizer 의 전체 기능을 사용할 수 있습니다.

Q: AMS 계정에서 Compute Optimizer를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 계정에서 서비스를 활성화하려면 AMS Ops에 권한을 부여하는 RFC(관리 | 기타 | 기타 | 업데이트)를 제출해야 합니다. 배포 중에 지표 수집 및 보고서 생성을 허용하는 서비스 연결 역할(SLR)이 생성됩니다. SLR에는 “AWSServiceRoleForComputeOptimizer” 레이블이 지정되어 있습니다. 자세한 내용은 에 대한 서비스 연결 역할 사용을 참조하세요. AWS Compute Optimizer
- 다음 지표에 대해 CloudWatch 지표를 활성화해야 합니다.
  - CPU 사용률: 인스턴스에서 사용 중인 할당된 Amazon EC2 컴퓨팅 유닛의 백분율입니다. 이 지표는 선택한 인스턴스에서 애플리케이션을 실행하는 데 필요한 처리 능력을 식별합니다.
  - 메모리 사용률: 샘플 기간 동안 어떤 식으로든 사용된 메모리의 양입니다. 이 지표는 선택한 인스턴스에서 애플리케이션을 실행하는 데 필요한 메모리를 식별합니다. 메모리 사용률은 통합된 CloudWatch 에이전트가 설치된 리소스에 대해서만 분석됩니다. 자세한 내용은 CloudWatch 에이전트를 사용하여 메모리 사용률 활성화(10페이지)를 참조하세요.
  - 네트워크 입력: 인스턴스가 모든 네트워크 인터페이스에서 수신한 바이트 수입니다. 이 지표는 단일 인스턴스로 들어오는 네트워크 트래픽의 볼륨을 식별합니다.
  - 네트워크 출력: 인스턴스가 모든 네트워크 인터페이스에서 보낸 바이트 수입니다. 이 지표는 단일 인스턴스에서 나가는 네트워크 트래픽의 볼륨을 식별합니다.
  - 로컬 디스크 입/출력(I/O): 로컬 디스크의 입/출력 작업 수입니다. 이 지표는 인스턴스의 루트 볼륨 성능을 식별합니다.

AMS SSP를 사용하여 AMS 계정 AWS DataSync 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정의 AWS DataSync 기능에 직접 액세스할 수 있습니다.는 온프레미스 스토리지와 Amazon S3, Amazon Elastic File System(Amazon Elastic File System) 또는 Amazon FSx 간에 대량의 데이터를 온라인으로 AWS DataSync 이동합니다. 데이터 전송과 관련된 수동 작업은 마이그레이션 속도를 늦추고 IT 운영에 부담을 줄 수 있습니다. DataSync는 복사 작업 스크립팅, 전송 예약 및 모니터링, 데이터 검증, 네트워크 사용률 최적화 등 이러한 많은 작업을 제거하거나 자동으로 처리합니다. DataSync 소프트웨어 에이전트는 NFS(Network File System) 및 SMB(Server Message Block) 스토리지에 연결되므로 애플리케이션을 수정할 필요가 없습니다. DataSync는 인터넷 또는 AWS Direct Connect 링크를 통해 오픈 소스 도구보다 최대 10배 빠른 속도로 수백 테라바이트와 수백만 개의 파일을 전송할 수 있습니다. DataSync를 사용하여 활성 데이터 세트 또는 아카이브를 로 마이그레이션하거나 AWS, 시기 적절한 분석 및 처리를 위해 클라우드로 데이터를 전송하거나, 비즈니스 연속성 AWS 을 위해에 데이터를 복제할 수 있습니다.

자세한 내용은 AWS DataSync를 참조하세요.

AWS Managed Services DataSync FAQ

Q: AMS 계정에서 DataSync에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_datasync_console_role`.

계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

작업 로그를 스트리밍하는 데 사용할 CloudWatch 로그 그룹은 "/aws/datasync"입니다.

Q: AMS 계정에서 DataSync를 사용할 때 제한 사항은 무엇인가요?

AMS 계정에서 AWS DataSync 의 전체 기능을 사용할 수 있습니다.

Q: AMS 계정에서 DataSync를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- DataSync 서비스 역할를 사용하여 수행할 DataSync 작업과 연결된 모든 S3 버킷에는 Amazon S3 ARNs(Amazon 리소스 이름)이 필요합니다`customer_datasync_service_role`. DataSync
- DataSync 에이전트의 VPC 엔드포인트 및 보안 그룹은 VPC 엔드포인트를 사용하기 전에 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76) 변경 유형이 있는 RFC로 요청해야 합니다.
- AWS DataSync 에이전트는 AMS에서 어플라이언스로 실행됩니다. AWS DataSync 에이전트는 서비스에 의해 패치되고 업데이트됩니다. 자세한 내용은 AWS DataSync FAQ를 참조하세요.

- AWS DataSync 에이전트를 시작하려면 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76) 변경 유형을 사용하여 RFC를 제출하여 에이전트 배포를 요청합니다. AWS DataSync Amazon EC2 AMI ID, 인스턴스 유형, 서브넷, 보안 그룹을 제공하고 기존 Amazon EC2 키 페어를 참조하거나 새 키 페어 생성을 요청합니다.

> **Note**
>
> AMS는 고객을 대신하여 AWS DataSync 에이전트를 수동으로 프로비저닝하며 AWS DataSync Amazon EC2 AMI에서 WIGS 수집 프로세스가 필요하지 않습니다.

AMS SSP를 사용하여 AMS 계정 AWS Device Farm 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Device Farm 기능에 액세스할 수 있습니다. AWS Device Farm 는 테스트 인프라를 프로비저닝하고 관리할 필요 없이 광범위한 데스크톱 브라우저와 실제 모바일 디바이스에서 웹 및 모바일 앱을 테스트하여 웹 및 모바일 앱의 품질을 개선할 수 있는 애플리케이션 테스트 서비스입니다. 이 서비스를 사용하면 여러 데스크톱 브라우저 또는 실제 디바이스에서 동시에 테스트를 실행하여 테스트 제품군 실행 속도를 높이고 비디오와 로그를 생성하여 앱 문제를 빠르게 식별할 수 있습니다.

자세한 내용은 AWS Device Farm를 참조하세요.

AWS Device Farm AWS Managed Services FAQ의

Q: AMS 계정 AWS Device Farm 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_devicefarm_role`.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Device Farm 에서 사용에 대한 제한 사항은 무엇인가요?

'Name' 태그에서 AMS 네임스페이스를 사용하는 경우를 제외하고 AWS Device Farm 서비스에 대한 전체 액세스 권한이 제공됩니다.

Q: AMS 계정 AWS Device Farm 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

없음.

AMS SSP를 사용하여 AMS 계정 AWS Elastic Disaster Recovery 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Elastic Disaster Recovery 기능에 액세스할 수 있습니다.는 저렴한 스토리지, 최소 컴퓨팅 및 point-in-time으로 복구를 사용하여 온프레미스 및 클라우드 기반 애플리케이션을 빠르고 안정적으로 복구하여 가동 중지 시간과 데이터 손실을 AWS Elastic Disaster Recovery 최소화합니다. AWS Elastic Disaster Recovery 를 사용하여 지원되는 운영 체제에서 실행되는 온프레미스 또는 클라우드 기반 애플리케이션을 복제할 때 IT 복원력을 높일 수 있습니다. AWS Management Console 를 사용하여 복제 및 시작 설정을 구성하고, 데이터 복제를 모니터링하고, 드릴 또는 복구를 위해 인스턴스를 시작합니다.

자세한 내용은 AWS Elastic Disaster Recovery를 참조하세요.

AWS Elastic Disaster Recovery AWS Managed Services FAQ의

Q: AMS 계정 AWS Elastic Disaster Recovery 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_drs_console_role`.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Elastic Disaster Recovery 에서 사용에 대한 제한 사항은 무엇인가요?

AMS 계정 AWS Elastic Disaster Recovery 에서 사용할 수 있는 제한은 없습니다.

Q: AMS 계정 AWS Elastic Disaster Recovery 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

- 콘솔 역할에 액세스한 후에는 Elastic Disaster Recovery 서비스를 초기화하여 계정 내에서 필요한 IAM 역할을 생성해야 합니다.
  - 인스턴스 프로파일의 복제본을 생성하고 `AWSElasticDisasterRecoveryEc2InstancePolicy` 정책을 `customer-mc-ec2-instance-profile` 연결하려면 변경 유형 관리 | 애플리케이션 | IAM 인스턴스 프로파일 | 생성(관리형 자동화) 변경 유형 ct-0ixp4ch2tiu04 RFC를 제출해야 합니다. 새 정책을 연결할 시스템을 지정해야 합니다.
  - 인스턴스가 기본 인스턴스 프로파일을 사용하지 않는 경우 AMS는 자동화를 `AWSElasticDisasterRecoveryEc2InstancePolicy` 통해 연결할 수 있습니다.

- 교차 계정 복구에는 고객 소유 KMS 키를 사용해야 합니다. 대상 계정 액세스를 허용하려면 정책에 따라 소스 계정의 KMS 키를 업데이트해야 합니다. 자세한 내용은 대상 계정과 EBS 암호화 키 공유를 참조하세요.
- 볼 역할을 전환하지 않으려면 허용에서 정책을 `customer_drs_console_role` 볼 수 있도록 KMS 키 정책을 업데이트해야 합니다.
- 교차 계정, 교차 리전 재해 복구의 경우 AMS는 소스 및 대상 계정을 신뢰할 수 있는 계정으로 설정하고 장애 복구 및AWS 오른쪽 크기 조정 역할을를 통해 배포해야 합니다 CloudFormation.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaConvert 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaConvert 기능에 액세스할 수 있습니다. AWS Elemental MediaConvert 는 브로드캐스트 등급 기능이 있는 파일 기반 비디오 트랜스코딩 서비스입니다. 이를 통해 대규모로 브로드캐스트 및 멀티스크린 전송을 위한 video-on-demand(VOD) 콘텐츠를 생성할 수 있습니다. 이 서비스는 고급 비디오 및 오디오 기능을 간단한 웹 서비스 인터페이스 및 종량제 요금과 결합합니다. 를 사용하면 자체 비디오 처리 인프라를 구축하고 운영하는 복잡성에 대해 걱정할 필요 없이 매력적인 미디어 경험을 제공하는 데 집중할 AWS Elemental MediaConvert수 있습니다.

자세한 내용은 AWS Elemental MediaConvert를 참조하세요.

AWS Managed Services FAQ의 MediaConvert

Q: AMS 계정에서 MediaConvert에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_mediaconvert_author_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

소스 S3 버킷에서 읽고 대상 S3 버킷에 출력을 쓰S3고 디지털 권한 관리(DRM)`customer_MediaConvert_Default_Role`가 필요한 경우 API 게이트웨이를 호출하기 위해 MediaConvert에서 사용하는 두 번째 역할인이 제공됩니다.

Q: AMS 계정에서 MediaConvert를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaConvert를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaConvert를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 MediaConvert를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaLive 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaLive 기능에 액세스할 수 있습니다. AWS Elemental MediaLive 는 브로드캐스트급 라이브 비디오 처리 서비스입니다. 이를 통해 TV 방송 및 연결된 TV, 태블릿, 스마트폰, 셋톱 박스와 같은 인터넷 연결 멀티스크린 디바이스로 전송하기 위한 고품질 비디오 스트림을 생성할 수 TVs. 이 서비스는 라이브 비디오 스트림을 실시간으로 인코딩하고, 더 큰 크기의 라이브 비디오 소스를 가져와 뷰어에게 배포할 수 있도록 더 작은 버전으로 압축하는 방식으로 작동합니다. AWS Elemental MediaLive를 사용하면 고급 방송 기능, 고가용성 및 pay-as-you-go 요금을 사용하여 라이브 이벤트와 24x7 채널 모두에 대한 스트림을 쉽게 설정할 수 있습니다. AWS Elemental MediaLive 를 사용하면 방송 등급 비디오 처리 인프라를 구축하고 운영하는 복잡성 없이 시청자에게 매력적인 라이브 비디오 경험을 만드는 데 집중할 수 있습니다.

자세한 내용은 AWS Elemental MediaLive를 참조하세요.

AWS Managed Services FAQ의 MediaLive

Q: AMS 계정에서 MediaLive에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_medialive_author_role`.

이 RFC의 일부로 두 번째 역할이 계정에 배포됩니다. `customer_medialive_service_role` 역할은 Media Live 채널 및 입력에 할당되어 Amazon S3, MediaStore 및 CloudWatch Logs와 같은 다른 서비스와 상호 작용할 수 있습니다.

계정에 역할이 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 MediaLive를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaLive를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaLive를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 MediaLive를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaPackage 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaPackage 기능에 액세스할 수 있습니다.는 인터넷을 통한 전송을 위해 비디오를 AWS Elemental MediaPackage 안정적으로 준비하고 보호합니다. AWS Elemental MediaPackage 는 단일 비디오 입력으로 연결된 TV, 컴퓨터, 태블릿 및 게임 콘솔에서 재생할 수 있는 형식의 비디오 스트림을 생성합니다. 이를 통해 DVRs에서 일반적으로 볼 수 있는 것과 같이 뷰어에게 인기 있는 비디오 기능(시작, 일시 중지, 되감기 등)을 쉽게 구현할 수 있습니다. AWS Elemental MediaPackage 는 디지털 권한 관리(DRM)를 사용하여 콘텐츠를 보호할 수도 있습니다.는 로드에 따라 자동으로 AWS Elemental MediaPackage 규모를 조정하므로 뷰어는 필요한 용량을 미리 정확하게 예측하지 않고도 항상 훌륭한 경험을 할 수 있습니다.

자세한 내용은 AWS Elemental MediaPackage를 참조하세요.

AWS Managed Services MediaPackage FAQ

Q: AMS 계정 AWS Elemental MediaPackage 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_mediapackage_author_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

S3 및 Secrets Manager와 같은 다른 서비스와 상호 작용하기 위해 Media Live 채널 및 입력에 할당할 수 있는 두 번째 역할 `customer_mediapackage_service_role`가 제공됩니다.

Q: AMS 계정에서 MediaPackage를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaPackage를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaPackage를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 MediaPackage를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaStore 에서 프로비저닝

> **Note**
>
> 신중한 고려 후 AWS 는 2025년 11월 13일부터 MediaStore를 중단하기로 결정했습니다. MediaStore의 활성 고객인 경우 서비스 지원이 종료되는 2025년 11월 13일까지 MediaStore를 정상적으로 사용할 수 있습니다. 이 날짜 이후에는 MediaStore 또는이 서비스에서 제공하는 기능을 더 이상 사용할 수 없습니다.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaStore 기능에 액세스할 수 있습니다. AWS Elemental MediaStore 는 미디어에 최적화된 AWS 스토리지 서비스입니다. 라이브 스트리밍 비디오 content. AWS Elemental MediaStore acts를 비디오 워크플로의 오리진 스토어로 제공하는 데 필요한 성능, 일관성 및 짧은 지연 시간을 제공합니다. 고성능 기능은 장기적이고 비용 효율적인 스토리지와 함께 가장 까다로운 미디어 전송 워크로드의 요구 사항을 충족합니다. 자세한 내용은 AWS Elemental MediaStore를 참조하세요.

AWS Managed Services FAQ의 MediaStore

Q: AMS 계정에서 MediaStore에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 MediaStore에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_mediastore_author_role`. 이 RFC의 일부로 두 번째 역할이 계정에 배포됩니다. 이 역할은 해당 기능을 활성화하도록 선택한 경우 MediaStore 서비스가 CloudWatch에서 활동을 로깅하는 데 사용하는 `MediaStoreAccessLogs` 역할입니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

현재 AMS Operations는 계정에이 서비스 역할인 도 배포합니다`aws_code_pipeline_service_role_policy`.

Q: AMS 계정에서 MediaStore를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaStore를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaStore를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 MediaStore를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaTailor 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Elemental MediaTailor 기능에 액세스할 수 있습니다. AWS Elemental MediaTailor lets 비디오 공급자는 브로드캐스트 수준 quality-of-service 저하시키지 않고 비디오 스트림에 개별 대상 광고를 삽입합니다. 를 사용하면 라이브 또는 온디맨드 비디오의 AWS Elemental MediaTailor시청자는 콘텐츠를 맞춤형 광고와 결합하는 스트림을 수신합니다. 그러나 다른 개인 맞춤형 광고 솔루션과 달리 AWS Elemental MediaTailor 전체 스트림, 즉 비디오 및 광고는 시청자의 경험을 개선하기 위해 브로드캐스트 등급 비디오 품질로 제공됩니다.는 클라이언트 및 서버 측 광고 전송 지표를 모두 기반으로 자동 보고를 AWS Elemental MediaTailor 제공하여 광고 노출 및 시청자 동작을 정확하게 측정합니다. 를 사용하면 선결제 비용 없이 예상치 못한 고수요 시청 이벤트를 쉽게 수익화할 수 있습니다 AWS Elemental MediaTailor. 또한 광고 전송률을 개선하여 모든 비디오에서 더 많은 비용을 절감할 수 있으며 다양한 콘텐츠 전송 네트워크, 광고 결정 서버 및 클라이언트 디바이스에서 작동합니다.

자세한 내용은 AWS Elemental MediaTailor를 참조하세요.

AWS Managed Services FAQ의 MediaTailor

Q: AMS 계정에서 MediaTailor에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 MediaTailor에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer-mediatailor-role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 MediaTailor를 사용할 때 적용되는 제한 사항은 무엇인가요?

AMS에서 MediaTailor를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaTailor를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 MediaTailor를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Global Accelerator 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Global Accelerator 기능에 액세스할 수 있습니다. Global Accelerator는 글로벌 고객이 사용하는 인터넷 애플리케이션의

가용성과 성능을 개선하기 위해 액셀러레이터를 생성하는 네트워크 계층 서비스입니다. 자세한 내용은 Global Accelerator를 참조하세요.

AWS Managed Services FAQ의 Global Accelerator

일반적인 질문과 답변:

Q: AMS 계정에 Global Accelerator를 설정하도록 요청하려면 어떻게 해야 하나요?

AWS 서비스 RFC(관리 | AWS 서비스 | 자체 프로비저닝 서비스) 제출을 통해 액세스를 요청합니다. 이 RFC를 통해 계정에 다음 IAM 역할이 프로비저닝됩니다`customer_global_accelerator_console_role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션에서 콘솔 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Global Accelerator를 사용하는 데 따르는 제한 사항은 무엇인가요?

Global Accelerator는 리전 AWS 테이블에 나열된 여러 AWS 리전의 엔드포인트를 지원하는 글로벌 서비스입니다.

Q: AMS 계정에서 Global Accelerator를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Global Accelerator를 사용하여 액셀러레이터를 설정할 때 정적 IP 주소를 하나 이상의 AWS 리전의 리전 엔드포인트에 연결합니다. 표준 액셀러레이터의 경우, 엔드포인트는 Network Load Balancer, Application Load Balancer, Amazon EC2 인스턴스 또는 탄력적 IP 주소입니다. 사용자 지정 라우팅 액셀러레이터의 경우 엔드포인트는 하나 이상의 EC2 인스턴스가 있는 Virtual Private Cloud(VPC) 서브넷입니다.

AMS SSP를 사용하여 AMS 계정 AWS Glue 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Glue 기능에 액세스할 수 있습니다. AWS Glue 는 분석을 위해 데이터를 준비하고 로드하는 데 도움이 되는 완전 관리형 추출, 변환 및 로드(ETL) 서비스입니다. 에서 몇 번의 클릭으로 ETL 작업을 생성하고 실행할 수 있습니다 AWS Management Console. 에 저장된 데이터를 AWS Glue 가리키면 AWS가 데이터를 AWS Glue 검색하고 관련 메타데이터(예: 테이블 정의 및 스키마)를에 저장합니다 AWS Glue Data Catalog. 카탈로그가 작성되면 데이터를 즉시 검색하고 쿼리할 수 있으며 ETL 작업에 사용할 수 있습니다. 자세한 내용은 AWS Glue를 참조하세요.

AWS Glue AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS Glue 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Glue 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다.

- `customer_glue_console_role`
- `customer_glue_service_role`

앞의 역할에는 다음과 같은 연결된 정책이 포함됩니다.

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

계정에 역할이 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

크롤러, 작업 및 개발 엔드포인트(특정 사용 사례에 필요한 역할)에 액세스하려면 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(ct-3dpd8mdd9jn1r)을 사용하여 RFC를 제출합니다.

Q: AMS 계정 AWS Glue 에서 사용에 대한 제한 사항은 무엇인가요?

제한은 없습니다. 의 전체 기능은 AMS 계정에서 AWS Glue 사용할 수 있습니다. ETL 스크립트를 작성하고 테스트할 수 있는 대화형 환경의 경우 AWS Glue Studio에서 노트북을 사용합니다. AWS Glue 대화형 세션 및 작업 노트북은에서 사용할 AWS Glue 수 AWS Glue 있고 AWS Glue 서비스 역할을 사용하는의 서버리스 기능입니다.

AWS Glue 2.0 이전: AWS Glue Notebooks는 계정에서 Amazon EC2 인스턴스를 시작하는 비관리형 리소스입니다. 자체 Amazon EC2 인스턴스를 시작하고 노트북 환경 및 개발을 지원하는 데 필요한 소프트웨어를 설치하는 것이 모범 사례입니다. 자세한 내용은 자습서: ETL 스크립트를 테스트 및 디버깅하기 위한 로컬 Apache Zeppelin 노트북 설정 및 스크립트 개발을 위한 개발 엔드포인트 사용을 참조하세요.

Q: AMS 계정 AWS Glue 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AWS Glue 에는 Amazon S3, CloudWatch 및 CloudWatch Logs에 대한 종속성이 있습니다. 전이적 종속성은 데이터 소스에 따라 다르며, 다른 AWS Glue 서비스 기능은와 상호 작용할 수 있습니다(예: Amazon Redshift, Amazon RDS, Athena).

AMS SSP를 사용하여 AMS 계정 AWS Lake Formation 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Lake Formation 기능에 액세스할 수 있습니다. AWS Lake Formation 는 며칠 내에 보안 데이터 레이크를 쉽게 설정할 수 있는 서비스입니다. 데이터 레이크는 모든 데이터를 원래 형식과 분석을 위한 형식 모두로 저장하는 큐레이팅된 중앙 집중식 보안 리포지토리입니다. 데이터 레이크를 사용하면 데이터 사일로를 분해하고 다양한 유형의 분석을 결합하여 인사이트를 얻고 더 나은 비즈니스 결정을 내릴 수 있습니다.

Lake Formation을 사용하여 데이터 레이크를 생성하는 작업은 아주 간단해서, 데이터 소스와 적용할 데이터 액세스 및 보안 정책을 정의하면 됩니다. 그런 다음 Lake Formation을 사용하여 데이터베이스 및 객체 스토리지에서 데이터를 수집하여 카탈로그화하고, 데이터를 새로운 Amazon S3 데이터 레이크로 이동하고, Machine Learning 알고리즘을 사용하여 데이터를 정리 및 분류하고, 중요한 데이터에 안전하게 액세스할 수 있습니다. 사용자는 사용 가능한 데이터 세트와 적절한 사용을 설명하는 중앙 집중식 데이터 카탈로그(자세한 내용은 AWS Glue FAQ 참조)에 액세스할 수 있습니다. 그런 다음 사용자는 Amazon Redshift, Amazon Amazon Athena 및 (베타) Amazon EMR for Apache Spark와 같은 다양한 분석 및 기계 학습 서비스와 함께 이러한 데이터 세트를 활용합니다. Lake Formation은에서 사용할 수 있는 기능을 기반으로 합니다AWS Glue.

자세한 내용은 AWS Lake Formation를 참조하세요.

AWS Managed Services FAQ의 Lake Formation

Q: AMS 계정 AWS Lake Formation 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_lakeformation_data_analyst_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

또한 다음 두 가지 역할은 선택 사항입니다.

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

관리자 권한의 경우 동일한 SSPS 변경 유형(ct-3qe6io8t6jtny)의 `customer_lakeformation_admin_role` 일부로 역할을 온보딩하도록 선택할 수 있습니다.

AWS Lake Formation 콘솔에서 블루프린트를 생성하려면 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하고 명시적으로를 추가하여를 배포해야 합니다`customer_lakeformation_workflow_role`. RFC에서 블루프린트가 생성될 때 버킷이 소스인 경우 S3 버킷 이름을 제공해야 합니다. S3 버킷은 블루프린트 유형이 AWS CloudTrail Classic Load Balancer Logs 또는 Application Load Balancer Logs인 경우에 적용됩니다.

Q: AMS 계정 AWS Lake Formation 에서 사용에 대한 제한 사항은 무엇인가요?

Lake Formation의 전체 기능은 AMS에서 사용할 수 있습니다.

Q: AMS 계정 AWS Lake Formation 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

Lake Formation은 AWS Glue 서비스와 통합되므로 AWS Glue 사용자는 Lake Formation 권한이 있는 데이터베이스 및 테이블에만 액세스할 수 있습니다. 또한 AWS Athena 및 Amazon Redshift 사용자는 Lake Formation 권한이 있는 AWS Glue 데이터베이스와 테이블만 쿼리할 수 있습니다.

AMS SSP를 사용하여 AMS 계정 AWS Lambda 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Lambda 기능에 액세스합니다. 서버를 프로비저닝하거나 관리하지 않고 코드를 실행할 수 AWS Lambda 있습니다. 사용한 컴퓨팅 시간에 대해서만 비용을 지불하면 코드가 실행되지 않을 때 요금이 부과되지 않습니다. Lambda를 사용하면 사실상 모든 유형의 애플리케이션 또는 백엔드 서비스에 대한 코드를 제로 관리로 실행할 수 있습니다. 코드를 업로드하면 Lambda가 고가용성으로 코드를 실행하고 확장하는 데 필요한 모든 것을 처리합니다. 코드를 설정하여 다른 AWS 서비스에서 자동으로 트리거하거나 웹 또는 모바일 앱에서 직접 호출할 수 있습니다. 자세한 내용은 AWS Lambda를 참조하세요.

AWS Managed Services FAQ의 Lambda

Q: AMS 계정 AWS Lambda 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_lambda_admin_role`.`customer_lambda_basic_execution_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Lambda 에서 사용에 대한 제한 사항은 무엇인가요?

- Lambda 함수는 이벤트 소스에서 호출하도록 설계되었습니다. Lambda 이벤트 소스로 사용할 수 있는 서비스 목록은 다른 서비스와 AWS Lambda 함께 사용을 참조하세요. 현재 AMS 계정에서 이러한 서비스를 모두 사용할 수 있는 것은 아닙니다. 사용할 수 없는 서비스가 필요한 경우 AMS CSDM과 협력하여 예외를 제출합니다.

- 기본적으로 AMS는 `AWSLambdaBasicExecutionRole` 및 `AWSXrayWriteOnlyAccess` 권한이 포함된 기본 Lambda 시작 역할을 제공합니다. 자세한 내용은 AWS Lambda 시작 역할을 참조하세요. AMS VPC 내에서 Lambda 함수를 프로비저닝하는 기능과 같은 추가 권한이 필요한 경우 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출합니다.

Q: AMS 계정 AWS Lambda 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

시작하기 위한 사전 조건이나 종속성은 없지만 AWS Lambda특정 사용 사례에 따라 이벤트 소스를 생성하기 위해 다른 AWS 서비스에 액세스해야 하거나 함수가 다양한 작업을 수행할 수 있는 추가 권한이 필요할 수 있습니다. 추가 권한이 필요한 경우 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화) 변경 유형(ct-3qe6io8t6jtny)을 사용하여 RFC를 제출합니다.

Q: 내 계정에서 Lambda 함수를 실행하려면 어떻게 해야 하나요?

코어 계정에 Lambda 함수를 배포하려면 다음 지침을 사용합니다.

- 에 대한 SSPS AWS Lambda 가 온보딩되었는지 확인합니다.
- AMS 리소스가 보호되고 규정을 준수하는 한 AMS 책임에 따라이 배포를 금지하는 구체적인 제한은 없습니다.
- AMS가 Lambda 함수를 생성하도록 하려면 먼저 제공된 SSPS 역할을 사용해야 합니다 AWS Lambda. 그런 다음 AMS 지원이 함수를 배포하거나 지원하도록 하려면 CA에 문의하여 범위 외(OOS) 프로세스를 시작합니다.

AMS SSP를 사용하여 AMS 계정 AWS License Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS License Manager 기능에 액세스할 수 있습니다.는 AWS 서비스와 AWS License Manager 통합되어 단일 AWS 계정을 통해 여러 AWS 계정, IT 카탈로그 및 온프레미스에서 라이선스 관리를 간소화합니다.를 AWS License Manager 사용하면 관리자가 라이선스 계약 조건을 에뮬레이션하는 사용자 지정 라이선스 규칙을 생성한 다음 Amazon EC2 인스턴스가 시작될 때 이러한 규칙을 적용할 수 있습니다. 의 규칙을 AWS License Manager 사용하면 인스턴스 시작을 물리적으로 중지하거나 관리자에게 위반 사실을 알림으로써 라이선스 위반을 제한할 수 있습니다. 자세한 내용은 AWS License Manager를 참조하세요.

AWS Managed Services FAQ의 License Manager

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS License Manager 하도록 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 AWS License Manager 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_license_manager_role`. License Manager IAM 역할이 계정에 프로비저닝되면 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS License Manager 에서 사용에 대한 제한 사항은 무엇인가요?

소유한 AMI에 AWS License Manager 규칙을 연결할 수 있습니다("Owned by me"에서 필터링됨). AMIs AMI에 대한 제한 연결을 적용하고(예:이 AMI의 vCPU 100개만 지원 가능) 제한을 소진하도록 선택하면 해당 AMI를 사용한 향후 시작이 차단되고 "사용 가능한 라이선스 없음"이라는 오류가 반환됩니다. 이는이 서비스의 의도된 동작입니다(라이선스 소진을 허용하지 않음). 한도를 소진했지만 AMI를 다시 시작해야 하는 경우에 구성된 규칙을 수정해야 합니다 AWS License Manager.

Q: AMS 계정 AWS License Manager 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS License Manager 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Migration Hub 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Migration Hub 기능에 액세스할 수 있습니다.는 여러 AWS 및 파트너 솔루션에서 애플리케이션 마이그레이션의 진행 상황을 추적할 수 있는 단일 위치를 AWS Migration Hub 제공합니다. Migration Hub를 사용하면 필요에 가장 적합한 AWS 및 파트너 마이그레이션 도구를 선택하는 동시에 애플리케이션 포트폴리오 전반의 마이그레이션 상태를 파악할 수 있습니다. 또한 Migration Hub는 마이그레이션에 사용되는 도구에 관계없이 개별 애플리케이션에 대한 주요 지표와 진행 상황을 제공합니다. 이를 통해 모든 마이그레이션에서 진행 상황을 빠르게 업데이트하고, 문제를 쉽게 식별 및 해결하며, 마이그레이션 프로젝트에 소요되는 전체 시간과 노력을 줄일 수 있습니다. 자세한 내용은 AWS Migration Hub를 참조하세요.

AWS Managed Services FAQ의 Migration Hub

일반적인 질문과 답변:

Q: AMS 계정에서 Migration Hub에 대한 액세스를 요청하려면 어떻게 해야 합니까?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Migration Hub에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_migrationhub_author_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: Migration Hub의 제한 사항은 무엇인가요?

없음.

Q: Migration Hub를 활성화하기 위한 사전 조건은 무엇입니까?

AMS 계정에서 Migration Hub 사용을 시작하기 위한 사전 조건은 없습니다. 그러나 서비스 관리 중에 서버 정보를 업로드하기 위해 Amazon S3에 권한을 쓰는 등 Migration Hub 외부의 권한이 필요할 수 있습니다.

AMS SSP를 사용하여 AMS 계정 AWS Outposts 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Outposts 기능에 액세스할 수 있습니다. AWS Outposts 는 인프라 AWS , AWS 서비스, APIs 및 도구를 사실상 모든 데이터 센터, 코로케이션 공간 또는 온프레미스 시설로 확장하여 일관된 하이브리드 환경을 제공하는 완전 관리형 서비스입니다. AWS Outposts 는 온프레미스 시스템, 로컬 데이터 처리 또는 로컬 데이터 스토리지에 대한 짧은 지연 시간 액세스가 필요한 워크로드에 적합합니다. 자세한 내용은 AWS Outposts를 참조하세요.

AWS Outposts AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS Outposts 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 AWS Outposts 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_outposts_role`. 계정에 역할이 프로비저닝되면 페더레이션 솔루션에 온보딩해야 합니다.

Q: AMS 계정 AWS Outposts 에서 사용에 대한 제한 사항은 무엇입니까?

AMS 계정 AWS Outposts 에서를 사용하는 데는 제한이 없습니다.

Q: AMS 계정 AWS Outposts 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Outposts 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Resilience Hub 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Resilience Hub 기능에 액세스할 수 있습니다.는 AWS 애플리케이션을 사전에 준비하고 중단으로부터 보호할 수 있도록 AWS Resilience Hub 지원합니다. Resilience Hub는 소프트웨어 개발 수명 주기에 통합되는 복원력 평가 및 검증을 제공하여 복원력 약점을 찾아냅니다. Resilience Hub는 애플리케이션이 Recovery

Time Objective(RTO) 및 Recovery Point Objective(RPO) 목표를 충족할 수 있는지 여부를 추정하고 프로덕션으로 릴리스되기 전에 문제를 해결하는 데 도움이 됩니다. AWS 애플리케이션을 프로덕션에 배포한 후 Resilience Hub를 사용하여 애플리케이션의 복원력 상태를 계속 추적할 수 있습니다. 중단이 발생하면 Resilience Hub는 운영자에게 관련 복구 프로세스를 시작하라는 알림을 보냅니다.

AWS Resilience Hub AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Resilience Hub 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Resilience Hub에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음과 같은 IAM 역할 및 정책을 프로비저닝합니다.

IAM 역할

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

정책

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

계정에 역할이 프로비저닝된 후 페더레이션 솔루션`customer_resiliencehub_console_role`에서 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Resilience Hub 에서 사용에 대한 제한 사항은 무엇입니까?

제한은 없습니다. Resilience Hub의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정 AWS Resilience Hub 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 Resilience Hub를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Secrets Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Secrets Manager 기능에 액세스할 수 있습니다. 애플리케이션, 서비스 및 IT 리소스에 액세스하는 데 필요한

보안 암호를 AWS Secrets Manager 보호할 수 있습니다. 서비스를 사용하면 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 보안 암호를 쉽게 교체, 관리 및 검색할 수 있습니다. 사용자와 애플리케이션은 Secrets Manager APIs를 호출하여 보안 암호를 검색하므로 민감한 정보를 일반 텍스트로 하드코딩할 필요가 없습니다. Secrets Manager는 Amazon RDS, Amazon Redshift 및 Amazon DocumentDB에 대한 통합 기능이 내장된 보안 로테이션을 제공합니다. 또한 이 서비스는 API 키 및 OAuth 토큰을 비롯한 다른 유형의 보안 암호로 확장할 수 있습니다. 자세한 내용은 AWS Secrets Manager를 참조하세요.

> **Note**
>
> 기본적으로 AMS 운영자 AWS Secrets Manager 는 계정의 기본 AWS KMS 키(CMK)를 사용하여 암호화된의 보안 암호에 액세스할 수 있습니다. AMS 작업에 보안 암호에 액세스할 수 없도록 하려면 보안 암호에 저장된 데이터에 적합한 권한을 정의하는 AWS Key Management Service (AWS KMS) 키 정책과 함께 사용자 지정 CMK를 사용합니다.

AWS Managed Services FAQ의 Secrets Manager

Q: AMS 계정 AWS Secrets Manager 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출하여 Secrets Manager에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_secrets_manager_console_role``customer-rotate-secrets-lambda-role`. `customer_secrets_manager_console_role`는 보안 암호를 프로비저닝하고 관리하는 관리자 역할로 사용되며 보안 암호를 교체하는 Lambda 함수의 Lambda 실행 역할로 `customer-rotate-secrets-lambda-role` 사용됩니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 `customer_secrets_manager_console_role` 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Secrets Manager 에서 사용에 대한 제한 사항은 무엇인가요?

의 전체 기능은 보안 암호의 자동 교체 기능과 함께 AMS 계정에서 AWS Secrets Manager 사용할 수 있습니다. 그러나 '교체 수행을 위한 새 Lambda 함수 생성'을 사용하여 교체를 설정하는 것은 지원되지 않습니다. 변경 관리 프로세스를 우회하는 CloudFormation 스택을 생성하려면 승격된 권한(IAM 역할 및 Lambda 함수 생성)이 필요하기 때문입니다. AMS Advanced는 Lambda SSPS 관리자 역할을 사용하여 보안 암호를 교체하는 Lambda 함수를 관리하는 '기존 AWS Lambda 함수를 사용하여 교체 수행'만 지원합니다. AMS Advanced는 보안 암호를 교체하기 위해 Lambda를 생성하거나 관리하지 않습니다.

Q: AMS 계정 AWS Secrets Manager 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

다음 네임스페이스는 AMS에서 사용하도록 예약되어 있으며 AWS Secrets Manager직접 액세스의 일부로 사용할 수 없습니다.

- arn:aws:secretsmanager:*:*:secret:ams-shared/*
- arn:aws:secretsmanager:*:*:secret:customer-shared/*
- arn:aws:secretsmanager:*:*:secret:ams/*

Secrets Manager(AMS SSPS)를 사용하여 키 공유

RFC, 서비스 요청 또는 인시던트 보고서의 일반 텍스트로 AMS와 암호를 공유하면 정보 공개 인시던트가 발생하고 AMS는 사례에서 해당 정보를 수정하고 키를 재생성하는 요청을 수정합니다.

이 네임스페이스에서 AWS Secrets Manager (Secrets Manager)를 사용할 수 있습니다`customer-shared`.

Secrets Manager FAQ를 사용하여 키 공유

Q: Secrets Manager를 사용하여 공유해야 하는 보안 암호 유형은 무엇입니까?

몇 가지 예는 VPN 생성을 위한 사전 공유 키, 인증 키(IAM, SSH), 라이선스 키 및 암호와 같은 기밀 키입니다.

Q: Secrets Manager를 사용하여 AMS와 키를 공유하려면 어떻게 해야 합니까?

1. 페더레이션 액세스 및 적절한 역할을 사용하여 AWS 관리 콘솔에 로그인합니다.

   SALZ의 경우 `Customer_ReadOnly_Role`

   MALZ의 경우 `AWSManagedServicesChangeManagementRole`.
2. AWS Secrets Manager 콘솔로 이동하여 새 보안 암호 저장을 클릭합니다.
3. 다른 유형의 보안 암호(Other type of secrets)를 선택합니다.
4. 보안 암호 값을 일반 텍스트로 입력하고 기본 KMS 암호화를 사용합니다. 다음을 클릭합니다.
5. 보안 암호 이름과 설명을 입력합니다. 이름은 항상 customer-shared/로 시작합니다. 예: customer-shared/mykey2022. 다음을 클릭합니다.
6. 자동 교체를 비활성화한 상태로 두고 다음을 클릭합니다.
7. 검토 후 저장을 클릭하여 보안 암호를 저장합니다.

8. 보안 암호를 식별하고 검색할 수 있도록 서비스 요청, RFC 또는 인시던트 보고서를 통해 보안 암호 이름으로 회신합니다.

Q: Secrets Manager를 사용하여 키를 공유하려면 어떤 권한이 필요합니까?

SALZ: `customer_secrets_manager_shared_policy` 관리형 IAM 정책을 찾아 정책 문서가 아래 생성 단계에 연결된 것과 동일한지 확인합니다. 정책이 다음 IAM 역할에 연결되어 있는지 확인합니다`Customer_ReadOnly_Role`.

MALZ: `AMSSecretsManagerSharedPolicy`가 `ams-shared`네임스페이스에서 `GetSecretValue` 작업을 허용하는 `AWSManagedServicesChangeManagementRole` 역할에 연결되어 있는지 확인합니다.

예제:

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> 를 AWS Secrets Manager 셀프 서비스 프로비저닝된 서비스로 추가할 때 필요한 권한이 부여됩니다.

AMS SSP를 사용하여 AMS 계정 AWS Security Hub CSPM 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Security Hub CSPM 기능에 액세스할 수 있습니다.는 내의 보안 상태와 보안 업계 표준 및 모범 사례 AWS 준수에 대한 포괄적인 보기를 AWS Security Hub CSPM 제공합니다. Security Hub CSPM은 AWS 계정, 서비스 및 지원되는 타사 파트너의 보안 및 규정 준수 조사 결과를 중앙 집중화하고 우선순위를 지정하여 보안 추세를 분석하고 우선순위가 가장 높은 보안 문제를 식별하는 데 도움이 됩니다. 자세한 내용은 AWS Security Hub CSPM를 참조하세요.

AWS Managed Services FAQ의 Security Hub CSPM

Q: AMS 계정 AWS Security Hub CSPM 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Security Hub CSPM에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_securityhub_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Security Hub CSPM을 사용할 때 제한 사항은 무엇인가요?

아카이빙 기능은 잠재적 보안 및 운영 위험으로 기록되었으며 자체 프로비저닝된 서비스 보안 역할의 일부로 제한되었습니다.

Q: AMS 계정 AWS Security Hub CSPM 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Security Hub CSPM 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Service Catalog AppRegistry 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AppRegistry 기능에 직접 액세스할 수 있습니다. AppRegistry를 사용하면 중앙 위치에서 애플리케이션 검색, 보고 및 관리 작업을 수행할 수 있습니다. 빌더는 단일 AWS 계정에서 애플리케이션을 거의 생성하지 않습니다. 일반적으로 개발, 테스트 및 프로덕션과 같은 수명 주기 단계별로 애플리케이션 리소스를 구분합니다. AppRegistry를 사용하면 정의한 AWS 계정에서 모든 리소스 컬렉션을 그룹화하고 볼 수 있습니다.

AppRegistry를 사용하면 AWS 애플리케이션, 애플리케이션과 연결된 리소스 모음 및 애플리케이션 속성 그룹을 저장할 수 있습니다. 자세한 내용은 AppRegistry란 무엇입니까?를 참조하세요.

AMS AWS Service Catalog AppRegistry 의 FAQ:

Q: AMS 계정 AWS Service Catalog AppRegistry 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(관리형 자동화)(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출하여 AppRegistry에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer-appregistry-console-role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Service Catalog AppRegistry 에서 사용에 대한 제한 사항은 무엇인가요?

'Name' 태그에서 AMS 네임스페이스를 사용하는 경우를 제외하고 AppRegistry 서비스에 대한 전체 액세스 권한이 제공됩니다.

Q: AMS 계정 AWS Service Catalog AppRegistry 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 AppRegistry를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Shield Advanced 에서 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Shield Advanced 기능에 액세스할 수 있습니다. AWS Shield Advanced 는에서 실행되는 애플리케이션을 보호하는 관리형 분산 서비스 거부(DDoS) 보호 서비스입니다 AWS. Shield Advanced는 애플리케이션 가동 중지 시간과 지연 시간을 최소화하는 상시 감지 및 자동 인라인 완화 기능을 제공하므로 DDoS 보호의 이점을 활용하기 위해 AWS Support를 참여시킬 필요가 없습니다. AWS Shield 표준과 고급이라는 두 가지 티어가 있으며, AMS는 Shield Advanced를 제공합니다. 자세한 내용은 Shield Advanced를 참조하세요.

모든 AWS 고객은 추가 비용 없이 AWS Shield Standard의 자동 보호를 이용할 수 있습니다.는 웹 사이트 또는 애플리케이션을 대상으로 하는 가장 일반적이고 자주 발생하는 네트워크 및 전송 계층 DDoS 공격으로부터 AWS Shield Standard 보호합니다. Amazon CloudFront 및 Amazon Route 53과 AWS Shield Standard 함께를 사용하면 알려진 모든 인프라(계층 3 및 4) 공격에 대한 포괄적인 가용성 보호를 받을 수 있습니다.

Amazon Elastic Compute Cloud(Amazon EC2), Elastic Load Balancing(ELB), Amazon CloudFront AWS Global Accelerator및 Amazon Route 53 리소스에서 실행되는 애플리케이션을 대상으로 하는 공격에 대해 더 높은 수준의 보호를 받으려면를 구독하면 됩니다 AWS Shield Advanced.

와 함께 제공되는 네트워크 및 전송 계층 보호 외에도 AWS Shield Standard는 대규모의 정교한 DDoS 공격에 대한 추가 탐지 및 완화, 공격에 대한 실시간에 가까운 가시성, 웹 애플리케이션 방화벽과의 통합 AWS WAF을 AWS Shield Advanced 제공합니다. AWS Shield Advanced 또한는 Amazon Elastic Compute Cloud(Amazon EC2), Elastic Load Balancing(Elastic Load Balancing), Amazon CloudFront AWS Global Accelerator및 Amazon Route 53 요금의 DDoS 관련 스파이크에 대한 보호 및 AWS Shield 대응 팀(SRT)에 대한 연중무휴 액세스를 제공합니다.

AWS Managed Services의 Shield Advanced FAQ

Q: AMS 계정에서 Shield Advanced에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Shield Advanced에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다`customer_shield_role`aws_drt_shield_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

역할이 계정에 배포된 후 `customer_shield_role`를 사용하여 계정 AWS Shield Advanced 에서에 대한 구독을 확인할 수 있습니다.

> **Note**
>
> 의 사용과 관련된 월별 요금 및 1년 약정이 있습니다 AWS Shield Advanced. 또한 AMS AWS Shield Advanced 에서를 사용하면 AMS가 에스컬레이션된 분산 서비스 거부 AWS Shield (DDoS) 인시던트 중에 웹 애플리케이션 방화벽(AWS WAF) 규칙을 변경할 수 있는 (SRT)로 에스컬레이션할 수 있는 권한이 부여됩니다. 이러한 변경은 AMS와 협력하여 이루어집니다.

Q: AMS 계정에서 Shield Advanced를 사용하는 데 따르는 제한 사항은 무엇인가요?

제한은 아니지만 Shield Advanced를 사용하면가 배포`aws_drt_shield_role`되므로 에스컬레이션된 DDoS 인시던트 중에 AWS Shield 팀(SRT)이 AMS 계정 내부의 AWS WAF 규칙을 긴급하게 변경할 수 있습니다. 이는 DDoS 공격의 가장 빠른 문제 해결을 위해 AMS에서 권장하며, AMS가 SRT로 에스컬레이션한 후에 발생합니다.

Q: AMS 계정에서 Shield Advanced를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Shield Advanced를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Snowball Edge 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Snowball Edge 기능에 직접 액세스할 수 있습니다. Snowball Edge는 안전하게 설계된 디바이스를 사용하여 AWS 클라우드 안팎으로 대량의 데이터를 전송하는 페타바이트 규모의 데이터 전송 솔루션입니다. Snowball Edge는 높은 네트워크 비용, 긴 전송 시간 및 보안 문제를 포함하여 대규모 데이터 전송과 관련된 일반적인 문제를 해결합니다. Snowball Edge를 사용하여 분석 데이터, 게놈 데이터, 비디오 라이브러리, 이미지 리포지토리, 백업을 마이그레이션하고 데이터 센터 종료, 테이프 교체 또는 애플리케이션 마이그레이션 프로젝트의 일부를 보관할 수 있습니다. Snowball Edge를 사용한 데이터 전송은 간단하고 빠르고 안전하며 고속 인터넷을 통한 데이터 전송 비용의 1/5에 불과할 수 있습니다.

Snowball Edge를 사용하면 데이터를 전송하기 위해 코드를 작성하거나 하드웨어를 구매할 필요가 없습니다. 먼저 AWS 관리 콘솔을 사용하여 Snowball용 가져오기 작업을 생성하면 Snowball 디바이스가

자동으로 배송됩니다. 디바이스가 도착하면 로컬 네트워크에 디바이스를 연결하고 Snowball 클라이언트("클라이언트")를 다운로드하여 실행하여 연결을 설정한 다음 클라이언트를 사용하여 디바이스로 전송할 파일 디렉터리를 선택합니다. 그런 다음 클라이언트는 파일을 암호화하여 디바이스에 고속으로 전송합니다. 전송이 완료되고 디바이스를 반환할 준비가 되면 E Ink 배송 레이블이 자동으로 업데이트되고 Amazon Simple Notification Service(Amazon SNS), 문자 메시지 또는 콘솔에서 직접 작업 상태를 추적할 수 있습니다. 자세한 내용은 AWS Snowball Edge를 참조하세요.

AWS Managed Services의 Snowball Edge FAQ

일반적인 질문과 답변:

Q: AMS 계정 AWS Snowball Edge 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS에서 Snowball Edge 구현은 2단계 프로세스입니다.

1. 관리 제출 | 기타 | 기타 | (ct-1e1xtak34nx76) 변경 유형을 생성하고 AMS 계정의 Snowball Edge에 대한 서비스 역할을 요청합니다.
2. 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 사용자 액세스를 요청합니다. 이 RFC는 계정에 `customer_snowball_console_role`, `customer_snowball_export_role`및 IAM 역할을 프로비저닝합니다`customer_snowball_import_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Snowball Edge 에서 사용에 대한 제한 사항은 무엇입니까?

의 전체 기능은 AMS 계정에서 AWS Snowball Edge 사용할 수 있습니다.

Q: AMS 계정 AWS Snowball Edge 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

위에서 언급한 대로 서비스 역할 계정이 있어야 합니다.

AMS SSP를 사용하여 AMS 계정 AWS Step Functions 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Step Functions 기능에 액세스할 수 있습니다. AWS Step Functions 는 시각적 워크플로를 사용하여 분산 애플리케이션 및 마이크로서비스의 구성 요소를 조정할 수 있는 웹 서비스입니다. 각각 기능 또는 작업을 수행하는 개별 구성 요소를 사용하여 애플리케이션을 구축하면 애플리케이션을 빠르게 확장하거나 변경할 수 있습니다. Step Functions는 구성 요소를 조정하고 애플리케이션 기능을 단계별로 실행할 수 있는 안정적인 방법을 제공합니다. Step Functions는 애플리케이션의 구성 요소를 일련의 단계로 시각화하는 그래픽 콘솔을 제공합니다. 각 단계를 자동으로 트리거 및 추적하고 오류가 있을 때 재시도하므로

애플리케이션은 매번 예상대로 순서대로 실행됩니다. Step Functions는 각 단계의 상태를 기록합니다. 따라서 무언가 잘못된 경우 빠르게 문제를 진단하고 디버깅할 수 있습니다. 자세한 내용은 AWS Step Functions를 참조하세요.

AWS Managed Services Step Functions FAQ

일반적인 질문과 답변:

Q: AMS 계정 AWS Step Functions 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Step Functions 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_step_functions_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Step Functions 에서 사용에 대한 제한 사항은 무엇인가요?

의 전체 기능은 AMS 계정에서 AWS Step Functions 사용할 수 있습니다.

Q: AMS 계정 AWS Step Functions 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

런타임 시 Step Functions에서 사용하는 역할은 단계 함수에서 사용하는 서비스에 액세스할 수 있어야 합니다. 예를 들어 단계 함수는 Lambda 함수에 의존할 수 있습니다. 단계 함수를 작성하는 사람은 Lambda 함수를 동시에 생성할 가능성이 높으므로 해당 서비스에 대한 액세스도 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 AWS Systems Manager 파라미터 스토어 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Systems Manager Parameter Store 기능에 직접 액세스할 수 있습니다. AWS Systems Manager Parameter Store는 구성 데이터 관리 및 보안 암호 관리를 위한 안전한 계층적 스토리지를 제공합니다. 암호, 데이터베이스 문자열, 라이선스 코드와 같은 데이터를 파라미터 값으로 저장할 수 있습니다. 값을 일반 텍스트 또는 암호화된 데이터로 저장할 수 있습니다. 그런 다음 파라미터를 생성할 때 지정한 고유한 이름을 사용하여 값을 참조할 수 있습니다. 확장성, 가용성 및 내구성이 뛰어난 Parameter Store는 AWS 클라우드를 기반으로 합니다. 자세한 내용은 AWS Systems Manager 파라미터 스토어를 참조하세요.

> **Note**
>
> 수명 주기 관리가 포함된 전용 보안 암호 스토어를 원하는 경우 Parameter Store AMS SSP를 사용하여 AMS 계정 AWS Secrets Manager 에서 프로비저닝 대신를 사용합니다. Secrets

Manager를 사용하면 보안 암호를 자동으로 교체할 수 있으므로 보안 및 규정 준수 요구 사항을 충족할 수 있습니다. Secrets Manager는 Amazon RDS의 MySQL, PostgreSQL 및 Amazon Aurora에 대한 내장 통합을 제공하며, Lambda 함수를 사용자 지정하여 다른 유형의 보안 암호로 확장할 수 있습니다.

AWS Systems Manager AWS Managed Services 파라미터 스토어 FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Systems Manager Parameter Store에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 AWS Systems Manager 파라미터 스토어에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_systemsmanager_parameterstore_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 AWS Systems Manager 파라미터 스토어를 사용할 때 제한 사항은 무엇인가요?

AWS 관리형 키를 사용해야 합니다. 사용자 지정 KMS 키 생성은 액세스가 제한됩니다. 그러나 사용자 지정 키가 필요한 경우 RFC를 제출하여 `IAMPrincipalsRequiringDecryptPermissions` 및 `IAMPrincipalsRequiringEncryptPermissionsPrincipal` 파라미터의 값으로 배포 | 고급 스택 구성 요소 | KMS 키 |이 IAM 역할을 사용하여 변경 유형 생성(ct-1d84keiri1jhg)`customer_systemsmanager_parameterstore_console_role`을 사용하여 고객 관리형 키(CMK)를 생성합니다. KMS 키가 생성된 후 이를 사용하여 보안 문자열을 생성할 수 있습니다.

Q: AMS 계정에서 AWS Systems Manager Parameter Store를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없지만 SSM 파라미터 스토어는 KMS를 사용하여 보안 문자열을 생성하므로 파라미터 스토어에 저장된 값을 암호화하고 해독할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 AWS Systems Manager 자동화 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Systems Manager 자동화 기능에 액세스할 수 있습니다. AWS Systems Manager 자동화는 실행서, 작업 및 서

비스 할당량을 사용하여 Amazon Elastic Compute Cloud 인스턴스 및 기타 AWS 리소스의 일반적인 유지 관리 및 배포 작업을 간소화합니다. 이를 통해 대규모로 자동화를 구축, 실행 및 모니터링할 수 있습니다. Systems Manager Automation은 Systems Manager가 관리형 인스턴스에서 수행하는 작업을 정의하는 Systems Manager 문서의 한 유형입니다. 관리형 인스턴스 내에서 명령 또는 자동화 스크립트 실행과 같은 일반적인 유지 관리 및 배포 작업을 수행하는 데 사용하는 실행서입니다. Systems Manager에는 Amazon Elastic Compute Cloud 태그를 사용하여 대규모 인스턴스 그룹을 대상으로 지정하는 데 도움이 되는 기능과 정의한 제한에 따라 변경 사항을 롤아웃하는 데 도움이 되는 속도 제어가 포함되어 있습니다. 실행서는 JavaScript Object Notation(JSON) 또는 YAML을 사용하여 작성됩니다. 그러나 Systems Manager Automation 콘솔에서 [문서 빌더(Document Builder)]를 사용하면 기본 JSON 또는 YAML로 작성하지 않고도 실행서를 생성할 수 있습니다. 또는 필요에 맞는 사전 정의된 단계가 있는 Systems Manager 제공 런북을 사용할 수 있습니다. 자세한 내용은 AWS Systems Manager 설명서의 런북 작업을 참조하세요.

> **Note**
>
> Systems Manager Automation은 실행서에서 사용할 수 있는 20가지 작업 유형을 지원하지만, AMS Advanced 계정에서 사용할 실행서를 작성하는 동안 사용할 수 있는 작업 수는 제한적입니다. 마찬가지로 제한된 수의 Systems Manager 제공 런북을 직접 사용하거나 자체 런북 내에서 사용할 수 있습니다. 자세한 내용은 다음 FAQ의 제한 사항을 참조하세요.

AWS Systems Manager AWS Managed Services의 자동화 FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Systems Manager Automation에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 AWS Systems Manager 자동화에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_systemsmanager_automation_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 AWS Systems Manager Automation을 사용할 때의 제한 사항은 무엇인가요?

관리형 인스턴스 내에서 명령 및/또는 스크립트만 실행하려면 자동화를 위해 제한된 Systems Manager 지원 작업 집합으로 실행서를 작성해야 합니다. 제한 사항과 함께 사용할 수 있는 작업은 다음과 같습니다.

AWS Systems Manager 자동화 제한 사항

작업	설명	제한 사항
aws:assertAwsResou rceProperty –	AWS 리소스 상태 또는 이벤트 상태 어설션	EC2 인스턴스만
aws:aws:branch –	조건부 자동화 단계 실행	제한 없음
aws:createTags –	AWS 리소스에 대한 태그 생성	작성한 SSM 자동화 런북에만 해당
aws:executeAutomation –	다른 자동화 실행	작성한 자동화 실행서만
aws:executeScript –	스크립트 실행	서비스에 대한 API 호출을 수행하지 않는 스크립트만 해당
aws:pause –	자동화 일시 중지	제한 없음
aws:runCommand –	관리형 인스턴스에서 명령 실행	System Manager 제공 문서만 사용 - AWS-RunShellScript 및 AWS-RunPowerShellScript
aws:sleep –	자동화 지연	제한 없음
aws:waitForAwsReso urceProperty –	AWS 리소스 속성 대기	EC2 인스턴스만

Systems Manager 콘솔에서 'Run Command' 기능을 사용하여 Systems Manager 제공 실행서 AWS-RunShellScript 및 AWS-RunPowerShellScript로 직접 명령 또는 스크립트를 실행하도록 선택할 수도 있습니다. 추가 사전 및/또는 사후 검증 또는 복잡한 자동화 로직을 지원하는 이러한 런북을 런북 내에 중첩할 수도 있습니다.

역할은 최소 권한 원칙을 준수하며 관리형 인스턴스 내에서 명령 및/또는 스크립트를 실행하기 위한 실행서의 실행 세부 정보를 작성, 실행 및 검색하는 데 필요한 권한만 제공합니다. AWS Systems Manager 서비스에서 제공하는 다른 기능에 대한 권한은 제공하지 않습니다. 이 기능을 사용하면 자동화 런북을 작성할 수 있지만 런북 실행은 AMS 소유 리소스에 대해 대상으로 지정할 수 없습니다.

Q: AMS 계정에서 AWS Systems Manager Automation을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없지만 런북을 작성하는 동안 내부 프로세스 및/또는 규정 준수 제어를 준수해야 합니다. 또한 프로덕션 리소스에 대해 실행하기 전에 런북을 철저히 테스트하는 것이 좋습니다.

Q: Systems Manager 정책을 다른 IAM 역할에 연결할 **`customer_systemsmanager_automation_policy`** 수 있나요?

아니요. 다른 자체 프로비저닝 지원 서비스와 달리이 정책은 프로비저닝된 기본 역할 에만 할당할 수 있습니다`customer_systemsmanager_automation_console_role`.

다른 SSPS 역할의 정책과 달리이 AMS 서비스는 관리형 인스턴스 내에서 명령 또는 자동화 스크립트를 실행하기 위한 것이므로이 SSM SSPS 정책은 다른 사용자 지정 IAM 역할과 공유할 수 없습니다. 이러한 권한을 다른 서비스에 대한 권한을 가진 다른 사용자 지정 IAM 역할에 연결할 수 있는 경우 허용된 작업 범위가 관리형 서비스로 확장되어 계정의 보안 태세가 저하될 수 있습니다.

AMS 기술 표준을 기준으로 변경 요청(RFCs)을 평가하려면 해당 클라우드 아키텍트 또는 서비스 제공 관리자와 협력하고 RFC 보안 검토를 참조하세요.

> **Note**
>
> AWS Systems Manager 를 사용하면 계정과 공유되는 런북을 사용할 수 있습니다. 공유 런북을 사용할 때는 주의를 기울이고 실사 검사를 수행하고 콘텐츠를 검토하여 런북을 실행하기 전에 실행되는 명령/스크립트를 이해하는 것이 좋습니다. 자세한 내용은 공유 SSM 문서의 모범 사례를 참조하세요.

AMS SSP를 사용하여 AMS 계정 AWS Transfer Family 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Transfer Family (Transfer Family) 기능에 액세스합니다. AWS Transfer Family 는 SFTP(Secure File Transfer Protocol)를 통해 Amazon Simple Storage Service(Amazon S3) 스토리지 안팎으로 파일을 전송할 수 있는 완전 관리형 AWS 서비스입니다. SFTP는 Secure Shell(SSH) File Transfer Protocol이라고도 합니다. SFTP는 금융 서비스, 의료, 광고, 소매를 비롯한 다양한 산업의 데이터 교환 워크플로우에서 활용됩니다.

SFTP를 사용하면 서버 인프라를 실행할 필요 AWS 없이 AWS 에서 SFTP 서버에 액세스할 수 있습니다. 이 서비스를 사용하여 최종 사용자의 클라이언트 및 구성을 그대로 AWS 유지하면서 SFTP 기반 워크플로를 로 마이그레이션할 수 있습니다. 먼저 호스트 이름을 SFTP 서버 엔드포인트와 연결한 다음 사용자를 추가하고 적절한 액세스 수준으로 프로비저닝합니다. 이렇게 하면 사용자의 전송 요청이 AWS SFTP 서버 엔드포인트에서 직접 처리됩니다. 자세한 내용은 단원과 SFTP 지원 서버

AWS Transfer for SFTP생성을 참조하십시오. https://docs.aws.amazon.com/transfer/latest/userguide/create-server-sftp.html

AWS Transfer for SFTP AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Transfer for SFTP 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Transfer for SFTP 제출하여에 대한 액세스를 요청합니다. 이 RFC를 통해 다음 IAM 역할과 정책이 계정에 프로비저닝됩니다.

- `customer_transfer_author_role`. 이 역할은 콘솔을 통해 SFTP 서비스를 관리하도록 설계되었습니다.
- `customer_transfer_sftp_server_logging_role`. 이 역할은 SFTP 서버에 연결되도록 설계되었습니다. 이를 통해 SFTP 서버가 CloudWatch로 로그를 가져올 수 있습니다.
- `customer_transfer_sftp_user_role`. 이 역할은 SFTP 사용자에게 연결되도록 설계되었습니다. 이를 통해 SFTP 사용자는 S3 버킷과 상호 작용할 수 있습니다.
- `policy customer_transfer_scope_down_policy`. 이 정책은 SFTP 사용자에게 적용하여 S3 버킷에 대한 액세스를 홈 폴더로 제한할 수 있는 범위 축소 정책입니다.
- `customer_transfer_sftp_efs_user_role`. 이 역할은 SFTP 사용자에게 연결되도록 설계되었습니다. 이를 통해 SFTP 사용자는 EFS 파일 시스템과 상호 작용할 수 있습니다.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Transfer for SFTP 에서 사용에 대한 제한 사항은 무엇인가요?

AWS SFTP 구성을 위한 전송은 AMS 인프라에 대한 수정을 방지하기 위해 "AMS-" 또는 "MC-" 접두사가 없는 리소스로 제한됩니다.

Q: AMS 계정 AWS Transfer for SFTP 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

- AWS Transfer for SFTP 서버 및 사용자를 생성하기 전에 키워드 "전송"이 포함된 이름을 가진 Amazon S3 버킷이 있어야 합니다.
- "고객 식별 공급자"를 사용하려면 API Gateway, Lambda 함수 및 사용자 리포지토리(AD, Secrets Manager 등)를 배포해야 합니다. 자세한 내용은 AWS Transfer for SFTP 사용 및 자격 증명 공급자 작업에 대한 암호 인증 활성화 AWS Secrets Manager를 참조하세요.

AMS SSP를 사용하여 AMS 계정 AWS Transit Gateway 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Transit Gateway 기능에 액세스할 수 있습니다. AWS Transit Gateway 는 Amazon Virtual Private Cloud(VPCs)와 온프레미스 네트워크를 단일 게이트웨이에 연결할 수 있는 서비스입니다. 에서 실행되는 워크로드 수가 증가함에 따라 여러 계정과 Amazon VPCs에서 네트워크를 확장하여 성장을 따라잡을 수 AWS있어야 합니다. 오늘날 피어링을 사용하여 Amazon VPCs 페어를 연결할 수 있습니다. 그러나 연결 정책을 중앙에서 관리할 수 없는 상태에서 많은 Amazon VPCs에서 point-to-point 연결을 관리하는 것은 운영 비용이 많이 들고 번거로울 수 있습니다. 온프레미스 연결을 위해 각 개별 Amazon VPC에 AWS VPN을 연결해야 합니다. 이 솔루션은 구축에 시간이 많이 걸리고 VPCs 수가 수백 개로 증가할 때 관리하기 어려울 수 있습니다. 자세한 내용은 AWS Transit Gateway를 참조하세요.

AWS Transit Gateway AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Transit Gateway 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Transit Gateway 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_tgw_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Transit Gateway 에서 사용에 대한 제한 사항은 무엇인가요?

Transit Gateway 라우팅에 대한 라우팅 테이블 수정 AWS Transit Gateway 을 제외하고 AMS 단일 계정 랜딩 존 계정에서의 전체 기능을 사용할 수 있습니다. 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)을 제출하여 라우팅 테이블 변경을 요청합니다.

> **Note**
>
> 이 서비스는 다중 계정 랜딩 존(MALZ)이 아닌 단일 계정 랜딩 존(SALZ)에서만 지원됩니다.

Q: AMS 계정 AWS Transit Gateway 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Transit Gateway 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 프로비저닝 AWS WAF - AMS 계정에서 웹 애플리케이션 방화벽

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS WAF 기능에 액세스합니다. AWS WAF 는 애플리케이션 가용성에 영향을 미치거나, 보안을 손상시키거나, 과도한 리소스를 소비할 수 있는 일반적인 웹 악용으로부터 웹 애플리케이션을 보호하는 데 도움이 되는 웹 애플리케이션 방화벽(AWS WAF)입니다. AWS WAF 는 사용자 지정 가능한 웹 보안 규칙을 정의하여 웹 애플리케이션에 허용하거나 차단할 트래픽을 제어합니다. AWS WAF 를 사용하여 SQL 삽입 또는 교차 사이트 스크립팅과 같은 일반적인 공격 패턴을 차단하는 사용자 지정 규칙과 특정 애플리케이션에 맞게 설계된 규칙을 생성할 수 있습니다.

자세한 내용은 AWS WAF - 웹 애플리케이션 방화벽을 참조하세요.

AMS는에 대한 모니터링(CloudWatch 경보/이벤트/MMS 알림)을 지원하지 않습니다 AWS WAF. 의 특성으로 인해 애플리케이션에 대한 사용자 지정 규칙을 생성 AWS WAF해야 합니다. AMS는 애플리케이션의 컨텍스트 없이는 경보를 정량화하고 생성할 수 없습니다. 자세한 내용은 AWS WAF - 웹 애플리케이션 방화벽을 참조하세요.

AWS WAF AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS WAF 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS WAF 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_waf_role`. 계정에 AWS WAF IAM 역할이 프로비저닝된 후 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS WAF?

권한이 프로비저닝되면의 전체 기능을 사용할 수 있습니다 AWS WAF.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS WAF?

AMS 계정 AWS WAF 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Well-Architected Tool 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Well-Architected Tool 기능에 직접 액세스할 수 있습니다. 는 워크로드의 상태를 검토하고 이를 최신 AWS 아키텍처 모범 사례와 비교하는 데 AWS Well-Architected Tool 도움이 됩니다. 이 도구는 클라우드 AWS 아키텍트가 안전하고 성능이 뛰어나며 복원력이 뛰어나고 효율적인 애플리케이션 인프라를 구축할 수 있도록 개발된 Well-Architected Framework를 기반으로 합니다. 이 프레임워크는 아키텍처를 평가하는 데 일관된 접근 방식을 제공하고, 솔루션 아키텍처 팀이 수행한 수만 개의 워크로드 검토에 사용되었으며, 시간이 지남에 따라 AWS 애플리케이션 요구 사항에 따라 확장되는 설계를 구현하는 데 도움이 되는 지침을 제공합니다. 자세한 내용은 AWS Well-Architected Tool를 참조하세요.

AWS WA Tool AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Well-Architected Tool 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Well-Architected Tool 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_well_architected_tool_console_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Well-Architected Tool 에서 사용에 대한 제한 사항은 무엇인가요?

의 전체 기능은 AMS 계정에서 AWS Well-Architected Tool 사용할 수 있습니다.

Q: AMS 계정 AWS Well-Architected Tool 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Well-Architected Tool 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS X-Ray 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS X-Ray (X-Ray) 기능에 액세스합니다. 개발자 AWS X-Ray 는 마이크로서비스 아키텍처를 사용하여 구축된 것과 같은 프로덕션 분산 애플리케이션을 분석하고 디버깅할 수 있습니다. X-Ray를 사용하면 애플리케이션과 기본 서비스가 어떻게 수행되고 있는지 이해하여 성능 문제 및 오류의 근본 원인을 식별하고 해결할 수 있습니다. X-Ray는 애플리케이션을 통해 이동하는 요청에 대한 end-to-end 보기를 제공하고 애플리케

이션의 기본 구성 요소 맵을 보여줍니다. X-Ray를 사용하여 간단한 3계층 애플리케이션에서 수천 개의 서비스로 구성된 복잡한 마이크로서비스 애플리케이션에 이르기까지 개발 중인 애플리케이션과 프로덕션 중인 애플리케이션을 모두 분석할 수 있습니다. 자세한 내용은 AWS X-Ray를 참조하세요.

AWS Managed Services FAQ의 X-Ray

일반적인 질문과 답변:

Q: AMS 계정 AWS X-Ray 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다`customer_xray_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다. 또한 Amazon EC2 인스턴스에서 X-Ray로 데이터를 푸시`customer_xray_daemon_write_instance_profile`하려면가 있어야 합니다. 이 인스턴스 프로파일은를 수신할 때 생성됩니다`customer_xray_console_role`.

AMS Operations에 서비스 요청을 제출하여 기존 인스턴스 프로파일에 `customer_xray_daemon_write_policy`를 할당하거나 AMS Operations가 X-Ray를 활성화할 때 생성된 인스턴스 프로파일을 사용할 수 있습니다.

Q: AMS 계정 AWS X-Ray 에서 사용에 대한 제한 사항은 무엇인가요?

AWS KMS 키(KMS 키)를 사용한 암호화를 제외하고 AMS 계정에서의 전체 기능을 사용할 수 있습니다. AWS X-Ray 는 기본적으로 모든 추적 데이터를 AWS X-Ray 암호화합니다. 기본적으로 X-Ray 는 추적 및 관련 저장 데이터를 암호화합니다. 키로 저장 데이터를 암호화해야 하는 경우 AWS관리형 KMS 키(aws/xray) 또는 KMS 고객 관리형 키를 선택할 수 있습니다. X-Ray 암호화를 위한 KMS 고객 관리형 키의 경우 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)을 제출합니다.

Q: AMS 계정 AWS X-Ray 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AWS X-Ray 에는 AMS 계정에 이미 구현된 Amazon S3, CloudWatch 및 CloudWatch Logs에 대한 종속성이 있습니다. 전송 종속성은 데이터 소스 및 기능이 상호 작용할 수 AWS X-Ray 있는 기타 AWS 서비스(예: Amazon Redshift, Amazon RDS, Athena)에 따라 달라집니다.

AMS SSP를 사용하여 AMS 계정에서 VM Import/Export 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 VM 가져오기/내보내기 기능에 직접 액세스할 수 있습니다. VM Import/Export를 사용하면 기존 환경에서 Amazon EC2 인스턴스

로 가상 머신 이미지를 쉽게 가져와 온프레미스 환경으로 다시 내보낼 수 있습니다. 이 제품을 사용하면 IT 보안, 구성 관리 및 규정 준수 요구 사항을 충족하도록 구축한 가상 머신에 대한 기존 투자를 즉시 ready-to-use 수 있는 인스턴스로 Amazon EC2로 가져와 활용할 수 있습니다. 가져온 인스턴스를 온프레미스 가상화 인프라로 다시 내보내 IT 인프라 전체에 워크로드를 배포할 수도 있습니다. 자세한 내용은 VM Import/Export를 참조하세요.

AWS Managed Services FAQ의 VM Import/Export

일반적인 질문과 답변:

Q: AMS 계정에서 VM Import/Export에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 VM Import/Export에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 정책을 프로비저닝합니다`customer_vmimport_policy`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

서비스가 계정에서 작업을 수행하려면 추가 역할인 VM Import/Export Service 역할이 필요합니다.

Q: AMS 계정에서 VM Import/Export를 사용할 때 제한 사항은 무엇인가요?

- 사용자 지정 머신 이미지와 데이터 볼륨을 가져오는 기능은 모두 AMS VM Import/Export에서 사용할 수 있습니다. 그러나 S3에 대한 권한은 계정 내 정보에 대한 액세스를 제한하기 `customer-vmimport-*` 위해 이름과 일치하는 버킷으로 작업을 제한하도록 범위가 축소되었습니다.
- 이미지 및 스냅샷 가져오기는 AMS VM Import/Export에서 지원됩니다. 그러나 보안 조치로 인해 인스턴스 가져오기 및 인스턴스 내보내기 기능을 사용할 수 없습니다.
- 또한 제한 및 민감한 데이터를 내보낼 위험을 완화하기 위해 내보내기 기능이 비활성화되었습니다.

Q: AMS 계정에서 VM Import/Export를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

- AWS 환경으로 가져오려면 지원되는 디스크 이미지를 제공해야 합니다. 자세한 내용은 VM Import/Export Requirements를 참조하세요.
- AWS 콘솔을 통해 VM Import/Export에 액세스할 수 없습니다. AWS CLI AWS Tools for PowerShell 또는 AWS SDKs를 통해이 서비스에 액세스해야 합니다. 또는 변경 유형 ct-117rmp64d5mvb: 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | EC2 인스턴스 프로파일 생성을 제출하여 인스턴스 프로파일을 요청할 수 있습니다. 이 인스턴스 프로파일을 사용하면 도구가 인스턴스에서 명령을 수행할 수 있습니다.

고객 관리형 모드

AWS Managed Services(AMS) 고객 관리형 모드는 유연한 거버넌스 모델을 제공하며 요구 사항에 맞게 조정할 수 있습니다. 이는 AMS가 작동하지 않는 서비스 및 애플리케이션에 대한 대체 옵션으로 간주될 수 있습니다. AMS는이 모드에서 생성된 계정에서 호스팅되는 인프라를 운영하지 않습니다. 그러나이 모드에서 중앙 집중식 다중 계정 관리를 활용할 수 있습니다. 이 모드에서는 다음과 같은 다중 계정 랜딩 존 기능을 활용할 수 있습니다.

- 자동 계정 배포
- 네트워킹 계정의 Transit Gateway를 통한 연결
- AMS Config 규칙 라이브러리
- 로그 복사본을 로깅 계정에 저장
- 보안 계정에 대한 고객 관리형 Guard Duty 알림 집계
- 통합 결제
- 사용자 지정 서비스 제어 정책 활성화.

예: AMS에서 관리하는 운영 체제가 아닌 Ubuntu Pro에서 워크로드를 실행하려는 경우 고객 관리형 계정을 사용하여 호스팅할 수 있습니다. 고객 관리형 계정을 통해 워크로드를 통합하여 AWS 조직 간 공유를 통해 사용할 수 있는 예약 인스턴스/공유 플랜에 대한 대량 할인을 활용할 수도 있습니다.

고객 관리형 모드 시작하기

AMS 고객 관리형 모드는 특수 다중 계정 랜딩 존 애플리케이션 계정을 통해 사용할 수 있습니다.

고객 관리형 애플리케이션 계정을 생성하는 방법을 비롯한 자세한 내용은 고객 관리형 애플리케이션 계정을 참조하세요.

AMS 및 AWS Service Catalog

AWS Managed Services(AMS)의 Service Catalog를 사용하면 조직이 AWS IT(정보 기술) 서비스의 카탈로그를 생성 및 관리할 수 있으며, IT 관리자는 승인된 제품의 카탈로그를 생성 및 관리하고 계정의 최종 사용자에게 배포하여 맞춤형 서비스 포털에서 필요한 제품에 액세스할 수 있습니다. 관리자는 각 제품에 액세스할 수 있는 사용자를 제어하여 조직 비즈니스 정책을 준수할 수 있습니다. 관리자는 최종 사용자가 승인된 리소스를 배포하기 위해 Service Catalog에 대한 IAM 액세스만 요구하도록 역할을 설정할 수도 있습니다. Service Catalog를 사용하면 조직이 민첩성을 높이고 비용을 절감할 수 있습니다. 최종 사용자는 사용자가 제어하는 카탈로그에서 필요한 제품만 찾아 시작할 수 있기 때문입니다.

Service Catalog는 AMS 관리형 계정(들)에서 리소스를 프로비저닝하고 업데이트하기 위한 AMS 변경 요청(RFC) 프로세스의 대안을 제공합니다. AMS는 보안, 규정 준수, 프로비저닝, 가용성, 패치, 모니터링, 알림, 보고, 인시던트 대응, 비용 최적화를 포함하여 Service Catalog를 통해 프로비저닝된 모든 인프라 리소스에 대해 대규모로 AWS를 실행하는 데 필요한 모든 인프라 운영 작업을 관리합니다. AMS 관리형 계정에서 Service Catalog를 활용하면 일반적으로 배포되는 IT 서비스를 중앙에서 관리하고 일관된 거버넌스를 달성하는 동시에 사용자가 필요한 승인된 IT 서비스만 관리형 환경에 빠르게 배포할 수 있습니다.

Service Catalog 시작하기

AMS에서 Service Catalog를 시작하려면 AMS 콘솔을 통해 서비스 요청을 제출하여 Service Catalog에 대한 액세스를 요청합니다. 요청을 제출하면 AMS(이전에 `Transform` 설명됨)를 호출하는 CloudFormation 매크로가 포함된 AMS 관리형 스택과 함께 세 개의 IAM 역할이 계정에 배포되어 시스템에 제품을 등록하고 Service Catalog를 통해 프로비저닝된 인프라에 대해 작업을 수행할 수 있습니다. 배포된 세 가지 IAM 역할에는 IT 관리자가 제품을 Service Catalog 관리자로 관리하는 역할, 애플리케이션 소유자와 최종 사용자가 제품을 구성, 시작 및 관리하는 역할, Service Catalog가 제품을 시작하거나 업데이트하는 동안 사용할 권한을 정의하는 시작 제약 조건으로 사용할 역할이 포함됩니다.

시작하기 전에 AMS의 Service Catalog

Service Catalog가 기존 AMS 변경 요청(RFC) 프로세스를 대체하나요?

> Service Catalog가 활성화된 계정에서는 사전 정의된 제품 카탈로그를 통해 AMS 계정에서 IT 서비스를 프로비저닝하고 업데이트하는 변경 관리 시스템 역할을 합니다. AMS는 기본 포트폴리오/제품 카탈로그를 제공하며 IT 관리자는 직접 생성하고 구성할 수 있습니다. Service Catalog는 Service Catalog를 통해 프로비저닝된 스택만 승인합니다. 마찬가지로 Service Catalog 외부에서 수정하면 승인된 제품 구성에서 스택이 드리프트되므로 Service Catalog를 통해 프로비저닝된 서비스는 AMS RFC 프로세스를 통해 수정할 수 없습니다.

AMS 콘솔에서 서비스 카탈로그를 통해 프로비저닝된 스택을 볼 수 있나요?

> 예. AMS 콘솔에서 서비스 카탈로그를 통해 프로비저닝된 모든 스택을 볼 수 있습니다. 서비스 카탈로그를 통해 프로비저닝된 스택은 스택 ID "SC-"로 쉽게 식별할 수 있습니다. 스택은 AMS 콘솔에서 볼 수 있지만 AMS RFC 프로세스를 통해 업데이트할 수 없습니다. AMS 변경 관리 시스템(RFCs)에 대한 액세스는 액세스 요청, 패치 오케스트레이션 및 백업 RFCs로만 제한됩니다.

Service Catalog를 통해 스택을 프로비저닝 및/또는 업데이트하면 AMS 콘솔에 해당 RFC가 있습니까?

> AMS 콘솔에 표시되는 유일한 RFC는 스택이 처음 프로비저닝될 때 AMS에 스택을 등록하는 RFC입니다. 이 RFC는 Service Catalog를 통해 스택이 시작될 때 트리거되는 AMS 검증 프로세스에 의

해 자동으로 제출됩니다. 다른 모든 프로비저닝 및 변경 사항은 Service Catalog에서 직접 추적되며 Service Catalog 콘솔에서 볼 수 있습니다. 또한 Service Catalog의 프로비저닝된 제품 계획 기능을 사용하여 제품을 프로비저닝하거나 업데이트하기 전에 리소스에 적용될 변경 사항 목록을 볼 수 있습니다.

AMS 관리형 계정에서 제품을 프로비저닝할 때 특정 작업을 수행해야 합니까?

예. AMS 계정에 프로비저닝된 모든 Service Catalog 제품은 해당 제품을 정의하는 CFN 템플릿에 다음 JSON 행을 포함해야 합니다.

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

이 CloudFormation 코드 조각은 AMS 관리형 계정에서 리소스를 프로비저닝하기 위해 필요한 AMS 검증을 트리거합니다. 이 코드 줄을 제품 정의의 일부로 포함하는 것은 사용자의 책임입니다. 포함되지 않은 경우 프로비저닝이 실패하고 "Failed to create product. 이 계정은 AMS에서 관리합니다. AMS 계정의 모든 제품은 템플릿에 AMS `Transform` 코드가 있어야 합니다."

시작 시 AMS 고객이 사용할 수 없거나 제한되는 Service Catalog 기능이 있나요?

예, 초기 시작 시 AMS 고객은 다음 SC 기능을 사용할 수 없습니다.

- Service Catalog를 통한 계정 생성
- Service Catalog를 통해 AMS 관리형 계정으로 모든 AWS 서비스를 시작할 수 있습니다. AWS 서비스 가용성은 AMS 지원 서비스(관리형 및 자체 프로비저닝형)로 제한됩니다. AMS 지원 서비스에 대한 자세한 내용은 AMS 서비스 설명을 참조하세요.
- Service Catalog IT 서비스 관리자(ITSM) 커넥터는 AMS 인시던트 보고서 및 서비스 요청과 통신하지 않습니다.
- Service Catalog 빠른 시작을 활용하고 수정 없이 아키텍처를 참조할 수 있습니다. AMS 계정용 Service Catalog 제품에는 다음 JSON 코드 행이 포함되어야 합니다.

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  CNF 템플릿의 . 이 줄은 일반적인 AWS CloudFormation 템플릿의 일부가 아니므로 명시적으로 추가해야 합니다.
- Terraform은 현재 Service Catalog 제품 프로비저닝을 위해 AMS에서 지원되지 않습니다.
- AWS CFN 스택 세트는 AMS에서 지원되지 않습니다.
- 사용자 지정 IAM 역할은 생성할 수 없습니다.

- 서비스 작업은 다음으로 제한됩니다.
  - AWS-RebootRdsInstance
  - AWS-RestartEC2Instance
  - AWS-StartEC2Instance
  - AWS-StartRdsInstance
  - AWS-StopEC2Instance
  - AWS-StopRdsInstance
  - AWS-CreateImage
  - AWS-CreateRdsSnapshot
  - AWS-CreateSnapshot

> **Note**
>
> 서비스 작업을 생성할 때 최종 사용자의 권한, 시작 역할 또는 선택한 사용자 지정 IAM 역할로 실행 역할을 구성할 수 있습니다. 선택한 실행 역할에는 서비스 작업을 수행할 수 있는 충분한 권한이 있어야 하며 서비스 카탈로그에서 수임할 수 있는 TrustPolicy가 있어야 합니다. 그렇지 않으면 실행 시 해당 서비스 작업이 실패합니다. 서비스 작업으로 사용할 올바른 권한과 신뢰 정책이 있는 AWSManagedServicesServiceCatalogLaunchRole을 사용하는 것이 좋습니다.

AMS RFC 시스템을 계속 사용해야 하는 대상은 무엇입니까?

일반 가용성(GA)에서도 RFCS를 사용하여 다음 작업을 실행해야 합니다.

- 패치 오케스트레이터 구성
- 백업 정책 구성
- 인스턴스 액세스 요청
- AMS 지침을 벗어나는 보안 그룹 생성 및 할당.
- 워크로드 수집 수행(WIGS)
- IAM 역할 생성

Service Catalog CLI를 사용하여 AMS 관리형 계정의 Service Catalog에 액세스할 수 있나요?

예, Service Catalog APIs CLI를 통해 사용 및 활성화됩니다. 해당 아티팩트의 프로비저닝 및 종료를 통해 Service Catalog 아티팩트 관리의 작업을 사용할 수 있습니다. 자세한 내용은 AWS Service Catalog 리소스를 참조하거나 최신 AWS SDK 또는 CLI를 다운로드하세요.

누가 고객의 승인된 제품 카탈로그를 생성, 관리 및 배포하나요?

고객의 카탈로그 관리자 및/또는 IT 관리자 또는 할당된 리소스는 서비스 카탈로그 카탈로그 및 승인된 제품의 관리를 담당합니다.

AMS AMIs 사용할 수 있나요?

2020년 3월 이후에 판매된 AMS AMIs는 AWS Service Catalog를 통해 배포할 수 있습니다.

Service Catalog를 사용하여 AMS로 마이그레이션하려면 어떻게 해야 하나요?

Service Catalog를 사용하여 워크로드를 AMS로 마이그레이션하려면 먼저 워크로드 수집(WIGs) 프로세스에 따라 AMS에서 AMI를 생성합니다. WIGS에서 생성한 AMI를 사용하여 Service Catalog에서 제품을 생성합니다. 이 작업을 수행하는 방법은 AWS Service Catalog - 시작하기에 자세히 설명되어 있습니다.

AMS 다중 계정 랜딩 존(MALZ) 온보딩

MALZ 네트워크 아키텍처

다중 계정 랜딩 존 네트워크 아키텍처 정보

AWS Managed Services(AMS) 다중 계정 랜딩 존(MALZ)에 대한 온보딩 프로세스를 시작하기 전에 AMS가 사용자를 대신하여 생성하는 기본 아키텍처 또는 랜딩 존, 해당 구성 요소 및 함수를 이해하는 것이 중요합니다.

AMS 다중 계정 랜딩 존은 인증, 보안, 네트워킹 및 로깅을 용이하게 하기 위해 인프라로 사전 구성된 다중 계정 아키텍처입니다.

> **Note**
>
> 예상 비용은 AMS 다중 계정 랜딩 존 환경 기본 구성 요소를 참조하세요.

주제

- 서비스 리전
- 조직 단위
- 서비스 제어 정책 및 AWS Organization

다음 다이어그램은 계정 구조와 인프라가 각 계정으로 분리되는 방법을 개략적으로 설명합니다.

서비스 리전

AMS 다중 계정 랜딩 존 내의 모든 리소스는 Active Directory 및 Transit Gateway의 현재 교차 리전 제한으로 인해 선택한 단일 AWS 리전 내에 배포됩니다.

조직 단위

일반적인 AMS 다중 계정 랜딩 존은 4개의 최상위 조직 단위(OUs)로 구성됩니다.

- 핵심 조직 단위(OU)(계정을 그룹화하여 단일 단위로 관리하는 데 사용됨)
- 애플리케이션 OU

- 고객 관리형 OU
- 가속화된 OU

또한 AMS 관리형 다중 계정 랜딩 존을 사용하면 AWS 계정을 그룹화 및 구성하기 위한 사용자 지정 OUs를 생성하고 사용자 지정 SCPs를 해당 계정과 연결할 수 있습니다. 이에 대한 예제는 각각 관리 계정 | 사용자 지정 OUs 및 관리 계정 생성 | 사용자 지정 SCP 생성(관리형 자동화)을 참조하세요. AMS는 가속화, 애플리케이션 > 관리형, 애플리케이션 > 개발, 고객 관리형 등 새로운 OU와 계정을 요청할 수 OUs 있는 4가지 기존 OUs를 제공합니다.

- OU 가속화:

  AMS 다중 계정 랜딩 존(MALZ)의 최상위 OU입니다. 이 OU의 계정은 RFC(배포 | 관리형 랜딩 존 | 관리 계정 | Accelerate 계정 생성, 변경 유형 ID: ct-2p93tyd5angmi)를 사용하여 AMS에 의해 프로비저닝됩니다. 이러한 가속화된 애플리케이션 계정에서는 모니터링 및 알림, 인시던트 관리, 보안 관리, 백업 관리와 같은 가속화된 운영 서비스의 이점을 누릴 수 있습니다. 자세한 내용은 AMS Accelerate 계정을 참조하세요.

- 애플리케이션 > 관리형 OU:

  애플리케이션 OU의이 하위 조직 단위에서는 모든 운영 작업을 포함하여 AMS에서 계정을 완전히 관리합니다. 운영 작업에는 서비스 요청 관리, 인시던트 관리, 보안 관리, 연속성 관리, 패치 관리, 비용 최적화, 모니터링 및 이벤트 관리가 포함됩니다. 이러한 작업은 인프라 관리를 위해 수행됩니다. AWS 조직에서 중첩된 OUs의 최대 한도에 도달할 때까지 필요에 따라 여러 하위 OUs를 생성할 수 있습니다. 자세한 내용은 AWS Organizations 할당량을 참조하세요.

- 애플리케이션 > 개발 OU:

  AMS 관리형 랜딩 존에 있는 애플리케이션 OU의이 하위 OU에서 계정은 AMS 변경 관리 프로세스 외부에서 AWS 리소스를 프로비저닝하고 업데이트할 수 있는 승격된 권한을 제공하는 개발자 모드 계정입니다. 또한이 OU는 필요에 따라 새 하위 OU 생성을 지원합니다.

- 고객 관리형 OU:

  AMS 다중 계정 랜딩 존의 최상위 OU입니다. 이 OU의 계정은 RFC가 있는 AMS에 의해 프로비저닝됩니다. 이러한 계정에서 워크로드 및 AWS 리소스의 운영은 사용자의 책임입니다. 또한이 OU는 필요에 따라 새 하위 OU 생성을 지원합니다.

가장 좋은 방법은 이러한 OUs 및 사용자 지정 요청 하위 OUs의 계정을 기능 및 정책에 따라 그룹화하는 것입니다.

서비스 제어 정책 및 AWS Organization

AWS는 AWS Organization에서 권한 관리를 위한 서비스 제어 정책(SCPs)을 제공합니다. SCPs는 사용자가 OUs에서 수행할 수 있는 작업에 대한 추가 가드레일을 정의하는 데 사용됩니다. 기본적으로 AMS는 다양한 기본 OU 수준에서 보호를 제공하는 관리 계정에 배포된 SCPs 세트를 제공합니다. SCP 제한에 대해서는 CSDM에 문의하십시오.

사용자 지정 SCPs 생성하여 특정 OUs. 변경 유형 ct-33ste5yc7hprs를 사용하여 관리 계정에서 요청할 수 있습니다. 그런 다음 AMS는 요청된 사용자 지정 SCPs 대상 OUs에 적용하기 전에 검토합니다. 예제는 관리 계정 | 사용자 지정 OUs. https://docs.aws.amazon.com/managedservices/latest/ctref/deployment-managed-management-account-create-custom-scp-review-required.html

단일 MALZ 또는 여러 MALZs 선택

다음 표에서는 단일 다중 계정 랜딩 존(MALZ)과 여러 다중 계정 랜딩 존(예: 두 개의 다중 계정 랜딩 존 - Prod 및 비Prod)을 결정할 때 몇 가지 높은 수준의 고려 사항을 제공합니다. 일반적으로 선택은 개별 요구 사항, 법적 요구 사항 및 운영 관행에 따라 달라집니다.

단일 다중 계정 랜딩 존과 다중 계정 랜딩 존 비교

개체	단일 AMS 랜딩 존	여러(2개 이상) 랜딩 존
기본 비용	매월 약 3,000 USD로 최적화됩니다.	더 높으면 환경당 약 3,000 USD의 추가 비용이 발생합니다.
결제	단일 Billing/ Management 계정으로 인한 단일 청구서.	각 다중 계정 랜딩 존에 대해 청구서를 구분합니다. 현재 AWS Org는 단일 청구서가 있는 다중 관리 계정을 지원하지 않습니다.
기존 예약 인스턴스(RIs)의 이식성	낮음. AWS RIs는 현재 여러 결제 계정에서 전환할 수 없습니다. 다중 계정 랜딩 존에 대해 기존 RIs의 용도를 변경합니다.	더 낮습니다. 모든 다중 계정 랜딩 존에서 RIs 용도를 변경하고 배포합니다.
제품 계층화 할인	높음 볼륨 할인을 참조하세요.	낮음. 볼륨 할인을 참조하세요.

개체	단일 AMS 랜딩 존	여러(2개 이상) 랜딩 존
초기 설정 오버헤드(프로젝트/마이그레이션 타임라인)	낮음. Active Directory, 네트워킹 및 SSO(Single Sign-On) 통합은 한 번만 가능합니다.	높음 모든 랜딩 존에 대해 Active Directory, 네트워크 통합 및 SSO 통합을 수행합니다. 이로 인해 마이그레이션 프로젝트가 지연될 수 있습니다.
공통 서비스 구성 가능성	낮은 노력. DNS, 백업, 모니터링, 로깅 등과 같은 공통/공유 서비스를 구성합니다.	높은 노력. 공통 인프라 또는 서비스의 위치를 해결하려면 추가 계획이 필요합니다. 트래픽이 각 랜딩 존의 여러 전송 게이트웨이(TGWs)를 통과하면 추가 비용이 발생할 수 있습니다.
확장성	중간. AMS의 현재 실제 한도는 다중 계정 랜딩 존당 150개입니다. 동일한 계정에서 애플리케이션을 실행하는 여러 팀 또는 공급업체는 서로 다른 팀이 소유한 스택에 액세스할 수 있습니다. ServiceNow 계층에서 애플리케이션별 스택에 대한 액세스를 제어하여(AMS ServiceNow Connector 애플리케이션을 통합하고 태그를 사용하여) 이러한 제한을 완화할 수 있습니다. AMS 기술 제공 관리자(TDMs) 또는 클라우드 아키텍트(CAs)에게 이를 구현하는 방법을 문의하십시오.	높음 여러 다중 계정 랜딩 존을 활용하여 계정을 분산하는 동시에 계정 또는 애플리케이션 수준의 격리를 달성할 수 있습니다. 많은 수의 계정을 관리하면 운영 또는 비용 오버헤드가 발생할 수 있습니다.
운영 위험	(종속) 낮음. 운영 통합 및 준비는 한 번만 가능합니다. 프로세스 드리프트의 가능성이 줄어듭니다.	(종속) 낮음. 여러 통합 및 운영 활동. 일정 기간 동안 여러 랜딩 존의 드리프트는 운영 위험을 초래할 수 있습니다.
다중 AWS 리전	단일 AWS 리전. AMS 다중 계정 랜딩 존은 단일 AWS 리전으로 제한됩니다. 여러 AWS 리전을 확장하려면 여러 다중 계정 랜딩 존을 사용합니다.	다중 AWS 리전. 다중 계정 랜딩 존이 여러 개인 경우 각 MALZ를 한 리전에 배포하고 전송 게이트웨이(TGW) 피어링을 사용하여 상호 연결할 수 있습니다.

개체	단일 AMS 랜딩 존	여러(2개 이상) 랜딩 존
계정 마이그레이션 또는 이동성	예. 동일한 AWS 조직 내에서 한 OU에서 다른 OU로 계정을 이동할 수 있습니다.	아니요. AMS는 랜딩 존, 즉 AWS Organizations 간 계정 마이그레이션을 지원하지 않습니다. 워크로드는 전송 게이트웨이(TGW) 또는 VPC 피어링을 통해 랜딩 존에 도달할 수 있습니다.
변경 관리	중간. TGW, Active Directory(AD) 또는 아웃바운드(송신)와 같은 일반적인 구성 요소를 파괴적으로 변경하면 다중 계정 랜딩 존의 모든 워크로드에 영향을 미칠 수 있습니다. 그러나 AMS 관리형 구성 요소의 변경 사항은 내부적으로 테스트되며 롤링 업데이트에서 푸시됩니다.	낮음. TGW, AD 또는 아웃바운드(송신)와 같은 일반적인 구성 요소를 파괴적으로 변경하면 해당 특정 다중 계정 랜딩 존의 워크로드에만 영향을 미칠 수 있습니다.
데이터 및 액세스 제어	(종속) Prod 워크로드와 Non-Prod 워크로드를 위해 다양한 온프레미스 ADs 및 네트워크에 연결하려는 경우 제어가 낮습니다. SAML 페더레이션, TGW 도메인 및 보안 그룹(SGs)도 필요한 제어를 구현하는 데 도움이 될 수 있습니다.	(종속) Prod 워크로드와 Non-Prod 워크로드를 위해 다양한 온프레미스 ADs 및 네트워크에 연결하려는 경우 높은 제어가 가능합니다. 엄격한 규정 준수 요구 사항에 대해 별도의 랜딩 존을 사용합니다.
규정 준수 및 보안	(종속) 재료 워크로드와 비 재료 워크로드를 완전히 분리해야 하는 엄격한 규정 준수 요구 사항이 있는 경우 낮음. AMS 표준 예방 및 탐지 제어가 마련되어 있습니다.	(종속) 다중 계정 랜딩 존이 높으면 재료 워크로드와 비 재료 워크로드를 완전히 분리하여 엄격한 규정 준수 요구 사항을 달성하는 데 도움이 될 수 있습니다. AMS 표준 예방 및 탐지 제어가 마련되어 있습니다.

권장 사항: 엄격한 규정 준수 또는 다중 리전 요구가 없으면 단일 AMS 다중 계정 랜딩 존부터 시작하여 비용, 보안, 운영 우수성 및 마이그레이션 복잡성 간에 균형이 잘 맞습니다. 계정 또는 비즈니스 제약이 발생하는 경우 언제든지 추가 랜딩 존을 설정할 수 있습니다.

단일 다중 계정 랜딩 존과 다중 다중 계정 랜딩 존 FAQs

단일 다중 계정 랜딩 존 또는 다중 계정 랜딩 존을 설정하기로 선택할 때 자주 묻는 몇 가지 질문:

Q1: 계정 제한 또는 비즈니스 제약이 발생하는 경우 단일 다중 계정 랜딩 존으로 시작하여 다중 계정 랜딩 존으로 이동할 수 있습니까?

A: 예. 언제든지 다른 다중 계정 랜딩 존을 설정하도록 선택할 수 있습니다.

- 새 결제자 계정을 설정해야 합니다(현재 AWS는 단일 AWS 조직에서 다중 결제자 계정을 지원하지 않음).
- 다중 계정 랜딩 존 기본 빌드는 다중 계정 랜딩 존 설문지를 작성한 후 최대 2주가 걸립니다.
- 모든 다중 계정 랜딩 존은 월 최대 3,000 USD의 실행 비용이 추가됩니다.
- 새 MALZ에 대해를 설정하려면 N/W, AD, DNS 및 SSO 통합이 필요합니다.
- 모든 예약 인스턴스(RIs), 비용 절감형 플랜은 새 다중 계정 랜딩 존에 대해 설정해야 합니다(RIs는 이전할 수 없음).
- AMS 다중 계정 랜딩 존은 AWS 조직과 같은 다중 계정 랜딩 존 계정 간 계정 마이그레이션을 지원하지 않습니다. 그러나 표준 마이그레이션 방법을 사용하면 한 계정에서 다른 계정으로 애플리케이션을 이동할 수 있습니다.

Q2: 기본/공유 인프라에 대한 MALZ 업데이트/변경 및 고객에 대한 위험 정량화에 대한 AMS 접근 방식은 무엇입니까? 프로세스에 래핑되는 보증에 대한 세부 정보를 제공합니다. 고객은 MALZ 업데이트/변경이 고객에게 영향을 미치지 않을 것이라고 어떻게 확신하나요? 중단을 방지하기 위해 고객이 취해야 할 조치가 있나요?

A: AMS는 고객의 환경에 대한 변경 사항을 정의, 검토, 예약 및 실행할 수 있는 내부 도구를 사용하여 엄격한 변경 방법론을 따릅니다.

업데이트 릴리스 프로세스는 고객 환경에 릴리스하기 전에 코드 검토, 통합 테스트, 감마 및 베타 환경에서의 배포, 베타 및 감마 환경에서의 추가 베이킹 시간 및 테스트를 적용합니다. 모든 릴리스에는 롤백 절차가 포함되며 릴리스 팀과 변경을 생성하고 요청한 팀이 면밀히 모니터링합니다. 릴리스의 범위는 AMS가 소유하고 프로비저닝한 스택으로 제한됩니다. 평균적으로 매주 최소 1개의 릴리스를 실행합니다.

또한 다음과 같습니다.

- AMS SLA가 적용됩니다. AMS 서비스 설명에 따라 인시던트 발생 게시물 공유 인프라 유지 관리 활동은 해결 또는 크레딧을 위해 권한이 부여된 SLA를 준수합니다.

- 고객은 공통 인프라 중단을 방지하기 위해 특별한 예방 조치를 취할 필요가 없습니다. 고객은 AWS Org 또는 Core OU 계정에서 읽기 전용 권한을 보유하므로 MALZ 코어 환경을 파괴적으로 변경할 수 없습니다. 코어 인프라에 대한 모든 고객의 요청에는 AMS 검토 및 승인이 필요합니다.
- 고객은 앱 OU 수준에서 변경 사항을 전파하기 전에 개별 비프로드 계정 수준에서 SCPs/역할과 같은 특정 조직 수준 변경 사항을 테스트할 수 있습니다. AMS 로드맵에서는 여러 APP OUs(2020년 2분기)를 허용하므로 일부 ORG 수준 변경의 위험을 더욱 완화할 수 있습니다. MALZ 팀은 고객 소유권의 명확한 분리와 별도의 제어를 보장하기 위해 “빌드 모드” 계정에 대해 별도의 OU를 이미 릴리스했습니다.
- 이 중 대부분은 AMS가 효과적이고 효율적인 방식으로 워크로드를 운영할 수 있도록 허용하는 변경 사항이며 반드시 고객의 워크로드에 영향을 미치지는 않습니다. AMS가 공유된 인프라 변경이 고객의 워크로드에 영향을 미칠 수 있다고 생각하는 경우 고객의 변경 기간에 맞춰 조정됩니다.

다음과 같은 경우 여러 다중 계정 랜딩 존으로 시작하는 높은 수준의 권장 사항입니다.

- 특정 규정 준수를 달성하는 데 도움이 되는 경우.
- 다중 리전을 사용해야 하는 경우.
- 온프레미스 ADs 및 Network for Prod/Material과 Non-Prod/Non-Material 워크로드가 다른 경우 워크로드를 b/w로 명확하게 분리합니다.

다중 계정 랜딩 존 계정

주제

관리 계정

관리 계정은 AMS로 온보딩을 시작할 때 초기 AWS 계정입니다. AWS Organizations를 관리 계정(모든 멤버 계정의 요금을 지불하는 지급인 계정이라고도 함)으로 활용하므로 계정에서 멤버 계정을 생성

하고 재무적으로 관리할 수 있습니다. 여기에는 AWS 랜딩 존(ALZ) 프레임워크, 계정 구성 스택 세트, AWS 조직 서비스 제어 정책(SCPs) 등이 포함됩니다.

관리 계정 사용에 대한 자세한 내용은 관리 계정 모범 사례를 참조하세요.

다음 다이어그램은 관리 계정에 포함된 리소스에 대한 개략적인 개요를 제공합니다.

관리 계정의 리소스

위의 표준 서비스 외에는 온보딩 중에 관리 계정에 추가 AWS 리소스가 생성되지 않습니다. AMS에 온보딩하는 동안 다음 입력이 필요합니다.

- 관리 계정 ID: 사용자가 처음 생성한 AWS 계정 ID입니다.
- 코어 계정 이메일: 네트워킹, 공유 서비스, 로깅 및 보안 계정과 같은 각 코어 계정과 연결할 이메일을 제공합니다.
- 서비스 리전: AMS 랜딩 존의 모든 리소스가 배포될 AWS 리전을 제공합니다.

네트워킹 계정

네트워킹 계정은 AMS 다중 계정 랜딩 존 계정, 온프레미스 네트워크, 인터넷으로의 송신 트래픽 간의 네트워크 라우팅을 위한 중앙 허브 역할을 합니다. 또한이 계정에는 AMS 엔지니어가 AMS 환경의 호스트에 액세스할 수 있는 진입점인 퍼블릭 DMZ 접속이 포함되어 있습니다. 자세한 내용은 아래 네트워킹 계정의 다음 상위 수준 다이어그램을 참조하세요.

네트워킹 계정 아키텍처

다음 다이어그램은 계정 간 네트워크 트래픽 흐름을 보여주는 AMS 다중 계정 랜딩 존 환경을 보여주며 가용성이 높은 설정의 예입니다.

AMS는 표준 템플릿과 온보딩 중에 제공된 선택한 옵션을 기반으로 네트워킹의 모든 측면을 구성합니다. 표준 AWS 네트워크 설계가 AWS 계정에 적용되고 VPC가 자동으로 생성되어 VPN 또는 Direct Connect를 통해 AMS에 연결됩니다. Direct Connect에 대한 자세한 내용은 AWS Direct Connect를 참

조하세요. 표준 VPCs에는 DMZ, 공유 서비스 및 애플리케이션 서브넷이 포함됩니다. 온보딩 프로세스 중에 필요에 맞게 추가 VPCs를 요청하고 생성할 수 있습니다(예: 고객 부서, 파트너). 온보딩 후 네트워크 다이어그램, 즉 네트워크 설정 방법을 설명하는 환경 문서가 제공됩니다.

> **Note**
>
> 모든 활성 서비스의 기본 서비스 제한 및 제약 조건에 대한 자세한 내용은 AWS 서비스 제한 설명서를 참조하세요.

네트워크 설계는 Amazon "최소 권한 원칙"을 기반으로 구축되었습니다. 이를 위해 신뢰할 수 있는 네트워크에서 들어오는 트래픽을 제외한 모든 트래픽, 수신 및 송신을 DMZ를 통해 라우팅합니다. 유일하게 신뢰할 수 있는 네트워크는 VPN 및/또는 AWS Direct Connect(DX)를 사용하여 온프레미스 환경과 VPC 간에 구성된 네트워크입니다. 접속 인스턴스를 사용하여 액세스 권한이 부여되므로 프로덕션 리소스에 직접 액세스할 수 없습니다. 모든 애플리케이션과 리소스는 퍼블릭 로드 밸런서를 통해 연결할 수 있는 프라이빗 서브넷 내에 있습니다. 퍼블릭 송신 트래픽은 송신 VPC(네트워킹 계정)의 NAT 게이트웨이를 통해 인터넷 게이트웨이로 흐른 다음 인터넷으로 흐릅니다. 또는 트래픽이 VPN 또는 Direct Connect를 통해 온프레미스 환경으로 흐를 수 있습니다.

AMS 다중 계정 랜딩 존 환경에 대한 프라이빗 네트워크 연결

AWS는 가상 프라이빗 네트워크(VPN) 연결 또는 AWS Direct Connect를 통한 전용 라인을 통해 프라이빗 연결을 제공합니다. 다중 계정 환경의 프라이빗 연결은 다음에 설명된 방법 중 하나를 사용하여 설정됩니다.

- Transit Gateway를 사용한 중앙 집중식 엣지 연결
- Direct Connect(DX) 및/또는 VPN을 계정 Virtual Private Cloud(VPCs)에 연결

전송 게이트웨이를 사용한 중앙 집중식 엣지 연결

AWS Transit Gateway는 VPCs와 온프레미스 네트워크를 단일 게이트웨이에 연결할 수 있는 서비스입니다. 전송 게이트웨이(TGW)를 사용하여 기존 엣지 연결을 통합하고 단일 수신/송신 지점을 통해 라우팅할 수 있습니다. 전송 게이트웨이는 AMS 다중 계정 환경의 네트워킹 계정에 생성됩니다. 전송 게이트웨이에 대한 자세한 내용은 AWS Transit Gateway를 참조하세요.

AWS Direct Connect(DX) 게이트웨이는 전송 가상 인터페이스를 통해 전송 게이트웨이에 연결된 VPCs 또는 VPNs에 DX 연결을 연결하는 데 사용됩니다. Direct Connect 게이트웨이를 전송 게이트웨이와 연결합니다. 그런 다음 Direct Connect 게이트웨이에 대한 AWS Direct Connect 연결을 위한 전송

가상 인터페이스를 생성합니다. DX 가상 인터페이스에 대한 자세한 내용은 AWS Direct Connect 가상 인터페이스를 참조하세요.

이 구성을 사용하면 다음과 같은 이점이 있습니다. 다음을 수행할 수 있습니다.

- 동일한 AWS 리전에 있는 여러 VPCs 또는 VPNs에 대한 단일 연결을 관리합니다.
- 접두사를 온프레미스에서 AWS로, AWS에서 온프레미스로 알립니다.

> **Note**
>
> AWS 서비스에서 DX를 사용하는 방법에 대한 자세한 내용은 Resiliency Toolkit 섹션 Classic을 참조하세요. 자세한 내용은 Transit Gateway 연결을 참조하세요.

연결 복원력을 높이려면 서로 다른 AWS Direct Connect 위치의 전송 가상 인터페이스를 Direct Connect 게이트웨이에 두 개 이상 연결하는 것이 좋습니다. 자세한 내용은 AWS Direct Connect 복원력 권장 사항을 참조하세요.

계정 VPCs에 DX 또는 VPN 연결

이 옵션을 사용하면 AMS 다중 계정 랜딩 존 환경의 VPCs가 Direct Connect 또는 VPN에 직접 연결됩니다. 트래픽은 전송 게이트웨이를 통과하지 않고 VPCs에서 Direct Connect 또는 VPN으로 직접 흐릅니다.

네트워킹 계정의 리소스

네트워킹 계정 다이어그램에 표시된 대로 다음 구성 요소가 계정에 생성되며 입력이 필요합니다.

네트워킹 계정에는 송신 VPCs와 경계 VPC라고도 하는 DMZ VPC라는 두 개의 VPC가 포함되어 있습니다.

AWS Network Manager

AWS Network Manager는 AMS에 대한 추가 비용 없이 전송 게이트웨이(TGW) 네트워크를 시각화할 수 있는 서비스입니다. AWS 리소스와 온프레미스 네트워크 모두에서 중앙 집중식 네트워크 모니터링, 토폴로지 다이어그램과 지리적 맵에서 프라이빗 네트워크의 단일 글로벌 보기, 바이트 입/출력, 패킷 입/출력, 삭제된 패킷, 토폴로지, 라우팅 및 업/다운 연결 상태 변경 알림과 같은 사용률 지표를 제공합니다. 자세한 내용은 AWS Network Manager 단원을 참조하세요.

다음 역할 중 하나를 사용하여이 리소스에 액세스합니다.

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

송신 VPC

송신 VPC는 주로 인터넷으로의 송신 트래픽에 사용되며 최대 3개의 가용 영역(AZs)에 있는 퍼블릭/프라이빗 서브넷으로 구성됩니다. NAT(Network Address Translation) 게이트웨이는 퍼블릭 서브넷에 프로비저닝되고 TGW(Transit Gateway) VPC 연결은 프라이빗 서브넷에 생성됩니다. 모든 네트워크의 송신 또는 아웃바운드 인터넷 트래픽은 TGW를 통해 프라이빗 서브넷을 통해 들어오는 다음 VPC 라우팅 테이블을 통해 NAT로 라우팅됩니다.

퍼블릭 서브넷에 퍼블릭 애플리케이션을 포함하는 VPCs의 경우 인터넷에서 발생하는 트래픽은 해당 VPC 내에 포함됩니다. 반환 트래픽은 TGW 또는 송신 VPC로 라우팅되지 않고 VPC의 인터넷 게이트웨이(IGW)를 통해 다시 라우팅됩니다.

> **Note**
>
> 네트워킹 VPC CIDR 범위: VPC를 생성할 때 Classless Inter-Domain Routing(CIDR) 블록의 형태로 VPC에 대한 IPv4 주소 범위를 지정해야 합니다. 예: 10.0.16.0/24. 이것은 VPC의 기본 CIDR 블록입니다.
> AMS 다중 계정 랜딩 존 팀은 향후 다른 리소스/어플라이언스가 배포될 경우를 대비하여 일부 버퍼를 제공하기 위해 24(IP 주소 증가)의 범위를 권장합니다.

경계(DMZ) VPC

경계 또는 DMZ, VPC에는 AMS 운영 엔지니어가 AMS 네트워크에 액세스하는 데 필요한 리소스가 포함되어 있습니다. 여기에는 2~3AZs에 대한 퍼블릭 서브넷이 포함되어 있으며, AMS Operations 엔지니어가 로그인하거나 터널링할 수 있도록 Auto Scaling 그룹(ASG)에 SSH Bastions 호스트가 있습니다. DMZ 접속에 연결된 보안 그룹에는 Amazon Corp Networks의 포트 22 인바운드 규칙이 포함되어 있습니다.

DMZ VPC CIDR 범위:VPC를 생성할 때 Classless Inter-Domain Routing(CIDR) 블록의 형태로 VPC에 대한 IPv4 주소 범위를 지정해야 합니다. 예: 10.0.16.0/24. 이것은 VPC의 기본 CIDR 블록입니다.

> **Note**
>
> AMS 팀은 향후 방화벽과 같은 다른 리소스가 배포될 경우를 대비하여 버퍼를 제공하기 위해 24(IP 주소가 더 많음)의 범위를 권장합니다.

AWS Transit Gateway

AWS Transit Gateway(TGW)는 Amazon Virtual Private Cloud(VPCs)와 온프레미스 네트워크를 단일 게이트웨이에 연결할 수 있는 서비스입니다. 전송 게이트웨이는 AMS 계정 네트워크와 외부 네트워크 간의 라우팅을 처리하는 네트워킹 백본입니다. 전송 게이트웨이에 대한 자세한 내용은 AWS Transit Gateway를 참조하세요.

다음 입력을 제공하여이 리소스를 생성합니다.

- 전송 게이트웨이 ASN 번호*: 전송 게이트웨이의 프라이빗 ASN(자율 시스템 번호)을 제공합니다. 이 ASN은 BGP(Border Gateway Protocol) 세션의 AWS 측에 대한 ASN이어야 합니다. 16비트 ASN의 경우 범위는 64512~65534입니다.

공유 서비스 계정

공유 서비스 계정은 대부분의 AMS 데이터 영역 서비스의 중앙 허브 역할을 합니다. 계정에는 액세스 관리(AD), 엔드포인트 보안 관리(Trend Micro)에 필요한 인프라와 리소스가 포함되어 있으며, 여기에는 고객 접속(SSH/RDP)이 포함되어 있습니다. 공유 서비스 계정에 포함된 리소스에 대한 전반적인 개요는 다음 그림에 나와 있습니다.

공유 서비스 VPC는 세 개의 가용 영역(AZs)에 있는 AD 서브넷, EPS 서브넷 및 고객 접속 서브넷으로 구성됩니다. 공유 서비스 VPC에서 생성된 리소스는 아래에 나열되어 있으며 입력이 필요합니다.

- 공유 서비스 VPC CIDR 범위: VPC를 생성할 때 Classless Inter-Domain Routing(CIDR) 블록의 형태로 VPC에 대한 IPv4 주소 범위를 지정해야 합니다. 예: 10.0.1.0/24. VPC의 기본 CIDR 블록입니다.

> **Note**
>
> AMS 팀은 /23의 범위를 권장합니다.

- Active Directory 세부 정보: Microsoft Active Directory(AD)는 모든 AMS 다중 계정 랜딩 존 계정에서 사용자/리소스 관리, 인증/권한 부여 및 DNS에 사용됩니다. 또한 AMS AD는 신뢰 기반 인증을 위해 Active Directory에 대한 단방향 신뢰로 구성됩니다. AD를 생성하려면 다음 입력이 필요합니다.
  - Domain Fully Qualified Domain Name(FQDN): AWS Managed Microsoft AD 디렉터리의 정규화된 도메인 이름입니다. 도메인은 네트워크에 있는 기존 도메인 또는 기존 도메인의 하위 도메인이 아니어야 합니다.
  - 도메인 NetBIOS 이름: NetBIOS 이름을 지정하지 않으면 AMS는 이름을 디렉터리 DNS의 첫 번째 부분으로 기본 설정합니다. 예: 디렉터리 DNS corp.example.com corp.

- Trend Micro - 엔드포인트 보호 보안(EPS): Trend Micro 엔드포인트 보호(EPS)는 운영 체제 보안을 위한 AMS 내의 기본 구성 요소입니다. 시스템은 Deep Security Manager(DSM), EC2 인스턴스, 릴레이 EC2 인스턴스, 모든 데이터 영역 및 고객 EC2 인스턴스 내에 있는 에이전트로 구성됩니다.

  공유 서비스 계정`EPSMarketplaceSubscriptionRole`에서를 수임하고 Trend Micro Deep Security(BYOL) AMI 또는 Trend Micro Deep Security(Marketplace)를 구독해야 합니다.

  EPS를 생성하려면 다음 기본 입력이 필요합니다(기본값에서 변경하려는 경우).
  - 릴레이 인스턴스 유형: 기본값 - m5.large
  - SQL 인스턴스 유형: 기본값 - m5.xlarge
  - DB 인스턴스 크기: 기본값 - 200GB
  - RDS 인스턴스 유형: 기본값 - db.m5.large

- 고객 접속: AMS 환경의 다른 호스트에 액세스할 수 있도록 공유 서비스 계정에서 SSH 또는 RDP 접속(또는 둘 다)이 제공됩니다. 사용자로 AMS 네트워크(SSH/RDP)에 액세스하려면 "customer" Bastions를 진입점으로 사용해야 합니다. 네트워크 경로는 온프레미스 네트워크에서 시작되고 DX/VPN을 통해 전송 게이트웨이(TGW)로 이동한 다음 공유 서비스 VPC로 라우팅됩니다. 접속에 액세스할 수 있게 되면 액세스 요청이 부여된 경우 AMS 환경의 다른 호스트로 이동할 수 있습니다.
  - SSH 접속에는 다음 입력이 필요합니다.
    - SSH 접속 원하는 인스턴스 용량: 기본값 - 2.
    - SSH 접속 최대 인스턴스: 기본값 - 4.
    - SSH 접속 최소 인스턴스: 기본값 -2.
    - SSH 접속 인스턴스 유형: 기본값 - m5.large(비용 절감을 위해 변경할 수 있음. 예: t3.medium).
    - SSH 접속 수신 CIDRs: 네트워크의 사용자가 SSH 접속에 액세스하는 IP 주소 범위입니다.
  - Windows RDP 접속에는 다음 입력이 필요합니다.

- RDP 접속 인스턴스 유형: 기본값 - t3.medium.
- RDP 접속 원하는 최소 세션: 기본값 - 2.
- RDP 최대 세션: 기본값 -10.
- RDP 접속 구성 유형: 아래 구성 중 하나를 선택할 수 있습니다.
  - SecureStandard = 사용자가 하나의 Bastion을 수신하고 한 명의 사용자만 Bastion에 연결할 수 있습니다.
  - SecureHA = 사용자가 서로 다른 두 AZ에서 두 개의 Bastion을 수신하여에 연결하고 한 명의 사용자만 Bastion에 연결할 수 있습니다.
  - SharedStandard = 한 사용자는 하나의 접속을 수신하여에 연결하고 두 사용자는 한 번에 동일한 접속에 연결할 수 있습니다.
  - SharedHA = 한 사용자가 서로 다른 두 AZ에서 두 개의 접속을 수신하여 연결할 수 있고 두 사용자가 한 번에 동일한 접속에 연결할 수 있습니다.
- 고객 RDP 수신 CIDRs: 네트워크의 사용자가 RDP Bastions에 액세스할 IP 주소 범위입니다.

공유 서비스 업데이트: 다중 계정 랜딩 존

AMS는 데이터 영역 릴리스를 사전 통지 없이 매월 관리형 계정에 적용합니다.

AMS는 코어 OU를 사용하여 다중 계정 랜딩 존의 액세스, 네트워킹, EPS, 로그 스토리지, 알림 집계와 같은 공유 서비스를 제공합니다. AMS는 이러한 공유 서비스의 취약성, 패치 및 배포를 해결할 책임이 있습니다. AMS는 사용자가 최신 기능 및 보안 업데이트에 액세스할 수 있도록 이러한 공유 서비스를 제공하는 데 사용되는 리소스를 정기적으로 업데이트합니다. 업데이트는 일반적으로 매월 이루어집니다. 이러한 업데이트의 일부인 리소스는 다음과 같습니다.

- 코어 OU의 일부인 계정입니다.

  관리 계정, 공유 서비스 계정, 네트워크 계정, 보안 계정 및 로그 아카이브 계정에는 일반적으로 매월 업데이트되는 RDP 및 SSH 접속, 프록시, 관리 호스트 및 엔드포인트 보안(EPS)에 대한 리소스가 있습니다. AMS는 변경 불가능한 EC2 배포를 공유 서비스 인프라의 일부로 사용합니다.
- 최신 업데이트를 통합하는 새로운 AMS AMIs.

> **Note**
>
> AMS 연산자는 데이터 영역 변경을 실행할 때 내부 경보 억제 변경 유형(CT)을 활용하며 해당 CT의 RFC는 RFC 목록에 표시됩니다. 이는 데이터 영역 릴리스가 배포될 때 다양한 인프라가

종료, 재부팅, 오프라인으로 전환되거나 데이터 영역 배포 중에 불필요한 경보를 트리거하는 배포의 CPU 급증 또는 기타 영향이 있을 수 있기 때문입니다. 배포가 완료되면 모든 인프라가 제대로 실행되고 있는지 확인하고 경보를 다시 활성화합니다.

로그 아카이브 계정

로그 아카이브 계정은 AMS 다중 계정 랜딩 존 환경에서 로그를 보관하기 위한 중앙 허브 역할을 합니다. 계정에는 각 AMS 다중 계정 랜딩 존 환경 계정의 AWS CloudTrail 및 AWS Config 로그 파일 사본이 포함된 S3 버킷이 있습니다. 이 계정을 AWS Firehose 또는 Splunk 등과 함께 중앙 집중식 로깅 솔루션에 사용할 수 있습니다. 이 계정에 대한 AMS 액세스는 몇 명의 사용자로 제한되며, 계정 활동과 관련된 규정 준수 및 포렌식 조사를 위해 감사자 및 보안 팀으로 제한됩니다.

보안 계정

보안 계정은 보안 관련 작업을 수용하기 위한 중앙 허브이자 AMS 컨트롤 플레인 서비스에 알림 및 알림을 퍼널링하기 위한 주요 지점입니다. 또한 보안 계정에는 Amazon Guard Duty 관리 계정과 AWS Config 애그리게이터가 있습니다.

애플리케이션 계정 유형

애플리케이션 계정은 워크로드를 호스팅하는 데 사용하는 AMS 관리형 랜딩 존 아키텍처 내의 AWS 계정입니다. AMS는 세 가지 유형의 애플리케이션 계정을 제공합니다.

- AMS 관리형 애플리케이션 계정
- AMS Accelerate 계정
- 고객 관리형 애플리케이션 계정

애플리케이션 계정은 애플리케이션 계정 유형에 따라 AWS Organizations의 다양한 OUs로 그룹화됩니다.

- 루트 OU:
  1. 애플리케이션 OU
     - 관리형 OU: AMS 관리형 계정
     - 개발 OU: 개발자 모드가 활성화된 AMS 관리형 계정

2. OU 가속화: AMS Accelerate 애플리케이션 계정
3. 고객 관리형 OU: 고객 관리형 애플리케이션 계정

애플리케이션 계정은 관리 계정에서 제출된 RFC를 통해 프로비저닝됩니다.

- VPC ct-1zdasmc2ewzrs를 사용하여 애플리케이션 계정 생성
- Accelerate 계정 생성 ct-2p93tyd5angmi
- 고객 관리형 애플리케이션 계정 생성 ct-3pwbixz27n3tn

AMS 관리형 애플리케이션 계정

AMS에서 완전히 관리하는 애플리케이션 계정을 AMS 관리형 애플리케이션 계정이라고 하며, 서비스 요청 관리, 인시던트 관리, 보안 관리, 연속성 관리(백업), 패치 관리, 비용 최적화 또는 인프라 모니터링 및 이벤트 관리와 같은 일부 또는 모든 운영 작업이 AMS에서 수행됩니다.

AMS에서 수행하는 작업의 양은 선택한 변경 관리 모드에 따라 달라집니다. AMS 관리형 계정은 다양한 변경 관리 모드를 지원합니다.

- RFC 모드
- AMS의 직접 변경 모드
- AMS 및 AWS Service Catalog
- AMS 고급 개발자 모드
- AMS의 셀프 서비스 프로비저닝 모드

변경 관리 및 다양한 모드에 대한 자세한 내용은 섹션을 참조하세요변경 관리 모드.

AMS 관리 없이 AMS 관리형 계정에서 사용할 수 있는 몇 가지 AWS 서비스가 있습니다. 이러한 AWS 서비스의 목록과 이를 AMS 계정에 추가하는 방법은 셀프 서비스 프로비저닝 섹션에 설명되어 있습니다.

AMS Accelerate 계정

AMS Accelerate는 워크로드를 지원하는 AWS 인프라를 운영할 수 있는 AMS 운영 계획입니다. 새로운 마이그레이션, 가동 중지 시간 경험 또는 AWS 사용 방법 변경 없이 모니터링 및 알림, 인시던트 관리, 보안 관리, 백업 관리와 같은 AMS Accelerate 운영 서비스의 이점을 누릴 수 있습니다. 또한 AMS Accelerate는 정기적인 패치가 필요한 EC2 기반 워크로드에 대한 선택적 패치 추가 기능을 제공합니다.

AMS Accelerate를 사용하면 모든 AWS 서비스를 기본적으로 또는 원하는 도구를 사용하여 사용, 구성 및 배포할 수 있습니다. 선호하는 액세스 및 변경 메커니즘을 사용하는 반면 AMS는 팀을 확장하고, 비용을 최적화하고, 보안 및 효율성을 높이고, 복원력을 개선하는 데 도움이 되는 검증된 사례를 일관되게 적용합니다.

> **Note**
>
> AMS Advanced의 AMS Accelerate 계정에는 AMS 변경 관리(RFCs) 또는 AMS Advanced 콘솔이 없습니다. 대신 AMS Accelerate 콘솔과 기능이 있습니다.

Accelerate 계정은 AMS 다중 계정 랜딩 존 관리 계정에서만 프로비저닝할 수 있습니다. Accelerate는 다양한 운영 기능을 제공합니다. 자세한 내용은 Accelerate 서비스 설명을 참조하세요.

- 중앙 집중식 로깅, 단일 결제, 보안 계정의 Config 집계자 및 SCPs.
- AMS Accelerate는 EPS, 액세스 관리, 변경 관리 및 프로비저닝과 같은 일부 AMS 고급 서비스를 제공하지 않습니다. 다음 단계에 따라 액세스 권한을 얻고 전송 게이트웨이(TGW)를 구성하는 것이 좋습니다.

Accelerate에 대한 자세한 내용은 Accelerate란 무엇입니까?를 참조하십시오.

Accelerate 계정 생성

Accelerate 계정을 생성하려면 Accelerate 계정 생성에 설명된 단계를 따르세요.

Accelerate 계정에 액세스

다중 계정 랜딩 존(MALZ) 계정에서 Accelerate 계정을 프로비저닝한 후 관리 액세스 권한이 있는 역할은 사용자가 수임할 계정에 `AccelerateDefaultAdminRole`있습니다.

새 Accelerate 계정에 액세스하려면:

1. `CustomerDefaultAssumeRole` 역할을 사용하여 관리 계정의 IAM 콘솔에 로그인합니다.
2. IAM 콘솔의 탐색 모음에서 사용자 이름을 선택합니다.
3. 역할 전환을 선택합니다. 이 옵션을 처음 선택하면 자세한 정보를 제공하는 페이지가 나타납니다. 그 정보를 읽은 후에 역할 전환(Switch Role)을 클릭합니다. 브라우저 쿠키를 청소하면 이 페이지가 다시 나타나게 할 수 있습니다.
4. 역할 전환 페이지에서 Accelerate 계정 ID와 수임할 역할의 이름을 입력합니다`AccelerateDefaultAdminRole`.

이제 액세스 권한이 있으므로 새 IAM 역할을 생성하여 환경에 계속 액세스할 수 있습니다. Accelerate 계정에 SAML 페더레이션을 활용하려면 SAML 2.0 페더레이션 사용자가 AWS Management Console에 액세스하도록 활성화를 참조하세요.

Transit Gateway에 Accelerate 계정 연결

AMS는 Accelerate 계정의 네트워크 설정을 관리하지 않습니다. AWS APIs를 사용하여 자체 네트워크를 관리하거나(네트워크 솔루션 참조) AMS MALZ에 배포된 기존 Transit Gateway(TGW)를 사용하여 AMS에서 관리하는 MALZ 네트워크에 연결할 수 있습니다.

> **Note**
>
> Accelerate 계정이 동일한 AWS 리전에 있는 경우에만 VPC를 TGW에 연결할 수 있습니다. 자세한 내용은 전송 게이트웨이를 참조하세요.

Accelerate 계정을 Transit Gateway에 추가하려면 배포 | 관리형 랜딩 존 | 네트워킹 계정 | 정적 경로 추가(ct-3r2ckznmt0a59) 변경 유형을 사용하여 새 경로를 요청하고 다음 정보를 포함합니다.

- 블랙홀: 경로의 대상을 사용할 수 없음을 나타내는 True입니다. Transit Gateway에서 정적 경로의 트래픽을 삭제할 때이 작업을 수행합니다. 지정된 TGW 연결 ID로 트래픽을 라우팅하려면 False입니다. 기본값은 false입니다.
- DestinationCidrBlock: 대상 일치에 사용되는 IPV4 CIDR 범위입니다. 라우팅 결정은 가장 구체적인 일치 항목을 기준으로 이루어집니다. 예: 10.0.2.0/24.
- TransitGatewayAttachmentId: 라우팅 테이블 대상으로 사용할 TGW 연결 ID입니다. 블랙홀이 false인 경우이 파라미터가 필요하며, 그렇지 않으면이 파라미터를 비워 둡니다. 예: tgw-attach-04eb40d1e14ec7272.
- TransitGatewayRouteTableId: TGW 라우팅 테이블의 ID입니다. 예: tgw-rtb-06ddc751c0c0c881c.

TGW 라우팅 테이블에서 경로를 생성하여이 VPC에 연결합니다.

1. 기본적으로이 VPC는 MALZ 네트워크의 다른 VPCs와 통신할 수 없습니다.
2. 솔루션 아키텍트와 함께이 Accelerate VPCs가 통신할 VPC를 결정합니다.
3. 배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 정적 경로(ct-3r2ckznmt0a59) 변경 유형을 추가하고 다음 정보를 포함합니다.

- 블랙홀: 경로의 대상을 사용할 수 없음을 나타내는 True입니다. Transit Gateway에서 정적 경로의 트래픽을 삭제할 때이 작업을 수행합니다. 지정된 TGW 연결 ID로 트래픽을 라우팅하려면 False입니다. 기본값은 false입니다.
- DestinationCidrBlock: 대상 일치에 사용되는 IPV4 CIDR 범위입니다. 라우팅 결정은 가장 구체적인 일치 항목을 기준으로 이루어집니다. 예: 10.0.2.0/24.
- TransitGatewayAttachmentId: 라우팅 테이블 대상으로 사용할 TGW 연결 ID입니다. 블랙홀이 false인 경우이 파라미터가 필요하며, 그렇지 않으면이 파라미터를 비워 둡니다. 예: tgw-attach-04eb40d1e14ec7272.
- TransitGatewayRouteTableId: TGW 라우팅 테이블의 ID입니다. 예: tgw-rtb-06ddc751c0c0c881c.

새 Accelerate 계정 VPC를 AMS 다중 계정 랜딩 존 네트워크에 연결(TGW VPC 연결 생성):

1. 다중 계정 랜딩 존 네트워킹 계정에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway를 선택합니다. 표시되는 전송 게이트웨이의 TGW ID를 기록합니다.
3. Accelerate 계정에서 Amazon VPC 콘솔을 엽니다.
4. 탐색 창에서 전송 게이트웨이 연결 > 전송 게이트웨이 연결 생성을 선택합니다. 다음과 같이 선택합니다.
   - 전송 게이트웨이 ID에서 2단계에서 기록한 전송 게이트웨이 ID를 선택합니다.
   - 연결 유형(Attachment type)에서 VPC를 선택합니다.
   - 선택적으로 VPC Attachment(VPC 연결)에서 Attachment name tag(연결 이름 태그)에 대한 이름을 입력합니다.
   - DNS 지원 및 IPv6 지원을 활성화할지 선택합니다.
   - VPC ID에서 Transit Gateway에 연결할 VPC를 선택합니다. 이 VPC에는 적어도 하나의 서브넷이 연결되어 있어야 합니다.
   - 서브넷 ID에서 트래픽을 라우팅하기 위해 Transit Gateway에서 사용할 각 가용 영역에 대해 하나의 서브넷을 선택합니다. 하나 이상의 서브넷을 선택해야 합니다. 가용 영역당 서브넷 한 개만 선택할 수 있습니다.
5. 연결 생성(Create attachment)을 선택합니다. 새로 생성된 TGW 연결의 ID를 기록합니다.

TGW 연결을 라우팅 테이블에 연결:

1. VPC를 연결할 TGW 라우팅 테이블을 결정합니다. 배포 | 관리형 랜딩 존 | 네트워킹 계정 | 전송 게이트웨이 라우팅 테이블 생성(ct-3dscwaeyi6cup) 변경 유형을 사용하여 계정 VPCs 가속화를 위한 새 애플리케이션 라우팅 테이블을 생성하는 것이 좋습니다.

2. 관리 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정의 TGW 연결(ct-3nmhh0qr338q6) RFC를 연결하여 VPC 또는 TGW 연결을 선택한 라우팅 테이블에 연결합니다.

TGW 라우팅 테이블에서 경로를 생성하여이 VPC에 연결합니다.

1. 기본적으로이 VPC는 다중 계정 랜딩 존 네트워크의 다른 VPCs와 통신할 수 없습니다.
2. 솔루션 아키텍트와 함께이 Accelerate 계정 VPCs와 통신할 VPC를 결정합니다.
3. 배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정에 정적 경로(ct-3r2ckznmt0a59) RFC를 추가하여 필요한 TGW 경로를 생성합니다.

AMS 다중 계정 랜딩 존 전송 게이트웨이를 가리키도록 VPC 라우팅 테이블 구성:

1. 솔루션 아키텍트와 함께 AMS 다중 계정 랜딩 존 전송 게이트웨이로 전송할 트래픽을 결정합니다.
2. 배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정에 정적 경로(ct-3r2ckznmt0a59) RFC를 추가하여 필요한 TGW 경로를 생성합니다.

고객 관리형 애플리케이션 계정

AMS가 표준 방식으로 관리하지 않는 계정을 생성할 수 있습니다. 이러한 계정을 고객 관리형 계정이라고 하며 AMS에서 관리하는 중앙 집중식 아키텍처의 이점을 활용하면서 계정 내의 인프라를 자체 운영할 수 있는 완전한 제어 기능을 제공합니다.

고객 관리형 계정은 AMS 콘솔 또는 제공하는 서비스(패치, 백업 등)에 액세스할 수 없습니다.

고객 관리형 계정은 AMS 다중 계정 랜딩 존 관리 계정에서만 프로비저닝할 수 있습니다.

다양한 AMS 모드는 애플리케이션 계정에서 다르게 작동합니다. 모드에 대한 자세한 내용은 AWS Managed Services 모드를 참조하세요.

고객 관리형 애플리케이션 계정을 생성하려면 관리 계정 | 고객 관리형 애플리케이션 계정 생성을 참조하세요.

고객 관리형 애플리케이션 계정을 삭제하려면 관리 계정 | 오프보드 애플리케이션 계정을 사용합니다. (오프보딩 확인 CT는 고객 관리형 애플리케이션 계정에 적용되지 않습니다.)

고객 관리형 계정에 액세스

다중 계정 랜딩 존에서 고객 관리형 계정(CMA)을 프로비저닝한 후 (MALZ) 관리자 역할인 `CustomerDefaultAdminRole`는 SAML 페더레이션을 통해 계정을 구성하기 위해 수임할 계정에 있습니다.

CMA에 액세스하려면:

1. CustomerDefaultAssumeRole 역할을 사용하여 관리 계정의 IAM 콘솔에 로그인합니다.
2. IAM 콘솔의 탐색 모음에서 사용자 이름을 선택합니다.
3. 역할 전환을 선택합니다. 이 옵션을 처음 선택하면 자세한 정보를 제공하는 페이지가 나타납니다. 그 정보를 읽은 후에 역할 전환(Switch Role)을 클릭합니다. 브라우저 쿠키를 청소하면 이 페이지가 다시 나타나게 할 수 있습니다.
4. 역할 전환 페이지에서 고객 관리형 계정 ID와 수임할 역할 이름인 CustomerDefaultAdminRole을 입력합니다.

이제 액세스 권한이 있으므로 새 IAM 역할을 생성하여 환경에 계속 액세스할 수 있습니다. CMA 계정에 SAML 페더레이션을 활용하려면 SAML 2.0 페더레이션 사용자가 AWS 관리 콘솔에 액세스하도록 활성화를 참조하세요.

Transit Gateway에 CMA 연결

AMS는 고객 관리형 계정(CMAs)의 네트워크 설정을 관리하지 않습니다. AWS APIs 사용하여 자체 네트워크를 관리하거나(네트워크 솔루션 참조) AMS MALZ에 배포된 기존 Transit Gateway(TGW)를 사용하여 AMS에서 관리하는 다중 계정 랜딩 존 네트워크에 연결할 수 있습니다.

> **Note**
>
> CMA가 동일한 AWS 리전에 있는 경우에만 VPC를 TGW에 연결할 수 있습니다. 자세한 내용은 전송 게이트웨이를 참조하세요.

Transit Gateway에 CMA를 추가하려면 네트워킹 계정 | 정적 경로 추가(ct-3r2ckznmt0a59) 변경 유형을 사용하여 새 경로를 요청하고 다음 정보를 포함합니다.

- 블랙홀: 경로의 대상을 사용할 수 없음을 나타내는 True입니다. Transit Gateway에서 정적 경로의 트래픽을 삭제할 때이 작업을 수행합니다. 트래픽을 지정된 TGW 연결 ID로 라우팅하려면 False입니다. 기본값은 false입니다.

- DestinationCidrBlock: 대상 일치에 사용되는 IPV4 CIDR 범위입니다. 라우팅 결정은 가장 구체적인 일치 항목을 기준으로 이루어집니다. 예시: `10.0.2.0/24`.
- TransitGatewayAttachmentId: 라우팅 테이블 대상으로 사용할 TGW 연결 ID입니다. 블랙홀이 false이면이 파라미터가 필요하고, 그렇지 않으면이 파라미터를 비워 둡니다. 예시: `tgw-attach-04eb40d1e14ec7272`.
- TransitGatewayRouteTableId: TGW 라우팅 테이블의 ID입니다. 예시: `tgw-rtb-06ddc751c0c0c881c`.

AMS 다중 계정 랜딩 존 네트워크에 새 고객 관리형 VPC 연결(TGW VPC 연결 생성):

1. 다중 계정 랜딩 존 네트워킹 계정에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 전송 게이트웨이를 선택합니다. 표시되는 전송 게이트웨이의 TGW ID를 기록합니다.
3. 고객 관리형 계정에서 Amazon VPC 콘솔을 엽니다.
4. 탐색 창에서 전송 게이트웨이 연결 > 전송 게이트웨이 연결 생성을 선택합니다. 다음과 같이 선택합니다.
    a. 전송 게이트웨이 ID에서 2단계에서 기록한 전송 게이트웨이 ID를 선택합니다.
    b. 연결 유형(Attachment type)에서 VPC를 선택합니다.
    c. 선택적으로 VPC Attachment(VPC 연결)에서 Attachment name tag(연결 이름 태그)에 대한 이름을 입력합니다.
    d. DNS 지원 및 IPv6 지원을 활성화할지 선택합니다.
    e. VPC ID에서 Transit Gateway에 연결할 VPC를 선택합니다. 이 VPC에는 적어도 하나의 서브넷이 연결되어 있어야 합니다.
    f. 서브넷 ID에서 트래픽을 라우팅하기 위해 Transit Gateway에서 사용할 각 가용 영역에 대해 하나의 서브넷을 선택합니다. 하나 이상의 서브넷을 선택해야 합니다. 가용 영역당 서브넷 한 개만 선택할 수 있습니다.
5. 연결 생성(Create attachment)을 선택합니다. 새로 생성된 TGW 연결의 ID를 기록합니다.

TGW 연결을 라우팅 테이블에 연결:

VPC를 연결할 TGW 라우팅 테이블을 결정합니다. 배포 | 관리형 랜딩 존 | 네트워킹 계정 | 전송 게이트웨이 라우팅 테이블 생성(ct-3dscwaeyi6cup) RFC를 제출하여 고객 관리형 VPCs에 대한 새 애플리케이션 라우팅 테이블을 생성하는 것이 좋습니다. VPC 또는 TGW 연결을 선택한 라우팅 테이블에 연

결하려면 네트워킹 계정에서 배포 | 관리형 랜딩 존 | 네트워킹 계정 | TGW 연결(ct-3nmhh0qr338q6) RFC를 제출합니다.

TGW 라우팅 테이블에서 경로를 생성하여이 VPC에 연결합니다.

1. 기본적으로이 VPC는 다중 계정 랜딩 존 네트워크의 다른 VPCs와 통신할 수 없습니다.
2. 솔루션 아키텍트와 함께이 고객 관리형 VPCs와 통신할 VPC를 결정합니다. 배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정에 정적 경로(ct-3r2ckznmt0a59) RFC를 추가하여 필요한 TGW 경로를 생성합니다.

> **Note**
>
> 이 CT(ct-3r2ckznmt0a59)는 코어 라우팅 테이블 EgressRouteDomain에 정적 경로를 추가하는 것을 허용하지 않습니다. CMA가 송신 트래픽을 허용해야 하는 경우 ct-0xdawir96cy7k를 사용하여 관리 | 기타 | 기타(MOO) RFC를 제출합니다.

AMS 다중 계정 랜딩 존 전송 게이트웨이를 가리키도록 VPC 라우팅 테이블 구성:

솔루션 아키텍트와 함께 AMS 다중 계정 랜딩 존 전송 게이트웨이로 전송할 트래픽을 결정합니다. 이전에 생성된 TGW 연결로 트래픽을 전송하도록 VPC 라우팅 테이블 업데이트

고객 관리형 계정에 대한 운영 지원 받기

AMS는 계정을 AMS Accelerate에 온보딩하여 고객 관리형 계정에 배포한 워크로드를 운영하는 데 도움이 될 수 있습니다. AMS Accelerate를 사용하면 새 마이그레이션을 거치거나 가동 중지 시간을 경험하거나 사용 방법을 변경하지 않고도 모니터링 및 알림, 인시던트 관리, 보안 관리, 백업 관리와 같은 운영 서비스의 이점을 누릴 수 있습니다 AWS. 또한 AMS Accelerate는 정기적인 패치가 필요한 EC2-based 워크로드에 대한 선택적 패치 추가 기능을 제공합니다. AMS Accelerate를 사용하면 AMS Advanced Customer Managed 계정과 마찬가지로 모든 AWS 서비스를 기본적으로 또는 원하는 도구를 사용하여 계속 사용, 구성 및 배포할 수 있습니다. 선호하는 액세스 및 변경 메커니즘을 사용하는 반면 AMS는 팀을 확장하고, 비용을 최적화하고, 보안 및 효율성을 높이고, 복원력을 개선하는 데 도움이 되는 검증된 사례를 적용합니다. 자세한 내용은 Accelerate 서비스 설명을 참조하세요.

고객 관리형 계정을 Accelerate에 온보딩하려면 CSDM에 문의하고 AMS Accelerate 시작하기의 단계를 따릅니다.

> **Note**
>
> AMS Advanced의 AMS Accelerate 계정에는 AMS 변경 관리(변경 요청 또는 RFCs) 또는 AMS Advanced 콘솔이 없습니다. 대신 AMS Accelerate 콘솔과 기능이 있습니다.

AMS 도구 계정(워크로드 마이그레이션)

다중 계정 랜딩 존 도구 계정(VPC 포함)은 마이그레이션 작업을 가속화하고, 보안 위치를 높이고, 비용과 복잡성을 줄이고, 사용 패턴을 표준화하는 데 도움이 됩니다.

도구 계정은 다음을 제공합니다.

- 프로덕션 워크로드 외부의 시스템 통합자를 위한 복제 인스턴스에 액세스하기 위한 잘 정의된 경계입니다.
- 격리된 체임버를 생성하여 다른 워크로드가 있는 계정에 배치하기 전에 워크로드에 맬웨어 또는 알 수 없는 네트워크 경로가 있는지 확인할 수 있습니다.
- 정의된 계정 설정으로서 워크로드 마이그레이션을 위해 온보딩하고 설정하는 데 더 빠른 시간을 제공합니다.
- 격리된 네트워크는 온프레미스 -> CloudEndure -> 도구 계정 -> AMS 수집 이미지에서 트래픽을 보호하기 위해 라우팅됩니다. 이미지가 수집되면 AMS 관리 | 고급 스택 구성 요소 | AMI | 공유 (ct-1eiczxw8ihc18) RFC를 통해 대상 계정과 이미지를 공유할 수 있습니다.

상위 수준 아키텍처 다이어그램:

배포 | 관리형 랜딩 존 | 관리 계정 | 도구 계정 생성(VPC 사용) 변경 유형(ct-2j7q1hgf26x5c)을 사용하여 다중 계정 랜딩 존 환경 내에서 도구 계정을 빠르게 배포하고 워크로드 수집 프로세스를 인스턴스화합니다. 관리 계정, 도구 계정: 생성(VPC 사용)을 참조하세요.

> **Note**
>
> 마이그레이션 허브이므로 가용 영역(AZs)이 두 개 있는 것이 좋습니다.
> 기본적으로 AMS는 모든 계정에 다음과 같은 두 개의 보안 그룹(SGs)을 생성합니다. 이 두 SGs 있는지 확인합니다. 없는 경우 AMS 팀과 함께 새 서비스 요청을 열어 요청하세요.
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

온프레미스로 돌아가는 경로가 있는 프라이빗 서브넷에 CloudEndure 복제 인스턴스가 생성되었는지 확인합니다. 프라이빗 서브넷의 라우팅 테이블에 TGW로 돌아가는 기본 라우팅이 있는지 확인하여 확인할 수 있습니다. 그러나 CloudEndure 시스템 전환을 수행하면 온프레미스로 돌아가는 경로가 없는 "격리된" 프라이빗 서브넷으로 이동해야 하며 인터넷 아웃바운드 트래픽만 허용됩니다. 온프레미스 리소스에 대한 잠재적 문제를 방지하려면 격리된 서브넷에서 전환이 발생하도록 하는 것이 중요합니다.

사전 조건:

1. Plus 또는 Premium 지원 수준.
2. AMIs IDs입니다.
3. 앞서 설명한 대로 생성된 도구 계정입니다.

AWS Application Migration Service(AWS MGN)

AWS MGN(AWS Application Migration Service)은 도구 계정 프로비저닝 중에 자동으로 생성되는 `AWSManagedServicesMigrationRole` IAM 역할을 통해 MALZ 도구 계정에서 사용할 수 있습니다. AWS MGN을 사용하여 지원되는 버전의 Windows 및 Linux 운영 체제에서 실행되는 애플리케이션과 데이터베이스를 마이그레이션할 수 있습니다.

AWS 리전 지원에 대한 up-to-date 정보는 AWS 리전 서비스 목록을 참조하세요.

선호하는 AWS 리전 가 현재 AWS MGN에서 지원되지 않거나 애플리케이션이 실행되는 운영 체제가 현재 AWS MGN에서 지원되지 않는 경우 도구 계정에서 CloudEndure 마이그레이션을 대신 사용하는 것이 좋습니다.

AWS MGN 초기화 요청

AWS MGN은 처음 사용하기 전에 AMS로 초기화해야 합니다. 새 도구 계정에 대해 이를 요청하려면 도구 계정에서 다음 세부 정보와 함께 관리 | 기타 | 기타 RFC를 제출합니다.

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using
 all default values
    to 'Create template' and complete the initialization process.
```

AMS가 RFC를 성공적으로 완료하고 도구 계정에서 AWS MGN을 초기화하면 `AWSManagedServicesMigrationRole`를 사용하여 요구 사항에 맞는 기본 템플릿을 편집할 수 있습니다.

새 AMS 도구 계정에 대한 액세스 활성화

도구 계정이 생성되면 AMS는 계정 ID를 제공합니다. 다음 단계는 새 계정에 대한 액세스를 구성하는 것입니다. 단계는 다음과 같습니다.

1. 적절한 Active Directory 그룹을 적절한 계정 IDs.

   새 AMS 생성 계정은 사용자가 RFC를 제출할 수 있도록 허용하는 역할뿐만 아니라 ReadOnly 역할 정책으로 프로비저닝됩니다. RFCs

   도구 계정에는 추가 IAM 역할 및 사용 가능한 사용자도 있습니다.

   - IAM 역할: `AWSManagedServicesMigrationRole`
   - IAM 사용자: `customer_cloud_endure_user`

2. 서비스 통합 팀원이 다음 수준의 도구를 설정할 수 있도록 정책 및 역할을 요청합니다.

   AMS 콘솔로 이동하여 다음 RFCs를 제출합니다.

   a. KMS 키를 생성합니다. KMS 키 생성(자동) 또는 KMS 키 생성(관리형 자동화)을 사용합니다.

      KMS를 사용하여 수집된 리소스를 암호화할 때 다중 계정 랜딩 존 애플리케이션 계정의 나머지 부분과 공유되는 단일 KMS 키를 사용하면는 대상 계정에서 복호화할 수 있는 수집된 이미지에 대한 보안을 제공합니다.

   b. KMS 키를 공유합니다.

      관리 | 고급 스택 구성 요소 | KMS 키 | 공유(관리형 자동화) 변경 유형(ct-05yb337abq3x5)을 사용하여 수집된 AMIs가 상주할 애플리케이션 계정과 새 KMS 키를 공유하도록 요청합니다.

최종 계정 설정의 예제 그래픽:

AMS 사전 승인된 IAM CloudEndure 정책 예

AMS 사전 승인된 IAM CloudEndure 정책을 보려면: WIGS Cloud Endure Landing Zone 예제 파일의 압축을 풀고를 엽니다`customer_cloud_endure_policy.json`.

AMS 도구 계정 연결 및 end-to-end 설정 테스트

1. 먼저 CloudEndure를 구성하고 AMS에 복제할 서버에 CloudEndure 에이전트를 설치합니다.
2. CloudEndure에서 프로젝트를 생성합니다.
3. 보안 암호 관리자를 통해 사전 조건을 수행할 때 공유된 AWS 자격 증명을 입력합니다.
4. 복제 설정에서:
   a. 복제 서버에 적용할 보안 그룹 선택 옵션에서 AMS "Sentinel" 보안 그룹(프라이빗 전용 및 EgressAll)을 모두 선택합니다.
   b. 머신(인스턴스)에 대한 전환 옵션을 정의합니다. 자세한 내용은 5단계를 참조하세요. 컷오버
   c. 서브넷: 프라이빗 서브넷입니다.
5. 보안 그룹:
   a. 두 AMS "Sentinel" 보안 그룹(프라이빗 전용 및 EgressAll)을 모두 선택합니다.
   b. 전환 인스턴스는 AMS 관리형 Active Directory(MAD) 및 AWS 퍼블릭 엔드포인트와 통신해야 합니다.
      i. 탄력적 IP: 없음
      ii. 퍼블릭 IP: 아니요
      iii. IAM 역할: customer-mc-ec2-instance-profile
   c. 내부 태그 지정 규칙에 따라 태그를 설정합니다.
6. 시스템에 CloudEndure 에이전트를 설치하고 EC2 콘솔의 AMS 계정에 표시될 복제 인스턴스를 찾습니다.

AMS 수집 프로세스:

AMS 도구 계정 위생

계정에서 AMI를 공유했으며 복제된 인스턴스가 더 이상 필요하지 않은 경우 정리해야 합니다.

- 사후 인스턴스 WIGs 수집:
  - 전환 인스턴스: AWS 콘솔을 통해 작업이 완료된 후 최소한이 인스턴스를 중지하거나 종료합니다.
  - 사전 수집 AMI 백업: 인스턴스가 수집되고 온프레미스 인스턴스가 종료되면 제거
  - AMS 수집 인스턴스: AMI가 공유되면 스택을 끄거나 종료합니다.
  - AMS 수집 AMIs: 대상 계정과의 공유가 완료되면 삭제

- 마이그레이션 정리 종료: 정기적으로 정리가 이루어지도록 개발자 모드를 통해 배포된 리소스를 문서화합니다. 예를 들면 다음과 같습니다.
  - 보안 그룹
  - 클라우드 형식을 통해 생성된 리소스
  - 네트워크 ACK
  - 서브넷
  - VPC
  - 라우팅 테이블
  - 역할
  - 사용자 및 계정

대규모 마이그레이션 - Migration Factory

AWS CloudEndure Migration Factory 솔루션 소개를 참조하세요.

MALZ: 코어 계정 온보딩

AWS 다중 계정 랜딩 존 코어 계정에 온보딩할 때 수행해야 하는 주요 작업은 다음과 같습니다.

주제

- AMS에서 AWS 다중 계정 랜딩 존 코어 계정 생성
- AMS가 계정에 액세스할 수 있도록 IAM 역할 생성
- AMS의 루트 사용자에 대한 다중 인증(MFA)으로 새 계정 보호
- AWS Marketplace Trend Micro 엔드포인트 보호(EPS) 구독
- 네트워킹 설정
- 액세스 관리 설정

온보딩 관련 질문은 클라우드 아키텍트에 문의하세요.

AMS에서 AWS 다중 계정 랜딩 존 코어 계정 생성

AMS 다중 계정 랜딩 존은 AMS 다중 계정 랜딩 존 환경에서 관리 계정 역할을 하려면 새 Amazon Web Services(AWS) 계정을 프로비저닝해야 합니다. 를 생성하려면 다음 step-by-step 지침을 AWS 계정따르세요. 새 Amazon Web Services 계정을 생성하고 활성화하려면 어떻게 해야 하나요?

간단한 단계는 계정 생성으로 이동하여 지금 가입을 클릭하고 열리는 페이지에서 새 생성을 AWS 계정 클릭합니다. 전화 수신 및 전화 키패드를 사용하여 PIN 입력이 포함된 화면의 지침을 따릅니다. 신용 카드도 입력해야 합니다. AMS는이 계정을 새 다중 계정 랜딩 존의 관리 계정 또는 지급인 계정으로 사용합니다.

Note

온보딩되면 클라우드 서비스 제공 관리자(CSDM)에게 신용카드에서 인보이스 시스템으로 결제를 이전하는 방법을 문의하세요. 다음 정보가 필요합니다.

- 결제 회사 이름
- 결제 연락처 이름
- 청구 연락처 전화번호
- 결제 연락처 이메일
- 청구지 주소

CSDM이이 업데이트를 도와드릴 것입니다. 완료되면 결제 방법을 변경하려면 AWS 결제 방법 관리를 참조하세요.

Note

새 계정을 기존 관리 계정 또는 지급인 계정에 연결하지 마십시오.
계정이 기존의 일부가 아닌지 확인합니다 AWS Organizations. 자세한 내용은 란 무엇입니까 AWS Organizations?를 참조하세요.

Important

잠재적 보안 인시던트에 대한 응답을 받을 수 있도록 이메일 주소(개인의 이메일 주소가 아닌 배포 목록)와 전화번호가 계정과 연결되어 있는지 확인하는 것이 매우 중요합니다. 계정의 전화번호와 이메일 주소는 계정 암호를 재설정하지 않으면 변경할 수 없습니다. 이는 AMS 루트 계정에 중요한 작업입니다. 이러한 값이 안정적인지 확인하려면 개인과 연결되지 않은 연락처 정보를 선택하는 것이 중요하며, 이는 변경될 수 있습니다. 그룹을 가리킬 수 있는 이메일 별칭을 선택합니다. 전화번호를 선택할 때도 동일한 방법을 따릅니다. 즉, 개인이 아닌 회사가 소유한 번호 또는 그룹을 가리킬 수 있는 번호를 선택합니다.

코어 계정을 AMS 다중 계정 랜딩 존에 온보딩하라는 질문에 대한 자세한 내용은 섹션을 참조하세요부록: 다중 계정 랜딩 존(MALZ) 온보딩 고려 사항 목록.

AMS가 계정에 액세스할 수 있도록 IAM 역할 생성

이제 새를 성공적으로 생성했으므로 프로세스의 AWS 계정다음 단계는 새 계정에 대한 AMS 액세스를 허용하여 AMS 환경을 생성 및 구성하고 지속적인 변경 및 프로비저닝 요청을 이행하는 것입니다. 자세한 내용은 IAM 역할을 사용하여 AWS 계정 간 액세스 권한 위임을 참조하세요.

AWS Identity and Access Management (IAM)는 사용자의 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 웹 서비스입니다. IAM을 사용하여 AWS 리소스를 사용할 수 있는 사용자(인증)와 사용할 수 있는 리소스 및 방법(권한 부여)을 제어할 수 있습니다.

AWS 콘솔에 대한 IAM 액세스 활성화

1. 루트 계정 자격 증명(을 생성하는 데 사용한 이메일 및 암호)을 사용하여 AWS 관리 콘솔에 로그인합니다 AWS 계정. 다른 IAM 자격 증명으로 로그인하지 마십시오. AWS 관리 콘솔 홈 페이지가 열립니다.
2. 상단 탐색 모음에서 계정 이름의 드롭다운 메뉴를 연 다음 계정을 선택합니다. 결제 홈 페이지가 열립니다.
3. 결제 정보에 대한 IAM 사용자 및 역할 액세스까지 아래로 스크롤하고 편집을 선택합니다. IAM 액세스 활성화 영역이 열립니다.
4. 확인란을 선택한 다음 업데이트를 선택합니다. 이제 사용자가 액세스할 수 있는 페이지는 IAM 정책을 통해 제어할 수 있습니다.

AMS에서 사용할 IAM 역할 생성

1. AMS가 인프라를 생성하는 데 사용할 IAM 역할을 정의하는 JSON 또는 YAML 파일을 가져옵니다. 다음 중 하나를 사용합니다.
   - AMS 클라우드 아키텍트(CA)는 JSON 또는 YAML 파일을 제공합니다.
   - onboarding_iam_roles.zip을 다운로드하고 다음 중 하나를 선택할 수 있습니다.
     - onboarding_role_admin.json(짧음, 전체 관리자 액세스 권한 부여)
     - onboarding_role_minimal.json(장기, 최소 권한 부여)
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudformation CloudFormation 콘솔을 엽니다.

3. 스택 생성을 선택합니다. 다음 페이지가 표시됩니다.

4. 템플릿 파일 업로드를 선택하고 IAM 역할의 JSON 또는 YAML 파일을 업로드한 후 다음을 선택합니다. 다음 페이지가 표시됩니다.

5. 스택 이름 섹션에 **`ams-onboarding-role`**를 입력하고 아래로 스크롤하여이 페이지에 도달할 때까지 다음을 선택합니다.

6. 확인란이 선택되어 있는지 확인한 다음 스택 생성을 선택합니다.
7. 스택이 성공적으로 생성되었는지 확인합니다.

AMS의 루트 사용자에 대한 다중 인증(MFA)으로 새 계정 보호

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 AWS 아티팩트 시작하기를 참조하세요.

AWS Marketplace Trend Micro 엔드포인트 보호(EPS) 구독

Trend Micro Endpoint Protection(EPS)은 운영 체제 보안을 위한 AMS 내의 기본 구성 요소입니다. AMS 랜딩 존 생성이 시작된 후 EPS를 설정하려면 공유 서비스 코어 계정에 로그인하고 Trend Micro Deep Security AMI on을 구독해야 합니다 AWS Marketplace. CSDM 또는 CA가 알려줄 것입니다.

1. 온보딩 설문에서 지정한 역할 또는 사용자를 사용하여 AWS 콘솔에 로그인합니다. `CustomerEPSSubscriptionIAMRoleOrUser`
2. 역할 전환 화면으로 이동합니다.

- 계정: AMS에서 제공
- 역할: `EPSMarketplaceSubscriptionRole`

- 표시 이름: EPS 구독 세션

  에서 Trend Micro Deep Security를 구독하려면 콘솔에서 역할을 전환한 후 다음 단계를 AWS Marketplace따르세요.

  1. AWS Marketplace로 이동합니다.
  2. 필요에 맞는 AWS Marketplace 제품 찾기에서 다음 옵션을 선택합니다.
     a. 공급업체: Trend Micro
     b. 요금제: 라이선스가 있거나 호스트별 결제가 있는 경우 기존 보유 라이선스 사용
     c. 전송 방법: Amazon Machine Image
  3. 오른쪽 패널에서 계속을 클릭하여 구독합니다.
  4. 이용 약관을 검토하고 오른쪽 상단 모서리에서 약관 수락을 클릭합니다.
  5. 계정에서 로그아웃하고 Cloud Architect에 절차가 완료되었는지 확인합니다.

이 시점에서 AMS는 인프라를 AMS 환경에 배포하며, 네트워크를 연결하고 액세스를 설정하면 환경을 사용할 준비가 된 것입니다.

네트워킹 설정

AMS 환경의 네트워킹은 주로 네트워킹 코어 계정에서 처리됩니다.

AWS Managed Services(AMS)에 대한 네트워킹을 설정하려면 몇 가지 프로세스를 완료해야 합니다.

- AMS 환경에 IP 공간 할당
- 에 대한 프라이빗 네트워크 연결 설정 AWS
- AMS 작업을 허용하도록 방화벽 설정

AMS 환경에 IP 공간 할당

온보딩 설문지를 작성하는 동안 이미 Cloud Architect와 협력하여 AMS 환경의 IP 공간을 정의했어야 합니다.

AMS AWS 에서에 대한 프라이빗 네트워크 연결 설정

AWS 는 AWS Direct Connect를 통해 VPN 연결 및 전용 라인을 사용하여 프라이빗 연결을 제공합니다. 프라이빗 연결은 두 가지 방법으로 설정할 수 있습니다.

- Transit Gateway를 사용한 중앙 집중식 엣지 연결

- Direct Connect 및/또는 VPN을 계정 VPCs에 연결

Transit Gateway를 사용한 중앙 집중식 엣지 연결

AWS Transit Gateway는 Amazon Virtual Private Cloud(VPCs)와 온프레미스 네트워크를 단일 게이트웨이에 연결할 수 있는 서비스입니다. Transit Gateway를 사용하여 기존 엣지 연결을 통합하고 단일 수신/송신 지점을 통해 라우팅할 수 있습니다. 자세한 내용은 AWS Transit Gateway를 참조하세요.

전송 게이트웨이에 Direct Connect 연결

기존 Direct Connect 연결을 사용하거나 기존 AWS 계정 중 하나에서 새 Direct Connect 연결을 생성할 수 있습니다. Direct Connect 연결은 1Gbps 이상에서 실행되는 전용 또는 호스팅 연결이어야 합니다.

> **Note**
>
> AWS 서비스와 함께 Direct Connect를 사용하는 방법에 대한 자세한 내용은 AWS Direct Connect 위치에서 시작하기를 참조하세요.

기존 Direct Connect 전용 연결을 사용하려면 연결에 3개 이상의 전송 가상 인터페이스가 생성되지 않아야 합니다. 전용 Direct Connect 연결에는 연결당 4개의 전송 가상 인터페이스 제한이 있기 때문입니다.

Direct Connect 제한에 대한 자세한 내용은 AWS Direct Connect 제한을 참조하세요.

Direct Connect 연결을 사용할 수 있게 되면 다음이 발생합니다.

1. AMS는 네트워킹 계정에 Direct Connect 게이트웨이를 생성합니다. Direct Connect 게이트웨이의 자율 시스템 번호(ASN) 번호와 Direct Connect 게이트웨이에서 알려야 하는 접두사를 제공해야 합니다. 이 ASN은 Amazon ASN으로 사용됩니다.
2. 새 Transit VIF를 생성하고 가상 인터페이스 소유자를 네트워킹 계정으로 설정합니다.
3. AMS는 네트워킹 계정에 로그인하고 연결 제안을 수락합니다.
4. AMS는 전송 게이트웨이를 Direct Connect 게이트웨이와 연결합니다.
5. AMS는 연결을 온프레미스 Transit Gateway 라우팅 테이블과 연결합니다.

> **Note**
>
> Direct Connect 게이트웨이와 Transit Gateway에 제공된 ASN은 달라야 합니다.

연결 복원력을 높이려면 서로 다른 AWS Direct Connect 위치에서 Direct Connect 게이트웨이로 최소 2개의 전송 가상 인터페이스를 연결하는 것이 가장 좋습니다. 자세한 내용은 Direct Connect 복원력 권장 사항을 참조하세요.

Transit Gateway에 VPN 연결

Transit Gateway에 VPN 연결을 연결하려면 고객 게이트웨이를 지정해야 합니다. 고객 게이트웨이의 요구 사항에 대한 자세한 내용은 Amazon VPC 네트워크 관리자 안내서의 고객 게이트웨이 요구 사항을 참조하세요.

BGP ASN 번호, 정적 퍼블릭 IP 주소 및 라우팅 옵션(정적 또는 동적)을 제공해야 합니다. 이러한 세부 정보가 제공되면 AMS는 VPN 연결을 생성하고 연결을 온프레미스 Transit Gateway 라우팅 테이블과 연결합니다.

Transit Gateway 연결에 대한 자세한 내용은 Transit Gateway VPN 연결을 참조하세요.

Direct Connect 및/또는 VPN을 계정 VPCs에 연결

VPCs Direct Connect 또는 VPN에 직접 연결할 수도 있습니다. 트래픽은 전송 게이트웨이를 통과하지 않고 VPCs에서 Direct Connect 또는 VPN으로 직접 흐릅니다.

> **Note**
>
> 프라이빗 연결을 설정하려면 공유 서비스 VPC 및 애플리케이션 계정 VPCs를 Direct Connect 또는 VPN 연결에 연결해야 합니다.

Direct Connect AMS에서 설정

AMS 관리형 VPC와 내부 네트워크 간에 통신 Direct Connect 하도록를 설정합니다.

> **Note**
>
> AWS 서비스와 함께 Direct Connect를 사용하는 방법에 대한 자세한 내용은 Direct Connect 위치에서 시작하기를 참조하세요.

Direct Connect 연결을 설정하려면 다음 단계를 완료합니다.

1. Amazon Web Services(AWS) 가입
2. Direct Connect 연결 요청을 제출합니다.
3. Cross Connect를 완료합니다.
4. (선택 사항) 와의 중복 연결을 구성합니다 Direct Connect.
5. AMS에서 수행: 가상 인터페이스를 생성합니다.
6. AMS에서 수행: 라우터 구성을 다운로드합니다.
7. 가상 인터페이스를 확인합니다.

VPN 설정

AMS가 AMS 관리형 VPC와 내부 네트워크 간에 통신하도록 VPN을 설정하기 위해 수행하는 기본 단계입니다.

> **Note**
>
> AWS 서비스와 함께 VPN을 사용하는 방법에 대한 전반적인 이해는 What is AWS Site-to-Site VPN and Your Customer Gateway(VPN 어플라이언스)를 참조하세요.

AWS VPN 사용 설명서 시작하기 및 Site-to-Site VPN 연결 테스트 섹션에 따라 다음 단계를 완료합니다.

1. AWS VPC에서 고객 게이트웨이를 생성합니다.
2. AWS VPC에서 가상 프라이빗 게이트웨이를 생성합니다.
3. AWS VPC의 라우팅 테이블에서 라우팅 전파를 활성화합니다.
4. AWS VPC에서 인바운드 SSH, RDP 및 ICMP 액세스를 활성화하도록 보안 그룹을 업데이트합니다.
5. 내부 네트워크에서 VPN 연결을 생성하고 고객 게이트웨이를 구성합니다.
6. VPC와 내부 네트워크 간의 VPN 연결을 테스트합니다.

액세스 관리 설정

AWS Managed Services(AMS)에서 관리하는 네트워크를 사용하는 것은 AMS에 클라우드 인프라를 관리할 수 있는 액세스 권한을 부여하는 것을 의미합니다. 프라이빗 네트워크와 AMS 간에 안전하게 연결하는 수단을 구성해야 합니다. 이는 몇 가지 결정으로 시작됩니다.

- AMS API/CLI 및 콘솔 액세스: AMS CLI를 설치하려고 합니다(이 문서에서는 지침 제공). AMS 변경 관리 API를 사용하여 AMS 및 AMS SKMS API에 대한 변경 요청을 하여 AMS 관리형 리소스에 대해 알아봅니다. Active Directory Federation Services(AD FS)를 사용하여 AMS 콘솔에 액세스할 수 있습니다.
- 사용자 액세스: AMS 측의 AD(Directory Services를 통해)와 사용자를 관리하는 데 사용하는 디렉터리 간에 연결을 설정해야 합니다.
- 인스턴스 액세스: 인스턴스 수준 액세스는 단방향 신뢰 구성을 통해 수행됩니다. Directory Services는 CORP AD의 자격 증명을 신뢰하므로 AMS 측 내의 스택에서 CORP 자격 증명으로 로그인할 수 있습니다.

> **Note**
>
> AMS가 신뢰를 설정하는 Active Directory(AD)는 AWS 리소스에 대한 액세스 권한을 부여받은 사용자의 계정이 있는 디렉터리여야 합니다.

Active Directory 신뢰 설정

신뢰를 설정하려면 AMS에 도메인 컨트롤러 로컬 정책 -> 보안 옵션 -> 네트워크 액세스: 익명으로 액세스할 수 있는 명명된 파이프가 있어야 합니다. Netlogon 및 lsarpc 파이프가 나열됩니다. 이러한 파이프는 기본적으로 나열되지만 보안 문제로 인해 제거되는 경우도 있습니다. 신뢰가 설정되면 목록에서 다시 제거할 수 있습니다.

조건부 전달자 구성

1. AD DNS 관리자 -> 새 조건부 전달자 생성의 DNS 도메인에서: 제공된 도메인 이름 AMS를 사용합니다. 예: A523434123.amazonaws.com(온보딩 설문에서 선택한 도메인 이름으로 변경합니다.
2. 마스터 서버의 IP 주소에서 AMS에서 제공하는 IP 주소를 추가합니다. 두 주소를 모두 검증하여 연결 문제가 없는지 확인합니다.
3. 이 조건부 전달자를 Active Directory에 저장을 선택하고 다음과 같이 복제합니다.이 도메인의 모든 DNS 서버를 선택하고 확인을 누릅니다.

AD 신뢰 구성

이 Microsoft AD 문서에 따라이 섹션에 설명된 설정 및 선택 사항을 사용하여 신뢰의 한쪽에 대한 단방향 수신 포리스트 신뢰를 생성합니다.

1. 시작 -> 관리 도구 -> Active Directory 도메인 및 신뢰 대화 상자를 엽니다. 신뢰를 설정할 도메인의 도메인 노드를 마우스 오른쪽 버튼으로 클릭한 다음 속성 -> 신뢰 -> 새 신뢰를 클릭하여 새 신뢰 마법사를 엽니다. 신뢰 이름에 AMS에서 제공한 도메인 이름을 입력하고 다음을 누릅니다.
2. 신뢰 유형에서 적절한 신뢰 수준(예: 포리스트 신뢰)을 선택합니다. 다음을 누릅니다.
3. 신뢰 방향에서 단방향: 수신을 선택합니다. 다음(Next)을 누릅니다.
4. 신뢰의 측면에서 이 도메인만 선택합니다. 다음(Next)을 누릅니다.
5. 암호 신뢰에서 선택한 암호를 입력합니다. 다음(Next)을 누릅니다.
6. 신뢰 선택 완료 및 신뢰 생성 완료에서 다음을 누릅니다.
7. 수신 신뢰 확인에서 아니요, 수신 신뢰를 확인하지 않음을 선택합니다. 다음(Next)을 누릅니다.
8. 새 신뢰 마법사 완료에서 완료를 선택한 다음 확인을 선택하여 닫습니다.
9. 신뢰 암호를 입력합니다(보안상의 이유로 CSDM의 전화번호를 통해 문의). AMS는 신뢰 구성을 완료합니다.

Active Directory 사이트 및 서비스

로그인 지연 시간을 줄이려면 Active Directory 사이트 및 서비스(시작 -> 관리 도구 -> Active Directory 사이트 및 서비스)에 VPC CIDR 범위를 추가합니다. AWS에 가장 가까운 도메인 컨트롤러가 포함된 Active Directory 사이트에 VPC CIDR 범위를 추가합니다.

AMS 전용 사이트의 AD 사이트 이름을 CSDM에 제공합니다. AMS는 제공된 이름과 일치하도록 AD의 AMS 측에 있는 기본 사이트의 이름을 바꿉니다.

Active Directory 이름 접미사 라우팅

단방향 포리스트 신뢰가 설정되면 다음 단계를 완료하여 접미사 라우팅을 검증합니다.

1. 시작 > 모든 프로그램 > 관리 도구에서 Active Directory 도메인 및 신뢰를 클릭합니다.

   Active Directory 도메인 및 신뢰 콘솔이 열립니다.
2. 회사 도메인을 마우스 오른쪽 버튼으로 클릭하고 속성을 클릭합니다.

   해당 도메인의 속성 대화 상자가 열립니다.

3. 신뢰 탭을 클릭합니다.

   신뢰 페이지가 열립니다.

4. Amazon 도메인 이름을 클릭하고 속성을 클릭합니다.

   Amazon 도메인 신뢰의 속성 페이지가 열립니다.

5. 이름 접미사 라우팅을 클릭하고 새로 고침을 클릭합니다.

   서비스 보안 주체 이름(SPNs)이 신뢰를 통해 해결할 수 있도록 충돌이 없는지 확인합니다.

Active Directory를 AMS IAM 역할과 연동

디렉터리를 AMS IAM 역할과 페더레이션하는 목적은 기업 사용자가 회사 자격 증명을 사용하여 AWS 콘솔 및 AWS APIs, 따라서 AMS 콘솔 및 APIs.

페더레이션 프로세스 예제

이 예제에서는 Active Directory Federation Services(AD FS)를 사용하지만 AWS IAM Federation을 지원하는 모든 기술이 지원됩니다. AWS 지원 IAM 페더레이션에 대한 자세한 내용은 IAM 파트너 및 자격 증명 공급자 및 페더레이션을 참조하세요. CSDM은 AD 팀 및 AMS와의 공동 노력이 필요한이 프로세스를 안내합니다.

API 액세스를 위한 SAML 통합에 대한 자세한 내용은이 AWS 블로그인 SAML 2.0 및 AD FS를 사용하여 페더레이션 API 및 CLI 액세스를 구현하는 방법을 참조하세요.

AMS CLI 및 SAML을 설치하는 예제는 부록: AD FS 클레임 규칙 및 SAML 설정을 참조하세요.

AMS 콘솔에 대한 페더레이션 구성(MALZ)

다음 표에 자세히 설명된 IAM 역할 및 SAML 자격 증명 공급자(신뢰할 수 있는 엔터티)는 AMS 인프라의 일부로 프로비저닝되었습니다. 이러한 역할을 통해 AMS 코어 계정을 감사하고 볼 수 있습니다.

역할	권한
AWSManagedServicesReadOnlyRole	코어 계정에서 AMS 인프라를 볼 수 있습니다.
AWSManagedServicesCaseRole	새 애플리케이션 계정의 리소스를 보고 AMS 인시던트 및 서비스 요청을 제출할 수 있습니다.

역할	권한
AWSManagedServicesChangeManagementRole	코어 계정에서 AMS 인프라를 보고, AWS Support 티켓을 제출하고, 일부 RFCs.

다른 계정에서 사용할 수 있는 역할의 전체 목록은 섹션을 참조하세요AMS의 IAM 사용자 역할.

콘솔 액세스 확인

ADFS로 설정하고 인증에 사용할 AMS URL이 있으면 다음 단계를 따릅니다.

Active Directory Federated Service(ADFS) 구성을 사용하면 다음 단계를 수행할 수 있습니다.

1. 브라우저 창을 열고 계정에 제공된 로그인 페이지로 이동합니다. 계정의 ADFS IdpInitiatedSignOn 페이지가 열립니다.
2. 다음 사이트 중 하나에 로그인 옆의 라디오 버튼을 선택합니다. 로그인 사이트 선택 목록이 활성화됩니다.
3. signin.aws.amazon.com 사이트를 선택하고 로그인을 클릭합니다. 자격 증명을 입력하는 옵션이 열립니다.
4. CORP 자격 증명을 입력하고 로그인을 클릭합니다. 가 AWS Management Console 열립니다.
5. AMS 콘솔의 URL을 위치 표시줄에 붙여넣고 Enter 키를 누릅니다. AMS 콘솔이 열립니다.

API 액세스 확인

AMS는 AMS API 참조에서 읽을 수 있는 일부 AMS 관련 작업과 함께 AWS API를 사용합니다.

AWS는 Amazon Web Services용 도구에서 액세스할 수 있는 여러 SDKs 제공합니다. SDK를 사용하지 않으려면 직접 API를 호출할 수 있습니다. 인증에 대한 자세한 내용은 AWS API 요청 서명을 참조하세요. SDK를 사용하지 않거나 직접 HTTP API 요청을 하는 경우 변경 관리(CM) 및 SKMS용 AMS CLIs를 사용할 수 있습니다.

AMS CLIs 설치

AWS CLI는 AMS CLIs(변경 관리 및 SKMS)를 사용하기 위한 사전 조건입니다.

1. AWS CLI를 설치하려면 AWS 명령줄 인터페이스 설치를 참조하고 적절한 지침을 따릅니다. 해당 페이지 하단에는 Linux, MS Windows, macOS, 가상 환경, 번들 설치 관리자(Linux, macOS 또는 Unix) 등 다양한 설치 프로그램을 사용하기 위한 지침이 있습니다. macOS

2. 설치 후 aws 도움말을 실행하여 설치를 확인합니다.
3. AWS CLI가 설치되면 AMS CLI를 설치하거나 업그레이드하려면 AMS 배포 가능 zip 파일을 다운로드하고 압축을 풉니다. AMS 콘솔의 왼쪽 탐색에 있는 설명서 링크를 통해 AMS CLI 배포 파일에 액세스하거나 클라우드 서비스 제공 관리자(CSDM)에게 zip 파일을 보내 달라고 요청할 수 있습니다.
4. 운영 체제에 따라 관리형 클라우드 배포 가능 -> CLI -> Windows 또는 관리형 클라우드 배포 가능 -> CLI -> Linux/MacOS 디렉터리를 엽니다.
5. Windows의 경우 적절한 설치 관리자를 실행합니다(이 방법은 Windows 32 또는 64비트 시스템에서만 작동함).
   - 32비트: ManagedCloudAPI_x86.msi
   - 64비트: ManagedCloudAPI_x64.msi
6. Mac/Linux의 경우 sh MC_CLI.sh 명령을 실행하여 MC_CLI.sh라는 파일을 실행합니다. amscm 및 amsskms 디렉터리와 해당 콘텐츠는 MC_CLI.sh 파일과 동일한 디렉터리에 있어야 합니다.
7. 기업 자격 증명을 AWS와의 페더레이션(AMS 기본 구성)을 통해 사용하는 경우 페더레이션 서비스에 액세스할 수 있는 자격 증명 관리 도구를 설치해야 합니다. 예를 들어이 AWS 보안 블로그 SAML 2.0 및 AD FS를 사용하여 연합 API 및 CLI 액세스를 구현하는 방법을 사용하여 자격 증명 관리 도구를 구성할 수 있습니다.
8. 설치 후 `aws amscm help` 및를 실행`aws amsskms help`하여 명령과 옵션을 확인합니다.

MALZ: 애플리케이션 계정 온보딩

새 애플리케이션 계정을 요청하기 전에 코어 계정으로 다중 계정 AWS Managed Services(AMS) 환경을 설정해야 합니다. 다음은 환경을 설정한 후 수행해야 하는 단계입니다.

주제

- 새 애플리케이션 계정 요청
- AMS IAM 역할에 대한 액세스를 페더레이션하도록 Active Directory 설정
- 새 애플리케이션 계정으로 네트워킹 설정
- 애플리케이션 계정에서 추가 VPCs 설정

온보딩 관련 질문은 클라우드 서비스 제공 관리자(CSDM)에게 문의하세요. 애플리케이션 계정: AMS 관리형, 개발 모드, 고객 관리형도 참조하세요. 모드에 대한 일반적인 내용은 AMS 모드 단원을 참조하십시오AWS Managed Services의 서비스 관리.

애플리케이션 계정의 다양한 모드에 대한 자세한 내용은 애플리케이션 계정: AMS 관리형, 개발 모드, 고객 관리형을 참조하세요. 모드에 대한 일반적인 내용은 AMS 모드를 참조하세요.

새 애플리케이션 계정 요청

새 애플리케이션 계정을 요청하기 전에 코어 계정으로 다중 계정 AWS Managed Services(AMS) 환경을 설정해야 합니다. 코어 계정을 사용하여 다중 계정 환경을 설정하는 방법에 대한 자세한 내용은 섹션을 참조하세요MALZ: 코어 계정 온보딩.

애플리케이션 계정의 초기 VPC에 대해 다음 Amazon VPC 유형 중 하나를 선택할 수 있습니다.

- 프라이빗:이 VPC에는 인터넷 게이트웨이가 연결되어 있지 않습니다. 인터넷에 액세스하거나 인터넷에서 액세스할 필요가 없는 프라이빗 애플리케이션에 적합합니다.
- 퍼블릭:이 VPC에는 인터넷 게이트웨이가 연결되어 있으며 퍼블릭 및 프라이빗 서브넷이 있습니다. 인터넷에 액세스해야 하는 퍼블릭 애플리케이션에 적합합니다.

배포 | 관리형 랜딩 존 | 관리 계정 | 애플리케이션 계정 생성(VPC 사용)(ct-1zdasmc2ewzrs) RFC를 제출하고 RFC에 다음 값을 제공하여 새 애플리케이션 계정을 요청할 수 있습니다.

- 계정 이름: 계정의 사용자 지정 이름입니다. 계정 이름의 최대 길이는 50자입니다.
- 계정 이메일: 계정의 배포 목록 이메일입니다. 이 이메일 ID는 AWS 계정을 생성하는 데 사용됩니다.
- 지원 수준: AWS 지원 수준, Premium 또는 Plus.
- VPC 이름: VPC의 이름입니다.
- 가용 영역(AZs 수: 2 또는 3.
- VPC CIDR: VPC의 CIDR 블록입니다.
- 라우팅 유형: `routable` 또는 일 수 있습니다`isolated`. `Routable`는 Transit Gateway(TGW) 애플리케이션 라우팅 테이블과 연결된 애플리케이션 VPCs가이 VPC에 연결할 수 있음을 의미합니다. `Isolated`는 TGW 애플리케이션 라우팅 테이블과 연결된 애플리케이션 VPCs가이 VPC에 연결할 수 없음을 의미합니다. 기본값은 `routable`입니다.
- Transit Gateway Application Route Table: 애플리케이션 계정 VPC를 연결해야 하는 Transit Gateway 라우팅 테이블입니다. 값이 제공되지 않으면 기본값`defaultAppRouteDomain`이 사용됩니다. 즉,이 계정은 동일한 라우팅 테이블의 다른 모든 계정과 통신할 수 있습니다.
- AZ 1의 퍼블릭 서브넷에 대한 PublicSubnetAZ*<1-3>*CIDRCIDR: 가용 영역 1의 퍼블릭 서브넷에 대한 CIDR입니다.
- PrivateSubnet*<1-10>*AZ*<I-3>*AZ 1의 퍼블릭 서브넷용 CIDR: 가용 영역 1의 퍼블릭 서브넷용 CIDR입니다.

이때 AMS는 지정된 VPC 구성으로 AMS 관리 계정에 새 애플리케이션 계정을 배포합니다.

AMS IAM 역할에 대한 액세스를 페더레이션하도록 Active Directory 설정

디렉터리를 AMS IAM 역할과 연동하여 기업 사용자가 회사 자격 증명을 사용하여 AWS 콘솔 및 AWS APIs, AMS 콘솔 및 AMS APIs.

페더레이션 프로세스 예제

이 예제에서는 Active Directory Federation Services(ADFS)를 사용합니다. 그러나 AWS IAM 연동을 지원하는 모든 기술이 지원됩니다. AWS 지원 IAM 페더레이션에 대한 자세한 내용은 IAM 파트너 및 자격 증명 공급자 및 페더레이션을 참조하세요. CSDM은 AD 팀 및 AMS와의 공동 노력이 필요한이 프로세스를 안내합니다.

API 액세스를 위한 SAML 통합에 대한 자세한 내용은이 AWS 블로그인 SAML 2.0 및 AD FS를 사용하여 페더레이션 API 및 CLI 액세스를 구현하는 방법을 참조하세요.

AMS CLI 및 SAML을 설치하는 예제는 AMS 사용 설명서의 부록: AD FS 클레임 규칙 및 SAML 설정을 참조하세요.

AMS 콘솔에 대한 페더레이션 구성

다음 표에 자세히 설명된 IAM 역할 및 SAML 자격 증명 공급자(신뢰할 수 있는 엔터티)는 새 애플리케이션 계정에 프로비저닝됩니다. 이러한 역할을 통해 새 애플리케이션 계정 및 파일 RFCs에 액세스하고, S3 버킷에 쓰고, 기타 작업을 수행할 수 있습니다.

역할	권한
AWSManagedServicesReadOnlyRole	새 애플리케이션 계정의 리소스를 볼 수 있습니다.
AWSManagedServicesCaseRole	새 애플리케이션 계정의 리소스를 보고 AWS Support 티켓을 제출할 수 있습니다.
AWSManagedServicesChangeManagementRole	애플리케이션 계정, 파일 RFCs, 파일 AWS Support 티켓, S3 버킷에 쓰기, Secrets Manager 보안 암호 관리 및 예약 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 관리에서 AMS 인프라를 볼 수 있습니다.

역할	권한
AWSManagedServicesSecurityOpsRole	애플리케이션 계정에서 AMS 인프라를 보고, Secrets Manager 보안 암호를 관리하고, 웹 애플리케이션 방화벽 규칙을 관리하고, 인증서를 관리하고, AWS Support 티켓을 제출할 수 있습니다.
AWSManagedServicesAdminRole	애플리케이션 계정에서 AMS 인프라를 보고, Marketplace 구독을 관리하고, Secrets Manager 보안 암호를 관리하고, 웹 애플리케이션 방화벽 규칙을 관리하고, 인증서를 관리하고, RFCs 생성하고, 예약 Amazon EC2 인스턴스를 관리하고, S3 버킷에 쓰고, AWS Support 티켓을 제출하고, AWS Artifacts 계약을 관리할 수 있습니다.

AMS에 페더레이션 요청 제출

첫 번째 계정인 경우 CSDM(들) 및/또는 클라우드 아키텍트(들)와 협력하여 자격 증명 공급자에 대한 메타데이터 XML 파일을 제공합니다.

추가 계정 또는 자격 증명 공급자를 온보딩하고 관리 계정 또는 원하는 애플리케이션 계정에 액세스할 수 있는 경우 다음 단계를 따릅니다.

1. AMS 콘솔에서 서비스 요청을 생성합니다.

   > **Note**
   >
   > - 애플리케이션 계정에 대한 자격 증명 공급자를 생성하는 경우 애플리케이션 계정 자체 또는 관리 계정에서이 요청을 제출합니다.
   > - AMS 코어 계정에 대한 자격 증명 공급자를 생성하는 경우 관리 계정에서이 요청을 제출합니다.
   > - 관리 계정에 대한 자격 증명 공급자를 생성하는 경우 관리 계정에서이 요청을 제출하거나 CSDM에 문의하여 지원을 받으세요.

   서비스 요청에서 자격 증명 공급자를 추가하는 데 필요한 세부 정보를 제공합니다.

- 새 자격 증명 공급자가 생성될 계정의 AccountId입니다.
- 원하는 자격 증명 공급자 이름이 제공되지 않은 경우 기본값은 customer-saml입니다. 일반적으로 이는 페더레이션 공급자에 구성된 설정과 일치해야 합니다.
- 기존 계정의 경우 새 자격 증명 공급자를 모든 기존 콘솔 역할에 전파해야 하는지 여부를 포함하거나 새 자격 증명 공급자를 신뢰해야 하는 역할 목록을 제공합니다.
- 페더레이션 에이전트에서 내보낸 메타데이터 XML 파일을 서비스 요청에 첨부 파일로 연결합니다.

2. 서비스 요청을 생성한 계정과 동일한 계정에서 다음 정보와 함께 CT-ID ct-1e1xtak34nx76(관리 | 기타 | 기타 | 생성)을 사용하여 새 RFC를 생성합니다.

   - 제목: "계정 <AccountId>의 온보딩 SAML IDP <Name>".
   - 자격 증명 공급자가 생성될 계정의 AccountId입니다.
   - 자격 증명 공급자 이름입니다.
   - 기존 계정의 경우: 자격 증명 공급자를 모든 기존 콘솔 역할에 전파해야 하는지 아니면 새 자격 증명 공급자를 신뢰해야 하는 역할 목록.
   - 메타데이터 XML 파일이 연결된 1단계에서 생성된 서비스 요청의 사례 ID입니다.

콘솔 액세스 확인

AD FS로 설정하고 인증에 사용할 AMS URL이 있으면 다음 절차를 수행할 수 있습니다.

Active Directory Federated Service(AD FS) 구성을 사용하면 다음 단계를 수행할 수 있습니다.

1. 브라우저 창을 열고 계정에 제공된 로그인 페이지로 이동합니다. 계정의 AD FS IdpInitiatedSignOn 페이지가 열립니다.
2. 다음 사이트 중 하나에 로그인 옆의 라디오 버튼을 선택합니다. 로그인 사이트 목록이 활성화됩니다.
3. signin.aws.amazon.com 사이트를 선택하고 로그인을 선택합니다. 자격 증명을 입력하는 옵션이 열립니다.
4. CORP 자격 증명을 입력하고 로그인을 선택합니다. AWS Management Console이 열립니다.
5. AMS 콘솔의 URL을 위치 표시줄에 붙여넣고 Enter 키를 누릅니다. AMS 콘솔이 열립니다.

API 액세스 확인

AMS는 AMS API 참조에서 읽을 수 있는 일부 AMS 관련 작업과 함께 AWS API를 사용합니다.

AWS는 Amazon Web Services용 도구에서 액세스할 수 있는 여러 SDKs 제공합니다. SDK를 사용하지 않으려면 직접 API를 호출할 수 있습니다. 인증에 대한 자세한 내용은 AWS API 요청 서명을 참조하세요. SDK를 사용하지 않거나 직접 HTTP API 요청을 하는 경우 변경 관리(CM) 및 SKMS용 AMS CLIs를 사용할 수 있습니다.

새 애플리케이션 계정으로 네트워킹 설정

애플리케이션 계정에 대한 네트워킹 설정에는 방화벽 규칙 구성과 추가 Transit Gateway(TGW) 라우팅 테이블 설정이 포함됩니다.

방화벽 설정

AMS 환경에 배포된 애플리케이션을 사용하려면 일부 방화벽 규칙을 생성해야 합니다. 인스턴스에 액세스하는 데 이러한 규칙이 필요하지 않으므로 Bastion을 인스턴스로 건너뛸 수 있습니다.

애플리케이션 액세스를 위한 방화벽 규칙

방화벽을 통한 트래픽에 대해 다음 포트를 열어야 합니다.

- 수신 및 송신 방향 모두에서 온프레미스 네트워크에서 새 애플리케이션 VPC CIDRs로 전환합니다.
- 새 애플리케이션 VPC CIDRs에서 수신 방향과 송신 방향 모두에서 온프레미스 네트워크에 이르기까지(클라우드 애플리케이션이 온프레미스 애플리케이션에 연결해야 하는 경우).

포트	프로토콜	서비스:	시작/종료	수신/발신
80	TCP	HTTP 웹 액세스	온프레미스 네트워크	AMS 애플리케이션 VPC
443	TCP	HTTPS 웹 액세스	온프레미스 네트워크	AMS 애플리케이션 VPC

추가 전송 게이트웨이 애플리케이션 라우팅 테이블 설정

AWS Managed Services(AMS) 네트워킹은 유연하며 다양한 네트워킹 사용 사례를 지원합니다.

- 동일한 계정의 애플리케이션 VPCs 간 통신.
- 서로 다른 계정VPCs 간 통신.
- 서로 다른 계정VPCs 간 격리.
- 동일한 계정VPCs 간 격리.

네트워킹에 대한 고유/특수 요구 사항이 있는 경우 AMS 클라우드 아키텍트에 문의하면 AMS 네트워크 아키텍처에서 요구 사항을 충족하기 위한 계획을 개발할 것입니다.

애플리케이션 계정 VPCs에 대해 내린 네트워킹 결정에 따라 배포 | 관리형 랜딩 존 | 네트워킹 계정 | 전송 게이트웨이 라우팅 테이블 생성(ct-3dscwaeyi6cup) RFC를 제출하여 여러 Transit Gateway(TGW) 애플리케이션 라우팅 테이블을 생성할 수 있습니다.

변경 유형을 사용하려면 `TransitGatewayRouteTableName` (TGW 라우팅 테이블의 의미 있는 이름), `TransitGatewayId`및를 지정해야 합니다`TGWRouteTableType`.

> **Note**
>
> TGWRouteTableType에 createCustomRouteDomain을 선택하면 생성된 라우팅 테이블이 비어 있습니다. 배포 | 관리형 랜딩 존 | 네트워킹 계정 | 정적 경로 추가(ct-3r2ckznmt0a59) 변경 유형을 사용하여 RFC를 제출해야 합니다.

애플리케이션 계정에서 추가 VPCs 설정

배포 | 관리형 랜딩 존 | 애플리케이션 계정 | VPC 생성(ct-1j3503fres5a5) RFC를 제출하여 추가 애플리케이션 계정 VPC를 요청할 수 있습니다.

이는 새 애플리케이션 계정에 대한 VPC를 구성하는 것과 동일한 방식으로 작동합니다. 자세한 내용은 새 애플리케이션 계정 요청 섹션을 참조하십시오.

부록: 다중 계정 랜딩 존(MALZ) 온보딩 고려 사항 목록

AMS 다중 계정 랜딩 존 배포를 계획할 때 고려해야 할 몇 가지 주요 고려 사항이 있습니다. 선택한 항목은 필요한 인프라 구성 요소를 결정하는 데 필요한 정보를 AMS에 제공합니다. 클라우드 아키텍트(CA)는이 작업을 지원하는 설문지를 제공합니다.

주제

- AMS 다중 계정 랜딩 존 계정 구성
- AMS 다중 계정 랜딩 존 모니터링 알림
- 네트워크 구성
- Active Directory 구성
- Trend Micro 엔드포인트 보호(EPS)
- 액세스: Bastions, SSH 및 RDP
- 연동

> **Note**
>
> 인스턴스 유형에 대한 자세한 내용은 Amazon EC2 인스턴스 유형을 참조하세요.
> 데이터베이스 인스턴스 유형에 대한 자세한 내용은 Amazon RDS 인스턴스 유형을 참조하세요.
> Direct Connect가 필요한 경우 AMS 단일 계정 랜딩 존 온보딩 가이드를 참조하여 Direct Connect 연결을 생성합니다.

Cloud Service Delivery Manager(CSDM)로부터 계정의 원하는 구성 설정에 대한 질문이 포함된 온보딩 설문지를 받게 됩니다. 계속하기 전에 CSDM과 협력하여 설문지를 작성합니다.

AMS 다중 계정 랜딩 존 계정 구성

- 새 계정 ID

  AMS 다중 계정 랜딩 존에 대해 생성한 AWS 계정 ID입니다. AWS 조직의 일부가 되어서는 안 됩니다.
- 서비스 리전

  AMS 다중 계정 랜딩 존 환경을 배포할 기본 리전입니다.
- 코어 계정은 알림을 위해 이메일을 보냅니다(모두 동일한 도메인에 있어야 함). 각각에 대한 이메일 주소를 제공합니다.
  - 공유 서비스 계정
  - 네트워킹 계정
  - 계정 로깅
  - 보안 계정

- 서비스 유형, Premium 또는 Plus

  이는 환경의 문제를 해결하기 위한 서비스 수준 계약(SLAs)을 결정합니다.

AMS 다중 계정 랜딩 존 모니터링 알림

AMS는 특정 모니터링 알림에 대해 직접 알림을 받을 수 있는 방법(AMS 서비스 알림 받기와 비교)을 제공합니다. 가입하려면 Cloud Architect(CA) 또는 Cloud Service Delivery Manager(CSDM)가 다음 정보를 수신해야 합니다.

다이렉트 알림 이메일: AMS가 특정 리소스 기반 알림을 보낼 이메일 주소입니다. 이메일로 직접 전송되는 알림에 대한 자세한 내용은 AMS Advanced User Guide의 Alerts from baseline monitoring in AMS를 참조하세요. AMS 모니터링에 대한 자세한 내용은 단일 계정 랜딩 존용 AMS 사용 설명서의 모니터링 관리를 참조하세요.

네트워크 구성

- 전송 게이트웨이 ASN 번호

  이는 BGP(Border Gateway Protocol) 세션의 AWS 측에 대한 ASN(자율 시스템 번호)이며 고유해야 하며 Direct Connect 또는 VPN에 사용된 것과 같을 수 없습니다. 범위는 16비트 ASNs.
- AMS 다중 계정 랜딩 존 인프라 VPC CIDR 범위.

  이러한 CIDR 범위는 온프레미스 네트워크와 겹칠 수 없습니다.

  /22 CIDR 범위를 포함하거나 각 VPC CIDR을 개별적으로 제공할 수 있습니다. 이러한 CIDR 범위만 허용됩니다.
  - 10.0.0.0 - 10.255.255.255 (10/8 접두사)
  - 172.16.0.0 - 172.31.255.255 (172.16/12 접두사)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 접두사)

  IP 범위 198.18.0.0/15는 사용할 수 없습니다(AWS Directory Service에서 예약).
  - 코어 인프라 VPC CIDR 범위(/22 범위 권장)
  - 네트워킹 VPC CIDR 범위(/24 범위 권장)
  - 공유 서비스 VPC CIDR 범위(/23 범위 권장)
  - DMZ VPC CIDR 범위(/25 범위 권장)
- VPN ECMP(활성화 또는 비활성화)

VPN 연결 간에 ECMP(Equal Cost Multipath) 라우팅 지원이 필요한 경우 VPN ECMP support(VPN ECMP 지원)에서 enable(활성화)을 선택합니다. 연결에서 동일한 CIDR을 공고하는 경우 해당 트래픽은 이러한 CIDR 간에 균등하게 분산됩니다.

네트워크 액세스 제어 목록(NACL)

네트워크 액세스 제어 목록(NACL)은 하나 이상의 서브넷으로 들어오고 나가는 트래픽을 제어하는 방화벽 역할을 하는 VPC의 선택적 보안 계층입니다. 보안 그룹과 비슷한 규칙으로 네트워크 ACL을 설정하여 VPC에 보안 계층을 더 추가할 수 있습니다. 보안 그룹과 네트워크 ACLs의 차이점에 대한 자세한 내용은 보안 그룹과 네트워크 ACLs.

그러나 AMS 다중 계정 랜딩 존에서 AMS가 인프라를 효과적으로 관리하고 모니터링하기 위해 NACLs 사용은 다음 범위로 제한됩니다.

- NACLs은 관리, 네트워킹, 공유 서비스, 로깅 및 보안과 같은 다중 계정 랜딩 존 코어 계정에서 지원되지 않습니다.
- NACLs은 "거부" 목록으로만 사용되는 경우 다중 계정 랜딩 존 애플리케이션 계정에서 지원됩니다. 또한 AMS 모니터링 및 관리 작업을 보장하도록 "모두 허용"이 구성되어 있어야 합니다.

대규모 다중 계정 환경에서는 중앙 집중식 송신 방화벽과 같은 기능을 활용하여 AMS 다중 계정 랜딩 존의 아웃바운드 트래픽 및/또는 AWS Transit Gateway 라우팅 테이블을 제어하여 VPCs.

Active Directory 구성

AMS 관리형 Active Directory용 도메인 FQDN

Trend Micro 엔드포인트 보호(EPS)

- EC2 인스턴스 및 Auto Scaling 그룹의 인스턴스 크기

  Trend Micro Endpoint Protection(EPS)은 운영 체제 보안을 위한 AMS 내의 기본 구성 요소입니다. 시스템은 Deep Security Manager(DSM) EC2 인스턴스, 릴레이 EC2 인스턴스, 모든 AMS 데이터 영역 및 EC2 인스턴스 내에 있는 에이전트로 구성됩니다.

  - 릴레이 인스턴스 유형(AMS에서 지원하는 최소 m5.large)
  - DB 인스턴스 크기(200GB 권장)
  - RDS 인스턴스 유형(db.m5.large 또는 db.m5.xlarge만 허용됨)

- " 라이선스 유형(Marketplace 또는 BYOL)

  이미 라이선스가 있는 경우 BYOL(자체 라이선스 취득)을 선택합니다. AMS가 라이선스에 필요한 정보를 얻기 위해 연락을 드릴 것입니다.

- AWS Trend Micro Deep Security 구독을 위한 IAM 사용자 또는 역할 Amazon 리소스 이름(ARN)(역할 ARN: arn:aws:iam::*ACCOUNT_ID*:role/*ROLE_NAME*)

  액세스 권한이 있는 기존 중 하나의 IAM 역할, ARN 또는 IAM 사용자 ARN AWS 계정 을 제공합니다. AMS는 AMS 다중 계정 랜딩 존 Shared Services 계정에 IAM 역할을 생성하고 공유 서비스에서 IAM 역할의 신뢰에 제공된 역할 또는 사용자를 추가하여 사용자가 Trend Micro Deep Security를 구독하도록 역할을 수임할 수 있도록 합니다 AWS Marketplace.

액세스: Bastions, SSH 및 RDP

- SSH Bastion 설정

  AMS는 공유 서비스 계정에 SSH 접속을 제공하여 AMS 환경의 호스트에 액세스합니다. SSH 사용자로 AMS 네트워크에 액세스하려면 SSH Bastions를 진입점으로 사용해야 합니다. 네트워크 경로는 온프레미스 네트워크에서 시작되고 DX/VPN을 통해 전송 게이트웨이(TGW)로 이동한 다음 공유 서비스 VPC로 라우팅됩니다. Bastion에 액세스할 수 있게 되면 적절한 액세스 요청이 부여된 경우 AMS 환경의 다른 호스트로 이동할 수 있습니다.

  - 원하는 인스턴스 수(2개 권장)
  - 최대 인스턴스 수(4개 권장)
  - 최소 인스턴스(2개 권장)
  - 인스턴스 유형(m5.large 권장)
  - 수신 CIDRs: 네트워크의 사용자가 SSH Bastions에 액세스할 IP 주소 범위(ip 범위 1, ip 범위 2, ip 범위 3 등)

- RDP Bastion 설정

  AMS는 선택적으로 공유 서비스 계정에 RDP 접속을 제공하여 AMS 환경의 호스트에 액세스합니다. RDP 사용자로 AMS 네트워크에 액세스하려면 RDP Bastions를 진입점으로 사용해야 합니다. 네트워크 경로는 온프레미스 네트워크에서 시작되고 DX/VPN을 통해 TGW로 이동한 다음 공유 서비스 VPC로 라우팅됩니다. Bastion에 액세스할 수 있게 되면 적절한 액세스 요청이 부여된 경우 AMS 환경의 다른 호스트로 이동할 수 있습니다.

  - 인스턴스 유형(t3.medium 권장)
  - 원하는 최소 세션(2개 권장)

  - 원하는 최대 세션(10개 권장)
- RDP 접속 구성 유형, 공유 표준 또는 공유 HA(기본값은 공유 표준)

  SecureStandard = 사용자가 하나의 Bastion을 수신하고 한 명의 사용자만 Bastion에 연결할 수 있습니다.

  SecureHA = 사용자는 서로 다른 두 AZ에서 두 개의 Bastion을 수신하여 연결할 수 있으며 한 명의 사용자만 Bastion에 연결할 수 있습니다.

  SharedStandard = 사용자가 하나의 Bastion을 수신하여에 연결하고 두 사용자가 한 번에 동일한 Bastion에 연결할 수 있습니다.

  SharedHA = 한 사용자가 서로 다른 두 AZ에서 두 개의 접속을 수신하여 연결할 수 있고 두 사용자가 한 번에 동일한 접속에 연결할 수 있습니다.

연동

ID 제공업체(IDP) 이름

기본값은 `customer-saml`입니다.

AMS 단일 계정 랜딩 존(SALZ) 온보딩

AMS SALZ 온보딩 프로세스

AMS 단일 계정 랜딩 존(SALZ) 계정을 온보딩하려면 다음 단계를 수행해야 합니다.

1. AMS가 방화벽을 호스팅하기 위한 네트워킹 계정으로 구성하는 새 AWS 계정을 생성합니다. AWS 조직 내에 새 계정이 있는 경우 생성합니다. AMS는 일반 AMS 계정을 생성하는 절차를 따르므로 필요한 모든 정보(예: CIDR, EPS 라이선스 및 사용자)를 수집해야 합니다. 참고: CIDR 할당은 /24이면 좋습니다.
2. 송신 트래픽 계정에서 인터넷 게이트웨이(IGWs)를 제거할지 여부를 지정합니다.
3. 승인된 도메인을 확인합니다. AMS는 승인된 도메인 목록을 유지 관리하여 대상 필터링을 활성화합니다. 목록은 나중에 수정할 수 있습니다.
4. 예상 처리량에 따라 사용할 인스턴스 크기를 확인합니다. 기본적으로 인스턴스는 방화벽 처리량이 350Mbps인 것으로 확인된 m4.xlarge 인스턴스에 생성됩니다. AMS는 예상 처리량이 1.25Gbps인 c4.8xLarge 인스턴스로 크기를 늘릴 수 있습니다.
5. AMS와 프라이빗 네트워크 간에 네트워킹을 설정합니다. 여기에는 다음과 같은 다양한 작업이 포함됩니다.
    a. IP 공간 할당
    b. AWS에 대한 프라이빗 네트워크 연결 설정
    c. 방화벽 설정
    d. 액세스 관리 설정
    e. 백업 예약
6. 생성된 계정에 대한 액세스 권한을 AMS에 제공합니다.
7. AMS 서비스가 제대로 작동하는지 확인합니다.

AMS는 최초 요청일로부터 2주(영업일 기준 10일) 이내에 계정의 계정 빌드 아웃(온보딩)을 수행할 수 있습니다. 모든 후속 활동은 AMS 계획된 이벤트 관리(PEM)를 사용하여 수행할 수 있습니다.

> **Note**
>
> - 미국 동부(버지니아)

- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- 미국 동부(오하이오)
- 캐나다(중부)
- 남아메리카(상파울루)
- EU(아일랜드)
- EU(프랑크푸르트)
- EU(런던)
- EU 서부(파리)
- 아시아 태평양(뭄바이)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)

새 리전이 자주 추가됩니다. 최신 목록은 AWS 리전 및 가용 영역을 참조하세요.

SALZ 네트워크 아키텍처

다음 다이어그램은 AWS Managed Services(AMS) 단일 계정 랜딩 존(SALZ) VPC 네트워크 레이아웃을 나타내며 가용성이 높은 설정의 예입니다.

AMS는 표준 템플릿과 온보딩 중에 제공된 선택한 옵션을 기반으로 네트워킹의 모든 측면을 구성합니다. 표준 AWS 네트워크 설계가 AWS 계정에 적용되고 Virtual Private Cloud(VPC)가 생성되어 VPN 또는 Direct Connect를 통해 AMS에 연결됩니다. AWS Direct Connect에서 Direct Connect에 대해 자세히 알아보세요. 표준 VPCs에는 DMZ, 공유 서비스 및 애플리케이션 서브넷이 포함됩니다. 온보딩 프로세스 중에 필요에 맞게 추가 VPCs를 요청하고 생성할 수 있습니다(예: 고객 부서, 파트너). 온보딩 후에는 네트워크 다이어그램이 제공됩니다. 환경 문서는 네트워크 설정 방법을 설명합니다.

> **Note**
>
> 모든 활성 서비스의 기본 서비스 제한 및 제약 조건에 대한 자세한 내용은 AWS 서비스 제한 설명서를 참조하세요.

네트워크 설계는 Amazon "최소 권한 원칙"을 기반으로 구축되었습니다. 이를 위해 신뢰할 수 있는 네트워크에서 들어오는 트래픽을 제외한 모든 인바운드 및 아웃바운드 트래픽을 게이트웨이를 통해 라우팅합니다. 유일하게 신뢰할 수 있는 네트워크는 VPN 및/또는 AWS Direct Connect(DX)를 사용하여 온프레미스 환경과 VPC 간에 구성된 네트워크입니다. 접속 인스턴스를 사용하여 액세스 권한이 부여되므로 프로덕션 리소스에 직접 액세스할 수 없습니다. 모든 애플리케이션과 리소스는 퍼블릭 로드 밸런서를 통해 연결할 수 있는 프라이빗 서브넷 내에 있습니다. 퍼블릭 송신 트래픽은 순방향 프록시를 통해 인터넷 게이트웨이로 흐른 다음 인터넷으로 흐릅니다. 또는 트래픽이 VPN 또는 Direct Connect를 통해 온프레미스 환경으로 흐를 수 있습니다.

AMS 단일 계정 랜딩 존 공유 서비스

공유 서비스 서브넷에는 AMS Directory Services, 프로비저닝 및 일반 작업을 자동화하는 관리 호스트, 바이러스 백신(TrendMicro) 관리 서버 및 내부 접속 호스트가 포함됩니다.

- AMS 디렉터리 서비스 = AD 도메인 컨트롤러

  AMS 계정에서 Active Directory를 생성하고, AMS 도메인을 생성하고, 시작 시 관리형 스택을 도메인에 조인합니다.
- 관리 호스트 = AMS 관리 호스트(프로비저닝 및 일반 작업 자동화)

  API 엔드포인트 역할을 수행하여 Directory Service 도메인 컨트롤러를 수정 Directory Service하고 상호 작용합니다.
- 보안 서비스: 바이러스 백신(TrendMicro) 관리 서버 = EPS" + EPS 릴레이

  Trend Micro™ Deep Security 소프트웨어(DSM)를 활용하고, 클라이언트-서버 모델에서 작동하며, Deep Security 관리자, 에이전트 및 릴레이를 포함하는 백엔드 데이터베이스를 갖추고 있습니다.
- 내부 접속 호스트 = 고객 접속

  인터넷의 기본 액세스 포인트가 되고 다른 Amazon EC2 인스턴스에 대한 프록시 역할을 하도록 설계된 특수 목적 서버입니다.

SALZ: AMS에 대한 새 AWS 계정 생성

AWS Managed Services(AMS)에 대한 새 AWS 계정을 생성하는 5단계는 다음과 같습니다.

1. 생성 AWS 계정
2. 통합 결제 설정 - 새 계정을 지급인 계정에 연결
3. AMS 액세스를 AWS 계정 위한 구성
4. AMS의 루트 사용자에 대한 다중 인증(MFA)으로 새 계정 보호
5. AWS Marketplace EPS 구독

질문이 있는 경우 고객 서비스 제공 관리자(CSDM)에게 문의하십시오.

생성 AWS 계정

AMS 프로그램에는 새 Amazon Web Services(AWS) 계정을 프로비저닝해야 합니다. 단계별 지침은 다음 비디오에서 확인할 수 있습니다. 새 Amazon Web Services 계정을 생성하고 활성화하려면 어떻게 해야 하나요? 간단한 단계는 다음과 같습니다.

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 확인하고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요. AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

지침은 AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 그룹 추가를 참조하세요.

> **Note**
>
> 이미 계정이 있는 경우 AWS 요금 페이지로 이동하여 무료 계정 생성을 클릭할 수 있습니다. 최소한 EC2 서비스에 가입해야 합니다. 하나의 서비스에 가입하면의 모든 서비스에 액세스할 수 있습니다 AWS. 사용자에게는 사용한 서비스에 대해서만 요금이 청구됩니다.
> 통합 결제를 위해 새 계정을 지급인 계정에 연결하려는 경우 메시지가 표시되면 결제 방법 정보를 입력할 필요가 없습니다. 대신 화면에 도달하여 신용 카드 정보를 입력하면 탐색하기만 하면 됩니다. 다음 섹션에 자세히 설명된 통합 결제/연결 계정 요청을 보내려면 지급인 계정과 연결된 이메일 주소가 필요합니다.

> **Important**
>
> 잠재적 보안 인시던트에 대한 응답을 받을 수 있도록 이메일 주소와 전화번호가 계정과 연결되어 있는지 확인하는 것이 중요합니다. 계정의 전화번호와 이메일 주소는 계정 암호를 재설정하지 않으면 변경할 수 없습니다. 이는 AMS 루트 계정에 중요한 작업입니다. 이러한 값이 안정적인지 확인하려면 개인과 연결되지 않은 연락처 정보를 선택하는 것이 중요하며, 이는 변경될 수 있습니다. 그룹을 가리킬 수 있는 이메일 별칭을 선택합니다. 전화번호를 선택할 때와 동일한 모범 사례를 따릅니다. 즉, 개인이 아닌 회사가 소유한 번호 또는 그룹을 가리킬 수 있는 번호를 선택합니다.

통합 결제 설정 - 새 계정을 지급인 계정에 연결

새 AMS 관리형 AWS 계정 청구서를 기존 AWS Organizations 관리 계정의 결제로 롤업하려면 통합 결제를 설정하고 계정을 연결해야 합니다. 이에 대한 자세한 내용은 섹션을 참조하세요.

- 및 다중 계정 결제 전략에 대한 통합 AWS Organizations 결제. AWS
- 조직에 가입 AWS 계정 하도록 초대

> **Note**
>
> AMS로 계정을 인계하기 전에 다음 단계를 수행할 수 있습니다. 인계 후에는 변경 관리 프로세스를 통해 조직에 가입하기 위한 단계(위에 제공됨)를 수행할 수 있습니다. 도움이 필요한 경우 클라우드 서비스 제공 관리자(CSDM) 또는 클라우드 아키텍트(CA)에게 문의하세요.

통합 결제 관리를 포함한 일반 결제 정보는 AWS 결제란 무엇입니까?를 참조하세요. 계정이 함께 작동하는 방법에 대한 일반적인 AWS Organizations 내용은 란 AWS Organizations 무엇입니까?를 참조하십시오. AWS Organizations 관리 계정에 대한 권장 지침은 관리 계정, 신뢰할 수 있는 액세스 및 위임된 관리자를 참조하세요.

AMS 액세스를 AWS 계정 위한 구성

위의 단계를 완료하면 새를 성공적으로 보호하고 관련 비용이 적절하게 청구되도록 AWS 계정 할 수 있습니다. 프로세스의 마지막 단계는 초기 스택 구성과 지속적인 변경 및 프로비저닝 요청을 이행하기 위해 새 계정에 대한 AMS 액세스를 허용하는 것입니다. 자세한 내용은 IAM 역할을 사용하여 AWS 계정 간 액세스 권한 위임을 참조하세요. 기본 단계는이 단원에서 설명합니다.

AWS 웹 사이트에 대한 액세스 활성화

IAM 사용자에게 계정의 결제 정보 및 도구에 대한 액세스 권한을 부여하려면 기능을 활성화해야 합니다.

다음 단계를 따릅니다.

1. 루트 계정 자격 증명(을 생성하는 데 사용한 이메일 및 암호) AWS Management Console 을 사용하여에 로그인합니다 AWS 계정. IAM 사용자 자격 증명을 사용하여 로그인하지 마십시오.

   AWS Management Console 홈 페이지가 열립니다.
2. 상단 탐색 모음에서 계정 이름의 드롭다운 메뉴를 연 다음 내 계정을 선택합니다.

   결제 홈 페이지가 열립니다.
3. 결제 정보에 대한 IAM 사용자 액세스 영역까지 아래로 스크롤하고 오른쪽에 있는 편집을 클릭합니다. ## ## #### ##### ### ### #### ####.

   IAM 액세스 활성화 영역이 열립니다.
4. 확인란을 선택하고 업데이트를 클릭합니다.

이제 사용자가 액세스할 수 있는 페이지는 IAM 정책을 통해 제어할 수 있습니다.

의이 프로세스에 대한 자세한 내용은 액세스 권한 관리 개요를 AWS참조하세요. https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/control-access-billing.html

AWS 웹 사이트에 액세스할 수 있는 IAM 역할 생성

AWS Identity and Access Management (IAM)는 사용자의 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 웹 서비스입니다. IAM을 사용하여 AWS 리소스를 사용할 수 있는 사용자(인증)와 사용할 수 있는 리소스 및 방법(권한 부여)을 제어할 수 있습니다.

1. IAM 관리 콘솔로 이동하여 왼쪽 탐색 창에서 역할을 클릭합니다.

   IAM 역할에 대한 정보, 역할 생성 옵션 및 기존 역할 목록이 포함된 역할 관리 페이지가 열립니다.

2. 역할 생성을 클릭합니다.

   역할 생성 신뢰할 수 있는 엔터티 유형 선택 페이지가 열립니다. 다른 AWS 계정을 클릭하면 아래에 설정 영역이 열립니다.

   AMS에서 제공한 AMS 신뢰할 수 있는 계정 ID를 입력합니다.
   외부 ID 필요 및 MFA 필요 옵션을 선택 취소한 상태로 둡니다.

3. Next: Permissions(다음: 권한)를 클릭합니다.

   역할 생성 권한 정책 연결 페이지가 열리고 새 정책을 생성하고, 페이지를 새로 고치고, 기존 정책을 검색하는 옵션이 표시됩니다. 기존 정책 목록이 제공됩니다.

4. AdministratorAccess 정책을 선택한 후 다음: 검토를 클릭합니다.

   역할 생성 검토 페이지가 열립니다.

5. 새 역할의 이름을 aws_managedservices_onboarding_role로 지정하고 역할 설명에 "AMS 온보딩 역할"을 입력합니다. 새 역할의 설정을 검토하고 충족되면 역할 생성을 클릭합니다.

   새 역할이 나열된 역할 관리 페이지가 열립니다.

AWS Marketplace EPS 구독

최근 AMS 엔드포인트 보안(EPS)을 변경하려면를 통해 TrendMicro Deep Security를 구독 AWS Marketplace 하고 소프트웨어 약관에 동의해야 합니다.

TrendMicro는 보호된 인스턴스 시간당 및 기존 보유 라이선스 사용(BYOL)이라는 두 가지 라이선스 모델을 제공합니다.

- BYOL:
  1. 외부 채널을 통해 구매한 자체 라이선스를 사용합니다.
  2. EPS 인프라를 빌드하려면 AMS에 모든 라이선스 키를 제공해야 합니다. 모든 모듈에 라이선스를 부여하는 활성화 코드 또는 특정 모듈 세트에 라이선스를 부여하는 개별 활성화 코드를 제공할 수 있습니다. AMS는 사용자가 제공하는 활성화 코드에 해당하는 라이선스 파일만 생성합니다. 온보딩 중에 라이선스 활성화가 수행되므로 AMS 리드 엔지니어와 CSDM이 있는 경우 해당 정보를 공유할 수 있습니다.
  3. 또한 BYOL TrendMicro Market Place AMI 구독을 구독해야 합니다. Trend Micro Deep Security(BYOL)를 참조하세요.
- 보호된 인스턴스 시간당:
  1. 이 구독에서는 이전에 조달한 Trend 라이선스가 없어도 됩니다.
  2. 그러나 Marketplace 구독을 구독해야 합니다.
  3. 이 모델에서는 소프트웨어 라이선스 + EC2 인프라 사용량을 포함하여 추세 사용량이 자동으로 측정되므로 AMS와의 라이선스 키 공유가 필요하지 않습니다. Trend Micro Deep Security를 참조하세요.

Trend Micro를 구독하려면 다음 단계를 따르세요.

1. 에 로그인합니다 AWS 계정.
2. Trend Micro Deep Security(BYOL 또는 보호된 인스턴스 시간당) 제품 페이지로 이동합니다.
3. 오른쪽 패널에서 계속을 클릭하여 구독합니다.
4. 오른쪽 상단 모서리에서 약관 수락을 클릭합니다.

Trend Micro Deep Security에서 IDS 및 IPS 활성화

AMS가 계정에 대해 기본이 아닌 기능인 Trend Micro Intrusion Detection System(IDS) 및 Intrusion Protection Systems(IPS)를 활성화하도록 요청할 수 있습니다.

이렇게 하려면 업데이트 요청(관리 | 기타 | 기타 | 업데이트)을 제출하고 IDS 및 IPS 알림을 수신할 이메일 주소 목록을 포함합니다. 이러한 주소는 AMS가 자동으로 생성하는 계정의 SNS 주제에 추가됩니다.

> **Note**
>
> AMS는 다른 AMS 서비스를 제공하는 기능을 방해할 수 있는 Trend Micro 서비스를 추가할 수 없습니다.

다음 단계: AMS의 루트 사용자에 대한 다중 인증(MFA)으로 새 계정 보호

AWS Marketplace CentOS 7.6 구독

AMS는 이제 CentOS 7(x86_64) - Centos.org 판매된 Updates HVM을 AMS AMI로 제공합니다. 이 AMI를 활용하려면 무료 Cent OS 라이선스를 옵트인하고 모든 AMS 계정에서 라이선스를 수락해야 합니다.

구독하려면 AWS Marketplace 로 이동하여 옵트인 지침을 따르세요.

이 제품 사용에 대한 소프트웨어 요금은 발생하지 않지만 EC2 사용을 포함한 다른 AWS 요금은 여전히 사용자가 부담해야 합니다. '소유 라이선스 사용' 제품인 경우 사용하려면 유효한 소프트웨어 라이선스가 있어야 합니다.

CentOS 7(x86_64) - Updates HVM에서이 소프트웨어에 대한 정보를 검토할 수 있습니다.

AMS의 루트 사용자에 대한 다중 인증(MFA)으로 새 계정 보호

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 AWS 아티팩트 시작하기를 참조하세요.

SALZ: 네트워킹 설정

AWS Managed Services(AMS)에 대한 네트워킹을 설정하려면 몇 가지 프로세스를 완료해야 합니다.

1. AMS 환경에 IP 공간 할당
2. AWS에 대한 프라이빗 네트워크 연결 설정

3. AMS 작업을 허용하도록 방화벽 설정

AMS 환경에 IP 공간 할당

AMS는 권장 네트워크 할당으로 /16 CIDR 블록을 사용하여 설계되고 테스트되었습니다. AMS에 연결된 신뢰할 수 있는 네트워크는 AMS에 할당된 CIDR 블록과 겹치지 않는 CIDR 블록을 사용하는 것이 중요합니다. 이러한 주소는 Virtual Private Cloud(VPC) 및 서브넷을 설정하는 데 필요합니다. AWS VPCs에 대한 자세한 내용은 Amazon VPC 제한 및 Amazon VPC FAQs.

/16 CIDR 블록은 많은 IP 주소처럼 보일 수 있지만 일단 생성되면 VPC를 확장할 수 없습니다. 따라서 이 할당을 통해 AMS 관리형 VPC가 상당한 기간 동안 작동할 수 있습니다. CIDR 블록 내에서 최소 2개의 프라이빗 서브넷과 2개의 퍼블릭 서브넷에 IP 주소 범위를 할당해야 합니다.

AWS는 네이티브 AWS Virtual Private Network(VPN) 기능을 통해 AMS 환경에 대한 연결을 허용합니다. AWS Direct Connect(DX), 하드웨어 VPN 또는 소프트웨어 VPN을 통해 이를 달성할 수 있습니다. AMS 측에서는 VPCs의 가상 게이트웨이 기능을 사용합니다.

기본 환경 구성 요소

사용자 Network-to-Amazon VPC 연결 옵션	
하드웨어 VPN	원격 네트워크의 네트워크 장비에서 VPC에 연결된 AMS 관리형 네트워크 장비로의 하드웨어 VPN 연결을 설정합니다.
AWS Direct Connect(DX)	AWS Direct Connect를 활용하여 원격 네트워크에서 Amazon VPC로의 프라이빗 논리적(또는 VPN과 함께 사용되는 경우 암호화된) 연결을 설정합니다.
소프트웨어 VPN	원격 네트워크의 장비에서 Amazon VPC 내에서 실행되는 사용자 관리형 소프트웨어 VPN 어플라이언스로 VPN 연결을 설정합니다.

> **Note**
>
> AMS는 DX에 대한 중복 프라이빗 VPN 연결을 권장합니다. 고객 서비스 제공 관리자(CSDM)는 계정 온보딩 시이 설정을 지원합니다.

AWS에 대한 프라이빗 네트워크 연결 설정

회사 Active Directory에 AMS를 추가하여 연결을 설정합니다. 프라이빗 네트워킹 연결을 통해 관리 작업 또는 사용자 액세스를 수행할 수 있습니다. AWS는 VPN 연결과를 통한 전용 라인을 모두 제공합니다 Direct Connect. 다음 단계에서는 AMS로 작업하여 연결 수단 중 하나(또는 둘 다)를 설정하는 방법을 설명합니다.

VPN 설정

이 섹션에서는 AMS 관리형 VPC와 내부 네트워크 간에 통신하도록 VPN을 설정하는 기본 단계를 설명합니다.

> **Note**
>
> AWS 서비스에서 VPN을 사용하는 방법에 대한 전반적인 이해를 얻으려면 AWS Site-to-Site VPN이란 무엇입니까?와 고객 게이트웨이(VPN 어플라이언스)에 대한 모든 것을 참조하세요.

AWS VPN 사용 설명서 시작하기 및 Site-to-Site VPN 연결 테스트 섹션에 따라 다음 단계를 완료합니다.

- 1단계: AWS VPC에서 고객 게이트웨이 생성
- 2단계: AWS VPC에서 가상 프라이빗 게이트웨이 생성
- 3단계: AWS VPC에서 라우팅 테이블에서 라우팅 전파 활성화
- 4단계: AWS VPC에서 인바운드 SSH, RDP 및 ICMP 액세스를 활성화하도록 보안 그룹 업데이트
- 5단계: 내부 네트워크에서 VPN 연결 생성 및 고객 게이트웨이 구성
- 6단계: VPC와 내부 네트워크 간의 VPN 연결 테스트

Direct Connect 설정

이 섹션에서는 AMS 관리형 VPC와 내부 네트워크 간에 통신하도록 Direct Connect (DX)를 설정하는 기본 단계를 설명합니다.

> **Note**
>
> AWS 서비스에서 DX를 사용하는 방법에 대한 자세한 내용은 Direct Connect 위치에서 시작하기를 참조하세요.

DX 연결을 설정하려면 다음 단계를 완료해야 합니다.

1. Amazon Web Services 가입
2. AWS Direct Connect 연결 요청 제출
3. 교차 연결 완료
4. (선택 사항) AWS Direct Connect를 사용한 중복 연결 구성
5. AMS에서 수행: 가상 인터페이스 생성
6. AMS에서 수행: 라우터 구성 다운로드
7. 가상 인터페이스 확인

방화벽 설정

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 AWS 아티팩트 시작하기를 참조하세요.

애플리케이션 마이그레이션/온보딩 중 AMS 접속 옵션

마이그레이션 작업 중에 최상의 경험을 제공하기 위해 AMS가 현재 활용할 수 있는 잠재적 옵션은 다음과 같습니다.

- 옵션 1: 마이그레이션 작업에만 Bastions를 우회합니다(임시 조치로 보안을 위해 이를 승인해야 함).

  참고: AMS가 각 요청을 볼 수 있도록 감사 기능이 계속 유지됩니다.
- 옵션 2: 선택한 도구를 사용한 SSH 터널링. 예를 들어 그림과 같이 PuTTy.

  이 옵션을 사용하려면 설명된 환경 구성 요소가 이미 있어야 합니다.

  AMS는 추가 참고 사항과 지침을 제공합니다.

PuTTy를 사용한 SSH 터널링 단계:

PuTTY 내에서 Bastion Host의 퍼블릭 IP를 사용하여 SSH 세션을 생성하고 AUTH 섹션에 PEM 키를 제공한 다음 터널을 생성합니다. 터널의 소스 포트는 미사용 로컬 포트(예: 5000)여야 하며 IP는 RDP 포트(3389)가 추가된 대상 호스트(연결하려는 Windows 상자)의 IP입니다. 상자에 로그인할 때마다 구

성을 저장하지 않아도 되므로 구성을 저장해야 합니다. 접속 호스트에 연결하고 로그인합니다. 그런 다음 localhost:5000(또는 선택한 포트)에 대한 RDP 세션을 시작합니다.

1. 접속 호스트의 호스트 이름 또는 퍼블릭 IP 설정

2. SSH -> 인증에서 프라이빗 키 파일을 .ppk 형식으로 설정합니다.

3. SSH -> 터널에서 전달된 새 포트를 추가합니다. 소스 포트는 임의의 미사용 포트여야 하며, 대상은 RDP 포트가 추가된 Bastion Host 뒤의 대상 서버의 IP여야 합니다.

4. PuTTY를 통해 접속 호스트에 연결하고 로그인합니다.

5. localhost:5000에 대한 RDP 세션을 시작하여 대상 서버에 도달합니다.

SALZ: 액세스 관리 설정

AWS Managed Services(AMS)에서 관리하는 네트워크를 사용하는 것은 AMS에 클라우드 인프라를 관리할 수 있는 액세스 권한을 부여하는 것을 의미합니다. 프라이빗 네트워크와 AMS 간에 안전하게 연결하는 수단을 구성해야 합니다. 이는 제공하려는 액세스 유형에 대한 몇 가지 결정으로 시작됩니다.

- AMS API/CLI 및 콘솔 액세스의 경우: AMS CLI를 설치하려고 합니다(이 문서에서는 지침이 제공됨). AMS 변경 관리 API를 사용하여 AMS 및 AMS SKMS API에 대한 변경 요청을 하여 AMS 관리형 리소스에 대해 알아봅니다. Active Directory Federation Services(AD FS)를 사용하여 AMS 콘솔에 액세스할 수 있습니다.

  > **Note**
  >
  > 자체 ITSM을 설정하는 경우 서비스 요청 및 인시던트 보고서에 AWS Support API(SAPI)를 사용해야 합니다. SAPI는 AWS 지원 API 참조에 설명되어 있습니다.

- 사용자 액세스의 경우: Windows Active Directory(AD) 또는 Linux/LDAP 솔루션으로 사용자를 관리하든 AMS 측의 AD(디렉터리 서비스를 통해)와 디렉터리 간에 연결을 설정해야 합니다.
- 인스턴스 액세스의 경우: 인스턴스 수준 액세스는 단방향 포리스트 신뢰 구성을 통해 수행됩니다. Directory Services는 CORP AD에서 자격 증명을 신뢰하므로 AMS 측 내의 스택에서 CORP 자격 증명으로 로그인할 수 있습니다.

AMS가 신뢰를 설정하는 Active Directory(AD)는 AWS 리소스에 대한 액세스 권한을 부여받은 사용자의 계정이 있는 디렉터리여야 합니다.

> **Important**
>
> 포리스트 신뢰를 설정하려면 AMS에 도메인 컨트롤러 로컬 정책 -> 보안 옵션 -> 네트워크 액세스: 익명으로 액세스할 수 있는 명명된 파이프가 있어야 합니다. Netlogon 및 lsarpc 파이프가 나열됩니다. 이러한 파이프는 기본적으로 나열되지만 보안 문제로 인해 제거되는 경우도 있습니다. 신뢰가 설정되면 목록에서 다시 제거할 수 있습니다.

Active Directory(AD) 신뢰 설정

AWS Managed Services(AMS) 계정에 대한 Active Directory(AD) 신뢰를 설정하기 전에 적절한 방화벽 포트가 열려 있는지 확인합니다.

AMS 관리형 Active Directory 및 기업 디렉터리 서비스의 신뢰를 통해 기업 관리형 자격 증명을 사용하여 AMS 관리형 인스턴스에 액세스하여 개발, 테스트 또는 관리 기능을 수행할 수 있습니다.

신뢰 연결 생성은 두 부분으로 구성된 연습입니다.

먼저 DNS 쿼리가 어떤 DNS 서버로 이동할지 알 수 있도록 DNS 구성인 조건부 전달을 구성합니다.

둘째, 한 도메인의 사용자가 다른 도메인의 리소스를 사용하도록 액세스를 허용하는 Active Directory(AD) 구성인 신뢰를 구성합니다.

조건부 전달자 구성

이 Microsoft AD 문서 도메인 이름에 조건부 전달자 할당을 따르고 다음 설정 및 선택을 사용합니다.

1. AD DNS 관리자 -> 새 조건부 전달자 생성의 DNS 도메인에서 제공된 도메인 이름 AMS를 사용합니다. 예: *A523434123.amazonaws.com*.
2. 마스터 서버의 IP 주소에서 AMS에서 제공하는 IP 주소를 추가합니다. 두 주소를 모두 검증하여 연결 문제가 없는지 확인합니다.
3. 이 조건부 전달자를 Active Directory에 저장을 선택하고 다음과 같이 복제합니다.이 도메인의 모든 DNS 서버를 선택하고 확인을 누릅니다.

신뢰 구성

AWS Managed Services(AMS) 계정에 대한 신뢰를 구성하려면이 섹션에 설명된 설정 및 선택 사항을 사용하여 신뢰의 한쪽에 대한 단방향 수신 포리스트 신뢰 생성 MicroSoft AD 문서를 따르세요. https://technet.microsoft.com/en-us/library/cc756735%28v=ws.10%29.aspx

1. 시작 -> 관리 도구 -> Active Directory 도메인 및 신뢰 대화 상자를 엽니다. 신뢰를 설정할 도메인의 도메인 노드를 마우스 오른쪽 버튼으로 클릭한 다음 속성 -> 신뢰 -> 새 신뢰를 클릭하여 새 신뢰 마법사를 엽니다. 신뢰 이름에 AMS에서 제공한 도메인 이름을 입력하고 다음을 누릅니다.
2. 신뢰 유형에서 포리스트 신뢰를 선택합니다. 다음(Next)을 누릅니다.
3. 신뢰 방향에서 단방향: 수신을 선택합니다. 다음(Next)을 누릅니다.
4. 신뢰의 측면에서 이 도메인만 선택합니다. 다음(Next)을 누릅니다.
5. 암호 신뢰에서 선택한 암호를 입력합니다. 다음(Next)을 누릅니다.
6. 신뢰 선택 완료 및 신뢰 생성 완료에서 다음을 누릅니다.
7. 수신 신뢰 확인에서 아니요, 수신 신뢰 확인 안 함을 선택합니다. 다음(Next)을 누릅니다.
8. 새 신뢰 마법사 완료에서 완료를 선택한 다음 확인을 선택하여 닫습니다.
9. 신뢰 암호를 제공합니다(보안상의 이유로 CSDM의 전화번호를 통해 문의). AMS는 신뢰 구성을 완료합니다.

Active Directory 사이트 및 서비스

로그인 지연 시간을 줄이려면 Active Directory 사이트 및 서비스(시작 -> 관리 도구 -> Active Directory 사이트 및 서비스)에 VPC CIDR 범위를 추가합니다. AWS에 가장 가까운 도메인 컨트롤러가 포함된 Active Directory 사이트에 VPC CIDR 범위를 추가합니다.

Active Directory 이름 접미사 라우팅

단방향 포리스트 신뢰가 설정되면 추가 단계를 완료하세요.

1. 시작 > 모든 프로그램 > 관리 도구에서 Active Directory 도메인 및 신뢰를 클릭합니다.

   Active Directory 도메인 및 신뢰 콘솔이 열립니다.
2. 회사 도메인을 마우스 오른쪽 버튼으로 클릭하고 속성을 클릭합니다.

   해당 도메인의 속성 대화 상자가 열립니다.
3. 신뢰 탭을 클릭합니다.

신뢰 페이지가 열립니다.

4. Amazon 도메인 이름을 클릭하고 속성을 클릭합니다.

   Amazon 도메인 신뢰의 속성 페이지가 열립니다.

5. 이름 접미사 라우팅을 클릭하고 새로 고침을 클릭합니다.

   이 단계를 통해 서비스 보안 주체 이름(SPNs)이 신뢰를 통해 확인할 수 있습니다.

문제 해결

문제가 발생할 경우 몇 가지 시도할 사항은 다음과 같습니다.

- AMS 관리형 Active Directory 아웃바운드 보안 그룹은 CIDR 블록(예: 10.27.0.0/16)을 통해 도메인 컨트롤러에 연결할 수 있어야 합니다.
- AWS 콘솔에서 도메인 컨트롤러에서 도메인 컨트롤러로의 경로를 추적하여 모든 보안 그룹을 확인합니다.
- 인터넷 제어 메시지 프로토콜(ICMP)이 허용되는 경우 AMS 관리형 Active Directory 도메인 컨트롤러를 ping할 수 있는지 확인합니다.
- 도메인 컨트롤러가 AWS Directory Services와 통신할 수 있는지 확인합니다.
- 조건부 전달자가 확인되고 검증되었는지 확인합니다.
- 새 신뢰 마법사에 Forest Trust가 표시되지 않으면 조건부 전달자가 제대로 작동하지 않을 수 있습니다.
  - nslookup을 사용하여 해상도 테스트
  - 도메인 컨트롤러 재부팅 시도

AMS 관리형 Active Directory

AMS는 이제 AMS가 Active Directory(AD) 인프라 작업을 관리하는 동시에 Active Directory 관리를 제어할 수 있도록 하는 Managed Active Directory(Managed AD)라는 새로운 서비스를 제공합니다.

Managed AD에 대한 AMS 지원은 Amazon Relational Database Service(RDS)에 대한 AMS 지원과 유사합니다. 두 경우 모두 AWS (AMS 포함)는 액세스 제어 및 모든 관리 기능을 수행하는 동안 서비스를 실행하는 인프라의 생성 및 관리를 지원합니다. 이 모델의 장점은 다음과 같습니다.

- 보안 위험을 제한합니다. AWS 또한 AMS에는 도메인에 대한 관리 권한이 필요하지 않습니다.

- 직접 통합: AMS와 인터페이스할 필요 없이 현재 권한 부여 모델을 사용하고 AD와 통합할 수 있습니다.

참고:

- AMS와 사용자 모두 Managed AD 도메인 컨트롤러에 액세스할 수 없으므로 도메인 컨트롤러에 소프트웨어를 설치할 수 없습니다. 이는 도메인 컨트롤러에 소프트웨어를 설치해야 하는 타사 솔루션이 허용되지 않기 때문에 중요합니다.

  액세스는 다음과 같이 작동합니다.

  - AWS 디렉터리 서비스 팀: 도메인 컨트롤러에 액세스할 수 있습니다.
  - AMS: 디렉터리 서비스 APIs에 액세스하여 도메인에서 특정 작업을 수행할 수 있습니다. 이러한 작업에는 AD 스냅샷 생성, AD 스키마 변경 및 기타 작업이 포함됩니다.
  - 사용자: 사용자, 그룹 등을 생성하기 위해 도메인(AD)에 액세스할 수 있습니다.
- 기존 AD 환경의 모든 기능을 관리형 AD 환경에서 사용할 수 있는 것은 아니므로 기업 AD를 마이그레이션하기 전에 관리형 AD에 대한 개념 증명을 수행하는 것이 좋습니다.
- AMS는 AD 관리를 관리하거나 이에 대한 지침을 제공하지 않습니다. 예를 들어 AMS는 조직 단위 구조, 그룹 정책 구조, AD 사용자 이름 지정 규칙 등에 대한 지침을 제공하지 않습니다.

다음과 같이 작동합니다.

1. AMS는 AMS 계정과 AWS 계정 별개로 새를 온보딩하고 Directory Service를 통해 Active AWS Directory(AD) 환경을 프로비저닝합니다(AWS Directory Service란 무엇입니까? 참조).

   다음은 AMS가 Managed AD에 온보딩하기 위해 시스템 통합자가 사용자로부터 수집해야 하는 정보입니다.

   - 계정 정보
     - AMS 관리형 AD: AWS 계정 number에 대해 AWS 계정 생성된의 계정 ID
     - Managed AD를 온보딩할 리전: AWS 리전
   - 관리형 Active Directory 정보:
     - Microsoft AD Edition: Standard/Enterprise. AWS Microsoft AD(Standard Edition)에는 1GB의 디렉터리 객체 스토리지가 포함되어 있습니다. 이 용량은 최대 5,000명의 사용자 또는 사용자, 그룹, 컴퓨터를 포함한 30,000개의 디렉터리 객체를 지원할 수 있습니다. AWS Microsoft AD(Enterprise Edition)에는 최대 100,000명의 사용자 또는 500,000개의 객체를 지원할 수 있는 17GB의 디렉터리 객체 스토리지가 포함되어 있습니다.

자세한 내용은 AWS Directory Service FAQs.

- 도메인 FQDN: AMS 관리형 AD 도메인의 FQDN입니다.
- 도메인 NetBIOS 이름: AMS 관리형 AD 도메인의 NetBIOS 이름입니다.
- Managed AD 통합을 원하는 AMS 표준 계정의 계정 번호(AMS는 AMS 표준 계정의 AD에서 Managed AD로의 단방향 신뢰 구성)
- Active Directory 스키마 수정이 필요하고 필요한 경우 어떤 수정이 필요합니까?
- 기본적으로 두 개의 도메인 컨트롤러가 프로비저닝됩니다. 더 필요합니까? 그렇다면 필요한 것은 몇 개이며 그 이유는 무엇입니까?

- 관리형 Active Directory에 대한 네트워킹 정보:
  - 도메인 컨트롤러용 관리형 AD VPC CIDR(관리형 AD 도메인 컨트롤러용 프라이빗 서브넷 범위의 CIDR):
    - 도메인 컨트롤러용 서브넷 CIDR 1: [CIDR, AMS 관리형 AD VPC CIDR의 일부여야 함]
    - 도메인 컨트롤러용 서브넷 CIDR 2: [CIDR, AMS 관리형 AD VPC CIDR의 일부여야 함]

    예:

    - 관리형 AD VPC CIDR: 192.168.0.0/16
    - 도메인 컨트롤러의 CIDR 1: 192.168.1.0/24
    - 도메인 컨트롤러의 CIDR 2: 192.168.2.0/24

    IP 주소 충돌을 방지하려면 지정한 Managed AD VPC CIDR이 회사 네트워크에서 사용 중인 다른 프라이빗 서브넷 CIDR과 충돌하지 않도록 해야 합니다.
  - VPN 기술(선택 사항): [Direct Connect/Direct Connect 및 VPN]
    - 게이트웨이의 BGP 자율 시스템 번호(ASN): [고객 제공 ASN]
    - 게이트웨이 외부 인터페이스의 인터넷 라우팅 가능 IP 주소입니다. 주소는 정적이어야 합니다. [고객 제공 IP 주소]
    - VPN 연결에 정적 경로가 필요한지 여부: [예/아니요]

2. AMS는 AD 환경에 대한 관리자 계정 암호를 제공하고 AMS 엔지니어가 더 이상 AD 환경에 액세스할 수 없도록 암호를 재설정하도록 요청합니다.
3. 관리자 계정 암호를 재설정하려면 Active Directory 사용자 및 컴퓨터(ADUC)를 사용하여 Active Directory 환경에 연결합니다. ADUC 및 기타 원격 서버 관리 도구(RSAT)는 비 AMS 인프라에서 사용자가 프로비저닝한 관리 호스트에 설치하고 실행해야 합니다. Microsoft에는 이러한 관리 호스트를 보호하는 모범 사례가 있습니다. 자세한 내용은 보안 관리 호스트 구현을 참조하세요. 이러한 관리 호스트를 사용하여 Active Directory 환경을 관리합니다.

4. 일상적인 작업에서 AMS는 VPC 구성, AD 백업, AD 신뢰 생성 및 삭제 등과 같은 사물의 AWS 디렉터리 서비스 측 AWS 계정 까지를 관리합니다. 사용자 생성, 그룹 생성, 그룹 정책 생성 등과 같은 AD 환경을 사용하고 관리합니다.

최신 RACI 테이블은 서비스 설명 참조의 "역할 및 책임" 섹션을 참조하세요.

Active Directory를 AMS AWS Identity and Access Management 역할과 연동

디렉터리를 AMS IAM 역할과 페더레이션하는 목적은 기업 사용자가 회사 자격 증명을 사용하여 및 AWS APIs, 따라서 AMS 콘솔 및 API와 AWS Management Console 상호 작용할 수 있도록 하는 것입니다. APIs

페더레이션 프로세스 예제

이 예제에서는 Active Directory Federation Services(AD FS)를 사용하지만 AWS Identity and Access Management 페더레이션을 지원하는 모든 기술이 지원됩니다. AWS 지원되는 IAM 페더레이션에 대한 자세한 내용은 IAM 파트너 및 자격 증명 공급자 및 페더레이션을 참조하세요. CSDM은 AD 팀 및 AMS와의 공동 노력이 필요한이 프로세스를 안내합니다.

API 액세스를 위한 SAML 통합에 대한 자세한 내용은이 AWS 블로그인 SAML 2.0 및 AD FS를 사용하여 페더레이션 API 및 CLI 액세스를 구현하는 방법을 참조하세요.

> **Note**
>
> AMS CLI 및 SAML을 설치하는 예제는 섹션을 참조하세요부록: ActiveDirectory Federation Services(ADFS) 클레임 규칙 및 SAML 설정.

AMS 콘솔에 대한 페더레이션 구성(SALZ)

다음 표에 자세히 설명된 IAM 역할 및 SAML 자격 증명 공급자(신뢰할 수 있는 엔터티)가 계정 온보딩의 일부로 프로비저닝되었습니다. 이러한 역할을 사용하면 RFCs, 서비스 요청 및 인시던트 보고서를 제출 및 모니터링하고 VPCs 및 스택에 대한 정보를 얻을 수 있습니다.

역할	ID 제공업체	권한
Customer_ReadOnly_역할	SAML	표준 AMS 계정의 경우. RFCs 제출하여 AMS 관리형 인프라를 변경하고 서비스 요청 및 인시던트를 생성할 수 있습니다.
customer_managed_ad_user_역할	SAML	AMS Managed Active Directory 계정의 경우. AMS 콘솔에 로그인하여 서비스 요청 및 인시던트(RFCs.

다른 계정에서 사용할 수 있는 역할의 전체 목록은 섹션을 참조하세요AMS의 IAM 사용자 역할.

온보딩 팀원은 연동 솔루션의 메타데이터 파일을 미리 구성된 자격 증명 공급자에 업로드합니다. 조직의 사용자가 AWS 리소스에 액세스할 수 있도록 Shibboleth 또는 Active Directory Federation Services와 같은 SAML 호환 IdP(자격 증명 공급자) 간에 신뢰를 구축하려는 경우 SAML 자격 증명 공급자를 사용합니다. IAM의 SAML 자격 증명 공급자는 위의 역할을 가진 IAM 신뢰 정책에서 보안 주체로 사용됩니다.

다른 페더레이션 솔루션은 AWS에 대한 통합 지침을 제공하지만 AMS에는 별도의 지침이 있습니다. 아래 제공된 수정 사항과 함께 Windows Active Directory, AD FS 및 SAML 2.0을 사용하여 AWS에 페더레이션 활성화 블로그 게시물을 사용하면 기업 사용자가 단일 브라우저에서 여러 AWS 계정에 액세스할 수 있습니다.

블로그 게시물에 따라 신뢰 당사자 신뢰를 생성한 후 다음과 같이 클레임 규칙을 구성합니다.

- NameId: 블로그 게시물을 따릅니다.
- RoleSessionName: 다음 값을 사용합니다.
  - 클레임 규칙 이름: RoleSessionName
  - 속성 저장소: Active Directory
  - LDAP 속성: SAM-Account-Name
  - 발신 클레임 유형: https://aws.amazon.com/SAML/Attributes/RoleSessionName
- AD 그룹 가져오기: 블로그 게시물을 따릅니다.
- 역할 클레임: 블로그 게시물을 따르지만 사용자 지정 규칙의 경우 다음을 사용합니다.

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
RegExReplace(c.Value, "AWS-([^d]{12})-",
"arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

AD FS를 사용하는 경우 다음 표에 표시된 형식으로 각 역할에 대한 Active Directory 보안 그룹을 생성해야 합니다(customer_managed_ad_user_role은 AMS Managed AD 계정 전용).

그룹	역할
AWS-[AccountNo]-Customer_ReadOnly_Role	Customer_ReadOnly_역할
AWS-[AccountNo]-customer_managed_ad_user_role	customer_managed_ad_user_역할

자세한 내용은 인증 응답에 대한 SAML 어설션 구성을 참조하세요.

> **Tip**
>
> 문제 해결에 도움이 되도록 브라우저용 SAML 추적기 플러그인을 다운로드합니다.

AMS에 페더레이션 요청 제출

첫 번째 계정인 경우 CSDM(들) 및/또는 클라우드 아키텍트(들)와 협력하여 자격 증명 공급자에 대한 메타데이터 XML 파일을 제공합니다.

추가 계정 또는 자격 증명 공급자를 온보딩하고 관리 계정 또는 원하는 애플리케이션 계정에 액세스할 수 있는 경우 다음 단계를 따릅니다.

1. AMS 콘솔에서 서비스 요청을 생성하고 자격 증명 공급자를 추가하는 데 필요한 세부 정보를 제공합니다.
   - 새 자격 증명 공급자가 생성될 계정의 AccountId입니다.
   - 원하는 자격 증명 공급자 이름이 제공되지 않은 경우 기본값은 customer-saml입니다. 일반적으로 이는 페더레이션 공급자에 구성된 설정과 일치해야 합니다.
   - 기존 계정의 경우 새 자격 증명 공급자를 모든 기존 콘솔 역할에 전파해야 하는지 여부를 포함하거나 새 자격 증명 공급자를 신뢰해야 하는 역할 목록을 제공합니다.

- 페더레이션 에이전트에서 내보낸 메타데이터 XML 파일을 서비스 요청에 첨부 파일로 연결합니다.

2. 서비스 요청을 생성한 계정과 동일한 계정에서 다음 정보와 함께 CT-ID ct-1e1xtak34nx76(관리 | 기타 | 기타 | 생성)을 사용하여 새 RFC를 생성합니다.

   - 제목: "계정 <AccountId>의 온보딩 SAML IDP <Name>".
   - 자격 증명 공급자가 생성될 계정의 AccountId입니다.
   - 자격 증명 공급자 이름입니다.
   - 기존 계정의 경우: 자격 증명 공급자를 모든 기존 콘솔 역할에 전파해야 하는지 아니면 새 자격 증명 공급자를 신뢰해야 하는 역할 목록.
   - 메타데이터 XML 파일이 연결된 1단계에서 생성된 서비스 요청의 사례 ID입니다.

콘솔 액세스 확인

ADFS로 설정하고 인증에 사용할 AMS URL이 있으면 다음 단계를 따릅니다.

Active Directory Federated Service(ADFS) 구성을 사용하면 다음 단계를 수행할 수 있습니다.

1. 브라우저 창을 열고 계정에 제공된 로그인 페이지로 이동합니다. 계정의 ADFS IdpInitiatedSignOn 페이지가 열립니다.
2. 다음 사이트 중 하나에 로그인 옆의 라디오 버튼을 선택합니다. 로그인 사이트 선택 목록이 활성화됩니다.
3. signin.aws.amazon.com 사이트를 선택하고 로그인을 클릭합니다. 자격 증명을 입력하는 옵션이 열립니다.
4. CORP 자격 증명을 입력하고 로그인을 클릭합니다. 가 AWS Management Console 열립니다.
5. AMS 콘솔의 URL을 위치 표시줄에 붙여넣고 Enter 키를 누릅니다. AMS 콘솔이 열립니다.

API 액세스 확인

AMS는 AMS API 참조에서 읽을 수 있는 일부 AMS 관련 작업과 함께 AWS API를 사용합니다.

AWS는 Amazon Web Services용 도구에서 액세스할 수 있는 여러 SDKs 제공합니다. SDK를 사용하지 않으려면 직접 API를 호출할 수 있습니다. 인증에 대한 자세한 내용은 AWS API 요청 서명을 참조하세요. SDK를 사용하지 않거나 직접 HTTP API 요청을 하는 경우 변경 관리(CM) 및 SKMS용 AMS CLIs를 사용할 수 있습니다.

AMS CLIs 설치

SAML과 함께 사용할 AWS Managed Services(AMS) CLI를 설치하는 예제는 섹션을 참조하세요부록: ActiveDirectory Federation Services(ADFS) 클레임 규칙 및 SAML 설정.

임시 액세스가 필요한 경우 AWS Managed Services(AMS) SDKs. https://docs.aws.amazon.com/managedservices/latest/userguide/access-console-temp.html

> **Note**
>
> 이 절차를 수행하려면 관리자 자격 증명이 있어야 합니다.

AWS CLI는 AWS Managed Services(AMS) CLIs(변경 관리 및 SKMS)를 사용하기 위한 사전 조건입니다.

1. AWS CLI를 설치하려면 AWS 명령줄 인터페이스 설치를 참조하고 적절한 지침을 따릅니다. 해당 페이지 하단에는 Linux, MS Windows, macOS, 가상 환경, 번들 설치 관리자(Linux, macOS 또는 Unix) 등 다양한 설치 프로그램을 사용하기 위한 지침이 있습니다.

   설치 후를 실행`aws help`하여 설치를 확인합니다.
2. AWS CLI가 설치되면 AMS CLI를 설치하거나 업그레이드하려면 AMS AMS CLI 또는 AMS SDK 배포 가능 zip 파일을 다운로드하고 압축을 풉니다. AMS 콘솔 왼쪽 탐색 창의 개발자 리소스 링크를 통해 AMS CLI 배포 파일에 액세스할 수 있습니다.
3. README 파일은 모든 설치에 대한 지침을 제공합니다.

   다음 중 하나를 엽니다.

   - CLI zip: AMS CLI만 제공합니다.
   - SDK zip: 모든 AMS APIs와 AMS CLI를 제공합니다.

   Windows의 경우 적절한 설치 관리자(32 또는 64비트 시스템만 해당)를 실행합니다.

   - 32비트: ManagedCloudAPI_x86.msi
   - 64비트: ManagedCloudAPI_x64.msi

Mac/Linux의 경우 명령을 실행하여 AWSManagedServices_InstallCLI.sh라는 파일을 실행합니다sh AWSManagedServices_InstallCLI.sh. amscm 및 amsskms 디렉터리와 해당 콘텐츠는 AWSManagedServices_InstallCLI.sh 파일과 동일한 디렉터리에 있어야 합니다.

4. 기업 자격 증명을 AWS와의 페더레이션(AMS 기본 구성)을 통해 사용하는 경우 페더레이션 서비스에 액세스할 수 있는 자격 증명 관리 도구를 설치해야 합니다. 예를 들어이 AWS 보안 블로그 SAML 2.0 및 AD FS를 사용하여 연합 API 및 CLI 액세스를 구현하는 방법을 사용하여 자격 증명 관리 도구를 구성할 수 있습니다.
5. 설치 후 aws amscm help 및를 실행aws amsskms help하여 명령과 옵션을 확인합니다.

> **Note**
>
> 이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 --profile 옵션을 추가해야 할 수 있습니다. 예: aws amsskms *ams-cli-command* --profile SAML. 와 같이 모든 AMS 명령이 us-east-1에서 실행되므로 --region 옵션을 추가해야 할 수도 있습니다aws amscm *ams-cli-command* --region=us-east-1.

VPC 수준에서 AMS 백업 예약

대상 인스턴스가 할당된 VPC의 AWS Managed Services(AMS) 백업 예약은 VPC 생성 스키마의 기본 태그를 사용하여 계정 온보딩 중에 생성됩니다. 백업 시스템은 해당 VPC 태그에 따라 스냅샷 실행을 예약합니다. 서비스 요청을 생성하여 일정을 수정할 수 있습니다. 자세한 내용은 VPC 태그 및 기본값을 참조하세요.

백업 기본값은 AMS 기본값 이해를 참조하세요.

SALZ: 기본 설정

AWS Managed Services(AMS) 네트워크는 대부분의 서비스에 대해 기본값으로 표준화된 방식으로 구성됩니다.

이 섹션에서는 AMS가 보안, 액세스, 모니터링, 로깅, 연속성 및 패치 적용, 관리에 사용하는 기본 설정을 설명합니다.

인프라 비용의 예는 기본 구성 요소를 참조하세요.

방화벽 규칙은에서 제공됩니다. 방화벽 설정

엔드포인트 보안(EPS)

AMS Advanced 환경에서 프로비저닝하는 리소스에는 엔드포인트 보안(EPS) 모니터링 클라이언트 설치가 자동으로 포함됩니다. 이 프로세스를 통해 AMS Advanced 관리형 리소스를 모니터링하고 연중무휴로 지원할 수 있습니다. 또한 AMS Advanced는 모든 에이전트 활동을 모니터링하고 보안 이벤트가 감지되면 인시던트가 생성됩니다.

> **Note**
>
> 보안 인시던트는 인시던트로 처리됩니다. 자세한 내용은 인시던트 대응을 참조하세요.

엔드포인트 보안은 맬웨어 방지 보호를 제공합니다. 특히 다음 작업이 지원됩니다.

- EC2 인스턴스가 EPS에 등록
- EPS에서 EC2 인스턴스 등록 취소
- EC2 인스턴스 실시간 맬웨어 방지 보호
- EPS 에이전트 시작 하트비트
- 격리된 파일 EPS 복원
- EPS 이벤트 알림
- EPS 보고

AMS Advanced는 엔드포인트 보안(EPS)에 Trend Micro를 사용합니다. 이는 기본 EPS 설정입니다. Trend Micro에 대해 자세히 알아보려면 Trend Micro Deep Security Help Center를 참조하세요. Amazon 이외의 링크는 예고 없이 변경될 수 있습니다.

AMS 고급 다중 계정 랜딩 존(MALZ) 기본 설정은 다음 섹션에 설명되어 있습니다. 기본이 아닌 AMS 다중 계정 랜딩 존 EPS 설정은 AMS 고급 다중 계정 랜딩 존 EPS 기본이 아닌 설정을 참조하세요.

> **Note**
>
> 자체 EPS를 가져올 수 있습니다. AMS 자체 EPS 가져오기를 참조하세요.

일반 EPS 설정

엔드포인트 보안 일반 네트워크 설정.

EPS 기본값

설정	기본값
방화벽 포트(인스턴스의 보안 그룹)	EPS Deep Security Manager 에이전트(DSMs)는 Agent/Relay to Manager 통신을 위해 포트 4120이 열려 있고 Manager 콘솔을 위해 포트 4119가 열려 있어야 합니다. 관리자/에이전트에서 릴레이로 통신하려면 EPS 릴레이에 포트 4122가 열려 있어야 합니다. 에이전트가 모든 요청을 시작하기 때문에 고객 인스턴스 인바운드 통신을 위해 특정 포트를 열면 안 됩니다.
통신 방향	에이전트/어플라이언스 시작됨
하트비트 간격	10분
알림 전 누락된 하트비트 수	2
서버 시간 간에 허용되는 최대 드리프트(차이)	무제한
비활성(등록되었지만 온라인이 아닌) 가상 머신에 대한 오프라인 오류 발생	아니요
기본 정책	기본 정책(다음 설명 참조)
호스트 이름이 동일한 여러 컴퓨터 활성화	허용됨
보류 중인 업데이트에 대한 알림이 발생합니다.	7일 후
일정 업데이트	AMS는 Trend Micro Deep Security Manager(DSM)/Deep Security Agent(DSA) 소프트웨어 업데이트를 위한 월간 릴리스 주기를 목표로 합니다. 그러나 AMS는 업데이트를 위해 SLA를 유지 관리하지 않습니다. 업데이트는 배포 중에 AMS 개발자 팀이 플릿 전체에서 수행합니다.

설정	기본값
	DSA/DSA 업데이트는 AMS가 기본적으로 13주 동안 로컬로 보관하는 Trend MicroDSM 시스템 이벤트에 기록됩니다. 공급업체 설명서는 Trend Micro Deep Security Help Center의 시스템 이벤트를 참조하세요. 로그는 Amazon CloudWatch의 로그 그룹 /aws/ams/eps/var/log/DSM.log로도 내보내집니다.
소스 업데이트	Trend Micro 업데이트 서버(https://ipv6-ia us.trendmicro.com/iau_server.dll/)
이벤트 또는 로그 데이터 삭제	이벤트 및 로그는 7일 후에 Amazon 데이터베이스에서 삭제됩니다.
에이전트 소프트웨어 버전이 보류됨	최대 5개
최신 규칙 업데이트가 보류됨	최대 10개
로그 스토리지	기본적으로 로그 파일은 Amazon S3에 안전하게 저장되지만 감사 및 규정 준수 요구 사항을 충족하는 데 도움이 되도록 Amazon Glacier에 보관할 수도 있습니다.

기본 정책

엔드포인트 보안 기본 정책 기본 설정입니다.

EPS 기본 정책

설정	기본값
활성화된 모듈	맬웨어 방지
비활성화된 모듈	웹 평판
	방화벽
	침입 방지

설정	기본값
	무결성 모니터링
	로그 검사
	애플리케이션 제어

맬웨어 방지

엔드포인트 보안 맬웨어 방지 설정.

EPS 맬웨어 방지 기본값

설정	기본값	참고
실시간 스캔	모든 항목 스캔	의심되는 모든 바이러스를 격리합니다. IntelliTrap 및 스파이웨어/그레이웨어 보호를 활성화합니다. 스파이웨어 및 그레이웨어는 맬웨어 방지를 트리거하여 항목을 격리합니다.
	매일/전일(24시간)	
수동 스캔	모든 항목 스캔	요청해야 하며, 그런 다음 기본 실시간 스캔 구성을 따릅니다.
예약된 스캔	모든 항목 스캔	매월 마지막 일요일 오전 6시로 설정합니다.
스마트 보호	비활성	N/A
격리된 파일	Trend Micro Deep Security Manager(DSM)	격리용으로 예약된 디스크 약 1GB.

설정	기본값	참고
스캔 제한	Trend Micro"	모든 크기의 파일을 스캔합니다.
허용된 스파이웨어 또는 그레이웨어	없음	N/A
로컬 이벤트 알림	예	N/A

보안 그룹

AWS VPCs에서 AWS 보안 그룹은 하나 이상의 스택(인스턴스 또는 인스턴스 세트)에 대한 트래픽을 제어하는 가상 방화벽 역할을 합니다. 스택이 시작되면 하나 이상의 보안 그룹과 연결되어 스택에 도달할 수 있는 트래픽이 결정됩니다.

- 퍼블릭 서브넷의 스택의 경우 기본 보안 그룹은 모든 위치(인터넷)의 HTTP(80) 및 HTTPS(443) 트래픽을 수락합니다. 또한 스택은 회사 네트워크의 내부 SSH 및 RDP 트래픽과 AWS 접속을 허용합니다. 그러면 이러한 스택이 모든 포트를 통해 인터넷으로 나갈 수 있습니다. 또한 프라이빗 서브넷 및 퍼블릭 서브넷의 다른 스택으로 나갈 수 있습니다.
- 프라이빗 서브넷의 스택은 프라이빗 서브넷의 다른 스택으로 송신할 수 있으며, 스택 내의 인스턴스는 모든 프로토콜을 통해 서로 완전히 통신할 수 있습니다.

> **Important**
>
> 프라이빗 서브넷의 스택에 대한 기본 보안 그룹을 사용하면 프라이빗 서브넷의 모든 스택이 해당 프라이빗 서브넷의 다른 스택과 통신할 수 있습니다. 프라이빗 서브넷 내의 스택 간 통신을 제한하려면 제한을 설명하는 새 보안 그룹을 생성해야 합니다. 예를 들어 프라이빗 서브넷의 스택이 특정 포트를 통해서만 특정 애플리케이션 서버에서 통신할 수 있도록 데이터베이스 서버와의 통신을 제한하려면 특수 보안 그룹을 요청합니다. 이렇게 하는 방법은이 단원에서 설명합니다.

기본 보안 그룹

MALZ

다음 표에서는 스택의 기본 인바운드 보안 그룹(SG) 설정을 설명합니다. SG의 이름은 "SentinelDefaultSecurityGroupPrivateOnly-vpc-ID"이며, 여기서 *ID*는 AMS 다중 계정 랜딩 존 계정의 VPC ID입니다. 모든 트래픽은이 보안 그룹을 통해 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"로 아웃바운드할 수 있습니다(스택 서브넷 내의 모든 로컬 트래픽 허용).

모든 트래픽은 두 번째 보안 그룹 "SentinelDefaultSecurityGroupPrivateOnly"에 의해 0.0.0.0/0으로 아웃바운드할 수 있습니다.

> **Tip**
>
> EC2 생성 또는 OpenSearch 생성 도메인과 같은 AMS 변경 유형에 대한 보안 그룹을 선택하는 경우 여기에 설명된 기본 보안 그룹 중 하나 또는 생성한 보안 그룹을 사용합니다. AWS EC2 콘솔 또는 VPC 콘솔에서 VPC당 보안 그룹 목록을 찾을 수 있습니다.

내부 AMS용으로 사용되는 추가 기본 보안 그룹이 있습니다.

AMS 기본 보안 그룹(인바운드 트래픽)

Type	프로토콜	포트 범위	소스
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnly(동일한 보안 그룹의 구성원으로의 아웃바운드 트래픽 제한)
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnlyEgressAll(아웃바운드 트래픽을 제한하지 않음)
HTTP, HTTPS, SSH, RDP	TCP	80/443(소스 0.0.0.0/0) Bastion에서 SSH 및 RDP 액세스 허용	SentinelDefaultSecurityGroupPublic(아웃바운드 트래픽을 제한하지 않음)

Type	프로토콜	포트 범위	소스
MALZ 접속:			
SSH	TCP	22	SharedServices VPC CIDR 및 DMZ VPC CIDR과 고객이 제공한 온프레미스 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 접속:			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

SALZ

다음 표에서는 스택의 기본 인바운드 보안 그룹(SG) 설정을 설명합니다. SG의 이름은 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-*ID*"이며, 여기서 *ID*는 고유 식별자입니다. 모든 트래픽은이 보안 그룹을 통해 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"로 아웃바운드할 수 있습니다(스택 서브넷 내의 모든 로컬 트래픽 허용).

모든 트래픽은 두 번째 보안 그룹 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnlyEgressAll-*ID*"에 의해 0.0.0.0/0으로 아웃바운드할 수 있습니다.

> **Tip**
>
> EC2 생성 또는 OpenSearch 생성 도메인과 같은 AMS 변경 유형에 대한 보안 그룹을 선택하는 경우 여기에 설명된 기본 보안 그룹 중 하나 또는 생성한 보안 그룹을 사용합니다. AWS EC2 콘솔 또는 VPC 콘솔에서 VPC당 보안 그룹 목록을 찾을 수 있습니다.

내부 AMS용으로 사용되는 추가 기본 보안 그룹이 있습니다.

AMS 기본 보안 그룹(인바운드 트래픽)

Type	프로토콜	포트 범위	소스
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnly(동일한 보안 그룹의 구성원으로의 아웃바운드 트래픽 제한)
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnlyEgressAll(아웃바운드 트래픽을 제한하지 않음)
HTTP, HTTPS, SSH, RDP	TCP	80/443(소스 0.0.0.0/0) Bastion에서 SSH 및 RDP 액세스 허용	SentinelDefaultSecurityGroupPublic(아웃바운드 트래픽을 제한하지 않음)
MALZ 접속:			
SSH	TCP	22	SharedServices VPC CIDR 및 DMZ VPC CIDR과 고객이 제공한 온프레미스 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 접속:			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

보안 그룹 생성, 변경 또는 삭제

사용자 지정 보안 그룹을 요청할 수 있습니다. 기본 보안 그룹이 애플리케이션 또는 조직의 요구 사항을 충족하지 않는 경우 새 보안 그룹을 수정하거나 생성할 수 있습니다. 이러한 요청은 승인 필수로 간주되며 AMS 운영 팀에서 검토합니다.

스택 및 VPCs 외부에서 보안 그룹을 생성하려면 `Deployment | Advanced stack components | Security group | Create (managed automation)` 변경 유형(ct-1oxx2g2d7hc90)을 사용하여 RFC를 제출합니다.

Active Directory(AD) 보안 그룹 수정의 경우 다음 변경 유형을 사용합니다.

- 사용자를 추가하려면: 관리 | 디렉터리 서비스 | 사용자 및 그룹 | 그룹에 사용자 추가 [ct-24pi85mjtza8k]를 사용하여 RFC 제출
- 사용자를 제거하려면: 관리 | 디렉터리 서비스 | 사용자 및 그룹 | 그룹에서 사용자 제거 [ct-2019s9y3nfml4]를 사용하여 RFC 제출

> **Note**
>
> 수동 CTs를 사용하는 경우 ASAP 예약 옵션(콘솔에서 ASAP 선택, API/CLI에서 시작 및 종료 시간 비워 두기)을 사용하는 것이 좋습니다. 이러한 CTs는 AMS 운영자가 RFC를 검사하고 승인 및 실행 전에 사용자와 통신해야 하기 때문입니다. 이러한 RFCs 예약하는 경우 최소 24시간을 허용해야 합니다. 예정된 시작 시간 전에 승인이 이루어지지 않으면 RFC가 자동으로 거부됩니다.

보안 그룹 찾기

스택 또는 인스턴스에 연결된 보안 그룹을 찾으려면 EC2 콘솔을 사용합니다. 스택 또는 인스턴스를 찾은 후 스택 또는 인스턴스에 연결된 모든 보안 그룹을 볼 수 있습니다.

명령줄에서 보안 그룹을 찾고 출력을 필터링하는 방법은 섹션을 참조하세요describe-security-groups.

EC2 IAM 인스턴스 프로파일

인스턴스 프로파일은 IAM 역할을 위한 컨테이너로서 인스턴스 시작 시 EC2 인스턴스에 역할 정보를 전달하는 데 사용할 수 있습니다.

MALZ

AMS 기본 인스턴스 프로파일은 customer-mc-ec2-instance-profile 및 입니다customer-mc-ec2-instance-profile-s3. 이러한 인스턴스 프로파일은 다음 표에 설명된 권한을 제공합니다.

정책 설명

프로필	정책
customer-mc-ec2-instance-profile	AmazonSSMManagedInstanceCore : Ec2 인스턴스가 SSM 에이전트를 사용하도록 허용합니다.
	AMSInstanceProfileLoggingPolicy : Ec2 인스턴스가 로그를 S3 및 CloudWatch로 푸시하도록 허용합니다.
	AMSInstanceProfileManagementPolicy : Ec2 인스턴스가 Active Directory 조인과 같은 부팅 작업을 수행하도록 허용합니다.
	AMSInstanceProfileMonitoringPolicy : Ec2 인스턴스가 결과를 AMS 모니터링 서비스에 보고할 수 있도록 허용합니다.
	AMSInstanceProfilePatchPolicy : Ec2 인스턴스가 패치를 수신하도록 허용합니다.
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBYOEPSPolicy : Ec2 인스턴스가 AMS Bring Your Own EPS를 사용하도록 허용합니다.
	AMSInstanceProfileLoggingPolicy : Ec2 인스턴스가 로그를 S3 및 CloudWatch로 푸시하도록 허용합니다.
	AMSInstanceProfileManagementPolicy : Ec2 인스턴스가 Active Directory 조인과 같은 부팅 작업을 수행하도록 허용합니다.

프로필	정책
	AMSInstanceProfileMonitoringPolicy : Ec2 인스턴스가 결과를 AMS 모니터링 서비스에 보고할 수 있도록 허용합니다.
	AMSInstanceProfilePatchPolicy : Ec2 인스턴스가 패치를 수신하도록 허용합니다.
	AMSInstanceProfileS3WritePolicy : Ec2 인스턴스가 고객 S3 버킷을 읽고 쓸 수 있도록 허용합니다.

SALZ

IAM 인스턴스 정책의 권한을 customer-mc-ec2-instance-profile부여하는 AMS 기본 인스턴스 프로파일가 하나 있습니다customer_ec2_instance_profile_policy. 이 인스턴스 프로파일은 다음 표에 설명된 권한을 제공합니다. 프로파일은 인스턴스에 로그인하는 사용자가 아닌 인스턴스에서 실행되는 애플리케이션에 권한을 부여합니다.

정책에는 종종 여러 문이 포함되며, 각 문은 서로 다른 리소스 세트에 권한을 부여하거나 특정 조건에서 권한을 부여합니다.

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

EC2 기본 IAM 인스턴스 프로파일 권한

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).			
정책 문	Effect	작업	설명 및 리소스(ARN)
Amazon Elastic Compute Cloud(Amazon EC2)			
EC2 메시지 작업	허용	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages,	계정에서 EC2 Systems Manager 메시징 작업을 허용합니다.

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).			
정책 문	Effect	작업	설명 및 리소스(ARN)
		SendReply	
Ec2 설명	허용	* (모두)	콘솔이 계정에서 EC2의 구성 세부 정보를 표시하도록 허용합니다.
Iam 역할 ID 가져오기	허용	GetRole	EC2가 `aws:iam::*:role/customer-*` 및에서 IAM ID를 가져오도록 허용합니다`aws:iam::*:role/customer_*` .
로그 이벤트를 업로드할 인스턴스	허용	로그 그룹 생성	로그를 생성할 수 있는 위치: `aws:logs:*:*:log-group:i-*`
		로그 스트림 생성	로그를 다음으로 스트리밍할 수 있습니다. `aws:logs:*:*:log-group:i-*`
MMS용 CW	허용	DescribeAlarms, PutMetricAlarm, PutMetricData	CloudWatch가 계정에서 경보를 검색할 수 있도록 허용합니다. CW가 경보를 생성 또는 업데이트하고 지정된 지표와 연결할 수 있도록 허용합니다. CW가 지표 데이터 포인트를 계정에 게시할 수 있도록 허용합니다.
Ec2 태그	허용	CreateTags, DescribeTags,	계정의 지정된 인스턴스에서 태그를 추가, 덮어쓰기 및 설명할 수 있습니다.

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).			
정책 문	Effect	작업	설명 및 리소스(ARN)
CW 로그를 명시적으로 거부	거부	DescribeLogStreams, FilterLogEvents, GetLogEvents	다음에 대한 로그 스트림 나열, 필터링 또는 가져오기를 허용하지 않습니다. `aws:logs:*:*:log-group:/mc/*`
Amazon EC2 Simple Systems Manager(SSM)			
SSM 작업	허용	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	계정에서 다양한 SSM 함수를 허용합니다.
S3의 SSM 액세스	허용	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	EC2의 SSM이에서 객체를 가져오고 업데이트하며에 대한 멀티파트 객체 업로드를 중단하고에서 멀티파트 업로드에 사용할 수 있는 포트 및 버킷을 나열할 수 있도록 허용합니다`aws:s3:::mc-*-internal-*/aws/ssm*` .
Amazon EC2 Simple Storage Service(S3)			
S3에서 객체 가져오기	허용	Get List	EC2 애플리케이션이 계정의 S3 버킷에서 객체를 검색하고 나열할 수 있도록 허용합니다.

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

정책 문	Effect	작업	설명 및 리소스(ARN)
고객 암호화 로그 S3 액세스	허용	PutObject	EC2 애플리케이션이에서 객체를 업데이트하도록 허용 `aws:s3:::mc-*-logs-*/encrypted/app/*`
패치 데이터 객체 S3 추가	허용	PutObject	EC2 애플리케이션이에서 S3 버킷에 패치 적용 데이터를 업로드하도록 허용 `aws:s3:::awsms-a*-patch-data-*`
S3에 자체 로그 업로드	허용	PutObject	EC2 애플리케이션이 사용자 지정 로그를 다음에 업로드하도록 허용합니다. `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
MC 네임스페이스 S3 로그를 명시적으로 거부	거부	GetObject* Put*	EC2 애플리케이션이 다음과 같이 객체를 가져오거나 배치하는 것을 허용하지 않습니다. `aws:s3:::mc-*-logs-*/encrypted/mc*` , `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).			
정책 문	Effect	작업	설명 및 리소스(ARN)
S3 삭제를 명시적으로 거부	거부	* (모두)	EC2 애플리케이션이 다음의 객체에 대해 어떤 작업도 수행하는 것을 허용하지 않습니다. `aws:s3:::mc-a*-logs-*/*` , `aws:s3:::mc-a*-internal-*/*` ,
S3 CFN 버킷을 명시적으로 거부	거부	Delete*	다음에서 객체를 삭제하는 EC2 애플리케이션을 허용하지 않습니다. `aws:s3:::cf-templates-*`
명시적으로 거부 목록 버킷 S3	거부	ListBucket	다음에서 암호화된 객체, 감사 로그 또는 예약된 (mc) 객체를 나열할 수 없습니다. `aws:s3:::mc-*-logs-*`
AWS Secrets Manager Amazon EC2의			

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).			
정책 문	Effect	작업	설명 및 리소스(ARN)
Trend Cloud One 보안 암호 액세스	허용	GetSecretValue	Amazon EC2가 Trend Cloud One 마이그레이션을 위한 보안 암호에 액세스할 수 있도록 허용합니다. `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service Amazon EC2의			
Trend Cloud One 복호화 키	허용	Decrypt	Amazon EC2가 별칭 이름 /ams/eps/cloudone-migration으로 AWS KMS 키를 복호화하도록 허용 `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

Amazon IAM 정책에 익숙하지 않은 경우 중요 정보는 IAM 정책 개요를 참조하세요.

> **Note**
>
> 정책에는 종종 여러 문이 포함되며, 각 문은 서로 다른 리소스 세트에 권한을 부여하거나 특정 조건에서 권한을 부여합니다.

모니터링되는 지표 기본값

다음 표에는 모니터링되는 항목과 기본 알림 임계값이 나와 있습니다. 변경 관리 요청(RFC)을 사용하여 기본값을 변경할 수 있습니다.

> **Note**
>
> CloudWatch는 2016년 11월 1일에 지표 보존 기간을 연장했습니다. 자세한 내용은 CloudWatch 제한을 참조하세요.

기준 모니터링의 알림

서비스	보안 알림	알림 이름 및 트리거 조건	참고
별표가 지정된 (*) 알림의 경우 AMS는 가능한 경우 영향을 사전에 평가하고 수정합니다. 수정이 불가능한 경우 AMS는 인시던트를 생성합니다. 자동화로 문제를 해결할 수 없는 경우 AMS는 인시던트 사례를 알리고 AMS 엔지니어가 참여합니다. 또한 이러한 알림은 이메일로 직접 전송할 수 있습니다(Direct-Customer-Alerts SNS 주제에 옵트인한 경우).			
Application Load Balancer(ALB) 인스턴스	아니요	RejectedConnectionCount 1분 동안 합계 > 0, 연속 5회.	CloudWatch는 로드 밸런서가 최대값에 도달하여 거부된 연결 수를 경보합니다.
Application Load Balancer(ALB) 대상	아니요	TargetConnectionErrorCount 1분 동안 합계 > 0, 연속 5회.	로드 밸런서와 등록된 인스턴스 간에 연결 수가 설정되지 않은 경우 CloudWatch 경보가 발생합니다.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
Amazon EC2 인스턴스 – Windows	아니요	SecureChannelFailure 마지막 15개 데이터 포인트 중 10개에 대해 > 0.0.	채널 보안 연결이 실패할 때 경고하는 Windows 인스턴스의 CloudWatch 경보입니다.
Aurora 인스턴스	아니요	CPUUtilization 5분 동안 > 85%, 연속 2회.	CloudWatch 경보.
AWS Backup	예	DeleteRecoveryPoint 예기치 않은 IAM 역할 보안 주체 또는 IAM 사용자 보안 주체가 AWS Backup 복구 시점을 삭제했습니다.	CloudWatch 이벤트. 백업 복구 시점이 삭제될 때 발생합니다.
AWS Outposts	예	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 5분 동안 80%, 연속 12회.	리소스의 인스턴스 패밀리 용량 가용성에 대한 CloudWatch 경보입니다 AWS Outposts .
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 5분 동안 80%, 연속 12회.	리소스의 인스턴스 유형 용량 가용성에 대한 CloudWatch 경보입니다 AWS Outposts .
		AMSOutpostsConnectedStatusConnectedStatus 5분 동안 < 1, 연속 1회.	AWS Outposts 서비스 링크 연결에 대한 CloudWatch 경보가 1개 미만으로 손상되었습니다.
		AMSOutpostsCapacityExceptionCapacityExceptions 5분 동안 0, 연속 1회.	AWS Outposts리소스에 대한 인스턴스 시작의 용량 부족 오류에 대한 CloudWatch 경보 .

서비스	보안 알림	알림 이름 및 트리거 조건	참고
EC2 인스턴스 - 모든 OSs	아니요	CPUUtilization* 인스턴스가 폴링 Systems Manager 명령에 응답하지 않는 경우 5분 동안 >= 95%, 연속 6회.	CloudWatch 경보. CPU 사용률이 높다는 것은 데드록, 무한 루프, 악성 공격 및 기타 이상과 같은 애플리케이션 상태의 변화를 나타내는 지표입니다.
		StatusCheckFailed 5분 동안 > 0, 연속 3회.	CloudWatch 경보.
		루트 볼륨 사용량 5분, 연속 6회 동안 >= 95%.	
		루트가 아닌 볼륨 사용량 5분 동안 > 85%, 연속 2회. 기본적으로 비활성화되어 있습니다. 자세한 내용은 섹션을 참조하세요https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		메모리 없음* MemoryFree 5분 동안 < 5%, 연속 6회.	
	예	EPS 맬웨어 인스턴스에서 발견된 맬웨어입니다.	CloudWatch 이벤트.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
Amazon EC2 인스턴스 - Linux	아니요	루트 볼륨 Inode 사용량 5분, 연속 6회 동안 평균 >= 95%.	CloudWatch 경보. Linux 인스턴스에만 적용됩니다.
		스왑 프리* 메모리 5분 동안 스왑 < 5%, 연속 6회.	
ElastiCache 클러스터	아니요	CurrConnections = 65000	이 경보는 AMS에 ElastiCache 호스트의 최대 연결 제한을 알립니다. CloudWatch 경보. 이 임계값을 업데이트하려면 AMS 지원팀에 문의하십시오.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
ElastiCache 노드	아니요	CPUUtilization 평균 > 15분 동안 미리 정의된 값, 연속 2회.	CloudWatch 경보. 기본값은 90입니다. Redis인 경우 인스턴스 유형에 따라 다음 값 중 하나를 사용합니다. • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22.5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11.25% • cache.c1.xlarge: 11.25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22.5% • cache.m3.2xlarge: 11.25% • cache.r3.large: 45% • cache.r3.xlarge: 22.5% • cache.r3.2xlarge: 11.25% • cache.r3.4xlarge: 5.625% • cache.r3.8xlarge: 2.8125%
ElastiCache 노드 - memcached	아니요	SwapUsage 최대 > 50,000,000바이트, 5분, 5회 연속.	CloudWatch 경보. memcached에만 적용됩니다.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
OpenSearch 클러스터	아니요	ClusterStatus.red 최대값은 1분, 연속 1회 동안 >= 1입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	CloudWatch 경보. 하나 이상의 기본 샤드와 복제본이 노드에 할당되지 않았습니다. 자세한 내용은 빨간색 클러스터 상태를 참조하세요.
OpenSearch 도메인	아니요	KMSKeyError >= 1분, 연속 1회.	CloudWatch 경보. 도메인에서 저장된 데이터를 암호화하는 데 사용된 KMS 암호화 키가 비활성화되었습니다. 정상 작동으로 복원하려면 다시 활성화해야 합니다. 자세한 내용은 OpenSearch Service Service의 저장 데이터 암호화를 참조하세요.
		ClusterStatus.yellow 최대값은 1분, 연속 1회 동안 >= 1입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	하나 이상의 복제 샤드가 노드에 할당되지 않았습니다. 자세한 내용은 노란색 클러스터 상태를 참조하세요.
		FreeStorageSpace 최소값은 1분, 연속 1회 동안 <= 20480입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	클러스터 속 노드의 여유 스토리지 공간이 20GiB까지 떨어졌습니다. 자세한 내용은 사용 가능한 스토리지 공간 부족을 참조하세요.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
		ClusterIndexWritesBlocked 5분 동안 >= 1, 연속 1회 AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	클러스터가 쓰기 요청을 차단하고 있습니다. 자세한 내용은 ClusterBlockException을 참조하세요.
		Nodes(노드) 최소값은 1일 동안 < x, 연속 1회 AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	x는 클러스터의 노드 수입니다. 이 경보는 클러스터에서 하나 이상의 노드가 하루 동안 연결되지 않았음을 나타냅니다. 자세한 내용은 실패한 클러스터 노드를 참조하세요.
		CPUUtilization 평균은 15분, 연속 3회 동안 >= 80% 입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	100% CPU 사용률이 일반적이지만 지속적으로 높은 평균은 문제가 됩니다. 더 큰 인스턴스 유형을 사용하거나 인스턴스 추가를 고려하세요.
		JVMMemoryPressure 최대값은 5분, 연속 3회 동안 >= 80% 입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	사용량이 늘어나면 클러스터에서 메모리 부족 오류가 발생할 수 있습니다. 수직 확장을 고려하세요. Amazon ES는 Java 힙에 인스턴스 RAM의 절반을 사용하고 힙 크기는 최대 32GiB입니다. 인스턴스를 최대 64GiB의 RAM까지 수직 확장할 수 있으며 인스턴스를 추가하면 수평 확장도 가능합니다.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
		MasterCPUUtilization 평균은 15분, 연속 3회 동안 >= 50% 입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	전용 마스터 노드에 더 큰 인스턴스 유형을 사용하는 것이 좋습니다. 클러스터 안정성 및 블루/그린 배포에서의 역할 때문에 전용 마스터 노드는 데이터 노드보다 평균 CPU 사용량이 낮아야 합니다.
		MasterJVMMemoryPressure 최대값은 15분, 연속 1회 동안 >= 80%입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	전용 마스터 노드에 더 큰 인스턴스 유형을 사용하는 것이 좋습니다. 클러스터 안정성 및 블루/그린 배포에서의 역할 때문에 전용 마스터 노드는 데이터 노드보다 평균 CPU 사용량이 낮아야 합니다.
OpenSearch 인스턴스	아니요	AutomatedSnapshotFailure 최대값은 1분, 연속 1회 동안 >= 1입니다.	CloudWatch 경보. 자동 스냅샷에 오류가 발생했습니다. 이런 오류는 red 클러스터 상태로 인해 자주 발생했습니다. 빨간색 클러스터 상태를 참조하세요.
Elastic Load Balancing 인스턴스	아니요	SurgeQueueLength 1분 동안 > 100, 연속 15회.	초과 요청 수가 라우팅 보류 중인 경우 CloudWatch 경보가 발생합니다.
		HTTPCode_ELB_5XX_Count 5분 동안 합계 > 0, 연속 횟수 3회.	로드 밸런서에서 시작된 초과 HTTP 5XX 응답 코드 수에 대한 CloudWatch 경보입니다.
		SpilloverCount 1분 동안 > 1, 연속 15회.	서지 대기열이 가득 차서 거부된 요청 수가 초과되면 CloudWatch 경보가 발생합니다.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
GuardDuty 서비스	예	해당 사항 없음. 모든 결과(위협 목적)가 모니터링됩니다. 각 결과는 알림에 해당합니다. GuardDuty 조사 결과의 변경 사항. 이러한 변경은 새롭게 생성된 결과 또는 기존 결과의 후속 발생을 포함합니다.	지원되는 GuardDuty 결과 유형의 목록은 GuardDuty 활성 결과 유형에 있습니다.
Health	다양	AWS Health Dashboard	AMS Operations의 조치가 필요한 AMS에서 지원하는 기준 서비스와 관련하여 AWS Health Dashboard (AWS Health) 이벤트의 상태가 변경되면 알림이 전송됩니다. 자세한 내용은 지원되는 서비스를 참조하세요.
AWS Managed Microsoft AD	아니요	Active Directory 상태 AWS Managed Microsoft AD 인스턴스가 활성 상태 이벤트를 보냅니다.	서비스 이벤트. 이벤트 후 디렉터리가 정상적으로 작동할 때 발생합니다.
		손상된 디렉터리 상태 AWS Managed Microsoft AD 인스턴스가 손상된 디렉터리 상태 이벤트를 보냅니다.	서비스 이벤트. 디렉터리가 성능 저하 상태에서 실행 중일 때 내보내집니다. 1개 이상의 문제가 탐지되었고, 모든 디렉터리 작업이 전체 운영 용량에서 실행되지 못할 수 있습니다.
		사용할 수 없는 디렉터리 상태 AWS Managed Microsoft AD 인스턴스가 작동하지 않는 상태 이벤트를 보냅니다.	서비스 이벤트. 디렉터리가 작동하지 않을 때 발생합니다. 모든 디렉터리 엔드포인트가 문제를 보고했습니다.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
		디렉터리 상태 삭제 AWS Managed Microsoft AD 인스턴스는 디렉터리 상태 이벤트 삭제를 전송합니다.	서비스 이벤트. 디렉터리가 현재 삭제 중일 때 내보내집니다.
		실패한 디렉터리 상태 AWS Managed Microsoft AD 인스턴스가 실패한 상태 이벤트를 보냅니다.	서비스 이벤트. 디렉터리를 생성할 수 없을 때 발생합니다.
		RestoreFailed Directory 상태 AWS Managed Microsoft AD 인스턴스는 복원 실패 디렉터리 상태 이벤트를 전송합니다.	서비스 이벤트. 스냅샷에서 디렉터리를 복원하지 못한 경우 내보내집니다.
Amazon RDS 인스턴스	아니요	DB 인스턴스에 할당된 스토리지가 소진되면 스토리지 부족 알림이 트리거됩니다.	RDS-EVENT-0007, Amazon RDS 이벤트 알림 사용의 세부 정보를 참조하세요.
		DB 인스턴스 실패 호환되지 않는 구성 또는 기본 스토리지 문제로 인해 DB 인스턴스에 장애가 발생했습니다. DB 인스턴스에 대해 특정 시점으로 복구를 시작합니다.	서비스 이벤트. RDS-EVENT-0031, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		장애 조치가 시도되지 않음 최근에 DB 인스턴스에 장애 조치가 발생하였기 때문에 Amazon RDS가 요청한 장애 조치를 실행하지 않습니다.	서비스 이벤트. RDS-EVENT-0034, Amazon RDS 이벤트 범주 및 이벤트 메시지.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
		DB 인스턴스 잘못된 파라미터 예를 들어 이 인스턴스 클래스의 메모리 관련 파라미터가 너무 높게 설정되어 MySQL이 시작하지 않습니다. 따라서 메모리 파라미터 설정을 변경한 후 DB 인스턴스를 재부팅하는 것이 바람직합니다.	서비스 이벤트. RDS-EVENT-0035, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		잘못된 서브넷 IDs 인스턴스 DB 인스턴스가 호환되지 않는 네트워크에 있습니다. 특정 서브넷 ID 중 일부가 잘못되었거나 존재하지 않습니다.	서비스 이벤트. RDS-EVENT-0036, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		DB 인스턴스 읽기 전용 복제본 오류 읽기 전용 복제 프로세스에서 오류가 발생하였습니다. 자세한 내용은 이벤트 메시지 섹션을 참조하세요. 읽기 전용 복제본 오류 문제 해결에 대한 자세한 내용은 MySQL 읽기 전용 복제본 문제 해결을 참조하세요.	서비스 이벤트. RDS-EVENT-0045, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		DB 인스턴스 읽기 복제 종료 읽기 전용 복제본에 대한 복제가 종료되었습니다.	서비스 이벤트. RDS-EVENT-0057, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		statspack 사용자 계정 생성 오류 Statspack 사용자 계정인 PERFSTAT 생성 중 오류가 발생하였습니다. Statspack 옵션을 추가하기 전에 계정을 삭제합니다.	서비스 이벤트. RDS-EVENT-0058, Amazon RDS 이벤트 범주 및 이벤트 메시지.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
		DB 인스턴스 복구 시작 SQL Server DB 인스턴스가 미러를 재구성 중입니다. 이때 미러가 재구성될 때까지 성능이 저하됩니다. 복구 모델이 FULL이 아닌 데이터베이스가 발견되었습니다. 복구 모델이 FULL로 다시 변경되었고 미러링 복구가 시작되었습니다(<dbname>: <recovery model found>[,...]).	서비스 이벤트. RDS-EVENT-0066, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		DB 클러스터에 대한 장애 조치가 실패했습니다.	RDS-EVENT-0069, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		잘못된 권한 복구 S3 버킷 SQL Server 기본 백업 및 복원을 위해 Amazon S3 버킷에 액세스하는 데 사용하는 IAM 역할이 잘못 구성되었습니다. 자세한 내용은 기본 백업 및 복원 설정을 참조하세요.	서비스 이벤트. RDS-EVENT-0081, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		Aurora가 Amazon S3 버킷에서 백업 데이터를 복사할 수 없습니다.	RDS-EVENT-0082, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
		DB 인스턴스가 할당된 스토리지의 90% 이상을 소비한 경우 스토리지 부족 알림	RDS-EVENT-0089, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		Aurora Serverless DB 클러스터에 대한 조정 실패 시 알림 서비스입니다.	RDS-EVENT-0143, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
		DB 인스턴스가 잘못된 상태입니다. 아무 조치도 필요하지 않습니다. 자동 확장은 나중에 다시 시도합니다.	RDS-EVENT-0219, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		DB 인스턴스가 스토리지 전체 임계값에 도달했으며 데이터베이스가 종료되었습니다.	RDS-EVENT-0221, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		이 이벤트는 RDS 인스턴스 스토리지 Autoscaling을 조정할 수 없으며 Autoscaling이 실패한 여러 이유가 있을 수 있음을 나타냅니다.	RDS-EVENT-0223, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
		스토리지 자동 확장은 최대 스토리지 임계값에 도달하는 보류 중인 확장 스토리지 작업을 트리거했습니다.	RDS-EVENT-0224, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
		DB 인스턴스에는 현재 가용 영역에서 사용할 수 없는 스토리지 유형이 있습니다. 자동 확장은 나중에 다시 시도합니다.	RDS-EVENT-0237, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
		서브넷에서 사용할 수 있는 IP 주소가 충분하지 않기 때문에 RDS가 프록시 용량을 프로비저닝할 수 없습니다.	RDS-EVENT-0243, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		AWS 계정의 스토리지가 허용된 스토리지 할당량을 초과했습니다.	RDS-EVENT-0254, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
		CPUUtilization 15분 동안 평균 CPU 사용률 > 90%, 연속 2회.	CloudWatch 경보.

서비스	보안 알림	알림 이름 및 트리거 조건	참고
		DiskQueueDepth 합계는 1분, 연속 15회 동안 > 75입니다.	
		FreeStorageSpace 5분 동안 평균 < 1,073,741,824바이트, 연속 2회.	
		SwapUsage 평균 >= 5분 동안 104,857,600바이트, 연속 2회.	
Amazon Redshift 클러스터	아니요	RedshiftClusterStatus 유지 관리 모드 < 1이 아닌 상태에서 5분 동안 클러스터의 상태입니다.	1은 정상 클러스터를 나타냅니다.
Amazon Macie	예	새로 생성된 알림 및 기존 알림에 대한 업데이트. Macie는 조사 결과에서 변경 사항을 찾습니다. 이러한 변경은 새롭게 생성된 결과 또는 기존 결과의 후속 발생을 포함합니다.	Amazon Macie 알림. 지원되는 Macie 알림 유형 목록은 Amazon Macie 조사 결과 분석을 참조하세요. Macie는 모든 계정에 대해 활성화되어 있지 않습니다.

로그 보존 및 교체 기본값

이 섹션에서는 AMS 로그 관리 기본값을 설명합니다. 자세한 내용은 로그 관리를 참조하세요.

- 교체 = 인스턴스 내 로그 전환
- 보존 = Amazon CloudWatch Logs 및 Amazon Simple Storage Service(S3)에 로그를 보관하는 기간

로그는 필요에 따라 CloudWatch Logs(이를 구성할 수 있음) 및 S3에 보관됩니다. 만료되거나 삭제되지 않으며 서비스 내구성이 적용됩니다. 자세한 S3 내구성 정보는 Amazon S3의 데이터 보호를 참조하세요.

감사 및 보안상의 이유로 10년 동안 보관되는 로그를 제외한 모든 AWS CloudTrail 로그에 대한 로그 보존 변경을 요청할 수 있습니다.

로그 교체는 인스턴스 내에서 구성됩니다. 기본적으로 운영 체제 및 보안 로그는 100MB를 초과하는 경우 시간당 교체되며, 이는 인스턴스의 디스크에서 짧게 실행되지 않도록 하기 위해 수행됩니다.

인스턴스 내의 로그 에이전트는 로그를 CloudWatch Logs에 온라인으로 업로드하고, CloudWatch Logs에서 로그는 S3에 보관됩니다.

로그는 생성된 원시 형식으로 CloudWatch Logs 및 S3에 저장되며 사전 처리가 없습니다.

연속성 관리 기본값

이 섹션에서는 AMS 연속성 관리 기본값을 설명합니다. AMS 백업에 대한 자세한 내용은 AMS 사용 설명서 연속성 관리 장을 참조하세요.

백업 구성은 온보딩 시 수행됩니다. 기본(권장) 백업 설정입니다.

VPC 태그 및 기본값

AMS 백업에 대한 최신 정보는 연속성 관리를 참조하세요.

> **Important**
>
> 기본적으로 EC2 스택 백업은 비활성화됩니다(백업 = 거짓). RFC(CT ct-140EC27q0sjyt1h)를 통해 EC2 스택을 요청할 `Key: Backup, Value: True` 때 태그를 추가하여 생성 시 EC2 인스턴스 백업을 활성화할 수 있습니다. EC2 인스턴스가 생성된 후 태그를 추가하려면 관리 | 고급 스택 구성 요소 | EC2 인스턴스 스택 | CT 업데이트(ct-38s4s4tm4ic4u)를 사용하여 RFC를 제출합니다.

EC2 인스턴스 태그 및 기본값

EC2 스택 백업 태그는 스택에 연결된 EBS 볼륨의 스냅샷이 필요한지 여부를 지정합니다.

`태그 Key: Backup`

태그 `Value: True, False`

기본적으로 값은 `False` 백업 태그가 없고 스택에 예약된 백업이 없습니다.

백업을 활성화`Value: True`하려면 태그를 `Key: Backup` 로 변경하면 VPC 백업 태그로 설정된 일정에 따라 백업이 수행됩니다.

> **Note**
>
> 태그 값(값만 해당)의 대소문자는 구분되지 않으므로 True/true 또는 False/false는 모두 허용됩니다.

RDS 인스턴스 백업 및 기본값

Amazon Relational Database Service(RDS) 기본값은 스택 템플릿에 정의되어 있습니다.

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

패치 기본값

이 섹션에서는 AMS 패치 기본값을 설명합니다. AMS 패치에 대한 자세한 내용은 AMS 사용 설명서 패치 관리 장을 참조하세요.

AMS는 패치된 AMIs를 매월 릴리스합니다. 모든 새 스택 요청은 최신 AMS AMI로 구성해야 합니다.

> **Important**
>
> 태그 기반 패치인 AMS Patch Orchestrator는 AWS Systems Manager(SSM) 기능을 사용하여 인스턴스에 태그를 지정하거나 AMS 태그를 지정할 수 있으며, 구성한 기준 및 창을 사용하여 해당 인스턴스에 패치를 적용할 수 있습니다. 자세한 내용은 패치 오케스트레이터: 태그 기반 패치 모델을 참조하세요.

AMS 표준, 계정 기반, 패치: 인플레이스 패치를 수신하는 스택이 있는 각 계정에 대해 '패치 화요일' 직후 예정된 적용 가능한 패치에 대한 알림이 전송됩니다. 알림에는 모든 스택 및 해당 패치 목록과 제안

된 패치 창이 포함됩니다. 중요한 패치의 경우 기간은 10일 전에 설정되고 표준 패치의 경우 14일 전에 설정됩니다. 알림에 회신하지 않으면 패치가 적용되지 않습니다. 특정 패치를 제외하려면 알림에 회신하거나 서비스 요청을 제출합니다. 패치 적용에 대한 동의로 회신하지만 다른 일정을 구체적으로 요청하지 않으면 수신하는 알림에 설명된 대로 패치가 적용됩니다.

> **Note**
>
> 패치 서비스 알림은 계정 연락처로 전송되는 이메일이며 AWS Support 콘솔에 대한 링크가 포함되어 있습니다. AWS Support 콘솔 또는 알림이 서비스 알림으로 표시되는 AMS 서비스 요청 페이지를 통해 회신할 수 있습니다.

AMS 표준 패치 적용 프로세스 시 AMS는 다음을 수행합니다.

1. 제안된 패치 기간 14일 전에 패치 서비스 알림이 전송됩니다. 패치 서비스 알림은 계정의 파일에 있는 연락처 이메일 주소로 이메일을 통해 전송됩니다.
2. 패치 알림에 제공된 스택 목록을 기반으로 스택에서 연결 가능한 모든 EC2 인스턴스를 식별합니다. 이 경우 "Reachable"은 EC2 상태가 "Running"이고 EC2 Run Command 에이전트가 완전히 작동하는 인스턴스를 의미합니다.
3. AMS는 스택이 정상 상태를 유지하도록 충분한 수의 EC2 인스턴스가 동시에 실행(`healthy-host-threshold` 설정을 통해 구성)되도록 하는 방식으로 패치를 수행합니다.
4. 모든 EC2 인스턴스에 대한 패치 적용 작업이 완료되면 AMS는 RFC를 패치 적용 상태인 성공, 부분 성공 또는 실패로 업데이트합니다. 성공 이외의 상태인 경우 운영자가 패치 결과를 추적하고 수정 조치를 취할 수 있는 티켓이 생성됩니다.

AMS 서비스 검증(SALZ)

AWS Managed Services(AMS) 서비스가 예상대로 작동하는지 확인하기 위해이 장에서 수행할 수 있는 몇 가지 연습을 설명합니다.

AMS 계정 설정 찾기

AMS RFCs, 일정을 설정하고, 알림을 받는 사용자를 결정하는 데 사용되는 계정 설정입니다.

일부 설정은 온보딩 중에 생성되며 서비스 요청을 변경해야 합니다. AMS와 통신할 때 사용할 것이므로 이러한 계정 세부 정보를 기록해 두어야 합니다.

- 자격 증명: AMS 사용자 이름 또는 암호를 검색해야 하는 경우 로컬 IT 관리자에게 문의하세요. AMS는 회사 Active Directory를 사용합니다.
- Cloud Service Delivery Manager(CSDM):이 사용자는 AMS와의 연락 담당자이며 서비스 질문에 답변할 수 있습니다. 온보딩 시이 사람의 연락처 정보가 제공되므로 AMS와 상호 작용하는 조직의 모든 사용자가 해당 정보를 사용할 수 있도록 유지해야 합니다. 이 사용자로부터 AMS 서비스에 대한 월별 보고서를 받을 수 있습니다.
- 콘솔 액세스: 계정에 대해 특별히 설정된 URL로 AMS 콘솔에 액세스합니다. CSDM에서 URL을 가져올 수 있습니다.
- AMS CLI: AMS 콘솔 개발자의 리소스 페이지 또는 CSDM에서 가져오는 배포 가능 패키지를 통해 AMS CLI를 가져올 수 있습니다. 배포 가능 패키지가 있으면 AMS CLI 설치 또는 업그레이드에 설명된 단계를 따릅니다.
- 유지 관리 기간: 유지 관리 기간에 따라 EC2 인스턴스에 대한 패치 적용 시기가 결정됩니다. AWS Managed Services 유지 관리 기간(또는 유지 관리 기간)은 AWS Managed Services(AMS)에 대한 유지 관리 활동을 수행하고 태평양 표준시 기준 매월 두 번째 목요일 오후 3시부터 오후 4시까지 반복됩니다. AMS는 48시간 전에 통지하여 유지 관리 기간을 변경할 수 있습니다. 온보딩 시 다른 기간을 선택했을 수 있습니다. 선택한 유지 관리 기간의 레코드를 보관합니다.
- 모니터링: AMS는 기본적으로 CloudWatch 지표 세트를 제공하지만 추가 지표를 요청할 수도 있습니다. 그렇다면 기록해 둡니다.
- 로그: 기본적으로 로그는 ams-a-*ACCOUNT_ID*-log-management-*REGION*에 저장됩니다. 여기서 *REGION*은 로그가 생성된 리전입니다.
- 완화: 온보딩 시 AMS는 리소스에 대한 맬웨어 공격이 식별되는 경우 선택한 완화 조치를 기록합니다. 예를 들어 특정 사용자에게 문의합니다. AMS와 상호 작용하는 조직의 모든 사용자가이 정보를 사용할 수 있도록 합니다.
- 리전: AMS 콘솔에서 VPC 세부 정보 페이지를 볼 수 있습니다. AMS SKMS CLI를 설치한 후이 명령을 실행할 수도 있습니다(이 명령은 SAML 프로파일을 사용하며 인증 방법이 다른 경우 제거).

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실

행할 `--region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml`경우를 추가해야 할 수도 있습니다.

AMS에서 FQDNs 찾기

AWS Managed Services(AMS) 액세스 변경 유형(CTs)에는 AMS 신뢰 도메인의 정규화된 도메인 이름 또는 FQDN이 형식으로 필요합니다`C844273800838.amazonaws.com`. AWS FQDN을 검색하려면 다음 중 하나를 수행합니다.

- AWS 콘솔: AWS Directory Service 콘솔의 디렉터리 이름 열을 확인합니다.
- CLI: 도메인에 로그인한 상태에서 다음 명령을 사용합니다.

  Windows(사용자 및 FQDN 반환):

  ```
  whoami /upn
  ```

  또는 (DC+DC+DC=FQDN)

  ```
  whoami /fqdn
  ```

  Linux:

  ```
  hostname --fqdn
  ```

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다`us-east-1`. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 `--region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml`경우를 추가해야 할 수도 있습니다.

AMS에서 가용 영역(AZs) 찾기

가용 영역: 모든 계정에 가용 영역이 두 개 이상 있습니다. 가용 영역 이름을 정확하게 찾으려면 먼저 연결된 서브넷 ID를 알아야 합니다.

- AMS 콘솔: 탐색 창에서 VPCs 클릭한 다음 필요한 경우 관련 VPC를 클릭합니다. VPCs 세부 정보 페이지에서 서브넷 테이블의 관련 서브넷을 선택하여 연결된 가용 영역의 이름이 있는 서브넷 세부 정보 페이지를 엽니다.
- AMS SKMS API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다`us-east-1`. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 `--region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml`경우를 추가해야 할 수도 있습니다.

AMS에서 SNS 주제 찾기

SNS 주제에 따라 다양한 상황에서 알림을 받는 사람이 결정됩니다. AMS는 AMI 알림(SNS를 사용한 AMS AMI 알림 참조), CloudWatch 경보 및 EC2 리소스(AMS에서 생성한 알림 수신 참조) 등에 대한 SNS 주제를 제공합니다. CloudWatch EC2 https://docs.aws.amazon.com/managedservices/latest/userguide/sent-alert-views.html 기존 SNS 주제를 검색하려면:

- AWS 콘솔: SNS 콘솔을 사용하여 모든 주제, 애플리케이션 및 구독과 메시지 그래프를 볼 수 있습니다. 또한 주제를 생성, 삭제, 구독 및 게시합니다.
- API/CLI(AMS 계정에 로그인한 경우 AWS CLI 필요):

  SNS 주제를 나열합니다.

```
aws sns list-topics
```

SNS 구독을 나열합니다.

```
aws sns list-subscriptions
```

> **Note**
>
> AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 `--region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml`경우를 추가해야 할 수도 있습니다.

AMS에서 백업 설정 찾기

백업 및 스냅샷은 네이티브 AWS Backup 서비스를 통해 AMS에서 관리합니다.

구성은 AWS Backup 계획을 통해 관리됩니다. 태그가 지정된 리소스를 백업 일정 및 보존 정책과 연결하는 여러 AWS Backup 계획이 있을 수 있습니다. AMS 계정 AWS Backup 설정을 찾으려면 https://console.aws.amazon.com/backup 콘솔 또는 백업 명령에 대한 AWS CLI 명령 참조를 사용합니다.

AMS 및에 대한 자세한 내용은 연속성 관리를 AWS Backup참조하세요. https://docs.aws.amazon.com/managedservices/latest/userguide/continuity-mgmt.html

인스턴스 ID 또는 IP 주소 찾기

인스턴스에 로그인하려면 인스턴스 IP 주소가 필요합니다.

- 인스턴스에 대한 액세스를 요청하거나, 인스턴스에 로그인하거나, AMI를 생성하려면 인스턴스 ID가 있어야 합니다. EC2 인스턴스(독립 실행형 인스턴스 또는 스택의 일부) 또는 데이터베이스 인스턴스의 경우 다음과 같은 몇 가지 방법으로 ID를 찾을 수 있습니다.
  - ASG 스택의 인스턴스에 대한 AMS 콘솔: 스택을 생성한 RFC의 RFC 세부 정보 페이지를 확인합니다. 실행 출력 섹션에서 ASG 스택의 스택 ID를 찾은 다음 EC2 콘솔 Auto Scaling 그룹 페이지로 이동하여 해당 스택 ID를 검색하고 해당 스택에 대한 인스턴스를 찾을 수 있습니다. 인스턴스를 찾으면 인스턴스를 선택하면 페이지 하단에 IP 주소를 포함한 세부 정보가 포함된 영역이 열립니다.

- 독립 실행형 EC2 또는 데이터베이스(DB) 인스턴스용 AMS 콘솔: EC2 스택 또는 DB 인스턴스를 생성한 RFC의 RFC 세부 정보 페이지를 확인합니다. 실행 출력 섹션에서 인스턴스 ID 및 IP 주소를 찾을 수 있습니다.
- AWS EC2 콘솔:
  1. 탐색 창에서 [인스턴스(Instances)]를 선택합니다. 인스턴스 페이지가 열립니다.
  2. ID를 사용할 인스턴스를 클릭합니다. 인스턴스 세부 정보 페이지가 열리고 ID 및 IP 주소가 표시됩니다.
- AWS 데이터베이스 콘솔:
  1. 홈 페이지에서 DB 인스턴스를 선택합니다. 인스턴스 페이지가 열립니다.
  2. ID를 사용할 DB 인스턴스를 필터링합니다. 인스턴스 세부 정보 페이지가 열리고 ID가 표시됩니다.
- AMS CLI/API.

> **Note**
>
> 이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 `--profile` 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms` *`ams-cli-command`* `--profile SAML`. 와 같이 모든 AMS 명령이 us-east-1에서 실행되므로 `--region` 옵션을 추가해야 할 수도 있습니다`aws amscm` *`ams-cli-command`* `--region=us-east-1`.

> **Note**
>
> AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다`us-east-1`. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 `--region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml`경우를 추가해야 할 수도 있습니다.

다음 명령을 실행하여 스택 실행 출력 세부 정보를 가져옵니다.

```
aws amsskms get-stack --stack-id STACK_ID
```

출력은 하단 근처의 아래에 InstanceId가 나타나는 것과 비슷합니다Outputs(표시된 값은 예제임).

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
```

```
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```

DNS 친화적인 접속 이름

MALZ

다중 계정 랜딩 존(MALZ)의 경우 AMS 관리형 Active Directory의 FQDN에 있는 접속에 대한 DNS 레코드가 생성됩니다. AMS는 필요에 따라 Linux 및 Windows 접속을 대체합니다. 예를 들어 배포해야 하는 새 접속 AMI가 있는 경우 접속 DNS 레코드는 새롭고 유효한 접속을 가리키도록 동적으로 업데이트됩니다.

1. SSH(Linux) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니다. `sshbastion`*`(1-4)`*`.`*`Your_Domain`*`.com`

   예를 들어 도메인이 인 경우`Your_Domain`:

   - `sshbastion1.`*`Your_Domain`*`.com`
   - `sshbastion2.`*`Your_Domain`*`.com`
   - `sshbastion3.`*`Your_Domain`*`.com`
   - `sshbastion4.`*`Your_Domain`*`.com`
2. RDP(Windows) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니다`rdp-`*`Username`*`.`*`Your_Domain`*`.com`.

   예를 들어 사용자 이름이 , `alex`, `demo`또는 `testbob`이고 도메인이 인 경우*`Your_Domain`*`.com`:

   - `rdp-alex.`*`Your_Domain`*`.com`
   - `rdp-test.`*`Your_Domain`*`.com`
   - `rdp-demo.`*`Your_Domain`*`.com`
   - `rdp-bob.`*`Your_Domain`*`.com`

SALZ

단일 계정 랜딩 존(SALZ)은 필요에 따라 Linux 및 Windows 접속을 대체합니다. 예를 들어 배포해야 하는 새 접속 AMI가 있는 경우 접속 DNS 레코드는 새롭고 유효한 접속을 가리키도록 동적으로 업데이트됩니다.

1. SSH(Linux) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니다. `sshbastion(1-4).A*AccountNumber*.amazonaws.com.`

   예를 들어, 여기서 `123456789012`는 계정 번호입니다.

   - `sshbastion1.A123456789012.amazonaws.com`
   - `sshbastion2.A123456789012.amazonaws.com`
   - `sshbastion3.A123456789012.amazonaws.com`
   - `sshbastion4.A123456789012.amazonaws.com`

2. RDP(Windows) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니다. `rdpbastion(1-4).A*ACCOUNT_NUMBER*.amazonaws.com.`

   예를 들어, 여기서 `123456789012`는 계정 번호입니다.

   - `rdpbastion1.A123456789012.amazonaws.com`
   - `rdpbastion2.A123456789012.amazonaws.com`
   - `rdpbastion3.A123456789012.amazonaws.com`
   - `rdpbastion4.A123456789012.amazonaws.com`

접속 IP 주소 찾기

AMS 고객은 앞서 DNS 친화적인 접속 이름 설명한 SSH 및 RDP 접속 또는 접속 IP 주소를 사용할 수 있습니다.

계정의 접속 IP 주소, SSH 및 RDP를 찾으려면:

1. 다중 계정 랜딩 존만 해당: 공유 서비스 계정에 로그인합니다.
2. EC2 콘솔을 열고 인스턴스 실행을 선택합니다.

   인스턴스 페이지가 열립니다.

3. 상단의 필터 상자에 ssh-bastion 또는 rdp-bastion을 입력합니다.

상단의 필터 상자에 customer-ssh 또는 customer-rdp를 입력합니다.

계정의 SSH 및/또는 RDP 접속이 표시됩니다.

SSH 배스천 외에도 목록에 AMS 경계 네트워크 배스천이 표시될 수 있으며,이 배스천은 사용할 수 없습니다.

4. SSH 또는 RDP 접속을 선택합니다. Windows 컴퓨터를 사용하고 Linux 인스턴스에 로그인하려는 경우 SSH 접속을 사용합니다. Windows 인스턴스에 로그인하려면 RDP 접속을 사용합니다. Linux OS를 사용 중이고 Windows 인스턴스에 로그인하려는 경우 RDP 터널을 통해 SSH 접속을 사용합니다(Windows 데스크톱에 액세스할 수 있도록). Linux OS에서 Linux 인스턴스에 액세스하려면 SSH 접속을 사용합니다.

EC2 인스턴스: 생성

AMS 콘솔 또는 API/CLI를 사용하여 추가 볼륨이 있는 Amazon EC2 및 Amazon EC2를 생성할 수 있습니다.

스택 생성

콘솔을 사용하여 EC2 인스턴스 생성

다음은 AMS 콘솔에서이 변경 유형을 보여줍니다.

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.

3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다(변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

   실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.
4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 성공적으로 생성된 RFC 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 EC2 인스턴스 생성

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 `CreateRfc` 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 이스케이프 따옴표)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

템플릿 생성:

1. 이 변경 유형의 실행 파라미터를 JSON 파일로 출력합니다.이 예제에서는 CreateEC2Params.json:이라는 이름을 지정합니다.

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. CreateEC2Params 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

   ```
   {
     "Description": "Create a new EC2 Instance stack",
     "VpcId": "vpc-0a60eb65b4EXAMPLE",
     "Name": "My-EC2",
     "TimeoutInMinutes": 60,
     "Parameters": {
       "InstanceAmiId": "ami-1234567890EXAMPLE",
       "InstanceDetailedMonitoring": false,
       "InstanceEBSOptimized": false,
       "InstanceProfile": "customer-mc-ec2-instance-profile",
       "InstanceRootVolumeIops": 3000,
       "InstanceRootVolumeType": "gp3",
       "InstanceType": "t2.large",
       "InstanceUserData": "",
       "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
   ```

```
    "EnforceIMDSV2": "false"
  }
}
```

3. RFC 템플릿을 현재 폴더의 파일로 출력합니다.이 예제에서는 CreateEC2Rfc.json:이라는 이름을 지정합니다.

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. CreateEC2Rfc.json 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. CreateEC2Rfc 파일과 CreateEC2Params 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

보안 그룹

이 변경 유형의 버전 3.0부터 자체 보안 그룹을 지정하는 경우 AMS는 기본 AMS 보안 그룹을 연결하지 않습니다. 요청에 자체 보안 그룹을 지정하지 않으면 AMS가 AMS 기본 보안 그룹을 연결합니다. 이전 버전에서 AMS는 사용자가 자체 보안 그룹을 제공했는지 여부에 관계없이 기본 보안 그룹을 연결했습니다.

현재 사용자 지정 보안 그룹을 지정하는 경우 계정에 대한 기본 AMS 보안 그룹 `mc-initial-garden-SG-name` 및의 IDs도 지정해야 합니다`mc-initial-garden-SG-name`.

> **인스턴스 유형**
>
> AMS는 t2.micro/t3.micro 및 t2.nano/t3.nano 유형을 권장하지 않습니다. 이는 더 작은 인스턴스 유형이며 애플리케이션 및 AMS 도구의 성능을 저하시킬 수 있습니다. EC2 인스턴스에는 애플리케이션 워크로드 외에도 EPS, SSM 및 Cloudwatch와 같은 AMS 도구를 지원할 수 있는 충분한 용량이 필요합니다. 자세한 내용은 애플리케이션에 적합한 EC2 인스턴스 유형 선택을 참조하세요.

추가 볼륨이 있는 EC2 스택을 생성하려면 EC2 스택 | 생성(추가 볼륨 포함)을 참조하세요.

최대 50개의 태그를 추가할 수 있지만 추가하려면 추가 구성 보기를 활성화해야 합니다.

필요한 경우 EC2 인스턴스 스택 생성 실패를 참조하세요.

스택 생성(추가 볼륨 포함)

콘솔을 사용하여 EC2 인스턴스 및 추가 볼륨 생성

다음은 AMS 콘솔에서이 변경 유형을 보여줍니다.

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.
3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다(변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.

4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 RFC가 성공적으로 생성된 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 EC2 인스턴스 및 추가 볼륨 생성

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 `CreateRfc` 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

실행 파라미터가 인라인으로 제공된 상태에서 RFC 생성 명령을 실행한 다음(실행 파라미터를 인라인으로 제공할 때 따옴표 이스케이프 표시) 반환된 RFC ID를 제출합니다(예제에서는 필수 파라미터만 표시). 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

템플릿 생성:

1. 이 변경 유형의 실행 파라미터를 CreateEC2AVParams.json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
   ```

2. CreateEC2AVParams 파일을 수정하고 저장합니다(예: 대부분의 파라미터 표시). 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

   ```
   {
   "Description":      "EC2-Create-1-Addl-Volumes",
   "VpcId":            "VPC_ID",
   "StackTemplateId":  "stm-nn8v8ffhcal611bmo",
   "Name":             "My-EC2-1-Addl-Volume",
   "TimeoutInMinutes": 60,
   "Parameters":   {
       "InstanceAmiId":    "AMI_ID",
       "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
       "InstanceCoreCount": 1,
       "InstanceThreadsPerCore": 2,
       "InstanceDetailedMonitoring": "true",
       "InstanceEBSOptimized": "false",
       "InstanceProfile": "customer-mc-ec2-instance-profile",
       "InstanceRootVolumeIops": 100,
       "InstanceRootVolumeName": "/dev/xvda",
       "InstanceRootVolumeSize": 50,
       "InstanceRootVolumeType": "io1",
       "RootVolumeKmsKeyId": "default",
       "InstancePrivateStaticIp": "10.27.0.100",
       "InstanceSecondaryPrivateIpAddressCount": 0,
       "InstanceTerminationProtection": "false",
   ```

```
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. RFC 템플릿을 현재 폴더의 파일로 출력합니다.이 예제에서는 CreateEC2AVRfc.json:이라는 이름을 지정합니다.

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. CreateEC2AVRfc.json 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. CreateEC2AVRfc 파일과 CreateEC2AVParams 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

Important

다른 StackTemplateId(stm-nn8v8ffhcal611bmo)를 사용하는이 변경 유형의 새 버전 v 4.0이 있습니다. 이는 명령줄에이 변경 유형의 RFC를 제출하는 경우 중요합니다. 새 버전은 두 개의 새 파라미터(RootVolumeKmsKeyId 및 CreditSpecification)를 도입하고 하나의 기존 파라미터(InstanceType)의 기본값을 변경합니다.

인스턴스 유형

- 코어 또는 스레드 수를 지정하도록 선택한 경우 둘 다에 대한 값을 지정해야 합니다. `InstanceCoreCount` 및 파라미터를 사용합니다`InstanceThreadsPerCore`. 코어/스레드의 유효한 조합을 찾으려면 인스턴스 유형별 CPU 코어 및 CPU 코어당 스레드를 참조하세요.
- AMS는 t2.micro/t3.micro 또는 t2.nano/t3.nano 인스턴스 유형을 권장하지 않습니다. 이는 비즈니스 워크로드 외에도 EPS, SSM 및 Cloudwatch와 같은 AMS 도구를 지원하기에 너무 작습니다. 자세한 내용은 애플리케이션에 적합한 EC2 인스턴스 유형 선택을 참조하세요.
- 버전 4.0에서는 기본 유형이 t2.large에서 t3.large로 증가했습니다. T3 인스턴스는 기본적으로 '무제한 크레딧'으로 시작됩니다. 인스턴스가 모든 CPU 크레딧을 소비하더라도 CPU 제한이 발생하지 않습니다. 대신 T2 인스턴스를 선택하고 CreditSpecification 무제한 옵션을 사용할 수 있습니다.
- 크기 권장 사항을 포함하여 Amazon EC2에 대한 자세한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하세요.

볼륨이 생성된 후 추가 볼륨으로 EC2 스택을 업데이트하려면 EC2 인스턴스 스택: 업데이트(추가 볼륨 포함)를 참조하세요.

액세스, 요청

관리 액세스 요청

콘솔을 사용하여 관리자 액세스 요청

다음은 AMS 콘솔에서이 변경 유형을 보여줍니다.

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 널리 사용되는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.
3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다(변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

   실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.
4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 성공적으로 생성된 RFC 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 관리자 액세스 요청

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일을 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> CreateRfc 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}" RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 이스케이프 따옴표)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

템플릿 생성:

1. 이 변경 유형에 대한 실행 파라미터 JSON 스키마를 파일로 출력합니다.이 예제에서는 GrantAdminAccessParams.json:이라는 이름을 지정합니다.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantAdminAccessParams.json
   ```

   GrantAdminAccessParams 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   ```

```
"StackIds":              [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":              ["USERNAME", "USERNAME"],
"VpcId":                 "VPC_ID"
}
```

옵션은 TimeRequestedInHours 기본적으로 1시간으로 설정됩니다. 최대 12시간을 요청할 수 있습니다.

2. RFC 템플릿을 현재 폴더의 파일로 출력합니다.이 예제에서는 GrantAdminAccessRfc.json:이라는 이름을 지정합니다.

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. GrantAdminAccessRfc.json 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
{
"ChangeTypeId":          "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":     "3.0",
"Title":                 "Request-Admin-Access-to-EC2-RFC"
}
```

4. GrantAdminAccessRfc 파일과 GrantAdminAcessParams 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

Bastion을 통해 인스턴스에 로그인하려면 다음 절차인 인스턴스 액세스 예제를 따릅니다.

팁

> **Note**
>
> 액세스 요청이 만료되기 전에 업데이트를 제출할 수 있습니다. 자세한 내용은 스택 관리자 액세스 | 업데이트를 참조하세요.

ASG의 일부인 인스턴스에 로그인하려면 ASG 스택에 대한 액세스를 요청하면 연결된 모든 인스턴스에 액세스할 수 있습니다.

ReadOnly 액세스 요청에 대한 예는 ReadOnly 액세스: 요청을 참조하세요.

ReadOnly 액세스 요청

콘솔을 사용하여 ReadOnly 액세스 요청

다음은 AMS 콘솔에서이 변경 유형을 보여줍니다.

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.
3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다 (변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

   실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.
4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 RFC가 성공적으로 생성된 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 ReadOnly 액세스 요청

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일을 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id ID` 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id ID` 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> `CreateRfc` 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 따옴표 이스케이프)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

템플릿 생성:

1. 이 변경 유형에 대한 실행 파라미터 JSON 스키마를 파일로 출력합니다.이 예제에서는 GrantReadOnlyAccessParams.json:이라는 이름을 지정합니다.

```
aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 GrantReadOnlyAccessParams.json
```

GrantReadOnlyAccessParams 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Usernames":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

옵션은 TimeRequestedInHours 기본적으로 1시간으로 설정됩니다. 최대 12시간을 요청할 수 있습니다.

2. RFC 템플릿을 현재 폴더의 파일로 출력합니다.이 예제에서는 RFC 템플릿의 이름을 GrantReadOnlyAccessRfc.json:으로 지정합니다.

```
aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
```

3. GrantReadOnlyAccessRfc.json 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
{
"ChangeTypeId":         "ct-199h35t7uz6jl",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. GrantReadOnlyAccessRfc 파일과 GrantReadOnlyAcessParams 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

Bastion을 통해 인스턴스에 로그인하려면 다음 절차인 인스턴스 액세스 예제를 따릅니다.

팁

> **Note**
>
> 액세스 요청이 만료되기 전에 업데이트를 제출할 수 있습니다. 자세한 내용은 스택 읽기 전용 액세스 | 업데이트를 참조하세요.
> EC2 Auto Scaling 그룹(ASG)의 일부인 인스턴스에 로그인하려면 ASG 스택에 대한 액세스를 요청하면 연결된 모든 인스턴스에 액세스할 수 있습니다.

관리자 액세스 요청에 대한 연습은 관리자 액세스: 요청을 참조하세요.

기타 | 기타 RFC, 생성(CLI)

이 예제에서는 관리 | 기타 | 기타 | CTs 주소를 지정하지 않는 변경을 요청하는 방법을 보여줍니다.

원하는 항목에 대한 변경 유형을 찾을 수 없는 경우이 CT를 사용합니다. 그러나 기존 CT에서 파라미터를 지정하는 것이 확실하지 않은 경우 서비스 요청을 제출하여 도움을 받는 것이 좋습니다. 서비스 요청 제출에 대한 자세한 내용은 서비스 요청 예제를 참조하세요.

이 유형의 RFC는 승인 필수이므로 구현하려면 AMS 승인이 필요합니다. RFC를 제출하면 AMS 운영자가 사용자에게 연락하여 배포하려는 스택에 대해 설명합니다.

> **Note**
>
> 수동 CTs를 사용하는 경우 ASAP 예약 옵션(콘솔에서 ASAP 선택, API/CLI에서 시작 및 종료 시간 비워 두기)을 사용하는 것이 좋습니다. 이러한 CTs는 AMS 운영자가 RFC를 검사하고 승인 및 실행 전에 사용자와 통신해야 하기 때문입니다. 이러한 RFCs 예약하는 경우 최소 24시간을 허용해야 합니다. 예정된 시작 시간 전에 승인이 이루어지지 않으면 RFC가 자동으로 거부됩니다.

필수 데이터:

- Comment: RFC의 용도입니다.
- ChangeTypeId 및 ChangeTypeVersion: 기타 | 생성(ct-1e1xtak34nx76)을 사용하여 새 리소스를 요청하고, 기타 | 업데이트(ct-0xdawir96cy7k)를 사용하여 기존 리소스를 변경합니다. 둘 다 입니다v1.

선택적 데이터: Priority: 허용되는 값은 High, Medium또는 입니다Low.

인라인 생성:

- 인라인으로 제공된 실행 파라미터를 사용하여 RFC 생성 명령을 실행합니다(실행 파라미터를 인라인으로 제공할 때 따옴표 이스케이프). 예제에서는 기타 | 생성을 사용합니다.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- RFC 생성 작업에서 반환된 RFC ID를 사용하여 RFC를 제출합니다. 제출될 때까지 RFC는 Editing 상태를 유지하고 조치를 취하지 않습니다.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- RFC 상태를 모니터링하고 실행 출력을 봅니다.

```
aws amscm get-rfc --rfc-id RFC_ID
```

템플릿 생성:

1. 실행 파라미터에 대한 JSON 파일을 생성하고 저장합니다. 예제에서는이 파일의 이름을 OtherParams.json으로 지정하고 선택적 Priority 파라미터를 포함합니다.

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. RFC 파라미터에 대한 JSON 파일을 생성하고 저장합니다. 예제에서는 이름을 OtherRfc.json.

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
```

```
"Title":                "TITLE"
}
```

3. OtherRfc 파일과 OtherParams 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

응답에서 새 RFC의 RfcId를 수신합니다. 예제:

```
{
"RfcId": "RFC-ID"
}
```

4. RFC 제출:

```
aws amscm submit-rfc --rfc-id RFC-ID
```

오류가 보고되지 않으면 작업이 성공한 것입니다.

5. 요청 상태를 모니터링하고 실행 출력을 보려면:

```
aws amscm get-rfc --rfc-id RFC-ID
```

모든 스택: 삭제, 재부팅, 시작, 중지

AMS 콘솔 또는 API/CLI를 사용하여 AMS 스택을 삭제, 재부팅, 시작 또는 중지할 수 있습니다.

스택 삭제

콘솔을 사용하여 스택 삭제

AMS 콘솔에서이 변경 유형의 스크린샷:

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.

2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.
3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다(변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

   실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.
4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 성공적으로 생성된 RFC 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 스택 삭제

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 CreateRfc 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}" RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 이스케이프 따옴표)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

템플릿 생성:

1. RFC 템플릿을 현재 폴더의 파일로 출력합니다.이 예제에서는 DeleteStackRfc.json:이라는 이름을 지정합니다.

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. DeleteStackRfc.json 파일을 수정하고 저장합니다.

   ExecutionParameters JSON 확장의 내부 따옴표는 백슬래시(\)로 이스케이프 처리해야 합니다. 시작 및 종료 시간이 없는 예:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   ```

```
}
```

3. RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

> **Note**
>
> S3 버킷을 삭제하는 경우 먼저 객체를 비워야 합니다.

> **Important**
>
> 스택을 삭제하면 원치 않고 예상치 못한 결과가 발생할 수 있습니다. 중요한 주의 사항은 스택 삭제를 위한 RFC 문제 해결 섹션 RFCs를 참조하세요.

스택 재부팅

콘솔을 사용하여 스택 재부팅

AMS 콘솔에서이 변경 유형의 스크린샷:

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.

- 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.

3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다(변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

   실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.

4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 성공적으로 생성된 RFC 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.

5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 스택 재부팅

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.

2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 `CreateRfc` 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 이스케이프 따옴표)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

템플릿 생성:

1. RFC 템플릿을 현재 폴더의 파일로 출력합니다. 이 예제에서는 RebootStackRfc.json. 인스턴스를 중지(재부팅 또는 시작)하기 위한 실행 파라미터가 하나뿐이므로 실행 파라미터는 스키마 JSON 파일 자체에 있을 수 있으며 별도의 실행 파라미터 JSON 파일을 생성할 필요가 없습니다.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. RebootStackRfc.json 파일을 수정하고 저장합니다.

   `ExecutionParameters` JSON 확장의 내부 따옴표는 백슬래시(\)로 이스케이프 처리해야 합니다. 예제:

   ```
   {
   "ChangeTypeId":          "ct-02u0hoaa9grat",
   "Title":                 "Reboot-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

Application Load Balancer에 대한 자세한 내용은 Application Load Balancer를 참조하세요.

스택 시작

콘솔을 사용하여 스택 시작

AMS 콘솔에서이 변경 유형의 스크린샷:

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성이 가능한 이전 CT 버전은 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.
3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다(변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

   실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.

4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 RFC가 성공적으로 생성된 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 스택 시작

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일을 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 RFC에서 `CreateRfc` 파라미터를 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 이스케이프 따옴표)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

템플릿 생성:

1. RFC 템플릿을 현재 폴더의 파일로 출력합니다. 이 예제에서는 StartInstanceRfc.json. 스택을 시작하기 위한 실행 파라미터가 하나뿐이므로 실행 파라미터는 스키마 JSON 파일 자체에 있을 수 있으며 별도의 실행 파라미터 JSON 파일을 생성할 필요가 없습니다.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. StartStackRfc.json 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

   ```
   {
   "ChangeTypeId":          "ct-1h5xgl9cr4bzy",
   "Title":                 "Start-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. RFC를 생성합니다.

   ```
   aws amscm create-rfc --cli-input-json file://StartStackRfc.json
   ```

   응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

Application Load Balancer에 대한 자세한 내용은 Application Load Balancer를 참조하세요.

스택 중지

콘솔을 사용하여 스택 중지

AMS 콘솔에서이 변경 유형의 스크린샷:

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
   - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성이 가능한 이전 CT 버전은 선택할 수 없습니다.

     CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.
   - 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.
3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다 (변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

   실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.
4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 RFC가 성공적으로 생성된 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 스택 중지

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일을 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 명령을 제출합니다.

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 RFC에서 CreateRfc 파라미터를 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}" RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 AMS Change Management API 참조를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 이스케이프 따옴표)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

템플릿 생성:

1. RFC 템플릿을 현재 폴더의 파일로 출력합니다. 이 예제에서는 StopStackRfc.json. 인스턴스를 중지(재부팅 또는 시작)하기 위한 실행 파라미터가 하나뿐이므로 실행 파라미터는 스키마 JSON 파일 자체에 있을 수 있으며 별도의 실행 파라미터 JSON 파일을 생성할 필요가 없습니다.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
   ```

2. StopStackRfc.json 파일을 수정하고 저장합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

   ```
   {
   "ChangeTypeId":          "ct-3dgbnh6gpst4d",
   "Title":                 "Stop-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
   ```

```
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

AMS Resource Scheduler를 사용하여 재시작을 예약하지 않는 한 중지된 인스턴스는 중지된 상태로 유지됩니다.

필요한 경우 EC2 인스턴스 스택 중지 실패를 참조하세요.

액세스 예제

이 예제에서는 RFC를 통해 액세스 권한이 부여되면 Bastion을 통해 인스턴스에 로그인하는 방법을 보여줍니다. 액세스 권한 부여에 대한 자세한 내용은 액세스 요청을 참조하세요.

> **Note**
>
> Auto Scaling 그룹을 통해 생성된 EC2 인스턴스에는 순환 및 순환하는 IP 주소가 있으며 EC2 콘솔을 사용하여 해당 IP 주소를 찾아야 합니다.

필수 데이터:

- 접속 DNS 표시 이름 또는 IP 주소:에 설명된 DNS 표시 이름을 사용하거나에 설명된 접속 IP 주소를 DNS 친화적인 접속 이름 찾습니다접속 IP 주소 찾기.
- 사용자 이름(예: username@customerdomain.com) 및 암호: 계정의 자격 증명.
- 스택 IP 주소: 로그인하려는 스택의 AMS 콘솔 스택 페이지를 확인한 다음 계정의 EC2 콘솔에서 해당 스택 ID를 기준으로 필터링하여이 정보를 가져옵니다. 단일 EC2 인스턴스의 경우 AMS SKMS 명령을 사용할 수도 있습니다. AMS SKMS API 참조의 경우 AWS Artifact 콘솔의 보고서 탭을 참조하세요. 스택 ID를 찾으려면 AMS SKMS API 참조의 경우 AWS Artifact 콘솔의 보고서 탭을 참조하세요. 스택 IP 주소를 찾으려면 .

필요에 따라 SSH 또는 RDP의 접속 IP 주소에 액세스하고 다음 절차 중 하나를 사용하여 로그인합니다.

Linux 컴퓨터에서 Linux 인스턴스로

SSH를 사용하여 SSH 접속에 연결한 다음 Linux 인스턴스에 연결합니다.

MALZ

친숙한 접속 이름에 대한 자세한 내용은 DNS 접속을 참조하세요.

Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

1. 쉘 창을 열고 다음을 입력합니다.

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

Domain_FQDN이 "corp.domain.com"이고, 계정 번호가 "123456789123"이고, Your_Domain이 "amazonaws.com"이고, Bastion "4"를 선택하고, 사용자 이름이 "JoeSmith"인 경우 다음과 같습니다.

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 회사 Active Directory 자격 증명으로 로그인합니다.
3. Bash 프롬프트가 표시되면 인스턴스에 SSH를 입력한 다음 다음을 입력합니다.

```
ssh Domain_FQDN\\Username@Instance_IP
```

또는 로그인 플래그(-l)를 사용할 수 있습니다.

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

친숙한 접속 이름에 대한 자세한 내용은 DNS 접속을 참조하세요.

Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

1. 쉘 창을 열고 다음을 입력합니다.

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

계정 번호가 123456789123이고 Bastion 4를 선택하며 사용자 이름이 JoeSmith인 경우 다음과 같습니다.

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 회사 Active Directory 자격 증명으로 로그인합니다.
3. Bash 프롬프트가 표시되면 인스턴스에 SSH를 입력한 다음 다음을 입력합니다.

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

또는 로그인 플래그(-l)를 사용할 수 있습니다.

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux 컴퓨터에서 Windows 인스턴스로

SSH 터널과 RDP 클라이언트를 사용하여 Linux 컴퓨터에서 Windows 인스턴스에 연결합니다.

MALZ

이 절차에서는 Linux용 원격 데스크톱 연결 클라이언트가 필요합니다.이 예제에서는 Microsoft 원격 데스크톱(Windows 원격 데스크톱 서비스에 연결하기 위한 오픈 소스 UNIX 클라이언트)을 사용합니다. Rdesktop이 대안입니다.

> **Note**
>
> Windows 인스턴스에 로그인하는 방법은 사용 중인 원격 데스크톱 클라이언트에 따라 변경될 수 있습니다.

먼저 SSH 터널을 설정한 다음 로그인합니다.

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요DNS 친화적인 접속 이름.

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 액세스 요청을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).Your_Domain
```

Domain_FQDN이 "corp.domain.com"이고, AMS 관리형 Your_Domain이 "amazonaws.com"이고, Bastion "4"를 선택하고, 사용자 이름이 "JoeSmith"인 경우 다음과 같습니다.

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 인스턴스 ID 또는 IP 주소 찾기를 참조하세요.

1. Linux 데스크톱에서 Windows 인스턴스로 SSH 터널을 통해 RDP를 설정합니다. ssh 명령을 올바른 값으로 실행하려면 다음과 같은 몇 가지 방법으로 진행할 수 있습니다.

   - Linux 셸에서 변수를 설정한 다음 SSH 연결 명령을 입력합니다.

   ```
   BASTION="sshbastion(1-4).Your_Domain""
   WINDOWS="Windows_Instance_Private_IP"
   AD="AD_Account_Number"
   USER="AD_Username"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   다음 값이 사용되는 경우의 예:

   ```
   BASTION="sshbastion4.A123456789123.amazonaws.com"

   WINDOWS="172.16.3.254"

   AD="ACORP_example"

   USER="john.doe"
   ```

   - 변수 값을 ssh 명령에 직접 추가합니다.

   어느 경우든 렌더링된 요청은 다음과 같습니다(동일한 변수 값 집합을 가정).

   ```
   ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
   ```

2. 둘 중 하나: 원격 데스크톱 클라이언트를 열고 루프백 주소와 포트 127.0.0.1:3389를 입력한 다음 연결을 엽니다.

   또는 새 Linux 데스크톱 쉘에서 Windows 인스턴스에 로그인합니다. RDesktop을 사용하는 경우 명령은 다음과 같습니다.

   ```
   rdesktop 127.0.0.1:3389
   ```

   Windows 인스턴스의 원격 데스크톱 창이 Linux 데스크톱에 나타납니다.

   > **Tip**
   >
   > 원격 데스크톱 세션이 시작되지 않는 경우 SSH 접속에서 Windows 인스턴스로의 네트워크 연결이 1단계의 쉘에서 포트 3389에서 허용되는지 확인합니다(`private_ip_address_of_windows_instance`적절하게 교체).
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > 성공:
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >         Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >         netstat -anvp | grep 3389
   >         tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

SALZ

단일 계정 랜딩 존에 대한이 절차를 수행하려면 Linux용 원격 데스크톱 연결 클라이언트가 필요합니다.이 예제에서는 Microsoft 원격 데스크톱(Windows 원격 데스크톱 서비스에 연결하기 위한 오픈 소스 UNIX 클라이언트)을 사용합니다. Rdesktop이 대안입니다.

> **Note**
>
> Windows 인스턴스에 로그인하는 방법은 사용 중인 원격 데스크톱 클라이언트에 따라 변경될 수 있습니다.

먼저 SSH 터널을 설정한 다음 로그인합니다.

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요DNS 친화적인 접속 이름.

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 액세스 요청을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

계정 번호가 1234567891230이고 Bastion 4를 선택하면 다음과 같습니다.

```
sshbastion4.A123456789123.amazonaws.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 인스턴스 ID 또는 IP 주소 찾기를 참조하세요.

1. Linux 데스크톱에서 Windows 인스턴스로 SSH 터널을 통해 RDP를 설정합니다. ssh 명령을 올바른 값으로 실행하려면 다음과 같은 몇 가지 방법으로 진행할 수 있습니다.

   - Linux 셸에서 변수를 설정한 다음 SSH 연결 명령을 입력합니다.

   ```
   BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
   WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
   AD="AD_ACCOUNT_NUMBER"
   USER="AD_USERNAME"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   다음 값이 사용되는 경우의 예:

   ```
   BASTION="sshbastion4.A123456789123.amazonaws.com"

   WINDOWS="172.16.3.254"

   AD="ACORP_example"

   USER="john.doe"
   ```

   - 변수 값을 ssh 명령에 직접 추가합니다.

어느 경우든 렌더링된 요청은 다음과 같습니다(동일한 변수 값 집합을 가정).

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. 둘 중 하나: 원격 데스크톱 클라이언트를 열고 루프백 주소와 포트 127.0.0.1:3389를 입력한 다음 연결을 엽니다.

   또는 새 Linux 데스크톱 쉘에서 Windows 인스턴스에 로그인합니다. RDesktop을 사용하는 경우 명령은 다음과 같습니다.

   ```
   rdesktop 127.0.0.1:3389
   ```

   Windows 인스턴스의 원격 데스크톱 창이 Linux 데스크톱에 나타납니다.

   > **Tip**
   >
   > 원격 데스크톱 세션이 시작되지 않는 경우 SSH 접속에서 Windows 인스턴스로의 네트워크 연결이 1단계의 쉘에서 포트 3389에서 허용되는지 확인합니다(`private_ip_address_of_windows_instance`적절하게 교체).
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > 성공:
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >         Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >         netstat -anvp | grep 3389
   >         tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

Windows 컴퓨터에서 Windows 인스턴스로

Windows 원격 데스크톱 연결 클라이언트를 사용하여 Windows 컴퓨터에서 Windows 인스턴스에 연결합니다.

MALZ

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요DNS 친화적인 접속 이름.

1. 표준 Windows 프로그램인 원격 데스크톱 연결 프로그램을 열고 호스트 이름 필드에 Windows 접속의 친숙한 DNS 이름을 입력합니다.

2. 연결을 선택합니다. 원격 데스크톱 연결은 접속에 대한 RDP 연결을 시도합니다.

   성공하면 자격 증명 대화 상자가 열립니다. 액세스 권한을 얻으려면 Windows 인스턴스와 마찬가지로 회사 Active Directory 자격 증명을 사용합니다.

3. 접속에서 원격 데스크톱 연결 프로그램을 열고 연결하려는 Windows 인스턴스의 IP 주소(예: 10.0.0.100)를 입력한 다음 연결을 선택합니다. Windows 인스턴스에 연결하기 전에 회사 Active Directory 자격 증명이 다시 필요합니다.

SALZ

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요DNS 친화적인 접속 이름.

1. 표준 Windows 프로그램인 원격 데스크톱 연결 프로그램을 열고 호스트 이름 필드에 Windows Bastion의 친숙한 DNS 이름을 입력합니다. 예를 들어 계정 번호가 123456789123이고 Bastion 4,를 선택하면 다음과 `rdpbastion(1-4).A`*`AMSAccountNumber`*`.amazonaws.com`같습니다`rdpbastion4.A123456789123.amazonaws.com`.

2. 연결을 선택합니다. 원격 데스크톱 연결은 접속에 대한 RDP 연결을 시도합니다.

   성공하면 자격 증명 대화 상자가 열립니다. 액세스 권한을 얻으려면 Windows 인스턴스와 마찬가지로 회사 Active Directory 자격 증명을 사용합니다.

3. 접속에서 원격 데스크톱 연결 프로그램을 열고 연결하려는 Windows 인스턴스의 IP 주소(예: 10.0.0.100)를 입력한 다음 연결을 선택합니다. Windows 인스턴스에 연결하기 전에 회사 Active Directory 자격 증명이 다시 필요합니다.

Windows 컴퓨터에서 Linux 인스턴스로

Windows 환경에서 SSH 접속으로 RDP하려면 다음 단계를 따릅니다.

MALZ

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 액세스 요청을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).YOUR_DOMAIN
```

YOUR_DOMAIN이 myamsaddomain.com"이고 Bastion 4를 선택하면 다음과 같습니다.

```
sshbastion4.myamsaddomain.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 인스턴스 ID 또는 IP 주소 찾기를 참조하세요.

Windows 시스템에서 Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

기본 Windows OpenSSH 클라이언트를 사용하거나 로컬 시스템에 PuTTY를 설치합니다. OpenSSH에 대한 자세한 내용은 Windows의 OpenSSH를 참조하세요.

1. 기본 Windows를 사용하거나 PuTTY를 열고 SSH 접속 호스트 이름 또는 SSH 접속의 IP 주소를 입력합니다. 예를 들어 10.65.2.214(22는 SSH에 사용되는 포트이며 기본적으로 설정됨)입니다.
2. OpenSSH 또는 PuTTY는 접속에 대한 SSH 연결을 시도하고 쉘 창을 엽니다.
3. RDP 호스트와 마찬가지로 회사 Active Directory 자격 증명을 사용하여 액세스 권한을 얻습니다.
4. Bash 프롬프트가 표시되면 인스턴스로 SSH합니다. 입력:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 액세스 요청을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

계정 번호가 1234567891230이고 Bastion 4를 선택한 경우 다음과 같습니다.

```
sshbastion4.A123456789123.amazonaws.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 인스턴스 ID 또는 IP 주소 찾기를 참조하세요.

Windows 시스템에서 Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

기본 Windows OpenSSH 클라이언트를 사용하거나 로컬 시스템에 PuTTY를 설치합니다. OpenSSH에 대한 자세한 내용은 Windows의 OpenSSH를 참조하세요.

1. 기본 Windows를 사용하거나 PuTTY를 열고 SSH 접속 호스트 이름 또는 SSH 접속의 IP 주소를 입력합니다. 예를 들어 10.65.2.214(22는 SSH에 사용되는 포트이며 기본적으로 설정됨)입니다.
2. OpenSSH 또는 PuTTY는 접속에 대한 SSH 연결을 시도하고 쉘 창을 엽니다.
3. RDP 호스트와 마찬가지로 회사 Active Directory 자격 증명을 사용하여 액세스 권한을 얻습니다.
4. Bash 프롬프트가 표시되면 인스턴스로 SSH합니다. 입력:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

인시던트 보고

AMS 콘솔을 사용하여 인시던트를 보고합니다. 각 새 문제 또는 질문에 대해 새 인시던트를 생성하는 것이 중요합니다. 이전 문의와 관련된 사례를 개설할 때는 이전 서신을 참조할 수 있도록 관련 사례 번호를 포함하는 것이 좋습니다.

> **Note**
>
> 사례 대응 서신이 원래 문제에서 벗어나는 경우 AMS 운영자가 새 인시던트를 보고하도록 요청할 수 있습니다.

AMS 콘솔을 사용하여 인시던트를 보고하려면:

1. 왼쪽 탐색에서 인시던트를 선택합니다.

   인시던트 목록이 열립니다.

   인시던트 목록이 비어 있는 경우 필터 지우기 옵션은 필터를 모든 상태로 재설정합니다.

   전화 또는 채팅을 사용하려는 경우 지원 센터에서 인시던트 생성을 클릭하여 AMS 서비스 유형으로 자동 채워진 지원 센터 콘솔에서 인시던트 생성 페이지를 엽니다.

   > **Important**
   >
   > - 로 시작된 전화 통화가 녹음 지원 되어 응답을 더 잘 개선할 수 있습니다. 통화가 끊어지면 지원 센터 사례를 통해 다시 호출해야 합니다. AWS 에는 다시 호출하는 메커니즘이 없습니다.
   > - 전화 및 채팅 지원은 RFC 또는 보안 문제가 아닌 지원 사례, 인시던트 및 서비스 요청에 도움이 되도록 설계되었습니다.
   > - RFC 문제의 경우 관련 RFC 세부 정보 페이지의 서신 옵션을 사용하여 AMS 엔지니어에게 문의하세요.
   > - 보안 문제의 경우 우선 순위가 높은(P1 또는 P2) 지원 사례를 생성합니다. 실시간 채팅 기능은 보안 이벤트용이 아닙니다.

2. 기존 인시던트를 찾으려면 드롭다운 목록에서 인시던트 상태 필터를 선택합니다.

   - 아직 해결되지 않은 모든 인시던트입니다.
   - 아직 할당되지 않은 새 인시던트입니다.

	• 할당된 인시던트입니다. • 다시 연 인시던트입니다. • 할당되고 복잡한 인시던트입니다. • 다음 단계 전에 피드백이 필요한 인시던트입니다. • 최근에 정보를 제출한 인시던트입니다. • 종료된 인시던트입니다. • 계정의 모든 인시던트입니다.

3. 생성(Create)을 선택합니다.

   인시던트 생성 페이지가 열립니다.

4. 우선 순위 선택:

   - 낮음: AWS/AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션의 중요하지 않은 기능에 영향을 미칩니다.
   - 중간: AWS/AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션은 중간 정도로 영향을 받고 성능이 저하된 상태에서 작동합니다.
   - 높음: 비즈니스에 큰 영향을 미칩니다. AWS/AMS 리소스와 관련된 애플리케이션의 중요 함수는 사용할 수 없습니다. 프로덕션 시스템에 영향을 미치는 가장 중요한 중단에 대해 예약됩니다.

5. 범주를 선택합니다.

   > **Note**
   > 인시던트 기능을 테스트하려는 경우 인시던트 제목에 무작업 플래그 (AMSTestNoOpsActionRequired)를 추가합니다.

6. 다음에 대한 정보를 입력합니다.

   - 제목: 인시던트 보고서의 설명 제목입니다.
   - CC 이메일: 인시던트 보고서 및 해결 방법에 대한 정보를 제공하려는 사람의 이메일 주소 목록입니다.
   - 세부 정보: 인시던트, 영향을 받는 시스템 및 해결의 예상 결과에 대한 포괄적인 설명입니다. 미리 설정된 질문에 답변하거나 삭제하고 관련 정보를 입력합니다.

첨부 파일을 추가하려면 첨부 파일 추가를 선택하고 원하는 첨부 파일로 이동한 다음 열기를 클릭합니다. 첨부 파일을 삭제하려면 삭제 아이콘을 클릭합니다 .

7. 제출을 선택합니다.

   유형, 제목, 생성됨, ID, 상태 등 인시던트에 대한 정보와 생성한 요청에 대한 설명이 포함된 서신 영역이 포함된 세부 정보 페이지가 열립니다.

   회신을 클릭하여 대응 영역을 열고 상태에 추가 세부 정보 또는 업데이트를 제공합니다.

   인시던트가 해결되면 사례 종료를 클릭합니다.

   한 페이지에 맞는 것보다 더 많은 서신이 있는 경우 더 보기를 클릭합니다.

   커뮤니케이션을 평가하는 것을 잊지 마세요!

   인시던트가 인시던트 목록 페이지에 표시됩니다.

서비스 요청 생성

AWS Managed Services(AMS) 콘솔을 사용하여 서비스 요청을 생성하려면:

1. 왼쪽 탐색에서 서비스 요청을 선택합니다.

   서비스 요청 목록이 열립니다.

   서비스 요청 목록이 비어 있는 경우 필터 지우기 옵션은 필터를 모든 상태로 재설정합니다.

   전화 또는 채팅을 사용하려는 경우 지원 센터에서 서비스 요청 생성을 클릭하여 AMS 서비스 유형으로 자동 채워진 지원 센터 콘솔에서 서비스 요청 생성 페이지를 엽니다.

> **Note**
>
> 지원 중앙에서 시작된 전화 통화는 응답을 더 잘 개선하기 위해 녹음됩니다. 통화가 끊어지면 지원 센터 사례를 통해 다시 호출해야 합니다. AWS 에는 다시 호출하는 메커니즘이 없습니다.

> **Important**
>
> 전화 및 채팅 지원은 지원 사례, 인시던트 및 서비스 요청에 도움이 되도록 설계되었습니다. RFC 문제의 경우 관련 RFC 세부 정보 페이지의 서신 옵션을 사용하여 AMS 엔지니어에게 문의하세요.

2. 기존 서비스 요청을 찾으려면 드롭다운 목록에서 서비스 요청 상태 필터를 선택합니다.

	• 아직 해결되지 않은 모든 서비스 요청입니다. • 아직 할당되지 않은 새 서비스 요청입니다. • 할당된 서비스 요청입니다. • 다시 연 서비스 요청입니다. • 할당되고 복잡한 서비스 요청입니다. • 다음 단계 전에 피드백이 필요한 서비스 요청입니다. • 최근에 정보를 제출한 서비스 요청입니다. • 가 종료한 서비스 요청입니다. • 계정의 모든 서비스 요청입니다.

3. 생성(Create)을 선택합니다.

   서비스 요청 생성 페이지가 열립니다.

4. 범주를 선택합니다.

> **Note**
>
> 서비스 요청 기능을 테스트하려면 서비스 요청 제목에 무작업 플래그 `AMSTestNoOpsActionRequired`를 추가합니다.

5. 다음에 대한 정보를 입력합니다.

   - 제목: 그러면 목록 페이지에 서비스 요청 세부 정보에 대한 링크가 생성됩니다.
   - CC 이메일: 이러한 이메일은 기본 이메일 연락처 외에도 서신을 수신합니다.
   - 세부 정보: 여기에 최대한 많은 정보를 제공합니다.

   첨부 파일을 추가하려면 첨부 파일 추가를 선택하고 원하는 첨부 파일로 이동한 다음 열기를 클릭합니다. 첨부 파일을 삭제하려면 삭제 아이콘을 클릭합니다

6. 제출을 선택합니다.

   유형, 주체, 생성됨, ID, 상태 등 서비스 요청에 대한 정보와 생성한 요청에 대한 설명이 포함된 서신 영역이 포함된 세부 정보 페이지가 열립니다.

   또한 서비스 요청은 서비스 요청 목록 페이지에 표시됩니다. 알림이 있지만 아직 AMS에서 듣지 못한 경우이 옵션을 사용합니다.

   회신을 클릭하여 대응 영역을 열고 추가 세부 정보 또는 상태 업데이트를 제공합니다.

   서비스 요청이 해결되면 사례 해결을 클릭합니다.

   더 보기를 클릭하여 초기 페이지에 맞지 않는 추가 서신을 봅니다.

   커뮤니케이션을 평가하는 것을 잊지 마세요!

결제 관련 쿼리의 경우 AMS 콘솔의 기타 범주, AMS CM API`ChangeTypeId` `ct-1e1xtak34nx76`의 , AWS Support API의 `IssueType=AMS`를 사용합니다.

온보딩 후 단계

이제 AMS 계정에 가입했으므로 더 많은 AMS 설명서를 읽으려고 합니다. 다음 문서를 참조하세요.

- HA 2계층 스택 CT를 사용하여 완벽하게 작동하는 WordPress 스택을 생성하는 자습서에서는 전체 AMS 환경을 제공합니다.
- AMS 사용 설명서: AMS 사용 설명서는 AMS 기능을 설명하고, 주요 용어, 작업, 인터페이스를 나열하며, 일반적인 AMS 관리형 인프라 아키텍처에 대한 개요를 제공합니다. 또한 액세스 관리 세부 정보 및 AMS 기본값이 제공됩니다. 또한 AMS 변경 관리 시스템을 사용하는 방법에 대한 자세한 설명과 몇 가지 연습이 제공됩니다. 추가 관리 개념도 설명합니다.
- AMS API 참조:이 API 참조는 요청, 응답 및 예제를 포함하여 모든 API 호출에 대한 설명을 제공합니다.
- AMS 애플리케이션 가이드: AMS 애플리케이션 가이드에서는 AMS에서 애플리케이션을 배포하고 유지 관리하기 위한 다양한 옵션과 방법을 설명합니다.

자습서

다음 자습서에서는 CLI 및 콘솔을 사용하여 고가용성(고급) CT(ct-06mjngx5flwto)를 사용하여 2계층 스택을 생성하는 단계를 자세히 설명합니다. Linux Auto Scaling 그룹(ASG)을 배포하고 Windows ASG를 배포하기 위한 자습서가 제공됩니다.

ChangeTypeId를 포함한 모든 CT 옵션에 대한 설명은 AMS 변경 유형 참조에서 확인할 수 있습니다.

CLI 자습서: 고가용성 2계층 스택(Linux/RHEL)

이 섹션에서는 AMS CLI를 사용하여 AMS 환경에 고가용성(HA) 2계층 스택을 배포하는 방법을 설명합니다.

> **Note**
>
> 이 배포 연습은 AMZN Linux 및 RHEL 환경에서 테스트되었습니다.

작업 및 필수 RFCs 요약:

1. 인프라 생성(HA 2계층 스택)
2. CodeDeploy 애플리케이션용 S3 버킷 생성
3. WordPress 애플리케이션 번들을 생성하여 S3 버킷에 업로드합니다.
4. CodeDeploy를 사용하여 애플리케이션 배포
5. WordPress 사이트에 액세스하고 로그인하여 배포를 검증합니다.

시작하기 전

배포 | 고급 스택 구성 요소 | 고가용성 2계층 스택 고급 | CT 생성은 Auto Scaling 그룹, 로드 밸런서, 데이터베이스, CodeDeploy 애플리케이션 이름 및 배포 그룹(애플리케이션과 동일한 이름)을 생성합니다. CodeDeploy에 대한 자세한 내용은 CodeDeploy란 무엇입니까?를 참조하세요.

이 연습에서는 UserData가 포함된 고가용성 2계층 스택(고급) RFC를 사용하고 CodeDeploy가 배포할 수 있는 WordPress 번들을 생성하는 방법을 설명합니다.

예제에 `UserData` 표시된는 http://169.254.169.254/latest/meta-data/ 사용할 수 있는 EC2 인스턴스 메타데이터 서비스를 쿼리하여 실행 중인 인스턴스 내에서 인스턴스 ID, 리전 등과 같은 인스턴스 메타데이터를 가져옵니다. 사용자 데이터 스크립트의이 줄: `REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`는 메타데이터 서비스에서 지원되는 리전의 $REGION 변수로 가용 영역 이름을 검색하고 이를 사용하여 CodeDeploy 에이전트가 다운로드되는 S3 버킷의 URL을 완료합니다. 169.254.169.254 IP는 VPC 내에서만 라우팅할 수 있습니다(모든 VPCs 서비스를 쿼리할 수 있음). 서비스에 대한 자세한 내용은 인스턴스 메타데이터 및 사용자 데이터를 참조하세요. UserData로 입력된 스크립트는 "루트" 사용자로 실행되므로 "sudo" 명령을 사용할 필요가 없습니다.

이 연습에서는 다음 파라미터를 기본값으로 둡니다(그림 참조).

- Auto Scaling 그룹: `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.
- Load Balancer: `HealthCheckInterval=30, HealthCheckTimeout=5`.
- 데이터베이스: `BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.

- 애플리케이션: `DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- S3 버킷: `AccessControl=Private`.

추가 설정:

`RequestedStartTime` RFC를 예약하려는 `RequestedEndTime` 경우 및 : Time.is 사용하여 올바른 UTC 시간을 확인할 수 있습니다. 제공된 예제는 적절하게 조정해야 합니다. 시작 시간이 경과하면 RFC를 진행할 수 없습니다. 또는 이러한 값을 끄면 승인이 전달되는 즉시 실행되는 ASAP RFC를 생성할 수 있습니다.

> **Note**
>
> 표시된 것과 다르게 설정하도록 선택할 수 있는 파라미터가 많습니다. 예제에 표시된 파라미터의 값은 테스트되었지만 적합하지 않을 수 있습니다.

인프라 생성

시작하기 전에 다음 데이터를 수집하면 배포 속도가 빨라집니다.

필수 데이터 HA 스택:

- AutoScalingGroup:
  - `UserData`:이 값은이 자습서에서 제공됩니다. 여기에는 CodeDeploy에 대한 리소스를 설정하고 CodeDeploy 에이전트를 시작하는 명령이 포함되어 있습니다.
  - `AMI-ID`:이 값은 Auto Scaling 그룹(ASG)이 실행할 EC2 인스턴스의 종류를 결정합니다. 계정에서 "customer-"로 시작하고 원하는 운영 체제의 AMI를 선택해야 합니다. 를 사용하여 AMI IDs를 찾습니다. AMS SKMS API 참조의 경우 AWS 아티팩트 콘솔의 보고서 탭(CLI: list-amis) 또는 AMS 콘솔 VPCs VPCs 세부 정보 페이지를 참조하세요. 이 연습은 Linux ASGs를 위한 것입니다.
- 데이터베이스:
  - 예제에 표시된 값이 테스트되었지만 상황에 따라 이러한 파라미터 `EngineVersion`, 및 `DBEngine`를 설정해야 `LicenseModel` 합니다.
  - 이러한 파라미터 `RDSSubnetIds`, `MasterUsername`, 및 `DBNameMasterUserPassword`는 애플리케이션 번들을 배포할 때 필요합니다. RDSSubnetIds의 경우 두 개의 프라이빗 서브넷을 사용합니다.
- LoadBalancer:

  - 예제에 표시된 값이 테스트되었지만 상황에 따라 이러한 파라미터 EngineVersion, 및 DBEngine를 설정해야 LicenseModel 합니다.
  - ELBSubnetIds: 두 개의 퍼블릭 서브넷을 사용합니다.
- 애플리케이션:이 ApplicationName 값은 CodeDeploy 애플리케이션 이름과 CodeDeploy 배포 그룹 이름을 설정합니다. 이를 사용하여 애플리케이션을 배포합니다. 계정에서 고유해야 합니다. 계정에 CodeDeploy 이름이 있는지 확인하려면 CodeDeploy 콘솔을 참조하세요. 이 예제에서는 "WordPress"를 사용하지만 해당 값을 사용할 경우 아직 사용되지 않았는지 확인합니다.

이 절차는 고가용성 2계층 스택(고급) CT(ct-06mjngx5flwto) 및 S3 스토리지 CT 생성 (ct-1a68ck03fn98r)을 활용합니다. 인증된 계정에서 명령줄의 다음 단계를 따릅니다.

1. 인프라 스택을 시작합니다.

   a. HA 2계층 스택 CT의 실행 파라미터 JSON 스키마를 CreateStackParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateStackParams.json
```

   b. 스키마를 수정합니다. 변수를 적절하게 바꿉니다. 예를 들어 ASG가 생성할 EC2 인스턴스에 대해 원하는 OS를 사용합니다. 나중에 애플리케이션을 배포하는 데 ApplicationName 사용할를 기록합니다. 최대 50개의 태그를 추가할 수 있습니다.

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
```

```
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. CreateRfc JSON 템플릿을 CreateStackRfc.json:이라는 현재 폴더의 파일로 출력합니다.

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. 다음과 같이 RFC 템플릿을 수정하고 저장하면 콘텐츠를 삭제하고 바꿀 수 있습니다. 이제 `RequestedStartTime` 및 `RequestedEndTime`는 선택 사항입니다. 제외하면 승인되는 즉시 실행되는 ASAP RFC가 생성됩니다(일반적으로 자동으로 발생함). 예약된 RFC를 제출하려면 해당 값을 추가합니다.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. CreateStackRfc.json 파일과 CreateStackParams.json 실행 파라미터 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

응답에서 RFC ID를 수신합니다. 후속 단계를 위해 ID를 저장합니다.

f. RFC를 제출합니다.

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

RFC가 성공하면 출력이 수신되지 않습니다.

g. RFC 상태를 확인하려면를 실행합니다.

```
aws amscm get-rfc --rfc-id RFC_ID
```

RFC ID를 기록해 둡니다.

2. S3 버킷 시작

시작하기 전에 다음 데이터를 수집하면 배포 속도가 빨라집니다.

필수 데이터 S3 버킷:

- VPC-ID:이 값은 S3 버킷의 위치를 결정합니다. 이전에 사용한 것과 동일한 VPC ID를 사용합니다.
- BucketName:이 값은 S3 버킷 이름을 설정하며, 이를 사용하여 애플리케이션 번들을 업로드합니다. 계정의 리전 전체에서 고유해야 하며 대문자를 포함할 수 없습니다. 계정 ID를 BucketName의 일부로 포함하는 것은 요구 사항이 아니지만 나중에 버킷을 더 쉽게 식별할 수 있습니다. 계정에 있는 S3 버킷 이름을 확인하려면 계정의 Amazon S3 콘솔로 이동합니다.

a. S3 스토리지 생성 CT에 대한 실행 파라미터 JSON 스키마를 CreateS3StoreParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. 다음과 같이 스키마를 수정하면 콘텐츠를 삭제하고 바꿀 수 있습니다. *VPC_ID*를 적절하게 바꿉니다. 예제의 값은 테스트되었지만 적합하지 않을 수 있습니다.

> **Tip**
>
> 는 계정 리전 전체에서 고유BucketName해야 하며 대문자를 포함할 수 없습니다. 계정 ID를 BucketName의 일부로 포함하는 것은 요구 사항이 아니지만 나중에 버킷을 더 쉽게 식별할 수 있습니다. 계정에 있는 S3 버킷 이름을 확인하려면 계정의 Amazon S3 콘솔로 이동합니다.

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. CreateRfc용 JSON 템플릿을 CreateS3StoreRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. CreateS3StoreRfc.json 파일을 수정하고 저장하면 콘텐츠를 삭제하고 바꿀 수 있습니다. 이제 RequestedStartTime 및 RequestedEndTime는 선택 사항입니다. 제외하면 승인되는 즉시 실행되는 ASAP RFC가 생성됩니다(일반적으로 자동으로 발생함). 예약된 RFC를 제출하려면 해당 값을 추가합니다.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. CreateS3StoreRfc.json 파일과 CreateS3StoreParams.json 실행 파라미터 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

응답에서 새 RFC의 RfcId를 수신합니다. 후속 단계를 위해 ID를 저장합니다.

f. RFC를 제출합니다.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC가 성공하면 출력이 수신되지 않습니다.

g. RFC 상태를 확인하려면를 실행합니다.

```
aws amscm get-rfc --rfc-id RFC_ID
```

애플리케이션 생성, 업로드 및 배포

먼저 WordPress 애플리케이션 번들을 생성한 다음 CodeDeploy CTs를 사용하여 애플리케이션을 생성하고 배포합니다.

1. WordPress를 다운로드하고 파일을 추출한 다음 ./scripts 디렉터리를 생성합니다.

   Linux 명령:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: 브라우저 창에 붙여`https://github.com/WordPress/WordPress/archive/master.zip`넣고 zip 파일을 다운로드합니다.

   패키지를 어셈블할 임시 디렉터리를 생성합니다.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: "WordPress" 디렉터리를 생성합니다. 나중에 디렉터리 경로를 사용합니다.

2. WordPress 소스를 "WordPress" 디렉터리로 추출하고 ./scripts 디렉터리를 생성합니다.

   Linux:

```
unzip master.zip -d /tmp/WordPress_Temp
cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
rm -rf /tmp/WordPress_Temp
rm -f master
cd /tmp/WordPress
mkdir scripts
```

Windows: 생성한 "WordPress" 디렉터리로 이동하여 여기에 "scripts" 디렉터리를 생성합니다.

Windows 환경에 있는 경우 스크립트 파일의 브레이크 유형을 Unix(LF)로 설정해야 합니다. 메모장 ++에서 창 오른쪽 하단에 있는 옵션입니다.

3. WordPress 디렉터리에서 CodeDeploy appspec.yml 파일을 생성합니다(예제를 복사하는 경우 들여쓰기를 확인하고 각 공간을 계산합니다). 중요: WordPress 파일(이 경우 WordPress 디렉터리)을 예상 대상(/var/www/html/WordPress)으로 복사하기 위해 "소WordPress" 경로가 올바른지 확인합니다. 예제에서 appspec.yml 파일은 WordPress 파일이 있는 디렉터리에 있으므로 "/"만 있으면 됩니다. 또한 Auto Scaling 그룹에 RHEL AMI를 사용했더라도 "os: linux" 줄을 그대로 둡니다. appspec.yml 파일의 예:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. WordPress ./scripts 디렉터리에서 bash 파일 스크립트를 생성합니다.

   먼저 다음 콘텐츠`config_wordpress.sh`로를 생성합니다(원하는 경우 wp-config.php 파일을 직접 편집할 수 있음).

   > **Note**
   >
   > *DBName*을 HA 스택 RFC에 지정된 값으로 바꿉니다(예: `wordpress`).
   > *DB_MasterUsername*을 HA 스택 RFC에 지정된 `MasterUsername` 값으로 바꿉니다(예: `admin`).
   > *DB_MasterUserPassword*를 HA 스택 RFC에 지정된 `MasterUserPassword` 값으로 바꿉니다(예: `p4ssw0rd`).
   > *DB_ENDPOINT*를 HA 스택 RFC의 실행 출력에서 엔드포인트 DNS 이름으로 바꿉니다(예: `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). GetRfc 작업(CLI: get-rfc --rfc-id RFC_ID) 또는 이전에 제출한 HA 스택 RFC의 AMS 콘솔 RFC 세부 정보 페이지에서 이를 찾을 수 있습니다.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 동일한 디렉터리에서 다음 콘텐츠`install_dependencies.sh`로를 생성합니다.

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS는 상태 확인이 처음부터 작동하도록 시작 시 사용자 데이터의 일부로 설치됩니다.

6. 동일한 디렉터리에서 다음 콘텐츠`start_server.sh`로를 생성합니다.

   - Amazon Linux 인스턴스의 경우 다음을 사용합니다.

   ```
   #!/bin/bash
   service httpd start
   ```

   - RHEL 인스턴스의 경우 다음을 사용합니다(추가 명령은 SELINUX가 WordPress를 수락하도록 허용하는 정책임).

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. 동일한 디렉터리에서 다음 콘텐츠`stop_server.sh`로를 생성합니다.

   ```
   #!/bin/bash
   service httpd stop
   ```

8. zip 번들을 생성합니다.

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: "WordPress" 디렉터리로 이동하여 모든 파일을 선택하고 zip 파일을 생성합니다. 이름을 wordpress.zip으로 지정해야 합니다.

1. 애플리케이션 번들을 S3 버킷에 업로드합니다.

   스택을 계속 배포하려면 번들이 있어야 합니다.

생성한 모든 S3 버킷 인스턴스에 자동으로 액세스할 수 있습니다. Bastion 또는 S3 콘솔을 통해 액세스하고 zip 파일을 drag-and-drop거나 탐색하여 선택하여 WordPress 번들을 업로드할 수 있습니다.

쉘 창에서 다음 명령을 사용할 수도 있습니다. zip 파일의 경로가 올바른지 확인하세요.

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. WordPress 애플리케이션 번들을 배포합니다.

   시작하기 전에 다음 데이터를 수집하면 배포 속도가 빨라집니다.

   필수 데이터:

   - `VPC-ID`:이 값은 S3 버킷의 위치를 결정합니다. 이전에 사용한 것과 동일한 VPC ID를 사용합니다.
   - `CodeDeployApplicationName` 및 `CodeDeployApplicationName`: HA 2-Tier 스택 RFC에서 사용한 `ApplicationName` 값은 CodeDeployApplicationName 및 CodeDeployDeploymentGroupName을 설정합니다. 이 예제에서는 "WordPress"를 사용하지만 다른 값을 사용했을 수 있습니다.
   - `S3Location`:의 경우 이전에 생성한 `BucketName`를 `S3Bucket`사용합니다. `S3BundleType` 및는 S3 스토어에 배치한 번들`S3Key`에서 가져온 것입니다.

   a. CodeDeploy 애플리케이션의 실행 파라미터 JSON 스키마를 출력하여 DeployCDAppParams.json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    DeployCDAppParams.json
   ```

   b. 다음과 같이 스키마를 수정하고 다른 이름으로 저장하면 콘텐츠를 삭제하고 바꿀 수 있습니다.

   ```
   {
   "Description":                          "DeployWPCDApp",
   "VpcId":                                "VPC_ID",
   "Name":                                 "WordPressCDAppDeploy",
   "TimeoutInMinutes":                     60,
   "Parameters":   {
   ```

```
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
        }
    }
}
```

c. CreateRfc용 JSON 템플릿을 DeployCDAppRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. DeployCDAppRfc.json 파일을 수정하고 저장하면 콘텐츠를 삭제하고 바꿀 수 있습니다. 이제 RequestedStartTime 및 RequestedEndTime는 선택 사항입니다. 제외하면 승인되는 즉시 실행되는 ASAP RFC가 생성됩니다(일반적으로 자동으로 발생함). 예약된 RFC를 제출하려면 해당 값을 추가합니다.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. DeployCDAppRfc 파일과 DeployCDAppParams 실행 파라미터 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

응답에서 새 RFC의 RfcId를 수신합니다. 후속 단계를 위해 ID를 저장합니다.

f. RFC 제출:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC가 성공하면 출력이 수신되지 않습니다.

g. RFC 상태를 확인하려면를 실행합니다.

```
aws amscm get-rfc --rfc-id RFC_ID
```

애플리케이션 배포 검증

WordPress 배포 경로 /WordPress를 사용하여 이전에 생성한 로드 밸런서의 엔드포인트(ELB CName)로 이동합니다. 예:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

애플리케이션 배포 해체

자습서를 마치면 리소스에 대한 요금이 부과되지 않도록 배포를 해제해야 합니다.

다음은 일반 스택 삭제 작업입니다. HA 2-Tier 스택의 경우 한 번, S3 버킷 스택의 경우 한 번 두 번 제출하는 것이 좋습니다. 최종 후속 조치로 S3 버킷의 모든 스냅샷(서비스 요청에 S3 버킷 스택 ID 포함)을 삭제하라는 서비스 요청을 제출합니다. 10일 후에 자동으로 삭제되지만 조기에 삭제하면 약간의 비용이 절감됩니다.

이 연습에서는 AMS 콘솔을 사용하여 S3 스택을 삭제하는 예제를 제공합니다.이 절차는 AMS 콘솔을 사용하여 스택을 삭제하는 데 적용됩니다.

> **Note**
>
> S3 버킷을 삭제하는 경우 먼저 객체를 비워야 합니다.

필수 데이터:

- `StackId`: 사용할 스택입니다. 왼쪽 탐색 창의 링크를 통해 제공되는 AMS 콘솔 스택 페이지를 보면 이를 찾을 수 있습니다. AMS SKMS API/CLI를 사용하여 AMS SKMS API 참조의 경우 AWS 아티팩트 콘솔의 보고서 탭을 참조하세요(CLI의 `list-stack-summaries`).
- 이 연습의 변경 유형 ID는 `ct-0q0bic0ywqk6c`이고, 버전은 "1.0"이며, 최신 버전을 확인하려면 다음 명령을 실행합니다.

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

인라인 생성:

- 인라인으로 제공된 실행 파라미터를 사용하여 RFC 생성 명령을 실행합니다(실행 파라미터를 인라인으로 제공할 때 따옴표 이스케이프). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- RFC 생성 작업에서 반환된 RFC ID를 사용하여 RFC를 제출합니다. 제출될 때까지 RFC는 `Editing` 상태로 유지되며 적용되지 않습니다.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- RFC 상태를 모니터링하고 실행 출력을 봅니다.

```
aws amscm get-rfc --rfc-id RFC_ID
```

템플릿 생성:

1. RFC 템플릿을 현재 폴더의 파일로 출력합니다. 예제 이름은 DeleteStackRfc.json:입니다.

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. DeleteStackRfc.json 파일을 수정하고 저장합니다. 스택 삭제에는 실행 파라미터가 하나뿐이므로 실행 파라미터는 DeleteStackRfc.json 파일 자체에 있을 수 있습니다(실행 파라미터가 있는 별도의 JSON 파일을 생성할 필요가 없음).

   ExecutionParameters JSON 확장의 내부 따옴표는 백슬래시(\)로 이스케이프 처리해야 합니다. 시작 및 종료 시간이 없는 예:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

응답에서 새 RFC의 RfcId를 수신합니다. 예:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

후속 단계를 위해 ID를 저장합니다.

4. RFC 제출:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC가 성공하면 명령줄에서 확인 메시지가 표시되지 않습니다.

5. 요청 상태를 모니터링하고 실행 출력을 보려면:

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

콘솔 자습서: 고가용성 2계층 스택(Linux/RHEL)

이 섹션에서는 AMS 콘솔을 사용하여 AMS 환경에 고가용성(HA) WordPress 사이트를 배포하는 방법을 설명합니다.

> **Note**
>
> 이 배포 연습은 AMZN Linux 및 RHEL 환경에서 테스트되었습니다.

작업 및 필수 RFCs 요약:

1. 인프라 생성(HA 2계층 스택)
2. CodeDeploy 애플리케이션용 S3 버킷 생성
3. WordPress 애플리케이션 번들을 생성하여 S3 버킷에 업로드합니다.
4. CodeDeploy를 사용하여 애플리케이션 배포

5. WordPress 사이트에 액세스하고 로그인하여 배포를 검증합니다.
6. 배포를 중단합니다.

ChangeTypeId를 포함한 모든 CT 옵션에 대한 설명은 AMS 변경 유형 참조에서 확인할 수 있습니다.

시작하기 전

배포 | 고급 스택 구성 요소 | 고가용성 2계층 스택 | CT 생성은 Auto Scaling 그룹, 로드 밸런서, 데이터베이스, CodeDeploy 애플리케이션 이름 및 배포 그룹(애플리케이션과 동일한 이름)을 생성합니다. CodeDeploy에 대한 자세한 내용은 CodeDeploy란 무엇입니까?를 참조하세요.

이 연습UserData에서는 CodeDeploy가 배포할 수 있는 WordPress 번들을 생성하고 생성하는 방법을 포함하는 고가용성 2계층 스택 RFC를 사용합니다.

예제에 UserData 표시된는 http://169.254.169.254/latest/meta-data/ 사용할 수 있는 EC2 인스턴스 메타데이터 서비스를 쿼리하여 실행 중인 인스턴스 내에서 인스턴스 ID, 리전 등과 같은 인스턴스 메타데이터를 가져옵니다. 사용자 데이터 스크립트의이 줄: `REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`는 메타데이터 서비스에서 지원되는 리전의 $REGION 변수로 가용 영역 이름을 검색하고 이를 사용하여 CodeDeploy 에이전트가 다운로드되는 S3 버킷의 URL을 완료합니다. 169.254.169.254 IP는 VPC 내에서만 라우팅할 수 있습니다(모든 VPCs 서비스를 쿼리할 수 있음). 서비스에 대한 자세한 내용은 인스턴스 메타데이터 및 사용자 데이터를 참조하세요. UserData로 입력된 스크립트는 "루트" 사용자로 실행되므로 "sudo" 명령을 사용할 필요가 없습니다.

이 연습에서는 다음 파라미터를 기본값(그림 참조)으로 둡니다.

- Auto Scaling 그룹: `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.
- Load Balancer: `HealthCheckInterval=30, HealthCheckTimeout=5`.

- 데이터베이스: `BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- 애플리케이션: `DeploymentConfigName=CodeDeployDefault.OneAtATime`.

변수 파라미터:

콘솔은 시작 시간에 대한 ASAP 옵션을 제공하며이 연습에서는 이를 사용할 것을 권장합니다. ASAP를 사용하면 승인이 전달되는 즉시 RFC가 실행됩니다.

> **Note**
>
> 표시된 것과 다르게 설정하도록 선택할 수 있는 파라미터가 많습니다. 예제에 표시된 파라미터의 값은 테스트되었지만 적합하지 않을 수 있습니다. 예제에는 필요한 값만 표시됩니다. *## ## ##* 글꼴의 값은 계정에 특정하므로 변경해야 합니다.

인프라 생성

이 절차에서는 고가용성 2계층 스택 CT와 S3 스토리지 CT 생성을 차례로 활용합니다.

시작하기 전에 다음 데이터를 수집하면 배포 속도가 빨라집니다.

필수 데이터 HA 스택:

- AutoScalingGroup:
  - UserData:이 값은이 자습서에서 제공됩니다. 여기에는 CodeDeploy에 대한 리소스를 설정하고 CodeDeploy 에이전트를 시작하는 명령이 포함되어 있습니다.
  - AMI-ID:이 값은 Auto Scaling 그룹(ASG)이 실행할 EC2 인스턴스의 운영 체제를 결정합니다. 계정에서 "customer-"로 시작하고 원하는 운영 체제의 AMI를 선택합니다. AMS 콘솔 VPCs -> VPC 세부 정보 페이지에서 AMI IDs를 찾습니다. VPCs 이 연습은 Amazon Linux 또는 RHEL AMI를 사용하도록 구성된 ASGs를 위한 것입니다.
- 데이터베이스:
  - 예제에 표시된 값이 테스트되었지만 이러한 파라미터, DBEngine, EngineVersion 및 LicenseModel은 상황에 따라 설정해야 합니다. 이 자습서에서는 각각 *`MySQL`*, *`8.0.16`*, *`general-public-license`* 값을 사용합니다.

- 애플리케이션 번들을 배포할 때 이러한 파라미터, DBName, MasterUserPassword 및 MasterUsername이 필요합니다. 이 자습서에서는 각각 *wordpressDB*, *p4ssw0rd*, *admin* 등의 값을 사용합니다. DBName은 영숫자만 포함할 수 있습니다.
- RDS DB의 MasterUsername을 입력하면 일반 텍스트로 표시되므로 최대한 빨리 데이터베이스에 로그인하고 암호를 변경하여 보안을 보장합니다.
- RDSSubnetIds의 경우 두 개의 프라이빗 서브넷을 사용합니다. 다음에 "Enter"를 눌러 한 번에 하나씩 입력합니다. 를 사용하여 서브넷 IDs 찾기 AMS SKMS API 참조의 경우 AWS 아티팩트 콘솔의 보고서 탭을 참조하세요. 작업(CLI: list-subnet-summaries) 또는 AMS 콘솔 VPCs.

- LoadBalancer:
  - 이 파라미터를 퍼블릭으로 설정합니다. 자습서에서는 퍼블릭 ELB 서브넷을 사용하기 때문입니다.
  - ELBSubnetIds: 두 개의 퍼블릭 서브넷을 사용합니다. 다음에 "Enter"를 눌러 한 번에 하나씩 입력합니다. 를 사용하여 서브넷 IDs 찾기 AMS SKMS API 참조의 경우 AWS 아티팩트 콘솔의 보고서 탭을 참조하세요. 작업(CLI: list-subnet-summaries) 또는 AMS 콘솔 VPCs.
- 애플리케이션: ApplicationName 값은 CodeDeploy 애플리케이션 이름과 CodeDeploy 배포 그룹 이름을 설정합니다. 이를 사용하여 애플리케이션을 배포합니다. 계정에서 고유해야 합니다. 계정에 CodeDeploy 이름이 있는지 확인하려면 CodeDeploy 콘솔을 참조하세요. 이 예제에서는 *WordPress*를 사용하지만 해당 값을 사용할 경우 아직 사용되지 않았는지 확인합니다.

1. 고가용성 스택을 시작합니다.

   a. RFC 생성 페이지의 목록에서 범주 배포, 하위 범주 표준 스택, 고가용성 2계층 스택 및 생성 작업을 선택합니다.

   b. 중요: 고급을 선택하고 표시된 대로 값을 설정합니다.

      별표(*) 옵션에 대한 값만 입력하면 되며, 테스트된 값은 예제에 표시됩니다. 필수가 아닌 빈 옵션은 비워 둘 수 있습니다.

   c. RFC 설명 섹션의 경우:

      ```
      Subject: WP-HA-2-Tier-RFC
      ```

   d. 리소스 정보 섹션에서 AutoScalingGroup, 데이터베이스, LoadBalancer, 애플리케이션 및 태그에 대한 파라미터를 설정합니다.

또한 "AppName" 태그 키의 목적은 EC2 콘솔에서 ASG 인스턴스를 쉽게 검색할 수 있도록 하기 위한 것입니다.이 태그 키 "Name" 또는 원하는 다른 키 이름을 호출할 수 있습니다. 태그를 최대 50개까지 추가할 수 있습니다.

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:               AMI-ID
Description:         WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
    RDSSubnetIds:    PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. 완료되면 제출을 클릭합니다.

2. 생성한 데이터베이스에 로그인하고 암호를 변경합니다.
3. S3 버킷 스택을 시작합니다.

   시작하기 전에 다음 데이터를 수집하면 배포 속도가 빨라집니다.

   필수 데이터 S3 버킷:

   - VPC-ID:이 값은 S3 버킷의 위치를 결정합니다. 를 사용하여 VPC IDs 찾기 AMS SKMS API 참조의 경우 AWS Artifact 콘솔의 보고서 탭을 참조하세요. 작업(CLI: list-vpc-summaries) 또는 AMS 콘솔 VPCs.
   - BucketName:이 값은 S3 버킷 이름을 설정하며, 이를 사용하여 애플리케이션 번들을 업로드합니다. 계정의 리전 전체에서 고유해야 하며 대문자를 포함할 수 없습니다. 계정 ID를 BucketName의 일부로 포함하는 것은 요구 사항이 아니지만 나중에 버킷을 더 쉽게 식별할 수 있습니다. 계정에 존재하는 S3 버킷 이름을 확인하려면 계정의 Amazon S3 콘솔로 이동합니다.

   a. RFC 생성 페이지에서 범주 배포, 하위 범주 고급 스택 구성 요소, 항목 S3 스토리지 및 RFC CT 선택 목록에서 생성 작업을 선택합니다.

   b. 기본 기본 옵션을 유지하고 표시된 대로 값을 설정합니다.

```
Subject:              S3-Bucket-WP-HA-RFC
Description:          S3BucketForWordPressBundles
BucketName:           ACCOUNT_ID-BUCKET_NAME
AccessControl:        Private
VpcId:                VPC_ID
Name:                 S3-Bucket-WP-HA-Stack
TimeoutInMinutes:     60
```

   c. 완료되면 제출을 클릭합니다. 이 변경 유형으로 배포된 버킷은 전체 계정에 대한 전체 읽기/쓰기 액세스를 허용합니다.

애플리케이션 생성, 업로드 및 배포

먼저 WordPress 애플리케이션 번들을 생성한 다음 CodeDeploy CTs를 사용하여 애플리케이션을 생성하고 배포합니다.

1. WordPress를 다운로드하고 파일을 추출한 다음 ./scripts 디렉터리를 생성합니다.

   Linux 명령:

```
wget https://github.com/WordPress/WordPress/archive/master.zip
```

Windows: 브라우저 창에 붙여`https://github.com/WordPress/WordPress/archive/master.zip`넣고 zip 파일을 다운로드합니다.

패키지를 어셈블할 임시 디렉터리를 생성합니다.

Linux:

```
mkdir /tmp/WordPress
```

Windows: "WordPress" 디렉터리를 생성합니다. 나중에 디렉터리 경로를 사용합니다.

2. WordPress 소스를 "WordPress" 디렉터리로 추출하고 ./scripts 디렉터리를 생성합니다.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: 생성한 "WordPress" 디렉터리로 이동하여 여기에 "scripts" 디렉터리를 생성합니다.

   Windows 환경에 있는 경우 스크립트 파일의 브레이크 유형을 Unix(LF)로 설정해야 합니다. 메모장 ++에서 창 오른쪽 하단에 있는 옵션입니다.

3. WordPress 디렉터리에서 CodeDeploy appspec.yml 파일을 생성합니다(예제를 복사하는 경우 들여쓰기를 확인하고 각 공간을 계산합니다). 중요: WordPress 파일(이 경우 WordPress 디렉터리)을 예상 대상(/var/www/html/WordPress)으로 복사하기 위해 "소WordPress" 경로가 올바른지 확인합니다. 예제에서 appspec.yml 파일은 WordPress 파일이 있는 디렉터리에 있으므로 "/"만 있으면 됩니다. 또한 Auto Scaling 그룹에 RHEL AMI를 사용했더라도 "os: linux" 줄을 그대로 둡니다. appspec.yml 파일의 예:

   ```
   version: 0.0
   os: linux
   files:
     - source: /
   ```

```
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. WordPress ./scripts 디렉터리에서 bash 파일 스크립트를 생성합니다.

   먼저 다음 콘텐츠config_wordpress.sh로를 생성합니다(원하는 경우 wp-config.php 파일을 직접 편집할 수 있음).

   > **Note**
   >
   > *DBName*을 HA 스택 RFC에 지정된 값으로 바꿉니다(예: wordpress).
   > *DB_MasterUsername*을 HA 스택 RFC에 지정된 MasterUsername 값으로 바꿉니다(예: admin).
   > *DB_MasterUserPassword*를 HA 스택 RFC에 지정된 MasterUserPassword 값으로 바꿉니다(예: p4ssw0rd).
   > *DB_ENDPOINT*를 HA 스택 RFC의 실행 출력에서 엔드포인트 DNS 이름으로 바꿉니다(예: srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com). GetRfc 작업(CLI: get-rfc --rfc-id RFC_ID) 또는 이전에 제출한 HA 스택 RFC의 AMS 콘솔 RFC 세부 정보 페이지에서 이를 찾을 수 있습니다.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
```

```
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 동일한 디렉터리에서 다음 콘텐츠`install_dependencies.sh`로를 생성합니다.

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS는 상태 확인이 처음부터 작동하도록 시작 시 사용자 데이터의 일부로 설치됩니다.

6. 동일한 디렉터리에서 다음 콘텐츠`start_server.sh`로를 생성합니다.

   - Amazon Linux 인스턴스의 경우 다음을 사용합니다.

   ```
   #!/bin/bash
   service httpd start
   ```

   - RHEL 인스턴스의 경우 다음을 사용합니다(추가 명령은 SELINUX가 WordPress를 수락하도록 허용하는 정책임).

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. 동일한 디렉터리에서 다음 콘텐츠`stop_server.sh`로를 생성합니다.

```
#!/bin/bash
service httpd stop
```

8. zip 번들을 생성합니다.

Linux:

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

Windows: "WordPress" 디렉터리로 이동하여 모든 파일을 선택하고 zip 파일을 생성합니다. 이름을 wordpress.zip으로 지정해야 합니다.

1. 애플리케이션 번들을 S3 버킷에 업로드

   스택을 계속 배포하려면 패키지가 있어야 합니다.

   생성한 모든 S3 버킷 인스턴스에 자동으로 액세스할 수 있습니다. Bastions(인스턴스 액세스 참조) 또는 S3 콘솔을 통해 액세스하고 drag-and-drop 또는 파일을 찾아 선택하여 CodeDeploy 패키지를 업로드할 수 있습니다.

   쉘 창에서 다음 명령을 사용할 수도 있습니다. zip 파일의 경로가 올바른지 확인하세요.

   ```
   aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
   ```

2. WordPress CodeDeploy 애플리케이션 번들 배포

   필수 데이터 코드 배포 애플리케이션 배포:

   - CodeDeployApplicationName: CodeDeploy 애플리케이션에 지정한 이름입니다.
   - CodeDeployGroupName: CodeDeploy 애플리케이션과 그룹은 모두 HA 스택 RFC에서 CodeDeploy 애플리케이션에 부여한 이름으로 생성되었으므로 CodeDeployApplicationName과 동일한 이름입니다.
   - S3Bucket: S3 버킷에 지정한 이름입니다.
   - S3BundleType 및 S3Key: 배포한 WordPress 애플리케이션 번들의 일부입니다.
   - VpcId: 관련 VPC입니다.

   a. RFC 생성 페이지의 RFC CT 선택 목록에서 범주 배포, 하위 범주 애플리케이션, 항목 CodeDeploy 애플리케이션 및 배포를 선택합니다.

   b. 기본 옵션을 유지하고 표시된 대로 값을 설정합니다.

> **Note**
>
> 이전에 생성한 CodeDeploy 애플리케이션, CodeDeploy 배포 그룹, S3 버킷 및 번들을 참조하세요.

```
Subject:                                    WP-CD-Deploy-RFC
Description:                                DeployWordPress
S3Bucket:                                   BUCKET_NAME
S3Key:                                      wordpress.zip
S3BundleType:                               zip
CodeDeployApplicationName:                  WordPress
CodeDeployDeploymentGroupName:              WordPress
CodeDeployIgnoreApplicationStopFailures:    false
RevisionType:                               S3



VpcId:                                      VPC_ID
Name:                                       WP-CD-Deploy-Op
TimeoutInMinutes:                           60
```

c. 완료되면 제출을 클릭합니다.

애플리케이션 배포 검증

WordPress 배포 경로 /WordPress를 사용하여 이전에 생성한 로드 밸런서의 엔드포인트(LoadBalancerCName)로 이동합니다. 예제:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

다음과 같은 페이지가 표시됩니다.

고가용성 배포 줄이기

배포를 해제하려면 HA 2계층 스택 및 S3 버킷에 대해 스택 삭제 CT를 제출하고 RDS 스냅샷을 삭제하도록 요청할 수 있습니다(10일 후에 자동으로 삭제되지만 그 동안 약간의 비용이 발생함). HA 스택과 S3 버킷의 스택 IDs를 수집한 다음 다음 다음 단계를 따릅니다. 스택 | 삭제를 참조하세요.

부록: SALZ 온보딩 설문지

주제

다음은 계정을 온보딩하기 전에 고려해야 할 몇 가지 정보입니다.

배포 요약

배포에 대한 설명입니다. 예:

- 이 계정은 (제품 애플리케이션 배포가 Line-of-Business 애플리케이션 배포용입니다.
- 배포에는 계정의 퍼블릭 또는 DMZ 서브넷 내에서 자동 조정된 ARP(인증된 역방향 프록시)가 포함됩니다.
- 웹 및 애플리케이션 서버는 계정의 프라이빗 서브넷 내에 배포됩니다.
- RDS(Amazon Relational Database Service) 인스턴스도 계정의 프라이빗 서브넷 내에 배포됩니다.
- 서버(ARP, 웹, 애플리케이션, 데이터베이스, 로드 밸런서 등)는 고유한 보안 그룹으로 구분됩니다.
- 계정에는 가용 영역(AZs) 전체에 분산된 HA(고가용성) 설계, 즉 "다중 AZ"가 필요합니다.

환경 아키텍처 고려 사항

환경 및 아키텍처를 구성하는 방법을 결정할 때 다음 기준을 고려하세요.

- 가상 데이터 센터가 회사 네트워크에 다시 연결되나요?
  - 기존 AWS DirectConnect 서비스가 있거나 새 DirectConnect 서비스가 필요합니까?
  - 기존 VPN 연결이 있거나 새 VPN 서비스가 필요합니까?
- 할당할 수 있는 내부 주소의 사용 가능한 CIDR 블록 범위는 무엇입니까? (/16 권장, 회사 네트워크 범위와 겹치지 않아야 함)
- 가상 데이터 센터에 인터넷 액세스가 필요합니까?
- 사용하려는 리전(들)은 어디입니까? (시드니/N. 버지니아/더블린)

- 다른 모든 서브넷에 연결된 애플리케이션을 호스팅하려면 공유 서비스 서브넷이 필요합니까?
- 별도의 서브넷으로 호스팅하려는 조직 부문은 무엇입니까? 각각에 대해:
  - 다른 서브넷에 어떤 연결이 필요합니까?
  - 서브넷에 인터넷 액세스가 필요합니까?
  - 해당 서브넷에 대한 애플리케이션 배포 제한이 있나요?
  - 해당 서브넷에 대한 특정 네트워크 요구 사항이 있습니까?
- 별도의 개발 및/또는 테스트 환경을 원하십니까? (언제든지 액세스할 수 있도록 중복된 공유 서비스 포함)
- 스냅샷 백업 요구 사항은 무엇인가요?
- 유지하려는 기존 유지 관리 프로세스 또는 패치 기간(들)이 있습니까?
- 도메인 등록 요구 사항은 무엇인가요?
- Single Sign-On 요구 사항이 있습니까?(예: AD, LDAP)
- 전반적인 예상 운영 체제 및 예상 용량 요구 사항은 무엇입니까?

단일 계정 랜딩 존 모니터링 알림

AMS는 특정 모니터링 알림에 대해 직접 알림을 받을 수 있는 방법(AMS 서비스 알림 받기와 비교)을 제공합니다. 이를 위해 가입하려면 Cloud Architect(CA 또는 Cloud Service Delivery Manager(CSDM)가 다음 정보를 수신해야 합니다.

Direct Alerts 이메일: AMS가 특정 리소스 기반 알림을 보낼 이메일 주소입니다. 이메일로 직접 전송되는 알림에 대한 자세한 내용은 단일 계정 랜딩 존용 AMS 사용 설명서의 AMS에서 기준 모니터링의 알림을 참조하세요. AMS 모니터링에 대한 자세한 내용은 단일 계정 랜딩 존용 AMS 사용 설명서의 모니터링 관리를 참조하세요.

유지 관리 기간

다양한 애플리케이션 요구 사항, 다양한 스트레스 기간 AWS 리전및 다양한 스트레스 기간을 고려하는 유지 관리 기간을 생성해야 합니다. 유지 관리 기간은 AMS가 패치를 적용하는 시점입니다. 여기에 몇 가지 지침이 있습니다.

- 사용자에게 미치는 영향을 제한하려면 환경이 배포 AWS 리전 된에 따라 유지 관리 기간을 계획합니다.
- 정규 업무 시간 외에 프로덕션 서버에서 트래픽이 가장 적을 것으로 예상되는 시간대를 예약합니다.
- 일반적으로 인프라 스택에는 월별 업데이트가 필요합니다.

- 최소 300분 동안 유지 관리 기간을 예약합니다. 운영 체제 패치 적용에는 60~90분이 걸리고 인프라 스택 패치 적용에는 180~300분이 걸립니다.

다음 단계

AMS 온보딩 팀은 계정을 AMS에 온보딩하는 모든 단계를 지원합니다. 온보딩 요구 사항은 다음과 같습니다.

- AMS AWS 계정 에 사용할 새를 프로비저닝하고 AWS 계정 ID를 제공합니다.
- 원하는 수준의 지원에 가입합니다.
- 교차 계정 IAM 역할을 생성하여 AMS 프로비저닝 계정에 액세스 권한을 부여하고 AMS에 역할 이름을 제공합니다.
- 계정 753102745277을 신뢰할 수 있는 엔터티로 추가합니다.

부록: ActiveDirectory Federation Services(ADFS) 클레임 규칙 및 SAML 설정

AD FS를 설치하고 구성하는 방법에 대한 step-by-step 지침은 Windows Active Directory, ADFS 및 SAML 2.0을 사용하여 AWS에 페더레이션 활성화를 참조하세요.

ADFS 클레임 규칙 구성

ADFS 구현이 이미 있는 경우 다음을 구성합니다.

- 신뢰 당사자 신뢰
- 클레임 규칙

신뢰 당사자 신뢰 및 클레임 규칙 단계는 Windows Active Directory, AD FS 및 SAML 2.0 블로그를 사용하여 AWS에 페더레이션 활성화에서 수행됩니다.

- 클레임 규칙:
  - Nameid: 블로그 게시물당 구성
  - RoleSessionName: 다음과 같이 구성
    - 클레임 규칙 이름: **`RoleSessionName`**
    - 속성 저장소: **`Active Directory`**
    - LDAP 속성: **`SAM-Account-Name`**
    - 발신 클레임 유형: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
    - AD 그룹 가져오기: 블로그 게시물당 구성
    - 역할 클레임: 다음과 같이 구성

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

웹 콘솔

아래 링크를 사용하여 *[ADFS-FQDN]*을 ADFS 구현의 FQDN으로 대체하여 AWS 웹 콘솔에 액세스할 수 있습니다.

https://*[ADFS-FQDN]*/adfs/ls/IdpInitiatedSignOn.aspx

IT 부서가 그룹 정책을 통해 사용자 집단에 위 링크를 배포할 수 있습니다.

SAML을 사용한 API 및 CLI 액세스

SAML을 사용하여 API 및 CLI 액세스를 구성하는 방법.

Python 패키지는 아래 블로그 게시물에서 제공됩니다.

- NTLM: SAML 2.0 및 AD FS를 사용하여 페더레이션 API 및 CLI 액세스를 구현하는 방법
- 양식: SAML 2.0을 사용하여 페더레이션 API/CLI 액세스를 위한 일반 솔루션을 구현하는 방법
- PowerShell: Windows PowerShell을 사용하여 AWS에 대한 페더레이션 API 액세스를 설정하는 방법

스크립트 구성

1. Notepad++를 사용하여 기본 리전을 올바른 리전으로 변경합니다.
2. Notepad++를 사용하여 테스트 및 개발 환경에 대한 SSL 확인 비활성화
3. Notepad++를 사용하여 idpentryurl 구성

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Windows 구성

아래 지침은 python 패키지에 대한 것입니다. 생성된 자격 증명은 1시간 동안 유효합니다.

1. python(2.7.11) 다운로드 및 설치
2. AWS CLI 도구 다운로드 및 설치
3. AMS CLI를 설치합니다.

a. 클라우드 서비스 제공 관리자(CSDM)가 제공하는 AMS 배포 가능 zip 파일을 다운로드하고 압축을 풉니다.

   여러 디렉터리와 파일을 사용할 수 있습니다.

b. 운영 체제에 따라 관리형 클라우드 배포 가능 -> CLI -> Windows 또는 관리형 클라우드 배포 가능 -> CLI -> Linux/MacOS 디렉터리를 엽니다.

   Windows의 경우 적절한 설치 관리자를 실행합니다(이 방법은 Windows 32 또는 64비트 시스템에서만 작동함).

   - 32비트: ManagedCloudAPI_x86.msi
   - 64비트: ManagedCloudAPI_x64.msi

   Mac/Linux의 경우 MC_CLI.sh라는 파일을 실행합니다. 명령을 실행하여이 작업을 수행할 수 있습니다`sh MC_CLI.sh`. amscm 및 amsskms 디렉터리와 해당 콘텐츠는 MC_CLI.sh 파일과 동일한 디렉터리에 있어야 합니다.

c. 기업 자격 증명을 AWS와의 페더레이션(AMS 기본 구성)을 통해 사용하는 경우 페더레이션 서비스에 액세스할 수 있는 자격 증명 관리 도구를 설치해야 합니다. 예를 들어이 AWS 보안 블로그 SAML 2.0 및 AD FS를 사용하여 연합 API 및 CLI 액세스를 구현하는 방법을 사용하여 자격 증명 관리 도구를 구성할 수 있습니다.

d. 설치 후 `aws amscm help` 및를 실행`aws amsskms help`하여 명령과 옵션을 확인합니다.

4. 필요한 SAML 스크립트 다운로드

   c:\aws\scripts로 다운로드

5. PIP 다운로드

   c:\aws\downloads로 다운로드

6. PowerShell을 사용하여 PIP 설치

   <pythondir>.\python.exe c:\aws\downloads\get-pip.py

7. PowerShell을 사용하여 boto 모듈 설치

   <pythondir\scripts>pip 설치 boto

8. PowerShell을 사용하여 요청 모듈 설치

   <pythondir\scripts>pip 설치 요청

9. PowerShell을 사용하여 요청 보안 모듈 설치

   <pythondir\scripts>pip 설치 요청[보안]

10. PowerShell을 사용하여 beautifulsoup 모듈 설치

    <pythondir\scripts>pip 설치 beautifulsoup4

11. PowerShell을 사용하여 사용자 프로필에 .aws라는 폴더를 생성합니다(%userprofile%\.aws).

    mkdir .aws

12. PowerShell을 사용하여 .aws 폴더에 자격 증명 파일 생성

    New-Item 자격 증명 -유형 파일 –force

    자격 증명 파일에 파일 확장자가 없어야 합니다.

    파일 이름은 모두 소문자여야 하며 이름 자격 증명이 있어야 합니다.

13. 메모장으로 자격 증명 파일을 열고 올바른 리전을 지정하여 다음 데이터를 붙여 넣습니다.

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. PowerShell, SAML 스크립트 및 로그온 사용

    <pythondir>.\python.exe c:\aws\scripts\samlapi.py

    사용자 이름: [USERNAME]@upn

    수임할 역할을 선택합니다.

Linux 구성

생성된 자격 증명은 1시간 동안 유효합니다.

1. WinSCP를 사용하여 SAML 스크립트 전송
2. WinSCP를 사용하여 루트 CA 인증서 전송(테스트 및 개발 무시)
3. 신뢰할 수 있는 루트 인증서에 ROOT CA 추가(테스트 및 개발 무시)

$ openssl x509 -in der -in [certname].cer -out certificate.pem(테스트 및 개발 무시)

certificate.pem의 내용을 /etc/ssl/certs/ca-bundle.crt 파일의 끝에 추가합니다((테스트 개발의 경우 무시).

4. home/ec2-user 5에서 .aws 폴더 생성

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. WinSCP를 사용하여 자격 증명 파일을 .aws 폴더로 전송합니다.
6. Boto 모듈 설치

   $ sudo pip install boto
7. 요청 모듈 설치

   $ sudo pip 설치 요청
8. beautifulsoup 모듈 설치

   $ sudo pip install beautifulsoup4
9. 스크립트를 home/ec2-user에 복사

   필요한 권한 설정

   스크립트 실행: samlapi.py

문서 이력

다음 표에서는 AMS의 마지막 릴리스 이후 설명서에 대한 중요한 변경 사항을 설명합니다.

- API 버전: 2019-05-21
- 최종 설명서 업데이트: 2025년 9월 23일

변경	설명	Date
SALZ: 기본 설정 섹션에서 로그 보존 및 교체 기본값 업데이트	로그 보존 및 교체 기본값은 입니다. AWS CloudTrail 로그에 대한 정보가 업데이트 되었습니다.	2026년 2월 11일
AWS Managed Services FAQ 섹션의 SageMaker AI에서 엔드포인트 Autoscaling에 대한 변경 유형 업데이트	AMS SSP를 사용하여 AMS 계정에서 Amazon SageMaker AI를 프로비저닝합니다. 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 업데이트(관리형 자동화) 변경 유형(ct-27tuth19k52b4)을 사용하여 RFC를 제출하여 자동 크기 조정 권한을 일시적으로 또는 영구적으로 승격합니다. 자동 크기 조정을 위해서는 CloudWatch 서비스에 대한 허용적인 액세스가 필요합니다.	2025년 9월 25일
정확한 변경 유형 참조	보안 그룹을 생성, 변경 또는 삭제합니다. 사용자를 추가하려면: 관리 | 디렉터리 서비스 | 사용자 및 그룹 | 그룹에 사용자 추가 [ct-24pi85mjtza8k] 및 사용자를 제거하려면: 관리 | 디렉터리 서비스 | 사용자 및 그룹 | 그룹에서 사용자 제거 [ct-2019s9y3nfml4]를 사용하여 RFC 제출	2025년 8월 8일
TOC 링크 제거됨	TOC AWS 용어집 링크가 제거되었습니다.	2025년 8월 8일

변경	설명	Date
처방 지침에 대한 링크를 추가했습니다.	통합 결제 설정 - 새 계정을 지급인 계정에 연결.	2025년 5월 8일
에 대한 IAM 액세스를 활성화하는 지침을 업데이트했습니다. AWS Management Console	에 대한 IAM 액세스 활성화 지침을 명확히 했습니다 AWS Management Console.	AWS 콘솔에 대한 IAM 액세스 활성화
Direct Connect 전용 연결에서 허용되는 전송 가상 인터페이스 수 업데이트	Direct Connect 전용 연결에는 이제 연결당 4개의 전송 가상 인터페이스 제한이 있습니다.	전송 게이트웨이에 Direct Connect 연결
문구를 개선합니다.	AMS 모니터링 및 관리 작업을 보장하려면 "'거부' 목록으로만 사용"에 '모두 허용'이 포함되어야 한다고 지정했습니다.	네트워크 구성
AMS CLI 사용에 대한 추가 정보입니다.	“일부 CLI 명령에 `--region` 옵션이 필요할 수 있다는 점에 유의하세요.”	AMS CLIs 설치
업데이트됨: 일관성 및 가독성을 위한 장 제목, 일부 주제 하위 섹션을 더 적절한 섹션으로 이동	“변경 관리를 위한 모드”는 “변경 관리”의 새로운 제목입니다.	변경 관리 모드
콘텐츠 업데이트	이전에는 "변경 관리 모드" 또는 "표준 CM 모드"라고 했던 AMS 모드를 이제 "RFC 모드"라고 합니다. 모드 섹션이 확장되었습니다.	RFC 모드.
콘텐츠 업데이트	이전에는 "변경 관리 모드" 또는 "표준 CM 모드"라고 했던 AMS 모드를 이제 "RFC 모드"라고 합니다. 모드 섹션이 단축되었으며 모드에 대한 AMS 고급 사용 설명서 섹션 링크가 추가되었습니다.	AMS 모드.
MALZ: 네트워크 아키텍처 다이어그램 업데이트	네트워킹 계정 아키텍처m	2022년 6월 16일

변경	설명	Date
주제 목록을 아래 열린 단락으로 이동	AWS Managed Services 온보딩 소개	2022년 6월 16일
업데이트된 콘텐츠, 포괄적인 언어 이니셔티브	"마스터 계정"이 아닌 "관리 계정".	AMS의 IAM 사용자 역할, "정책 예제" 섹션
업데이트된 콘텐츠, 도구 계정 역할 이름	역할 이름 CustomerMigrationAccessRole을 AWSManagedServicesMigrationRole로 업데이트했습니다.	AWS Application Migration Service(AWS MGN)
SALZ: 연속성 관리 기본값	링크를 업데이트하고에서 더 이상 사용되지 않는 정보를 제거했습니다. VPC 태그 및 기본값	2022년 2월 28일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.