aws

관리자 안내서

아마존 WorkMail

버전 1.0

아마존 WorkMail: 관리자 안내서

Table of Contents

아마존이란 WorkMail 무엇입니까?

WorkMail Amazon은 기존 데스크톱 및 모바일 이메일 클라이언트를 지원하는 안전한 관리형 비즈니스 이메일 및 일정 관리 서비스입니다. Amazon WorkMail 사용자는 Microsoft Outlook, 브라우저 또는 기본 iOS 및 Android 이메일 애플리케이션을 사용하여 이메일, 연락처 및 일정에 액세스할 수 있습니다. WorkMail Amazon을 기존 회사 디렉터리와 통합하여 데이터를 암호화하는 키와 데이터가 저장되는 위치를 모두 제어할 수 있습니다.

지원되는 AWS 리전 및 엔드포인트 목록은 AWS 리전 및 엔드포인트를 참조하십시오.

주제

아마존 WorkMail 시스템 요구 사항

Amazon WorkMail 관리자가 Amazon WorkMail 계정에 로그인하도록 초대하면 Amazon WorkMail 웹 클라이언트를 사용하여 로그인할 수 있습니다.

WorkMail 또한 Amazon은 Exchange ActiveSync 프로토콜을 지원하는 모든 주요 모바일 장치 및 운영 체제와 호환됩니다. 이러한 디바이스에는 iPad, iPhone, Android 및 Windows Phone이 포함됩니다. macOS 사용자는 Amazon WorkMail 계정을 메일, 캘린더 및 연락처 앱에 추가할 수 있습니다.

Amazon은 다음 운영 체제 버전을 WorkMail 지원합니다.

- 윈도우 — 윈도우 7 SP1 이상
- macOS — macOS 10.12 (시에라) 이상
- 안드로이드 — 안드로이드 5.0 이상
- 아이폰 — iOS 5 이상
- 윈도우 폰 - 윈도우 8.1 이상
- 블랙베리 — 블랙베리 OS 10.3.3.3216

유효한 Microsoft Outlook 라이선스가 있는 경우 다음 버전의 Microsoft WorkMail Outlook을 사용하여 Amazon에 액세스할 수 있습니다.

- 아웃룩 2013 이상
- 아웃룩 2013 간편 실행 이상
- 맥용 아웃룩 2016 이상

다음 브라우저 버전을 사용하여 Amazon WorkMail 웹 클라이언트에 액세스할 수 있습니다.

- 구글 크롬 — 버전 22 이상
- 모질라 파이어폭스 — 버전 27 이상
- 사파리 — 버전 7 이상
- 인터넷 익스플로러 — 버전 11
- Microsoft Edge

선호하는 IMAP 클라이언트와 WorkMail 함께 Amazon을 사용할 수도 있습니다.

아마존 WorkMail 컨셉

Amazon을 이해하고 사용하는 데 있어 핵심이 되는 용어와 개념은 아래에 WorkMail 설명되어 있습니다.

조직

Amazon용 테넌트 설정 WorkMail.

별칭

조직을 식별하는 전역적으로 고유한 이름입니다. 별칭은 아마존 WorkMail 웹 애플리케이션 (*https://alias* .awsapps.com/mail) 에 액세스하는 데 사용됩니다.

도메인

이메일 주소에서 @ 기호 뒤에 오는 웹 주소입니다. 조직 내에서 메일을 수신해 사서함으로 전달하는 도메인을 추가할 수 있습니다.

메일 도메인 테스트

도메인은 설정 중에 자동으로 구성되어 Amazon을 테스트하는 데 사용할 수 WorkMail 있습니다. 테스트 메일 도메인은 *alias*.awsapps.com이고 고유한 도메인을 구성하지 않은 경우 기본 도메인으

로 사용됩니다. 테스트 메일 도메인에는 여러 가지 제한이 있을 수 있습니다. 자세한 설명은 아마존 WorkMail 쿼터 섹션을 참조하세요.

디렉터리

AWS Directory Service에서 생성되는 AWS Simple AD, AWS Managed AD 또는 AD 커넥터입니다. Amazon WorkMail Quick Setup을 사용하여 조직을 생성하면 자동으로 WorkMail 디렉터리가 생성됩니다. 에서는 WorkMail 디렉터리를 볼 수 없습니다AWS Directory Service.

User

AWS Directory Service에서 생성된 사용자입니다. 사용자는 USER 또는 REMOTE_USER 역할로 생성할 수 있습니다. 사용자가 사용자 역할과 함께 생성되고 활성화되면 사용자에게 액세스할 자체 사서함이 부여됩니다. 비활성화된 사용자는 Amazon에 액세스할 수 없습니다 WorkMail.

REMOTE_USER 역할로 생성 및 활성화된 사용자는 주소록에 나열되지만 Amazon에는 사서함이 없습니다. WorkMail REMOTE_USER는 사서함을 Amazon 외부에 호스팅할 수 WorkMail 있지만 여전히 Amazon WorkMail 주소록에 사서함이 있는 다른 사용자로 표시되며 서로의 일정을 검색하여 빈 시간이나 바쁜 정보를 찾을 수 있습니다.

그룹

AWS Directory Service에서 사용되는 그룹입니다. 그룹은 Amazon에서 배포 목록 또는 보안 그룹으로 사용할 수 WorkMail 있습니다. 그룹에는 자체 사서함이 없습니다.

Resource

리소스는 Amazon WorkMail 사용자가 예약할 수 있는 회의실 또는 장비 리소스를 나타냅니다.

모바일 디바이스 정책

모바일 디바이스의 보안 기능 및 동작을 제어하는 다양한 IT 정책 규칙입니다.

관련 AWS 서비스

Amazon과 함께 사용되는 서비스는 다음과 WorkMail 같습니다.

- AWS Directory Service WorkMail —Amazon을 기존의 AWS 심플 AD, AWS 매니지드 AD 또는 AD 커넥터와 통합할 수 있습니다. 에서 디렉터리를 생성한 다음 이 디렉터리에 WorkMail 대해 Amazon을 활성화합니다. AWS Directory Service 이 통합을 구성한 후에는 기존 디렉터리의 사용자 WorkMail 목록에서 Amazon에서 활성화할 사용자를 선택할 수 있으며, 사용자는 기존 Active Directory 자격 증명을 사용하여 로그인할 수 있습니다. 자세한 내용은 AWS Directory Service 관리 안내서를 참조하세요.

- Amazon 심플 이메일 서비스 WorkMail —아마존은 Amazon SES를 사용하여 모든 발신 이메일을 전송합니다. 테스트 메일 도메인과 사용자의 도메인은 Amazon SES 콘솔에서 관리에 사용할 수 있습니다. WorkMailAmazon에서 보내는 발신 이메일에는 요금이 부과되지 않습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드를 참조하세요.
- AWS Identity and Access Management - AWS Management Console을 사용하려면 서비스에서 사용자가 리소스에 액세스할 수 있는 권한이 있는지 여부를 확인할 수 있도록 사용자 이름과 암호가 필요합니다. AWS 계정 자격 증명은 어떤 식으로든 취소하거나 제한할 수 없으므로 AWS에 액세스할 때는 가급적 AWS 계정의 자격 증명을 사용하지 않는 것이 좋습니다. 대신 IAM 사용자를 만들고 이 사용자를 관리 권한이 있는 IAM 그룹에 추가하는 것이 좋습니다. 그러면 IAM 사용자 자격 증명으로 콘솔에 액세스할 수 있게 됩니다.

  AWS에 가입했지만 IAM 사용자를 생성하지 않았다면 IAM 콘솔에서 생성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 개별 IAM 사용자 생성을 참조하세요.
- AWS Key Management Service WorkMail —Amazon은 고객 데이터 암호화를 AWS KMS 위해 통합되었습니다. 키 관리는 AWS KMS 콘솔에서 수행할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS Key Management Service란 무엇입니까?를 참조하세요.

아마존 WorkMail 가격

WorkMailAmazon에서는 선결제 금액이나 약정이 없습니다. 활성 사용자 계정에 대해서만 지불하면 됩니다. 요금에 대한 자세한 내용은 요금을 참조하십시오.

아마존 WorkMail 리소스

다음의 관련 리소스는 이 서비스를 이용할 때 도움이 될 수 있습니다.

- Classes & Workshops(교육 및 워크숍) – 역할 기반의 과정 및 전문 과정은 물론 자습형 실습에 대한 링크를 통해 AWS 기술을 연마하고 실무에 도움이 되는 경험을 쌓을 수 있습니다.
- AWSDeveloper Center(개발자 센터) – 튜토리얼을 살펴보고, 도구를 다운로드하고, AWS 개발자 이벤트에 대해 알아보세요.
- AWS 개발자 도구 – AWS 애플리케이션을 개발 및 관리하기 위한 개발자 도구, SDK, IDE 도구 키트 및 명령행 도구 링크입니다.
- Getting Started Resource Center(시작하기 리소스 센터) - AWS 계정을(를) 설정하고 AWS 커뮤니티에 가입하고 첫 번째 애플리케이션을 시작하는 방법을 알아보세요.
- 실습 자습서 — 자습서를 따라 step-by-step 첫 번째 애플리케이션을 시작하십시오. AWS

- AWSWhitepapers(백서) – AWS 솔루션 아키텍트 또는 기타 기술 전문가가 아키텍처, 보안 및 경제 등의 토픽에 대해 작성한 포괄적 AWS 기술 백서 목록의 링크입니다.
- AWS SupportCenter(센터) – AWS Support 사례를 생성하고 관리할 수 있는 허브입니다. 또한 포럼, 기술 FAQ, 서비스 상태 및 AWS Trusted Advisor 등의 기타 유용한 자료에 대한 링크가 있습니다.
- AWS Support— 클라우드에서 애플리케이션을 구축하고 실행하는 데 도움이 되는 one-on-one 빠른 응답 지원 채널에 대한 AWS Support 정보를 제공하는 기본 웹 페이지입니다.
- Contact Us(문의처) - AWS 결제, 계정, 이벤트, 침해 및 기타 문제에 대해 문의할 수 있는 중앙 연락 창구입니다.
- AWSSite Terms(사이트 약관) – 저작권 및 상표, 사용자 계정, 라이선스 및 사이트 액세스와 기타 토픽에 대한 세부 정보입니다.

필수 조건

Amazon WorkMail 관리자로 활동하려면 AWS 계정이 필요합니다. AWS에 아직 등록하지 않은 경우 다음 작업을 완료해 설정합니다.

주제

가입하십시오. AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면AWS 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 참조하십시오.

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 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

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 포털 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

IAM 사용자에게 Amazon에 대한 권한 부여 WorkMail

기본적으로 IAM 사용자에게는 Amazon WorkMail 리소스를 관리할 권한이 없습니다. AWS 관리형 정책 (AmazonWorkMailFullAccess또는 AmazonWorkMailReadOnlyAccess) 을 연결하거나 IAM 사용자에게 이러한 권한을 명시적으로 부여하는 고객 관리형 정책을 생성해야 합니다. 그런 다음 해당 권한이 필요한 IAM 사용자 또는 그룹에 이 정책을 연결합니다. 자세한 내용은 Amazon의 자격 증명 및 액세스 관리 WorkMail을(를) 참조하세요.

아마존의 보안 WorkMail

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. WorkMailAmazon에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 WorkMail 됩니다. 다음 주제는 보안 및 규정 준수 목표를 WorkMail 충족하도록 Amazon을 구성하는 방법을 보여줍니다. 또한 Amazon WorkMail 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

아마존에서의 데이터 보호 WorkMail

AWS 공동 책임 모델 Amazon의 데이터 보호에 적용됩니다 WorkMail. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호할 책임이 AWS 클라우드있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시를 참조하십시오FAQ. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 공동 책임 모델 및AWS 보안 GDPR 블로그의 블로그 게시물을 참조하십시오.

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

- 각 계정마다 다단계 인증 (MFA) 을 사용하십시오.
- SSLTLS/를 사용하여 AWS 리소스와 통신하세요. TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- API를 사용하여 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API an을 AWS 통해 액세스할 때 FIPS 140-3개의 검증된 암호화 모듈이 필요한 경우 엔드포인트를 사용하십시오. FIPS 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준 () 140-3을 참조하십시오. FIPS

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 Amazon WorkMail 또는 다른 콘솔을 AWS 서비스 사용하여 작업하거나 API AWS CLI, 또는 다른 사용자와 작업하는 경우가 포함됩니다 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 제공하는 경우 해당 서버에 대한 요청을 URL 검증하기 위해 자격 증명 정보를 에 포함하지 않는 것이 좋습니다. URL

아마존이 WorkMail 사용하는 방법 AWS KMS

Amazon은 메시지를 디스크에 쓰기 전에 모든 Amazon WorkMail 조직의 사서함에 있는 모든 메시지를 WorkMail 투명하게 암호화하고, 사용자가 메시지에 액세스할 때 메시지를 투명하게 해독합니다. 암호화는 비활성화할 수 없습니다. 메시지를 보호하는 암호화 키를 보호하기 위해 WorkMail Amazon은 AWS Key Management Service (AWS KMS) 와 통합되었습니다.

Amazon은 WorkMail 또한 사용자가 서명되거나 암호화된 이메일을 보낼 수 있는 옵션을 제공합니다. 이 암호화 기능은 AWS KMS를 사용하지 않습니다. 자세한 내용은 서명되거나 암호화된 이메일 활성화 단원을 참조하십시오.

주제

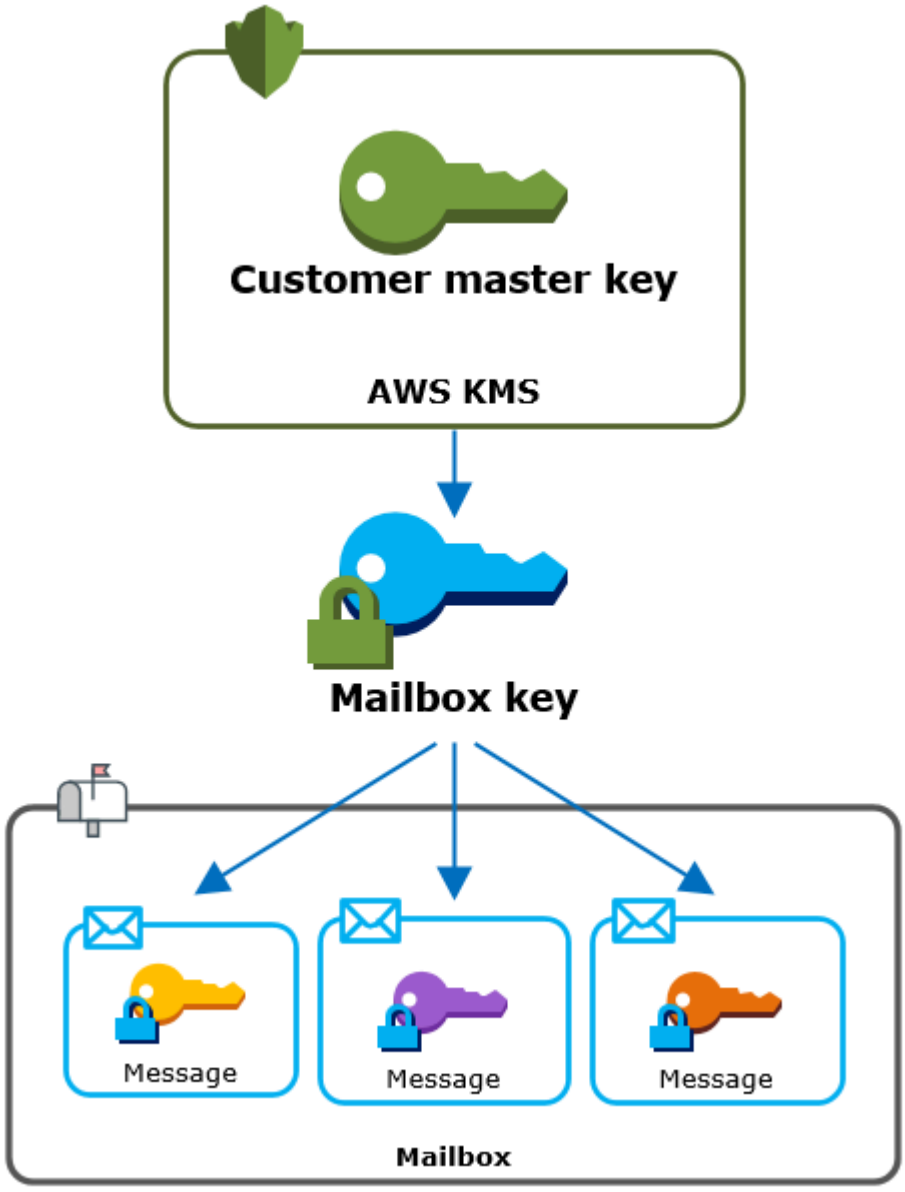
- 아마존 WorkMail 암호화
- 사용 권한 부여 CMK
- Amazon WorkMail 암호화 컨텍스트
- WorkMail Amazon과의 상호 작용 모니터링 AWS KMS

아마존 WorkMail 암호화

WorkMailAmazon에서는 각 조직에 조직의 사용자당 하나씩 여러 사서함을 포함할 수 있습니다. 이메일 및 일정 항목을 포함하여 모든 메시지는 사용자의 사서함에 저장됩니다.

Amazon WorkMail 조직의 사서함 콘텐츠를 보호하기 위해 Amazon은 모든 사서함 메시지를 디스크에 쓰기 전에 WorkMail 암호화합니다. 고객이 제공하는 정보는 일반 텍스트로 저장되지 않습니다.

각 메시지는 고유한 데이터 암호화 키로 암호화됩니다. 메시지 키는 해당 사서함에서만 사용되는 고유한 암호화 키인 사서함 키로 보호됩니다. 사서함 키는 조직의 AWS KMS 고객 마스터 키 (CMK) 로 암호화되므로 암호화되지 않은 상태로 유지되지 않습니다. AWS KMS 다음 다이어그램은 암호화된 메시지, 암호화된 메시지 키, 암호화된 사서함 키 및 조직의 관계를 보여줍니다. CMK AWS KMS



조직을 CMK 위한 a 설정

Amazon 조직을 생성할 때 WorkMail 조직의 AWS KMS 고객 마스터 키 (CMK) 를 선택할 수 있습니다. 이렇게 하면 해당 조직의 모든 사서함 키가 CMK 보호됩니다.

기본 CMK Amazon용 AWS 관리형을 선택하거나 WorkMail, 소유하고 관리하는 기존 고객 CMK 관리형을 선택할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 마스터 키 (CMKs) 를 참조하십시오. 각 조직에 CMK 대해 CMK 동일하거나 다른 것을 선택할 수 있지만 CMK 한 번 선택한 후에는 변경할 수 없습니다.

> **Important**
>
> WorkMail Amazon은 CMKs 대칭만 지원합니다. CMK비대칭은 사용할 수 없습니다. a가 대칭인지 CMK 비대칭인지 판단하는 데 도움이 필요하면 개발자 안내서의 대칭 및 비대칭 식별을 참조하십시오. CMKs AWS Key Management Service

조직에 맞는 것을 찾으려면 CMK 호출을 기록하는 AWS CloudTrail 로그 항목을 사용하세요. AWS KMS

각 사서함마다 고유한 암호화 키

사서함을 생성하면 Amazon은 사서함 외부에 대해 고유한 256비트 고급 암호화 표준 (AES) 대칭 암호화 키 (사서함 키라고 함) 를 WorkMail 생성합니다. AWS KMS WorkMail Amazon은 사서함 키를 사용하여 사서함에 있는 각 메시지의 암호화 키를 보호합니다.

사서함 키를 보호하기 위해 Amazon은 조직의 사서함 키를 AWS KMS 암호화하도록 WorkMail 요청합니다. CMK 그런 다음 암호화된 사서함 키를 사서함 메타데이터에 저장합니다.

> **Note**
>
> WorkMail Amazon은 대칭 메일박스 암호화 키를 사용하여 메시지 키를 보호합니다. 이전에 Amazon은 비대칭 키 쌍으로 각 사서함을 WorkMail 보호했습니다. 즉, 퍼블릭 키를 사용하여 각 메시지 키를 보호하고 프라이빗 키를 사용하여 해독했습니다. 개인 사서함 키는 조직을 CMK 위해 에서 보호했습니다. 이전 사서함은 비대칭 사서함 키 쌍을 사용할 수 있습니다. 이 변경 사항은 사서함 또는 그 안의 메시지의 보안에 영향을 미치지 않습니다.

각 메시지 암호화

사용자가 사서함에 메시지를 추가하면 Amazon은 외부 메시지에 대해 고유한 256비트 AES 대칭 암호화 키를 WorkMail 생성합니다. AWS KMS이 메시지 키를 사용하여 메시지를 암호화합니다. WorkMail Amazon은 사서함 키 아래의 메시지 키를 암호화하고 암호화된 메시지 키를 메시지와 함께 저장합니다. 그런 다음 조직의 사서함 키를 암호화합니다. CMK

새 사서함 생성

Amazon은 사서함을 WorkMail 생성할 때 다음 프로세스를 사용하여 암호화된 메시지를 보관할 사서함을 준비합니다.

- Amazon은 외부 사서함에 대해 고유한 256비트 AES 대칭 암호화 키를 WorkMail 생성합니다. AWS KMS
- Amazon은 AWS KMS 암호화 작업을 WorkMail 호출합니다. 사서함 키와 조직의 고객 마스터 키 (CMK) 식별자를 전달합니다. AWS KMS 로 암호화된 사서함 키의 암호문을 반환합니다. CMK
- Amazon은 암호화된 메일박스 키를 메일박스 메타데이터와 함께 WorkMail 저장합니다.

사서함 메시지 암호화

메시지를 암호화하기 위해 WorkMail Amazon은 다음 프로세스를 사용합니다.

1. Amazon은 메시지에 대해 고유한 256비트 AES 대칭 키를 WorkMail 생성합니다. 일반 텍스트 메시지 키와 고급 암호화 표준 (AES) 알고리즘을 사용하여 외부 메시지를 암호화합니다. AWS KMS
2. 사서함 키 아래의 메시지 키를 보호하려면 Amazon은 사서함 키를 WorkMail 해독해야 합니다. 사서함 키는 항상 암호화된 형태로 저장됩니다.

   Amazon은 AWS KMS 복호화 작업을 WorkMail 호출하고 암호화된 메일박스 키를 전달합니다. AWS KMS 조직에서 사서함 키를 해독하는 데 를 사용하고 Amazon에 일반 텍스트 사서함 키를 반환합니다. CMK WorkMail
3. WorkMail Amazon은 일반 텍스트 사서함 키와 고급 암호화 표준 (AES) 알고리즘을 사용하여 외부의 메시지 키를 암호화합니다. AWS KMS
4. Amazon은 암호화된 메시지 키를 암호화된 메시지의 메타데이터에 WorkMail 저장하므로 이를 해독할 수 있습니다.

사서함 메시지 해독

메시지를 해독하기 위해 WorkMail Amazon은 다음 프로세스를 사용합니다.

1. Amazon은 AWS KMS 복호화 작업을 WorkMail 호출하고 암호화된 메일박스 키를 전달합니다. AWS KMS 조직에서 사서함 키를 해독하는 데 를 사용하고 Amazon에 일반 텍스트 사서함 키를 반환합니다. CMK WorkMail
2. WorkMail Amazon은 일반 텍스트 사서함 키와 고급 암호화 표준 (AES) 알고리즘을 사용하여 외부에서 암호화된 메시지 키를 해독합니다. AWS KMS
3. WorkMail Amazon은 일반 텍스트 메시지 키를 사용하여 암호화된 메시지를 해독합니다.

사서함 키 캐싱

성능을 개선하고 호출을 최소화하기 위해 AWS KMS Amazon은 각 클라이언트의 각 일반 텍스트 사서함 키를 최대 1분 동안 로컬에 WorkMail 캐시합니다. 캐싱 기간이 만료되면 사서함 키가 제거됩니다. 캐싱 기간 동안 해당 클라이언트의 메일박스 키가 필요한 경우 Amazon은 AWS KMS호출하는 대신 캐시에서 메일박스 키를 가져올 WorkMail 수 있습니다. 사서함 키는 캐시에서 보호되며 절대로 일반 텍스트로 디스크에 기록되지 않습니다.

사용 권한 부여 CMK

Amazon이 암호화 작업에 고객 마스터 키 (CMK) 를 WorkMail 사용하는 경우 사서함 관리자를 대신하여 작동합니다.

AWS KMS 고객 마스터 키 (CMK) 를 사용자 대신 비밀로 사용하려면 관리자에게 다음 권한이 있어야 합니다. IAM정책 또는 키 정책에서 이러한 필수 권한을 지정할 수 있습니다.

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

WorkMailAmazon에서 시작된 요청에만 를 사용할 수 있도록 하려면 kms: ViaService 조건 키를 값과 함께 사용하면 됩니다`workmail.<region>.amazonaws.com`. CMK

암호화 컨텍스트의 키 또는 값을 암호화 작업에 사용하기 위한 조건으로 사용할 수도 있습니다. CMK 예를 들어, IAM 또는 키 정책 문서에서 문자열 조건 연산자를 사용하거나 권한 부여에 허가 제약 조건을 사용할 수 있습니다.

관리 대상 AWS 키 정책 CMK

AWS Managed CMK for Amazon의 키 정책은 WorkMail Amazon이 CMK 사용자를 대신하여 요청하는 경우에만 지정된 작업에 사용할 권한을 사용자에게 WorkMail 부여합니다. 키 정책에서는 어떤 사용자도 를 CMK 직접 사용하는 것을 허용하지 않습니다.

이 키 정책은 모든 AWS 관리형 키의 정책처럼 서비스에 의해 설정됩니다. 키 정책은 변경할 수 없지만 언제든지 볼 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 보기를 참조하세요.

키 정책의 정책 설명문은 다음 효과를 갖습니다.

- 계정 및 지역의 사용자가 암호화 작업과 권한 CMK 부여에 를 사용할 수 있도록 허용하되, 사용자를 대신하여 WorkMail Amazon에서 요청하는 경우에만 허용합니다. `kms:ViaService` 조건 키는 이 제한을 강제 적용합니다.
- AWS 계정에서 사용자가 CMK 속성을 보고 허가를 취소할 수 있는 IAM 정책을 생성할 수 있도록 허용합니다.

다음은 CMK Amazon용으로 AWS 관리되는 예제의 주요 WorkMail 정책입니다.

```
{
  "Version" : "2012-10-17",
  "Id" : "auto-workmail-1",
  "Statement" : [ {
    "Sid" : "Allow access through WorkMail for all principals in the account that are
 authorized to use WorkMail",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*", "kms:DescribeKey",
 "kms:Encrypt" ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "workmail.us-east-1.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
    }
  }, {
    "Sid" : "Allow direct access to key metadata to the account",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
    "Resource" : "*"
  } ]
}
```

보조금을 사용하여 Amazon을 승인하기 WorkMail

WorkMail Amazon은 주요 정책 외에도 권한 부여를 사용하여 각 조직의 권한을 추가합니다. CMK 계정 CMK 내 에 부여된 권한을 보려면 ListGrants작업을 사용하십시오.

WorkMail Amazon은 권한 부여를 사용하여 조직의 다음 권한을 추가합니다. CMK

- WorkMail Amazon이 메일박스 키를 암호화할 수 있도록 허용하는 `kms:Encrypt` 권한을 추가합니다.
- WorkMail Amazon이 를 사용하여 사서함 키를 CMK 해독할 수 있도록 `kms:Decrypt` 권한을 추가합니다. 사서함 메시지 읽기 요청은 메시지를 읽는 사용자의 보안 컨텍스트를 사용하기 때문에 Amazon은 권한 부여를 위해 이 권한을 WorkMail 요구합니다. 요청에는 AWS 계정의 자격 증명이 사용되지 않습니다. 조직에 지원금을 선택하면 Amazon에서 CMK 이 보조금을 WorkMail 생성합니다.

보조금을 생성하기 위해 Amazon은 조직을 만든 사용자를 CreateGrant대신하여 WorkMail 요청을 합니다. 권한 부여 생성 권한은 키 정책에 의해 부여됩니다. 이 정책은 WorkMail Amazon이 승인된 사용자를 `CreateGrant` 대신하여 요청할 때 계정 사용자가 조직을 대신하여 요청을 할 수 있도록 허용합니다. CMK

또한 키 정책은 계정 루트가 AWS 관리 키에 대한 권한을 취소할 수 있도록 허용합니다. 하지만 권한을 취소하면 Amazon에서 사서함의 암호화된 데이터를 WorkMail 해독할 수 없습니다.

Amazon WorkMail 암호화 컨텍스트

암호화 컨텍스트는 비밀이 아닌 임의의 데이터를 포함하는 키-값 페어 세트입니다. 데이터 암호화 요청에 암호화 컨텍스트를 포함하면 AWS KMS 암호화 컨텍스트를 암호화된 데이터에 암호화하여 바인딩합니다. 따라서 동일한 암호화 컨텍스트로 전달해야 이 데이터를 해독할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 가이드에서 암호화 컨텍스트를 참조하세요.

WorkMail Amazon은 모든 AWS KMS 암호화 작업에서 동일한 암호화 컨텍스트 형식을 사용합니다. 암호화 컨텍스트를 사용하여 AWS CloudTrail 같은 감사 레코드나 로그에서, 그리고 정책 및 권한 부여의 권한 부여 조건으로서, 암호화 작업을 식별할 수 있습니다.

AWS KMS Amazon은 암호화 및 복호화 요청에 대해 키가 `aws:workmail:arn` 있고 값이 조직의 Amazon 리소스 이름 (ARN) 인 암호화 컨텍스트를 WorkMail 사용합니다.

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization-ID"
```

예를 들어, 다음 암호화 컨텍스트에는 유럽 (아일랜드) (`eu-west-1`) ARN 지역의 예제 조직이 포함됩니다.

```
"aws:workmail:arn":"arn:aws:workmail:eu-west-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
```

WorkMail Amazon과의 상호 작용 모니터링 AWS KMS

Amazon CloudWatch Logs를 사용하여 AWS CloudTrail Amazon이 사용자를 대신하여 WorkMail 보내는 요청을 추적할 AWS KMS 수 있습니다.

암호화

사서함을 생성하면 Amazon에서 사서함 키를 WorkMail 생성하고 사서함 키를 AWS KMS 암호화하도록 호출합니다. Amazon은 일반 텍스트 사서함 키 및 Amazon 조직의 식별자와 AWS KMS 함께 Encrypt 요청을 CMK 에 WorkMail 보냅니다. WorkMail

`Encrypt` 작업을 기록하는 이벤트는 다음 예시 이벤트와 유사합니다. 사용자는 Amazon WorkMail 서비스입니다. 매개변수에는 Amazon WorkMail 조직의 CMK ID (`keyId`) 및 암호화 컨텍스트가 포함됩니다. Amazon은 사서함 WorkMail 키도 전달하지만 CloudTrail 로그에는 기록되지 않습니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
```

```
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```

Decrypt

사서함 메시지를 추가, 확인 또는 삭제하면 Amazon에서 사서함 키의 암호를 WorkMail AWS KMS 해독하도록 요청합니다. Amazon은 암호화된 사서함 키 및 Amazon CMK 조직의 식별자와 AWS KMS 함께 암호 해독 요청을 에게 WorkMail 보냅니다. WorkMail

Decrypt 작업을 기록하는 이벤트는 다음 예시 이벤트와 유사합니다. 사용자는 Amazon WorkMail 서비스입니다. 매개변수에는 로그에 기록되지 않는 암호화된 사서함 키 (암호문 블럽) 와 Amazon 조직의 암호화 컨텍스트가 포함됩니다. WorkMail AWS KMS 암호문에서 의 ID를 가져옵니다. CMK

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-20T11:51:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
    },
    "responseElements": null,
    "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",
```

```
    "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"
}
```


Amazon의 자격 증명 및 액세스 관리 WorkMail

AWS Identity and Access Management (IAM) 는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM관리자는 Amazon WorkMail 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM추가 비용 없이 사용할 AWS 서비스 수 있습니다.

주제

고객

WorkMailAmazon에서 수행하는 작업에 따라 AWS Identity and Access Management (IAM) 사용 방법이 다릅니다.

서비스 사용자 — Amazon WorkMail 서비스를 사용하여 업무를 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 Amazon WorkMail 기능을 사용하여 작업을 수행함에 따라 추가 권

한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. WorkMailAmazon에서 기능에 액세스할 수 없는 경우 을 참조하십시오Amazon WorkMail 자격 증명 및 액세스 문제 해결.

서비스 관리자 — 회사에서 Amazon WorkMail 리소스를 담당하는 경우 Amazon에 대한 전체 액세스 권한이 있을 것입니다 WorkMail. 서비스 사용자가 액세스해야 하는 Amazon WorkMail 기능 및 리소스를 결정하는 것은 귀하의 몫입니다. 그런 다음 IAM 관리자에게 서비스 사용자의 권한을 변경해 달라는 요청을 제출해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 IAM 이해하십시오. 회사에서 Amazon을 사용하는 방법에 대해 자세히 WorkMail 알아보려면 IAM 을 참조하십시오아마존은 어떻게 WorkMail 협력하나요? IAM .

IAM관리자 — IAM 관리자인 경우 Amazon에 대한 액세스를 관리하는 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다 WorkMail. 에서 IAM 사용할 수 있는 Amazon WorkMail ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkMail 자격 증명 기반 정책 예제

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM사용자로서 또는 역할을 위임하여 인증 (로그인 AWS) 을 받아야 합니다. AWS 계정 루트 사용자 IAM

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAMID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인하는 경우 관리자는 이전에 역할을 사용하여 ID 페더레이션을 설정했습니다. IAM 페더레이션을 AWS 사용하여 액세스하는 경우 간접적으로 역할을 수임하는 것입니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호로 서명할 수 있는 소프트웨어 개발 키트 (SDKCLI) 와 명령줄 인터페이스 () 가 AWS 제공됩니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 사용 IAM설명서의 AWS APIAWS 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 계정 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 AWS 것을 권장합니다. 자세한 내용은 사용 설명서의 다단계 인증 및 사용 AWS IAM Identity Center 설명서의 다단계 인증 사용 (MFA) 을 IAM 참조하십시오. AWS

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

IAM 사용자 및 그룹

IAM사용자란 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 ID입니다. AWS 계정 가능하면 암호 및 액세스 키와 같은 장기 자격 증명을 가진 IAM 사용자를 만드는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 특정 사용 사례에서 IAM 사용자의 장기 자격 증명이 필요한 경우에는 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 사용 설명서의 장기 자격 증명이 필요한 사용 사례에 대한 정기적인 액세스 키 IAM 교체를 참조하십시오.

IAM그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 이름을 지정한 IAMAdmins그룹을 만들고 해당 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세히 알아보려면 사용 설명서의 역할 대신 IAM 사용자를 만드는 시기를 참조하십시오. IAM

IAM역할

IAM역할은 특정 권한을 AWS 계정 가진 사용자 내의 ID입니다. IAM사용자와 비슷하지만 특정인과 관련이 있는 것은 아닙니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI or AWS API 작업을 호출하거나 사용자 지정을 사용하여 역할을 수임할 수 URL 있습니다. 역할 사용 방법에 대한 자세한 내용은 사용 IAM설명서의 IAM역할 사용을 참조하십시오.

IAM임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더

레이션을 위한 역할에 대한 자세한 내용은 IAM사용 설명서의 타사 ID 제공자를 위한 역할 생성을 참조하십시오. IAMIdentity Center를 사용하는 경우 권한 집합을 구성합니다. ID가 인증된 후 액세스할 수 있는 대상을 제어하기 위해 IAM Identity Center는 권한 집합을 역할의 상관 관계와 연결합니다. IAM 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할이 역할을 맡아 특정 작업에 대해 일시적으로 다른 권한을 부여받을 수 있습니다. IAM
- 계정 간 액세스 - IAM 역할을 사용하여 다른 계정의 사용자 (신뢰할 수 있는 사용자) 가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 교차 계정 리소스 액세스를 참조하십시오. IAM IAM
- 서비스 간 액세스 — 일부는 다른 기능을 AWS 서비스 사용합니다. AWS 서비스예를 들어, 서비스를 호출하면 해당 서비스가 Amazon에서 애플리케이션을 EC2 실행하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM 역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스
  - 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행 중인 애플리케이션 EC2 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS API 요청을 보내는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS CLI EC2인스턴스 내에 액세스 키를 저장하는 것보다 이 방법이 더 좋습니다. EC2인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 만들어야 합니다. 인스턴스 프로필에는 역할이 포함되며, 이를 통해 EC2 인스턴스에서 실행 중인 프로그램

이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 사용 설명서의 IAM역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 IAM 참조하십시오.

IAM역할을 사용할지 IAM 사용자를 사용할지 알아보려면 사용 설명서의 IAM 역할 생성 시기 (사용자 대신) 를 IAM참조하십시오.

정책을 사용한 액세스 관리

정책을 만들고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM사용 설명서의 JSON 정책 개요를 참조하십시오.

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

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

IAM정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 에서 역할 정보를 가져올 수 AWS API 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책과 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM사용 설명서의 관리형 정책과 인라인 정책 중 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

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

액세스 제어 목록 () ACLs

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

지원하는 서비스의 VPC 예로는 Amazon S3와 Amazon이 ACLs 있습니다. AWS WAF자세한 내용은 Amazon 심플 스토리지 서비스 개발자 안내서의 액세스 제어 목록 (ACL) 개요를 참조하십시오. ACLs

기타 정책 타입

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

- 권한 경계 - 권한 경계는 ID 기반 정책이 IAM 엔티티 (IAM사용자 또는 역할) 에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 사용 IAM설명서의 IAM 엔티티의 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCPs) - SCPs 조직 또는 OU (조직 구성 단위) 에 대한 최대 권한을 지정하는 JSON AWS Organizations정책입니다. AWS Organizations 기업이 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직의 모든 기능을 사용하도록 설정하면 일부 또는 모든 계정에 서비스 제어 정책 (SCPs) 을 적용할 수 있습니다. 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 SCP AWS 계정 루트 사용자제한합니다. Organizations 및 SCPs 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하십시오.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의

보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM사용 설명서의 세션 정책을 참조하십시오.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM사용 설명서의 정책 평가 로직을 참조하십시오.

아마존은 어떻게 WorkMail 협력하나요? IAM

IAM을 사용하여 WorkMail Amazon에 대한 액세스를 관리하려면 먼저 Amazon에서 사용할 수 있는 IAM 기능을 이해해야 WorkMail 합니다. Amazon WorkMail 및 기타 AWS 서비스가 어떻게 작동하는지 자세히 알아보려면 IAM사용 IAM 설명서에서 함께 작동하는AWS 서비스를 참조하십시오. IAM

주제

- Amazon WorkMail 자격 증명 기반 정책
- 아마존 WorkMail 리소스 기반 정책
- Amazon WorkMail 태그를 기반으로 한 인증
- 아마존 WorkMail IAM 역할

Amazon WorkMail 자격 증명 기반 정책

IAMID 기반 정책을 사용하면 허용 또는 거부된 작업 및 리소스는 물론 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. WorkMail Amazon은 특정 작업, 리소스 및 조건 키를 지원합니다. JSON정책에서 사용하는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAMJSON정책 요소 참조를 참조하십시오.

작업

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

정책 `Action` 요소는 JSON 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. API 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

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

Amazon의 정책 조치는 조치 앞에 다음 접두사를 WorkMail 사용합니다. `workmail:` 예를 들어 Amazon WorkMail `ListUsers` API 운영 사용자 목록을 검색할 권한을 누군가에게 부여하려면 해당 사용자의 정책에 `workmail:ListUsers` 작업을 포함해야 합니다. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Amazon은 이 서비스로 수행할 수 있는 작업을 설명하는 자체 작업 세트를 WorkMail 정의합니다.

명령문 하나에 여러 태스크를 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "workmail:ListUsers",
      "workmail:DeleteUser"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `List`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "workmail:List*"
```

Amazon WorkMail 작업 목록을 보려면 IAM사용 설명서의 WorkMailAmazon에서 정의한 작업을 참조하십시오.

리소스

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

`Resource`JSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. Amazon 리소스 이름 (ARN) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

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

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

WorkMail Amazon은 Amazon 조직에 대한 리소스 수준 권한을 지원합니다. WorkMail

Amazon WorkMail 조직 리소스에는 ARN 다음이 포함됩니다.

```
arn:aws:workmail:${Region}:${Account}:organization/${OrganizationId}
```

형식에 대한 자세한 내용은 Amazon 리소스 이름 (ARNs) 및 AWS 서비스 네임스페이스를 참조하십시오. ARNs

예를 들어 명세서에 m-n1pq2345678r901st2u3vx45x6789yza 조직을 지정하려면 다음을 사용하십시오. ARN

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza"
```

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

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/*"
```

리소스 생성 작업과 같은 일부 Amazon WorkMail 작업은 특정 리소스에서 수행할 수 없습니다. 이러한 경우, 와일드카드(*)를 사용해야 합니다.

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

Amazon WorkMail 리소스 유형 및 해당 ARNs 유형의 목록을 보려면 IAM사용 설명서의 WorkMailAmazon에서 정의한 리소스를 참조하십시오. 각 리소스에 지정할 수 있는 작업을 알아보려면 ARN Amazon의 작업, 리소스 및 조건 키를 참조하십시오 WorkMail.

조건 키

Amazon은 다음과 같은 글로벌 조건 키를 WorkMail 지원합니다.

- aws:CurrentTime
- aws:EpochTime
- aws:MultiFactorAuthAge
- aws:MultiFactorAuthPresent
- aws:PrincipalOrgID
- aws:PrincipalArn
- aws:RequestedRegion
- aws:SecureTransport

- `aws:UserAgent`

다음 예제 정책은 해당 지역의 MFA 인증된 IAM 보안 주체에게만 Amazon WorkMail 콘솔에 대한 액세스 권한을 부여합니다. `eu-west-1` AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:Describe*",
                "ses:Get*",
                "workmail:Describe*",
                "workmail:Get*",
                "workmail:List*",
                "workmail:Search*",
                "lambda:ListFunctions",
                "iam:ListRoles",
                "logs:DescribeLogGroups",
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "Bool": {
                    "aws:MultiFactorAuthPresent": true
                }
            }
        }
    ]
}
```

모든 AWS 글로벌 조건 키를 보려면 사용 설명서의 AWS 글로벌 조건 컨텍스트 키를 참조하십시오. IAM

`workmail:ImpersonationRoleId`Amazon에서 지원하는 유일한 서비스별 조건 키입니다. WorkMail

다음 예제 정책은 특정 WorkMail 조직 및 사칭 역할로 AssumeImpersonationRole 작업 범위를 축소합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workmail:AssumeImpersonationRole"
      ],
      "Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza",
      "Condition": {
        "StringEquals": {
          "workmail:ImpersonationRoleId":"12345678-1234-1234-1234-123456789012"
        }
      }
    }
  ]
}
```

예시

Amazon WorkMail ID 기반 정책의 예를 보려면 을 참조하십시오. Amazon WorkMail 자격 증명 기반 정책 예제

아마존 WorkMail 리소스 기반 정책

WorkMail Amazon은 리소스 기반 정책을 지원하지 않습니다.

Amazon WorkMail 태그를 기반으로 한 인증

Amazon WorkMail 리소스에 태그를 첨부하거나 Amazon에 요청하여 태그를 전달할 수 WorkMail 있습니다. 태그에 근거하여 액세스를 제어하려면 aws:ResourceTag/key-name, aws:RequestTag/key-name 또는 aws:TagKeys 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다. Amazon WorkMail 리소스 태깅에 대한 자세한 내용은 을 참조하십시오조직 태깅.

아마존 WorkMail IAM 역할

IAM역할은 AWS 계정 내에서 특정 권한을 가진 엔티티입니다.

Amazon에서 임시 자격 증명 사용 WorkMail

임시 자격 증명을 사용하여 페더레이션으로 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole또는 GetFederationToken와 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻을 수 있습니다.

WorkMail Amazon은 임시 자격 증명 사용을 지원합니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 표시되며 서비스에서 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

WorkMail Amazon은 서비스 연결 역할을 지원합니다. Amazon WorkMail 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. Amazon WorkMail에 대해 서비스 연결 역할 사용

서비스 역할

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 계정에 표시되며 해당 IAM 계정에서 소유합니다. 즉, IAM 관리자는 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

WorkMail Amazon은 서비스 역할을 지원합니다.

Amazon WorkMail 자격 증명 기반 정책 예제

기본적으로 IAM 사용자와 역할에는 Amazon WorkMail 리소스를 만들거나 수정할 권한이 없습니다. 또한 AWS Management Console AWS CLI, 또는 를 사용하여 작업을 수행할 수 없습니다 AWS API. IAM 관리자는 필요한 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자 및 역할에 부여하는 IAM 정책을 만들어야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 해당 정책을 연결해야 합니다.

이 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 만드는 방법을 알아보려면 사용 IAM설명서의 JSON 탭에서 정책 만들기를 참조하십시오.

주제

- 정책 모범 사례

- 아마존 WorkMail 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 사용자에게 Amazon WorkMail 리소스에 대한 읽기 전용 액세스 허용

정책 모범 사례

ID 기반 정책은 누군가가 사용자 계정에서 Amazon WorkMail 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하십시오. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 내용은 IAM사용 설명서의 AWS 관리형 정책 또는 작업 기능에 대한AWS 관리형 정책을 참조하십시오.
- 최소 권한 적용 — IAM 정책으로 권한을 설정하는 경우 작업 수행에 필요한 권한만 부여하십시오. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 IAM 적용하는 방법에 대한 자세한 내용은 사용 설명서의 정책 및 권한을 참조하십시오. IAM IAM
- IAM정책의 조건을 사용하여 액세스를 추가로 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 를 사용하여 모든 요청을 전송하도록 지정하는 정책 조건을 작성할 수 SSL 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 내용은 IAM사용 설명서의 IAMJSON정책 요소: 조건을 참조하십시오.
- IAMAccess Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 새 정책과 기존 정책을 검증하여 정책이 IAM 정책 언어 (JSON) 및 IAM 모범 사례를 준수하는지 확인합니다. IAMAccess Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 IAMAccess Analyzer 정책 검증을 참조하십시오. IAM
- 다단계 인증 필요 (MFA) - 사용자 또는 루트 IAM 사용자가 필요한 시나리오가 있는 경우 보안을 강화하려면 이 기능을 MFA 켜십시오. AWS 계정 API작업 호출 MFA 시기를 요구하려면 정책에 MFA 조건을 추가하세요. 자세한 내용은 IAM사용 설명서의 MFA -보호된 API 액세스 구성을 참조하십시오.

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 보안 모범 사례를 참조하십시오. IAM

아마존 WorkMail 콘솔 사용

Amazon WorkMail 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 AWS 계정의 Amazon WorkMail 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. 필요한 최소 권한보다 더 제한적인 ID 기반 정책을 생성하면 해당 정책을 사용하는 엔티티 (IAM사용자 또는 역할) 에 대해 콘솔이 의도한 대로 작동하지 않습니다.

이러한 엔티티가 Amazon WorkMail 콘솔을 계속 사용할 수 있도록 하려면 다음 AWS 관리형 정책도 엔티티에 연결하십시오. AmazonWorkMailFullAccess 자세한 내용은 사용 설명서의 IAM사용자에게 권한 추가를 참조하십시오.

이 AmazonWorkMailFullAccess정책은 IAM 사용자에게 Amazon WorkMail 리소스에 대한 전체 액세스 권한을 부여합니다. 이 정책을 통해 사용자는 모든 Amazon WorkMail AWS Key Management Service, Amazon 심플 이메일 서비스 및 AWS Directory Service 운영에 액세스할 수 있습니다. 여기에는 Amazon이 귀하를 대신하여 WorkMail 수행해야 하는 여러 Amazon EC2 작업도 포함됩니다. `logs`및 `cloudwatch` 권한은 Amazon WorkMail 콘솔에서 이메일 이벤트 로깅 및 지표 보기에 필요합니다. 감사 로깅은 CloudWatch 로그, Amazon S3 및 Amazon 데이터를 FireHose 사용하여 저장합니다`logs`. 자세한 내용은 아마존에서의 로깅 및 모니터링 WorkMail 단원을 참조하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailAdministration",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
```

```
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DeleteDeliveryDestination",
        "logs:DeleteDeliveryDestinationPolicy",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliveryDestinationPolicy",
        "logs:CreateDelivery",
        "logs:DeleteDelivery",
        "logs:DescribeDeliveries",
        "logs:GetDelivery",
        "logs:DeleteDeliverySource",
        "logs:DescribeDeliverySources",
        "logs:GetDeliverySource",
        "logs:PutDeliverySource",
        "logs:DescribeResourcePolicies",
        "cloudwatch:GetMetricData",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
```

```
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
        "Sid": "AuditLogDeliveryThroughCWLogs",
        "Effect": "Allow",
        "Action": [
            "firehose:TagDeliveryStream",
            "logs:PutResourcePolicy",
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:CalledViaLast": "logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "events.workmail.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AuditLoggingLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "delivery.logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsUnlink",
```

```
        "Effect": "Allow",
        "Action": [
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/
events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
        "Sid": "InboundOutboundEmailEventsAuth",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::*:role/*workmail*",
        "Condition": {
            "StringLike": {
                "iam:PassedToService": "events.workmail.amazonaws.com"
            }
        }
    }
  ]
}
```

AWS CLI 또는 에만 전화를 거는 사용자에게 최소 콘솔 권한을 허용할 필요는 AWS API 없습니다. 대신 수행하려는 작업과 일치하는 API 작업에만 액세스를 허용하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 하는 정책을 만드는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 OR를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS API

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

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

사용자에게 Amazon WorkMail 리소스에 대한 읽기 전용 액세스 허용

다음 정책 설명은 IAM 사용자에게 Amazon WorkMail 리소스에 대한 읽기 전용 액세스 권한을 부여합니다. 이 정책은 AWS 관리형 AmazonWorkMailReadOnlyAccess정책과 동일한 수준의 액세스를 제공합니다. 어떤 정책이든 사용자에게 모든 Amazon WorkMail `Describe` 작업에 대한 액세스 권한을 부여합니다. AWS Directory Service 디렉터리에 대한 정보를 얻으려면 AWS Directory Service `DescribeDirectories` 작업에 액세스해야 합니다. 구성된 도메인에 대한 정보를 얻으려면 Amazon SES 서비스에 액세스해야 합니다. 사용된 암호화 키에 대한 정보를 얻으려면 에 대한 AWS Key Management Service 액세스가 필요합니다. `logs`및 `cloudwatch` 권한은 Amazon WorkMail 콘솔에서 이메일 이벤트 로깅 및 지표 보기에 필요합니다. 감사 로깅은 CloudWatch 로그, Amazon S3 및 Amazon 데이터를 FireHose 사용하여 저장합니다`logs`. 자세한 내용은 아마존에서의 로깅 및 모니터링 WorkMail 단원을 참조하십시오.

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

```
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliverySources",
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon WorkMail 자격 증명 및 액세스 문제 해결

다음 정보를 사용하면 Amazon 및 에서 작업할 때 발생할 수 있는 일반적인 문제를 WorkMail 진단하고 해결하는 데 도움이 IAM 됩니다.

주제

- Amazon에서 작업을 수행할 권한이 없습니다. WorkMail
- 저는 iam을 수행할 권한이 없습니다. PassRole
- 내 AWS 계정 외부의 사용자가 내 Amazon WorkMail 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Amazon에서 작업을 수행할 권한이 없습니다. WorkMail

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 그룹에 대한 세부 정보를 보려고 하지만 workmail:DescribeGroup 권한이 없는 경우 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workmail:DescribeGroup on resource: group
```

이 경우 Mateo는 group 작업을 사용하여 workmail:DescribeGroup 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 iam을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류 메시지가 표시되는 경우 Amazon에 역할을 넘길 수 있도록 정책을 업데이트해야 WorkMail 합니다. iam:PassRole

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 Amazon에서 콘솔을 사용하여 작업을 marymajor 수행하려고 할 때 발생합니다 WorkMail. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하십시오. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사용자가 내 Amazon WorkMail 리소스에 액세스할 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록 (ACLs) 을 지원하는 서비스의 경우 해당 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Amazon에서 이러한 기능을 WorkMail 지원하는지 알아보려면 을 참조하십시오아마존은 어떻게 WorkMail 협력하나요? IAM .

- 소유하고 AWS 계정 있는 모든 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 사용 설명서의 다른 IAM AWS 계정 사용자에게 액세스 권한 제공을 IAM 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM사용 설명서의 제3자가 AWS 계정 소유한 리소스에 대한 액세스 제공을 참조하십시오. AWS 계정
- ID 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에게 액세스 제공 (ID 페더레이션) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM IAM

AWS 아마존 관리형 정책 WorkMail

사용자, 그룹 및 역할에 권한을 추가하려면 정책을 직접 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의AWS 관리형 정책을 참조하십시오.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 타입의 업데이트는 정책이 연결된 모든 보안 인증(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어, ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonWorkMailFullAccess

`AmazonWorkMailFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다. 이 정책은 Amazon에 대한 전체 액세스를 허용하는 권한을 WorkMail 부여합니다.

이 정책에 대한 권한을 보려면 AmazonWorkMailFullAccess을 참조하십시오 AWS Management Console.

AWS 관리형 정책: AmazonWorkMailReadOnlyAccess

`AmazonWorkMailReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다. 이 정책은 WorkMail Amazon에 대한 읽기 전용 액세스를 허용하는 권한을 부여합니다.

이 정책에 대한 권한을 보려면 AmazonWorkMailReadOnlyAccess을 AWS Management Console참조하십시오.

AWS 관리형 정책: AmazonWorkMailEventsServiceRolePolicy

이 정책은 Amazon WorkMail 이벤트에서 사용하거나 관리하는 서비스 및 리소스에 대한 액세스를 AmazonWorkMailEvents허용하도록 이름이 지정된 AWS 서비스 연결 역할에 연결됩니다. 자세한 정보는 Amazon WorkMail에 대해 서비스 연결 역할 사용을 참조하세요.

Amazon, AWS 관리형 정책 WorkMail 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 WorkMail 이후 Amazon의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오.

변경 사항	설명	날짜
AWS 관리형 정책 업데이트 — 기존 정책 업데이트	`AmazonWorkMailReadOnlyAccess` 및 `AmazonWorkMailFullAccess` 권한이 Amazon에서 감사 WorkMail 로깅을 지원하도록 업데이트되었습니다. 업데이트된 권한에 대한 자세한 내용은 을 참조하십시오Amazon WorkMail 자격 증명 기반 정책 예제. 감사 로깅에 대한 자세한 내용은 을 참조하십시오감사 로깅 활성화.	2024년 2월 14일
Amazon은 변경 사항 추적을 WorkMail 시작했습니다	Amazon은 AWS 관리형 정책의 변경 사항을 추적하기 WorkMail 시작했습니다.	2021년 3월 1일

Amazon WorkMail에 대해 서비스 연결 역할 사용

Amazon WorkMail은 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Amazon WorkMail에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Amazon WorkMail에서 사전 정의하며, 서비스에서 다른 AWS 서비스를 자동으로 호출하기 위해 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할로 Amazon WorkMail을 더 쉽게 설정할 수 있습니다. Amazon WorkMail에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Amazon WorkMail만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 삭제할 수 없기 때문에 Amazon WorkMail 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [예(Yes)] 링크를 선택합니다.

Amazon WorkMail에 대한 서비스 연결 역할 권한

Amazon WorkMail은 AmazonWorkMailEvents라는 서비스 연결 역할을 사용합니다. Amazon WorkMail은 이 서비스 연결 역할을 사용하여 CloudWatch에서 로깅한 이메일 이벤트 모니터링과 같이 Amazon WorkMail 이벤트에서 사용하거나 관리하는 AWS 서비스 및 리소스에 액세스할 수 있도록 합니다. Amazon WorkMail의 이메일 이벤트 로깅 활성화에 대한 자세한 내용은 이메일 이벤트 로깅 활성화 부분을 참조하세요.

AmazonWorkMailEvents 서비스 연결 역할은 역할을 위임하기 위해 다음 서비스를 신뢰합니다.

- `events.workmail.amazonaws.com`

역할 권한 정책은 Amazon WorkMail이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: `all AWS resources`에 대한 `logs:CreateLogGroup`
- 작업: `all AWS resources`에 대한 `logs:CreateLogStream`
- 작업: `all AWS resources`에 대한 `logs:PutLogEvents`

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Amazon WorkMail에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. Amazon WorkMail 이벤트 로깅을 활성화하고 Amazon WorkMail 콘솔의 기본 설정을 사용하면 Amazon WorkMail은 서비스 연결 역할을 자동으로 생성합니다.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. Amazon WorkMail 이벤트 로깅을 활성화하고 기본 설정을 사용하면 Amazon WorkMail은 사용자를 위해 서비스 연결 역할을 다시 생성합니다.

Amazon WorkMail에 대한 서비스 연결 역할 편집

Amazon WorkMail에서는 AmazonWorkMailEvents 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Amazon WorkMail에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 개체가 없도록 합니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 Amazon WorkMail 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AmazonWorkMailEvents에서 사용하는 Amazon WorkMail 리소스를 삭제하려면

1. Amazon WorkMail 이벤트 로깅을 끕니다.
    a. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.

b. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.

c. 탐색 창에서 조직 설정, 모니터링을 선택합니다.

d. Log settings(로그 설정)에서 편집을 선택합니다.

e. 메일 이벤트 활성화 슬라이더를 꺼짐 위치로 이동합니다.

f. Save를 선택합니다.

2. Amazon CloudWatch 로그 그룹을 삭제합니다.

a. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.

b. [Logs]를 선택합니다.

c. 로그 그룹에서 삭제할 로그 그룹을 선택합니다.

d. 작업에서 로그 그룹 삭제를 선택합니다.

e. 예, 삭제를 선택합니다.

IAM을 사용하여 수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AmazonWorkMailEvents 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제를 참조하세요.

Amazon WorkMail 서비스 연결 역할이 지원되는 리전

Amazon WorkMail은 서비스가 제공되는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 Amazon WorkMail 리전 및 엔드포인트를 참조하세요.

아마존에서의 로깅 및 모니터링 WorkMail

이메일과 로그를 모니터링하고 감사하는 것은 Amazon WorkMail 조직의 상태를 유지하는 데 중요합니다. WorkMail Amazon은 두 가지 유형의 모니터링을 지원합니다.

- 이벤트 로깅 — 조직의 이메일 전송 활동을 모니터링하면 도메인 평판을 보호하는 데 도움이 됩니다. 모니터링은 주고 받는 이메일을 추적하는 데도 도움이 됩니다. 이메일 이벤트 로깅을 활성화하는 방법에 대한 자세한 내용은 이메일 이벤트 로깅 활성화 단원을 참조하십시오.

- 감사 로깅 — 감사 로그를 사용하여 사서함에 대한 사용자 액세스 모니터링, 의심스러운 활동 감사, 액세스 제어 및 가용성 공급자 구성 디버깅 등 Amazon WorkMail 조직 사용에 대한 자세한 정보를 캡처할 수 있습니다. 자세한 정보는 감사 로깅 활성화을 참조하세요.

AWS 는 Amazon을 감시하고, 문제 발생 시 보고하고 WorkMail, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. 예를 들어 WorkMail Amazon에 대한 이메일 이벤트 로깅을 활성화하면 조직에서 보내고 받은 이메일을 CloudWatch 추적할 수 있습니다. 를 WorkMail 사용하여 Amazon을 모니터링하는 방법에 대한 자세한 내용은 을 CloudWatch 참조하십시오 CloudWatch 지표를 WorkMail 통한 Amazon 모니터링. 에 대한 CloudWatch 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.
- Amazon CloudWatch Logs를 사용하면 Amazon WorkMail 콘솔에서 이메일 및 감사 로깅이 활성화된 경우 WorkMail Amazon의 이메일 이벤트 및 감사 로그를 모니터링, 저장 및 액세스할 수 있습니다. CloudWatch 로그는 로그 파일의 정보를 모니터링할 수 있으며 내구성이 뛰어난 스토리지에 로그 데이터를 보관할 수 있습니다. CloudWatch 로그를 사용하여 Amazon WorkMail 메시지를 추적하는 방법에 대한 자세한 내용은 이메일 이벤트 로깅 활성화 및 을 참조하십시오감사 로깅 활성화. CloudWatch Logs에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.
- AWS CloudTrail사용자가 AWS 계정또는 사용자를 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 정보는 를 WorkMail 사용하여 Amazon API 호출을 로깅합니다. AWS CloudTrail을 참조하세요.
- Amazon S3를 사용하면 비용 효율적인 방식으로 Amazon WorkMail 이벤트를 저장하고 액세스할 수 있습니다. Amazon S3는 이벤트 데이터 수명 주기를 관리하는 메커니즘을 제공하므로 이전 이벤트의 자동 삭제를 구성하거나 Amazon S3 Glacier에 자동 보관을 구성할 수 있습니다. 참고: Amazon S3 전송은 감사 로깅 이벤트에만 사용할 수 있습니다. Amazon S3에 관한 자세한 내용은 Amazon S3 사용 설명서를 참조하세요.
- Amazon Data Firehose를 사용하면 Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service, OpenSearch Amazon Serverless, Splunk와 같은 다른 AWS 서비스와 Datadog, LogicMonitor Dynatrace, MongoDB, New Relic, Coralodb 등 지원되는 타사 서비스 공급자가 소유한 모든 사용자 지정 HTTP 엔드포인트 또는 HTTP 엔드포인트로 이벤트 데이터를 스트리밍할 수 있습니다. 글릭스, 엘라스틱. OpenSearch Firehose로의 전송은 감사 로깅 이벤트에만 사용할 수 있습니다. Firehose에 대한 자세한 내용은 Amazon Data Firehose 개발자 안내서를 참조하십시오.

주제

CloudWatch 지표를 WorkMail 통한 Amazon 모니터링

원시 데이터를 수집하여 읽을 수 있는 거의 실시간 지표로 처리하는 를 WorkMail 사용하여 CloudWatch Amazon을 모니터링할 수 있습니다. 무료 지표는 15개월 동안 저장되므로 과거 정보에 액세스하여 웹 애플리케이션 또는 서비스의 성능을 확인할 수 있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

CloudWatch 아마존용 메트릭스 WorkMail

Amazon은 다음 지표 및 차원 정보를 에 WorkMail CloudWatch 전송합니다.

`AWS/WorkMail` 네임스페이스에 포함된 지표는 다음과 같습니다.

지표	설명
`OrganizationEmailReceived`	Amazon WorkMail 조직에서 수신한 이메일의 수입니다. 조직 내 수신자 10명에게 이메일 1개를 보내는 경우 `OrganizationEmailReceived` 개수는 1입니다. 단위: 개
`MailboxEmailDelivered`	Amazon WorkMail 조직의 개별 사서함으로 전송된 이메일의 수입니다. 조직 내 10명의 수신자에게 이메일 1개가 성공적으로 전송된 경우 `MailboxEmailDelivered` 개수는 10개입니다.

지표	설명
	단위: 개
IncomingEmailBounced	사서함이 가득 차서 반송된 이메일 수입니다. 이 지표는 각 대상 수신자에 대해 계산됩니다. 예를 들어 조직의 수신자 10명에게 전자 메일 하나를 보내고 받는 사람 중 두 명의 사서함이 꽉 차서 반송 응답이 발생한 경우 개수는 2입니다. IncomingEmailBounced 단위: 개
OutgoingEmailBounced	발신 이메일 중 전달되지 못한 이메일 수입니다. 이 지표는 각 대상 수신자에 대해 계산됩니다. 예를 들어 10명의 수신자에게 이메일 1개가 전송되고 두 개의 이메일이 전달되지 못한 경우 OutgoingEmailBounced 개수는 2입니다. 단위: 개
OutgoingEmailSent	Amazon WorkMail 조직에서 성공적으로 보낸 이메일의 수입니다. 이 지표는 성공적으로 보낸 이메일의 각 수신자에 대해 계산됩니다. 예를 들어, 수신자 10명에게 이메일 1개를 보냈는데, 이 중 8명에게 이메일이 성공적으로 배달된 경우 OutgoingEmailSent 개수는 8입니다. 단위: 개

지표	설명
AuthenticationFailure	이 지표는 인증 시도 횟수를 계산합니다. 인증에 성공하면 개수는 0이고 인증에 실패하면 개수는 1입니다. Sum통계를 사용하여 실패한 인증 시도 횟수를 모니터링할 수 있습니다. Sample count통계를 사용하여 총 인증 이벤트 수를 모니터링할 수 있습니다. Average통계를 사용하여 실패한 인증 이벤트와 성공한 인증 이벤트의 비율을 모니터링할 수 있습니다. 단위: 개
AccessDenied	이 지표는 액세스 제어 평가 횟수를 계산합니다. 액세스 제어에 의해 작업이 거부된 경우 개수는 1이고, 작업이 허용되면 개수는 0입니다. Sum통계를 사용하여 거부된 작업의 양을 모니터링하고, Sample count 통계를 사용하여 시도된 총 작업 수를 모니터링하며, 통계를 사용하여 허용된 Average 작업과 거부된 작업의 비율을 모니터링할 수 있습니다. 단위: 개
ActionDenied	이 지표는 사서함 데이터에 대한 작업이 있을 때 계산됩니다. 작업이 거부된 경우 개수는 1이고 작업이 허용된 경우 개수는 0입니다. Sum통계를 사용하여 거부된 사서함 작업의 양을 모니터링하고, Sample count 통계를 사용하여 시도된 사서함 작업의 총 수를 모니터링하며, Average 통계를 사용하여 허용된 작업과 거부된 작업의 비율을 모니터링할 수 있습니다. 단위: 개

지표	설명
`AvailabilityProviderFailure`	이 지표는 Amazon이 외부 소스에서 캘린더 가용성을 검색하기 위해 WorkMail 실행하는 모든 가용성 공급자 요청에 대해 계산됩니다. 가용성 공급자에 대한 자세한 내용은 Amazon WorkMail 관리자 안내서를 참조하십시오.

Amazon WorkMail 이메일 이벤트 로그 모니터링

Amazon WorkMail 조직에 대한 이메일 이벤트 로깅을 활성화하면 Amazon은 을 사용하여 이메일 이벤트를 WorkMail CloudWatch 로깅합니다. 이메일 이벤트 로깅 켜기에 대한 자세한 내용은 이메일 이벤트 로깅 활성화 단원을 참조하십시오.

다음 표는 Amazon이 WorkMail 기록하는 이벤트 CloudWatch, 이벤트가 전송되는 시기, 이벤트 필드에 포함된 내용을 설명합니다.

`ORGANIZATION_EMAIL_RECEIVED`

이 이벤트는 Amazon WorkMail 조직이 이메일 메시지를 수신할 때 기록됩니다.

필드	설명
recipients	메시지의 대상 수신자입니다.
sender	다른 사용자를 대신하여 이메일 메시지를 전송한 사용자의 이메일 주소입니다. 이 필드는 다른 사용자를 대신하여 이메일을 전송할 때만 설정됩니다.
from	보낸 사람 주소이며, 일반적으로 메시지를 보낸 사용자의 이메일 주소로 지정됩니다. 사용자가 다른 사용자로 또는 다른 사용자를 대신하여 메시지를 전송한 경우 이 필드는 실제 발신자의 이메일 주소가 아니라 이메일을 대신 전송한 사용자의 이메일 주소를 반환합니다.
subject	이메일 메시지의 제목입니다.

필드	설명
messageId	SMTP 메시지 ID입니다.
spamVerdict	메시지가 Amazon SES에 의해 스팸으로 표시되었는지 여부를 나타냅니다. 자세한 정보는 Amazon Simple Email Service 개발자 안내서의 Amazon SES 이메일 수신에 대한 알림 콘텐츠를 참조하세요.
dkimVerdict	DomainKeys 식별 메일 (DKIM) 검사의 통과 여부를 나타냅니다. 자세한 정보는 Amazon Simple Email Service 개발자 안내서의 Amazon SES 이메일 수신에 대한 알림 콘텐츠를 참조하세요.
dmarcVerdict	도메인 기반 메시지 인증, 보고 및 준수 (DMARC) 검사의 통과 여부를 나타냅니다. 자세한 정보는 Amazon Simple Email Service 개발자 안내서의 Amazon SES 이메일 수신에 대한 알림 콘텐츠를 참조하세요.
dmarcPolicy	dmarcVerdict 필드에 "FAIL"이 포함된 경우에만 나타납니다. DMARC Check가 실패할 경우 이메일에 대해 취할 조치를 나타냅니다(없음, 격리 또는 거부). 이는 이메일 전송 도메인의 소유자에 의해 설정됩니다.
spfVerdict	발신자 정책 프레임워크 (SPF) 검사의 통과 여부를 나타냅니다. 자세한 정보는 Amazon Simple Email Service 개발자 안내서의 Amazon SES 이메일 수신에 대한 알림 콘텐츠를 참조하세요.
messageTimestamp	메시지가 수신된 시간을 나타냅니다.

`MAILBOX_EMAIL_DELIVERED`

이 이벤트는 조직의 사서함에 메시지가 배달될 때 기록됩니다. 이 메시지는 메시지가 배달되는 각 사서함에 대해 한 번 기록되므로 단일 ORGANIZATION_EMAIL_RECEIVED 이벤트로 인해 여러 MAILBOX_EMAIL_DELIVERED 이벤트가 발생할 수 있습니다.

필드	설명
수신자	메시지가 배달될 사서함입니다.
folder	메시지가 있는 사서함 폴더입니다.

RULE_APPLIED

이 이벤트는 수신 또는 발신 메시지가 이메일 흐름 규칙을 시작할 때 기록됩니다.

필드	설명
ruleName	규칙의 이름입니다.
ruleType	적용된 규칙 유형 (인바운드_규칙, 아웃바운드_규칙 또는 MAILBOX_RULE). 인바운드 및 아웃바운드 규칙은 Amazon WorkMail 조직에 적용됩니다. 사서함 규칙은 지정된 사서함에만 적용됩니다. 자세한 정보는 이메일 흐름 관리을 참조하세요.
ruleActions	규칙에 따라 수행된 작업입니다. 메시지 수신자마다 이메일 반송 또는 이메일 배달 성공과 같은 다양한 작업이 있을 수 있습니다.
targetFolder	Move 또는 Copy MAILBOX_RUL에 의도된 대상 폴더입니다.
targetRecipient	Forward 또는 Redirect MAILBOX_RULE에 의도된 수신인입니다.

JOURNALING_INITIATED

이 이벤트는 Amazon이 조직 관리자가 지정한 저널링 주소로 이메일을 WorkMail 보낼 때 기록됩니다. 조직에 저널링이 구성된 경우에만 전송됩니다. 자세한 정보는 Amazon WorkMail을 통해 이메일 저널링 사용을 참조하세요.

필드	설명
journalingAddress	저널링 메시지를 보낼 이메일 주소입니다.

INCOMING_EMAIL_BOUNCED

수신 메시지를 대상 수신자에게 배달할 수 없는 경우 이 이벤트가 기록됩니다. 대상 사서함이 꽉 찬 경우 등 여러 가지 이유로 이메일이 반송될 수 있습니다. 시스템은 이메일이 반송된 각 수신자에 대해 이 이벤트를 한 번씩 기록합니다. 예를 들어, 수신 메시지가 3명의 수신자에게 배달되었는데 이 중 두 수신자의 사서함이 가득 찬 경우 두 개의 INCOMING_EMAIL_BOUNCED 이벤트가 기록됩니다.

필드	설명
bouncedRecipient	Amazon에서 메시지를 WorkMail 반송한 대상 수신자입니다.

OUTGOING_EMAIL_SUBMITTED

이 이벤트는 조직의 사용자가 보낼 이메일 메시지를 제출할 때 기록됩니다. 이는 메시지가 WorkMail Amazon에서 발송되기 전에 기록되므로 이 이벤트는 이메일이 성공적으로 전송되었는지 여부를 나타내지 않습니다.

필드	설명
recipients	발신자가 지정한 메시지 수신자입니다. 받는 사람, 참조 및 숨은 참조 행의 수신자가 모두 포함됩니다.
sender	다른 사용자를 대신하여 이메일 메시지를 전송한 사용자의 이메일 주소입니다. 이 필드는 다른 사용자를 대신하여 이메일을 전송할 때만 설정됩니다.

필드	설명
from	보낸 사람 주소이며, 일반적으로 메시지를 보낸 사용자의 이메일 주소로 지정됩니다. 사용자가 다른 사용자로 또는 다른 사용자를 대신하여 메시지를 전송한 경우 이 필드는 실제 발신자의 이메일 주소가 아니라 이메일을 대신 전송한 사용자의 이메일 주소를 반환합니다.
subject	이메일 메시지의 제목입니다.

OUTGOING_EMAIL_SENT

이 이벤트는 발신 이메일이 대상 수신자에게 성공적으로 배달될 때 기록됩니다. 배달이 성공한 수신자마다 한 번씩 기록되므로 단일 OUTGOING_EMAIL_SUBMITTED로 인해 여러 OUTGOING_EMAIL_SENT 항목이 발생할 수 있습니다.

필드	설명
수신자	성공적으로 배달된 이메일의 수신자입니다.
sender	다른 사용자를 대신하여 이메일 메시지를 전송한 사용자의 이메일 주소입니다. 이 필드는 다른 사용자를 대신하여 이메일을 전송할 때만 설정됩니다.
from	보낸 사람 주소이며, 일반적으로 메시지를 보낸 사용자의 이메일 주소로 지정됩니다. 사용자가 다른 사용자로 또는 다른 사용자를 대신하여 메시지를 전송한 경우 이 필드는 실제 발신자의 이메일 주소가 아니라 이메일을 대신 전송한 사용자의 이메일 주소를 반환합니다.
messageId	SMTP 메시지 ID입니다.

OUTGOING_EMAIL_BOUNCED

발신 메시지를 대상 수신자에게 전달할 수 없는 경우 이 이벤트가 기록됩니다. 대상 사서함이 꽉 찬 경우 등 여러 가지 이유로 이메일이 반송될 수 있습니다. 시스템은 이메일이 반송된 각 수신자에 대해 반송을 한 번씩 기록합니다. 예를 들어, 발신 메시지가 3명의 수신자에게 배달되었는데 이 중 두 수신자의 사서함이 가득 찬 경우 두 개의 `OUTGOING_EMAIL_BOUNCED` 이벤트가 기록됩니다.

필드	설명
bouncedRecipient	대상 메일 서버가 메시지를 반송한 대상 수신자입니다.

`DMARC_POLICY_APPLIED`

DMARC 정책이 조직에 전송되는 이메일에 적용되는 경우 이 이벤트가 기록됩니다.

필드	설명
from	보낸 사람 주소이며, 일반적으로 메시지를 보낸 사용자의 이메일 주소로 지정됩니다. 사용자가 다른 사용자로 또는 다른 사용자를 대신하여 메시지를 전송한 경우 이 필드는 실제 발신자의 이메일 주소가 아니라 이메일을 대신 전송한 사용자의 이메일 주소를 반환합니다.
recipients	메시지의 대상 수신자입니다.
정책	적용된 DMARC 정책, DMARC Check가 실패할 경우 이메일에 대해 취할 조치를 나타냄(없음, 격리 또는 거부). 이 필드는 ORGANIZATION_EMAIL_RECEIVED 이벤트의 dmarcPolicy 필드와 동일합니다.

Amazon WorkMail 감사 로그 모니터링

감사 로그를 사용하여 Amazon WorkMail Organization의 사서함에 대한 액세스를 모니터링할 수 있습니다. Amazon은 네 가지 유형의 감사 이벤트를 WorkMail 기록하며 이러한 이벤트는 CloudWatch 로그, Amazon S3 또는 Amazon Firehouse에 게시할 수 있습니다. 감사 로그를 사용하여 조직의 사서함과의 사용자 상호 작용, 인증 시도, 액세스 제어 규칙 평가를 모니터링하고 외부 시스템에 대한 가용성

공급자 호출을 수행할 수 있습니다. 감사 로깅 구성에 대한 자세한 내용은 을 참조하십시오감사 로깅 활성화.

다음 섹션에서는 Amazon에서 기록하는 감사 이벤트 WorkMail, 이벤트가 전송되는 시기 및 이벤트 필드에 대한 정보를 설명합니다.

메일박스 액세스 로그

사서함 액세스 이벤트는 어떤 사서함 개체에서 어떤 작업이 수행되었거나 시도되었는지에 대한 정보를 제공합니다. 사서함의 항목 또는 폴더에서 실행하려는 모든 작업에 대해 사서함 액세스 이벤트가 생성됩니다. 이러한 이벤트는 사서함 데이터에 대한 액세스를 감사하는 데 유용합니다.

필드	설명
event_timestamp	이벤트 발생 시점 (Unix Epoch) 이후 밀리초 단위.
request_id	요청을 고유하게 식별하는 ID.
조직_arn	인증된 사용자가 속한 및 Amazon WorkMail 조직의 ARN입니다.
user_id	인증된 사용자의 ID.
가장자_id	가장한 사람의 ID. 요청에 사칭 기능을 사용한 경우에만 제시하십시오.
프로토콜	사용된 프로토콜. 프로토콜은 다음과 같을 수 있습니다. `AutoDiscover` `EWSIMAP`,`WindowsOutlook` ,`ActiveSync` ,`SMTP`,`WebMail`,`IncomingEmail` , 또는`OutgoingEmail` .
소스_ip	요청의 소스 IP 주소.
user_agent	요청을 한 사용자 에이전트.
작업	개체에 대해 수행된 작업은 다음과 같습니다.`read`,,`read_hierarchy` ,`read_summary` ,`read_attachment` ,`read_perm`

필드	설명
	issions ,create,update,update_permissions , update_read_state delete,submit_email_for_sending ,abort_sending_email ,move,move_to,copy, 또는copy_to.
owner_id	작업 중인 객체를 소유한 사용자의 ID.
object_type	개체 유형은 폴더, 메시지 또는 첨부 파일일 수 있습니다.
item_id	이벤트 제목인 메시지를 고유하게 식별하거나 이벤트 제목인 첨부 파일을 포함하는 ID입니다.
폴더_경로	작업 중인 폴더의 경로 또는 작업 중인 항목이 들어 있는 폴더의 경로.
folder_id	이벤트 대상인 폴더를 고유하게 식별하거나 이벤트 대상인 객체를 포함하는 ID입니다.
첨부_경로	영향을 받는 첨부 파일의 디스플레이 이름 경로.
액션_허용	작업이 허용되었는지 여부. 참일 수도 있고 거짓일 수도 있습니다.

액세스 제어 로그

액세스 제어 규칙이 평가될 때마다 액세스 제어 이벤트가 생성됩니다. 이러한 로그는 금지된 액세스를 감사하거나 액세스 제어 구성을 디버깅하는 데 유용합니다.

필드	설명
event_timestamp	이벤트 발생 시점 (Unix Epoch) 이후 밀리초 단위
request_id	요청을 고유하게 식별하는 ID.

필드	설명
조직_arn	인증된 사용자가 WorkMail 속한 조직의 ARN입니다.
user_id	인증된 사용자의 ID.
가장자_id	가장한 사람의 ID. 요청에 사칭 기능을 사용한 경우에만 제시하십시오.
프로토콜	사용된 프로토콜은 다음과 같습니다.`AutoDiscover` ,,,`EWS`,`IMAP`,`WindowsOutlook` ,`ActiveSync` , `SMTP` `WebMailIncomingEmail` , 또는. `OutgoingEmail`
소스_ip	요청의 소스 IP 주소.
scope	규칙의 범위는 다음과 같을 수 있습니다. `AccessControl` `DeviceAccessControl` , 또는`ImpersonationAccessControl` .
rule_id	일치하는 액세스 제어 규칙의 ID. 일치하는 규칙이 없는 경우 rule_id를 사용할 수 없습니다.
액세스_그랜트	액세스가 허용되었는지 여부. 참일 수도 있고 거짓일 수도 있습니다.

인증 로그

인증 이벤트에는 인증 시도에 대한 정보가 포함됩니다.

> **Note**
>
> Amazon WorkMail WebMail 애플리케이션을 통한 인증 이벤트에 대해서는 인증 이벤트가 생성되지 않습니다.

필드	설명
event_timestamp	이벤트 발생 시점 (Unix Epoch) 이후 밀리초 단위.
request_id	요청을 고유하게 식별하는 ID.
조직_arn	인증된 사용자가 WorkMail 속한 조직의 ARN입니다.
user_id	인증된 사용자의 ID.
사용자	인증을 시도할 때 사용한 사용자 이름.
프로토콜	사용된 프로토콜은 다음과 같습니다.`AutoDiscover` ,,`EWS`,`IMAP`,`WindowsOutlook` , `ActiveSync` `SMTP`,`WebMail`,`IncomingEmail` , 또는`OutgoingEmail` .
소스_ip	요청의 소스 IP 주소.
user_agent	요청을 한 사용자 에이전트.
method	인증 방법. 현재는 기본만 지원됩니다.
인증 성공	인증 시도가 성공했는지 여부. 참일 수도 있고 거짓일 수도 있습니다.
인증 실패 사유	인증 실패 사유. 인증이 실패한 경우에만 표시됩니다.

가용성 제공자 로그

가용성 공급자 이벤트는 WorkMail Amazon이 사용자를 대신하여 구성된 가용성 공급자에게 보내는 모든 가용성 요청에 대해 생성됩니다. 이러한 이벤트는 가용성 공급자 구성을 디버깅하는 데 유용합니다.

필드	설명
event_timestamp	이벤트가 발생한 시점 (Unix Epoch) 이후 밀리초 단위.
request_id	요청을 고유하게 식별하는 ID.
조직_arn	인증된 사용자가 WorkMail 속한 조직의 ARN입니다.
user_id	인증된 사용자의 ID.
유형	호출되는 가용성 공급자의 유형은 다음과 EWS 같을 수 있습니다. 또는. LAMBDA
도메인	가용성이 확보된 도메인.
function_arn	호출된 람다의 ARN (유형이 LAMBDA인 경우) 그렇지 않으면 이 필드는 존재하지 않습니다.
ews_endpoint	EWS 엔드포인트의 유형은 EWS입니다. 그렇지 않으면 이 필드는 표시되지 않습니다.
error_message	실패 원인을 설명하는 메시지입니다. 요청이 성공한 경우 이 필드는 표시되지 않습니다.
가용성_이벤트_성공	가용성 요청이 성공적으로 처리되었는지 여부.

Amazon에서 CloudWatch 인사이트 사용하기 WorkMail

Amazon WorkMail 콘솔에서 이메일 이벤트 로깅을 활성화하거나 감사 로그를 Logs로 전송하도록 활성화한 경우, Amazon CloudWatch Logs Insights를 사용하여 이벤트 CloudWatch 로그를 쿼리할 수 있습니다. 이메일 이벤트 로깅 켜기에 대한 자세한 내용은 이메일 이벤트 로깅 활성화 단원을 참조하십시오. CloudWatch Logs Insights에 대한 자세한 내용은 Amazon Logs 사용 설명서의 CloudWatch Logs Insights를 사용한 CloudWatch 로그 데이터 분석을 참조하십시오.

다음 예는 CloudWatch 로그에서 일반적인 이메일 이벤트를 쿼리하는 방법을 보여줍니다. CloudWatch 콘솔에서 이러한 쿼리를 실행합니다. 이러한 쿼리를 실행하는 방법에 대한 지침은 Amazon CloudWatch Logs 사용 설명서의 자습서: 샘플 쿼리 실행 및 수정을 참조하십시오.

Example 사용자 A가 보낸 이메일을 사용자 B가 받지 못한 이유를 알아보십시오.

다음 코드 예제는 사용자 A가 사용자 B에게 보낸 이메일을 타임스탬프별로 정렬하여 쿼리하는 방법을 보여줍니다.

```
fields @timestamp, traceId

| sort @timestamp asc
| filter (event.from like /(?i)userA@example.com/
and event.eventName = "OUTGOING_EMAIL_SUBMITTED"
and event.recipients.0 like /(?i)userB@example.com/)
```

보낸 메시지와 추적 ID를 반환합니다. 다음 코드 예제의 추적 ID를 사용하여 보낸 메시지의 이벤트 로그를 쿼리합니다.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

그러면 이메일 메시지 ID와 이메일 이벤트가 반환됩니다. OUTGOING_EMAIL_SENT는 이메일을 보냈음을 나타내고, OUTGOING_EMAIL_BOUNCED는 이메일이 반송되었음을 나타냅니다. 이메일의 수신 여부를 확인하려면 다음 코드 예제에서 메시지 ID를 사용하여 쿼리합니다.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter event.messageId like "$MESSAGEID"
```

동일한 메시지 ID를 가지고 있으므로 수신된 메시지도 반환해야 합니다. 배달을 쿼리하려면 다음 코드 예제의 추적 ID를 사용합니다.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

그러면 배달 작업 및 적용 가능한 규칙 작업이 반환됩니다.

Example 사용자 또는 도메인으로부터 받은 모든 메일 보기

다음 코드 예제는 지정된 사용자에게 받은 모든 메일을 쿼리하는 방법을 보여줍니다.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like /(?i)user@example.com/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

다음 코드 예제는 지정된 도메인에서 받은 모든 메일을 쿼리하는 방법을 보여줍니다.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like "example.com" and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

Example 반송 이메일을 보낸 사람 보기

다음 코드 예제는 반송된 발신 이메일을 쿼리하는 방법을 보여주고 반송 이유도 반환합니다.

```
fields @timestamp, event.destination, event.reason
| sort @timestamp desc
| filter event.eventName = "OUTGOING_EMAIL_BOUNCED"
```

다음 코드 예제는 반송된 수신 이메일을 쿼리하는 방법을 보여줍니다. 또한 반송된 수신자의 이메일 주소와 반송 사유도 반환합니다.

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
| sort @timestamp desc
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example 어떤 도메인이 스팸을 보내고 있는지 확인하세요.

다음 코드 예제는 조직에서 스팸을 받은 수신자를 쿼리하는 방법을 보여줍니다.

```
stats count(*) as c by event.recipients.0
| filter (event.eventName = "ORGANIZATION_EMAIL_RECEIVED" and event.spamVerdict =
 "FAIL")
| sort c desc
```

다음 코드 예제는 스팸 이메일의 발신자를 쿼리하는 방법을 보여줍니다.

```
fields @timestamp, event.recipients.0, event.sender, event.from
| sort @timestamp asc
```

```
| filter (event.spamVerdict = "FAIL")
```

Example 이메일이 수신자의 스팸 폴더로 전송된 이유 보기

다음 코드 예제는 제목으로 필터링하여 스팸으로 식별된 이메일을 쿼리하는 방법을 보여줍니다.

```
fields @timestamp, event.recipients.0, event.spamVerdict, event.spfVerdict,
 event.dkimVerdict, event.dmarcVerdict
| sort @timestamp asc
| filter event.subject like /(?i)$SUBJECT/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED"
```

이메일 추적 ID로 쿼리하여 이메일의 모든 이벤트를 볼 수도 있습니다.

Example 이메일 흐름 규칙과 일치하는 이메일 보기

다음 코드 예제는 아웃바운드 이메일 흐름 규칙과 일치하는 이메일을 쿼리하는 방법을 보여줍니다.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action
| sort @timestamp desc
| filter event.ruleType = "OUTBOUND_RULE"
```

다음 코드 예제는 인바운드 이메일 흐름 규칙과 일치하는 이메일을 쿼리하는 방법을 보여줍니다.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action,
 event.ruleActions.0.recipients.0
| sort @timestamp desc
| filter event.ruleType = "INBOUND_RULE"
```

Example 조직에서 받거나 보낸 이메일의 수를 확인하세요.

다음 코드 예제는 조직의 각 수신자가 받은 이메일 수를 쿼리하는 방법을 보여줍니다.

```
stats count(*) as c by event.recipient
| filter event.eventName = "MAILBOX_EMAIL_DELIVERED"
| sort c desc
```

다음 코드 예제는 조직의 각 발신자가 보낸 이메일 수를 쿼리하는 방법을 보여줍니다.

```
stats count(*) as c by event.from
```

```
| filter event.eventName = "OUTGOING_EMAIL_SUBMITTED"
| sort c desc
```

를 WorkMail 사용하여 Amazon API 호출을 로깅합니다. AWS CloudTrail

WorkMail Amazon은 사용자 AWS CloudTrail, 역할 또는 Amazon 내에서 수행한 작업의 기록을 제공하는 서비스와 AWS 서비스 통합되어 WorkMail 있습니다. CloudTrail Amazon WorkMail 콘솔에서의 호출 및 Amazon API에 대한 코드 호출을 포함하여 Amazon에 대한 모든 API 호출을 WorkMail 이벤트로 캡처합니다. WorkMail 트레일을 생성하면 Amazon 이벤트를 포함하여 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 WorkMail 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Amazon에 요청한 내용 WorkMail, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

아마존 WorkMail 정보 CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. WorkMailAmazon에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 이벤트와 함께 AWS 서비스 이벤트에 기록됩니다. 내 사이트에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

Amazon WorkMail 이벤트를 포함하여 AWS 계정의 이벤트를 지속적으로 기록하려면 트레일을 생성해야 합니다. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 정보는 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Amazon WorkMail 작업은 Amazon WorkMail API 참조에 의해 CloudTrail 기록되고 문서화됩니다. 예를 들어, `CreateUserCreateAlias`, 및 `GetRawMessageContent` API 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 IAM 사용자 보안 인증 정보로 했는지 여부.
- 역할 또는 페더레이션 사용자의 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부.

자세한 내용은 CloudTrailUserIdentity 요소를 참조하십시오.

Amazon WorkMail 로그 파일 항목의 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 Amazon WorkMail API의 `CreateUser` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T17:49:59Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "name": "janedoe",
    "displayName": "Jane Doe",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
```

```
  "responseElements": {
    "userId": "a3a9176d-EXAMPLE"
  },
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

다음 예제는 Amazon WorkMail API의 `CreateAlias` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
    "entityId": "a3a9176d-EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

다음 예는 Amazon WorkMail Message Flow API에서의 `GetRawMessageContent` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmailMessageFlow.amazonaws.com",
  "eventName": "GetRawMessageContent",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "messageId": "123A4A5A-67B8-90C1-D23E-45FG67H890J1"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```


이메일 이벤트 로깅 활성화

조직의 이메일 메시지를 추적하려면 Amazon WorkMail 콘솔에서 이메일 이벤트 로깅을 활성화합니다. 이메일 이벤트 로깅은 AWS Identity and Access Management 서비스 연결 역할 (SLR) 을 사용하여 Amazon에 이메일 이벤트 로그를 게시할 권한을 부여합니다. CloudWatch IAM 서비스 연결 역할에 대한 자세한 내용은 Amazon WorkMail에 대해 서비스 연결 역할 사용 단원을 참조하세요.

CloudWatch 이벤트 로그에서 CloudWatch 검색 도구 및 지표를 사용하여 메시지를 추적하고 이메일 문제를 해결할 수 있습니다. Amazon이 WorkMail 보내는 이벤트 로그에 대한 자세한 내용은 을 CloudWatch 참조하십시오Amazon WorkMail 이메일 이벤트 로그 모니터링. CloudWatch Logs에 대한 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.

주제

이메일 이벤트 로깅 켜기

기본 설정인 Amazon을 사용하여 이메일 이벤트 로깅을 켜면 다음과 같은 상황이 발생합니다 WorkMail.

- AWS Identity and Access Management 서비스 연결 역할 생성 —. `AmazonWorkMailEvents`
- CloudWatch 로그 그룹 생성 —. `/aws/workmail/emailevents/`*`organization-alias`*
- CloudWatch 로그 보존을 30일로 설정합니다.

이메일 이벤트 로깅을 켜려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 지역을 변경하십시오. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 로깅 설정을 선택합니다.
4. 이메일 흐름 로그 설정 탭을 선택합니다.
5. 이메일 흐름 로그 설정 섹션에서 편집을 선택합니다.
6. 메일 이벤트 활성화 슬라이더를 on 위치로 이동합니다.
7. 다음 중 하나를 수행하십시오.
   - (권장) 기본 설정 사용을 선택합니다.
   - (선택 사항) 기본 설정 사용 확인란의 선택을 취소하고 대상 로그 그룹 및 IAM 역할을 선택합니다.

> **Note**
>
> AWS CLI을(를) 사용하여 로그 그룹과 사용자 지정 역할을 이미 생성한 경우에만 이 옵션을 선택합니다. 자세한 정보는 이메일 이벤트 로깅을 위한 사용자 지정 로그 그룹 및 IAM 역할 생성을 참조하세요.

8. 이 구성을 사용하여 Amazon이 내 계정에 로그를 WorkMail 게시하도록 승인합니다를 선택합니다.
9. 저장을 선택합니다.

이메일 이벤트 로깅을 위한 사용자 지정 로그 그룹 및 IAM 역할 생성

Amazon에 대한 이메일 이벤트 로깅을 활성화할 때는 기본 설정을 사용하는 것이 좋습니다 WorkMail. 사용자 지정 모니터링 구성이 필요한 경우 를 사용하여 이메일 이벤트 AWS CLI 로깅을 위한 전용 로그 그룹과 사용자 지정 IAM 역할을 생성할 수 있습니다.

이메일 이벤트 로깅을 위한 사용자 지정 로그 그룹 및 IAM 역할을 생성하려면

1. 다음 AWS CLI 명령을 사용하여 Amazon WorkMail 조직과 동일한 AWS 지역에 로그 그룹을 생성합니다. 자세한 내용은 AWS CLI 명령 create-log-group참조를 참조하십시오.

```
aws --region us-east-1 logs create-log-group --log-group-name workmail-monitoring
```

2. 다음 정책이 포함된 파일을 생성합니다.

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

3. 다음 AWS CLI 명령을 사용하여 IAM 역할을 생성하고 이 파일을 역할 정책 문서로 연결합니다. 자세한 내용은 AWS CLI 명령 참조의 create-role을 참조하세요.

```
aws iam create-role --role-name workmail-monitoring-role --assume-role-policy-
document file://trustpolicyforworkmail.json
```

> **Note**
>
> WorkMailFullAccess관리형 정책 사용자인 경우 역할 이름에 해당 용어를 workmail 포함해야 합니다. 이 관리형 정책만 역할을 workmail과 함께 이름에 사용하도록 허용합니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 역할을 전달할 수 있는 사용자 권한 부여를 참조하십시오.

4. 이전 단계에서 생성한 IAM 역할에 대한 정책이 포함된 파일을 생성하십시오. 최소한 이 정책은 로그 스트림을 생성하고 1단계에서 생성한 로그 그룹에 로그 이벤트를 입력할 수 있는 권한을 역할에 부여해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:111122223333:log-group:workmail-
monitoring*"
        }
    ]
}
```

5. 다음 AWS CLI 명령을 사용하여 정책 파일을 IAM 역할에 연결합니다. 자세한 내용은 AWS CLI 명령 put-role-policy참조를 참조하십시오.

```
aws iam put-role-policy --role-name workmail-monitoring-role --policy-
name workmail-permissions --policy-document file://rolepolicy.json
```

이메일 이벤트 로깅 해제

Amazon WorkMail 콘솔에서 이메일 이벤트 로깅을 끕니다. 이메일 이벤트 로깅을 더 이상 사용할 필요가 없는 경우 관련 CloudWatch 로그 그룹 및 서비스 연결 역할도 삭제하는 것이 좋습니다. 자세한 정보는 Amazon WorkMail에 대한 서비스 연결 역할 삭제을 참조하세요.

이메일 이벤트 로깅을 해제하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 지역을 변경하십시오. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 모니터링을 선택합니다.
4. 로그 설정 섹션에서 편집을 선택합니다.
5. 메일 이벤트 활성화 슬라이더를 꺼짐 위치로 이동합니다.
6. 저장을 선택합니다.

교차 서비스 혼동된 대리인 방지

혼동된 대리인 문제는 작업을 수행할 권한이 없는 개체가 권한이 더 많은 개체에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS크로스 서비스 사칭으로 인해 대리인 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 호출할 때 발생할 수 있습니다.

통화 서비스는 다른 방법으로는 액세스 권한이 없는 다른 고객의 리소스에 대해 해당 권한을 사용하여 조치를 취하도록 조작될 수 있습니다.

이를 방지하기 위해 계정 내 리소스에 대한 액세스 권한이 부여된 서비스 주체를 사용하는 모든 서비스의 데이터를 보호하는 데 도움이 되는 도구를 AWS 제공합니다.

Logs `aws:SourceArn`및 Amazon S3가 CloudWatch 로그를 생성하는 서비스에 부여하는 권한을 제한하려면 리소스 정책에서 및 `aws:SourceAccount`글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다. 두 글로벌 조건 컨텍스트 키를 모두 사용하는 경우 동일한 정책 설명에서 값이 사용될 때 동일한 계정 ID를 사용해야 합니다.

`aws:SourceArn`의 값은 로그를 생성하는 전달 리소스의 ARN이어야 합니다.

혼동된 대리인 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용합니다.

감사 로깅 활성화

감사 로그를 사용하여 Amazon WorkMail 조직 사용에 대한 세부 정보를 캡처할 수 있습니다. 감사 로그는 사서함에 대한 사용자의 액세스를 모니터링하고, 의심스러운 활동을 감사하고, 액세스 제어 및 가용성 공급자 구성을 디버깅하는 데 사용할 수 있습니다.

> **Note**
>
> AmazonWorkMailFullAccess관리형 정책에는 로그 전달을 관리하는 데 필요한 모든 권한이 포함되어 있지는 않습니다. 이 정책을 사용하여 관리하는 WorkMail 경우 로그 전달을 구성하는 데 사용되는 주체 (예: 위임된 역할) 에게도 필요한 모든 권한이 있는지 확인하십시오.

Amazon은 감사 로그의 세 가지 전송 목적지, 즉 CloudWatch 로그, Amazon S3 및 Amazon Data Firehose를 WorkMail 지원합니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서의 추가 권한이 필요한 로깅 [V2] 를 참조하십시오.

추가 권한이 필요한 로깅에 나열된 권한 [V2] 외에도 Amazon은 로그 전달을 구성하기 위한 추가 권한이 WorkMail 필요합니다`workmail:AllowVendedLogDeliveryForResource`.

작업 로그 전달은 세 가지 요소로 구성됩니다.

- DeliverySource, 로그를 보내는 리소스 또는 리소스를 나타내는 논리적 객체입니다. 아마존의 WorkMail 경우 아마존 WorkMail 조직입니다.
- A는 DeliveryDestination실제 배송지를 나타내는 논리적 객체입니다.
- 배달: 배달 소스를 배달 목적지에 연결합니다.

WorkMail Amazon과 목적지 간의 로그 전송을 구성하려면 다음과 같이 하면 됩니다.

- 를 사용하여 배송 소스를 생성합니다 PutDeliverySource.
- 를 사용하여 배송지를 생성합니다 PutDeliveryDestination.

- 계정 간에 로그를 전송하는 경우 대상 PutDeliveryDestinationPolicy계정에서 사용하여 IAM 정책을 대상에 할당해야 합니다. 이 정책은 계정 A의 전송 소스에서 계정 B의 전송 목적지로 전송을 생성할 수 있는 권한을 부여합니다.
- 를 사용하여 정확히 하나의 배송처와 하나의 배송지를 페어링하여 배송을 생성합니다. CreateDelivery

다음 섹션에서는 각 유형의 목적지로 로그 전송을 설정하기 위해 로그인할 때 보유해야 하는 권한에 대한 세부 정보를 제공합니다. 이러한 권한은 로그인하는 데 사용한 IAM 역할에 부여할 수 있습니다.

> **Important**
>
> 로그 생성 리소스를 삭제한 후 로그 전송 리소스를 제거하는 것은 사용자의 책임입니다.

로그 생성 리소스를 삭제한 후 로그 전송 리소스를 제거하려면 다음 단계를 따르세요.

1. 작업을 사용하여 배달을 삭제합니다. DeleteDelivery
2. DeleteDeliverySource작업을 DeliverySource사용하여 삭제합니다.
3. 방금 삭제한 DeliveryDestinationDeliverySource항목과 관련된 항목이 이 특정 DeliverySource항목에만 사용되는 경우 DeleteDeliveryDestinations작업을 사용하여 제거할 수 있습니다.

Amazon WorkMail 콘솔을 사용하여 감사 로깅 구성

Amazon WorkMail 콘솔에서 감사 로깅을 구성할 수 있습니다.

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 지역을 변경하십시오. 콘솔 창 상단의 표시줄에서 지역 선택 목록을 열고 지역을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 로깅 설정을 선택합니다.
4. 감사 로그 설정 탭을 선택합니다.
5. 적절한 위젯을 사용하여 필요한 로그 유형에 대한 전달을 구성합니다.
6. 저장을 선택합니다.

로그로 CloudWatch 전송된 로그

사용자 권한

로그로 로그를 보낼 수 있게 하려면 다음 권한으로 로그인해야 합니다. CloudWatch

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "AllowUpdatesToResourcePolicyCWL",
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:*"
            ]
        }
        {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

로그 그룹 리소스 정책

로그를 보내는 로그 그룹에는 특정 권한이 포함된 리소스 정책이 있어야 합니다. 로그 그룹에 현재 리소스 정책이 없고 로깅을 설정하는 사용자에게 로그 그룹에 대한`logs:PutResourcePolicy`,`logs:DescribeResourcePolicies`, 및 `logs:DescribeLogGroups` 권한이 있는 경우 로그를 Logs로 CloudWatch 보내기 시작하면 다음과 같은 정책이 AWS 자동으로 생성됩니다.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryWrite20150319",
            "Effect":"Allow",
            "Principal":{
                "Service":[
                    "delivery.logs.amazonaws.com"
                ]
            },
```

```
            "Action":[
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:my-log-group:log-stream:*"
            ],
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:*"
                    ]
                }
            }
        }
    ]
}
```

로그 그룹 리소스 정책 크기 제한 고려 사항

이러한 서비스는 로그를 보내는 각 로그 그룹을 리소스 정책에 나열해야 합니다. CloudWatch 로그 리소스 정책은 5,120자로 제한됩니다. 다수의 로그 그룹에 로그를 전송하는 서비스는 이 한도에 도달할 수 있습니다.

이를 완화하기 위해 Logs는 CloudWatch 로그를 보내는 서비스가 사용하는 리소스 정책의 크기를 모니터링합니다. 정책의 크기 제한인 5,120자에 근접하는 것이 감지되면 CloudWatch Logs는 해당 서비스의 리소스 정책을 자동으로 `/aws/vendedlogs/*` 활성화합니다. 그런 다음 `/aws/vendedlogs/`로 시작하는 이름을 가진 로그 그룹을 이러한 서비스의 로그 대상으로 사용하기 시작할 수 있습니다.

Amazon S3 로 보낸 로그

사용자 권한

Amazon S3로 로그를 전송하려면 다음 권한으로 로그인해야 합니다.

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

```
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
          {
```

```
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

로그가 전송되는 S3 버킷에는 특정 권한을 포함하는 리소스 정책이 있어야 합니다. 현재 버킷에 리소스 정책이 없고 로깅을 설정하는 사용자에게 버킷에 대한 `S3:GetBucketPolicy` 및 `S3:PutBucketPolicy` 권한이 있는 경우 Amazon S3로 로그를 보내기 시작하면 해당 버킷에 대한 다음 정책을 AWS 자동으로 생성합니다.

```
{
    "Version":"2012-10-17",
    "Id":"AWSLogDeliveryWrite20150319",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryAclCheck",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:GetBucketAcl",
            "Resource":"arn:aws:s3:::my-bucket",
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
        },
        {
```

```
            "Sid":"AWSLogDeliveryWrite",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:PutObject",
            "Resource":"arn:aws:s3:::my-bucket/AWSLogs/account-id/*",
            "Condition":{
                "StringEquals":{
                    "s3:x-amz-acl":"bucket-owner-full-control",
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
        }
    ]
}
```

이전 정책에서는 로그가 이 버킷으로 전송되는 계정 ID 목록을 지정했습니다. aws:SourceAccount aws:SourceArn에 대해 로그를 생성하는 리소스의 ARN 목록을 arn:aws:logs:*source-region*:*source-account-id*:* 형식으로 지정합니다.

버킷에 리소스 정책이 있지만 해당 정책에 이전 정책에 표시된 설명이 포함되어 있지 않고 로깅을 설정하는 사용자에게 버킷에 대한 S3:GetBucketPolicy 및 S3:PutBucketPolicy 권한이 있는 경우 해당 명령문이 버킷의 리소스 정책에 추가됩니다.

> **Note**
>
> s3:ListBucket권한이 부여되지 않은 AWS CloudTrail 경우 AccessDenied 오류가 발생하는 경우가 있습니다. delivery.logs.amazonaws.com CloudTrail로그에서 이러한 오류를 방지하려면 s3:ListBucket 권한을 부여해야 합니다delivery.logs.amazonaws.com. 또한 이전 버킷 정책에 설정된 s3:GetBucketAcl 권한과 함께 표시된 Condition 파라미터를 포함해야 합니다. 이를 간소화하기 위해 새로 만드는 대신 를 Statement BE로 직접 업

데이트할 수 있습니다. AWSLogDeliveryAclCheck “Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]

Amazon S3 버킷 서버 측 암호화

Amazon S3 관리 키 (SSE-S3) 를 사용한 서버 측 암호화 또는 키가 저장된 서버 측 암호화 (SSE-KMS) 를 활성화하여 Amazon S3 버킷의 데이터를 보호할 수 있습니다. AWS KMS AWS Key Management Service 자세한 내용은 서버 측 암호화를 사용하여 데이터 보호를 참조하세요.

SSE-S3를 선택하면 추가 구성이 필요하지 않습니다. Amazon S3는 암호화 키를 처리합니다.

> **Warning**
>
> SSE-KMS를 선택하는 경우 고객 관리 키를 사용해야 합니다. 이 시나리오에서는 키 사용이 지원되지 않기 때문입니다. AWS 관리형 키 AWS 관리 키를 사용하여 암호화를 설정하는 경우 로그는 읽을 수 없는 형식으로 전달됩니다.

고객 관리 AWS KMS 키를 사용하는 경우 버킷 암호화를 활성화할 때 고객 관리 키의 Amazon 리소스 이름 (ARN) 을 지정할 수 있습니다. 다음을 고객 관리 키의 키 정책 (S3 버킷의 버킷 정책이 아님) 에 추가하여 로그 전송 계정이 S3 버킷에 쓸 수 있도록 하십시오.

SSE-KMS를 선택하는 경우 고객 관리 키를 사용해야 합니다. 이 시나리오에서는 AWS 관리 키 사용이 지원되지 않기 때문입니다. 고객 관리 AWS KMS 키를 사용하는 경우 버킷 암호화를 활성화할 때 고객 관리 키의 Amazon 리소스 이름 (ARN) 을 지정할 수 있습니다. 다음을 고객 관리 키의 키 정책 (S3 버킷의 버킷 정책이 아님) 에 추가하여 로그 전송 계정이 S3 버킷에 쓸 수 있도록 하십시오.

```
{
    "Sid":"Allow Logs Delivery to use the key",
    "Effect":"Allow",
    "Principal":{
        "Service":[
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action":[
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
```

```
            "kms:DescribeKey"
        ],
        "Resource":"*",
        "Condition":{
            "StringEquals":{
                "aws:SourceAccount":[
                    "account-id"
                ]
            },
            "ArnLike":{
                "aws:SourceArn":[
                    "arn:aws:logs:region:account-id:delivery-source:*"
                ]
            }
        }
}
```

의 경우aws:SourceAccount, 로그가 이 버킷으로 전송되는 계정 ID 목록을 지정하십시오. aws:SourceArn에 대해 로그를 생성하는 리소스의 ARN 목록을 arn:aws:logs:*source-region*:*source-account-id*:* 형식으로 지정합니다.

Firehose로 전송된 로그

사용자 권한

Firehose에 로그를 보낼 수 있게 하려면 다음 권한으로 로그인해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
```

```
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyFH",
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream"
            ],
            "Resource": [
                "arn:aws:firehose:region:account-id:deliverystream/*"
            ]
        },
        {
            "Sid": "CreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::account-id:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery"
        }
           {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
```

```
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

리소스 권한에 사용되는 IAM 역할

Firehose는 리소스 정책을 사용하지 않으므로 이러한 로그를 Firehose로 전송하도록 설정할 때 IAM 역할을 AWS 사용합니다. AWS 라는 서비스 연결 역할을 생성합니다. AWSServiceRoleForLogDelivery 이 서비스 연결 역할에는 다음 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:ListTagsForDeliveryStream"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/LogDeliveryEnabled": "true"
                }
            },
            "Effect": "Allow"
        }
    ]
}
```

이 서비스 연결 역할은 태그가 로 설정된 모든 Firehose 전송 스트림에 권한을 부여합니다`LogDeliveryEnabled`. `true` AWS 로깅을 설정할 때 대상 전송 스트림에 이 태그를 제공합니다.

또한 이 서비스 연결 역할에는 `delivery.logs.amazonaws.com` 서비스 보안 주체가 필요한 서비스 연결 역할을 맡도록 허용하는 신뢰 정책이 있습니다. 이러한 신뢰 정책은 다음과 같습니다.

```
{
```

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

콘솔별 권한

API 대신 콘솔을 사용하여 로그 전달을 설정하는 경우 이전 섹션에 나열된 권한 외에도 다음 권한이 필요합니다.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowLogDeliveryActions",
            "Effect":"Allow",
            "Action":[
                "firehose:DescribeDeliveryStream",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:*",
                "arn:aws:firehose:region:account-id:deliverystream/*",
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid":"ListAccessForDeliveryDestinations",
            "Effect":"Allow",
            "Action":[
                "logs:DescribeLogGroups",
                "firehose:ListDeliveryStreams",
                "s3:ListAllMyBuckets"
            ],
            "Resource":"*"
```

```
        }
    ]
}
```

Amazon에 대한 규정 준수 검증 WorkMail

타사 감사자는 여러 규정 AWS 준수 프로그램의 WorkMail 일환으로 Amazon의 보안 및 규정 준수를 평가합니다. 여기에는SOC,,ISO, C5가 포함됩니다.

특정 규정 준수 프로그램 범위 내 AWS 서비스 목록은 규정 준수 프로그램별 범위 내 AWS 서비스를 참조하십시오. 일반 정보는 AWS 규정 준수 프로그램을 참조하십시오.

를 사용하여 타사 감사 보고서를 다운로드할 수 AWS Artifact있습니다. 자세한 내용은 AWSArtifact에서 보고서 다운로드를 참조하십시오.

Amazon을 사용할 때의 규정 준수 WorkMail 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다. AWS
- AWS 규정 준수 리소스 — 이 통합 문서 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS Config— 이 AWS 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이 AWS 서비스는 보안 업계 표준 및 모범 사례를 준수하는지 확인하는 데 도움이 AWS 되는 보안 상태를 종합적으로 보여줍니다.

아마존의 레질리언스 WorkMail

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

Amazon은 AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 WorkMail 제공합니다.

아마존의 인프라 보안 WorkMail

> **Note**
>
> Amazon은 전송 계층 보안 (TLS) 1.0 및 1.1에 대한 지원을 WorkMail 중단했습니다. TLS1.0 또는 1.1을 사용하는 경우 TLS 버전을 1.2로 업그레이드해야 합니다. 자세한 내용은 모든 AWS API 엔드포인트의 최소 TLS 프로토콜 수준이 되는 TLS 1.2를 참조하십시오.

WorkMail Amazon은 관리형 서비스로서 AWS 글로벌 네트워크 보안의 보호를 받습니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 WorkMail 통해 Amazon에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안 (TLS). TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- (임시 디피-헬만) 또는 (타원 곡선 임시 디피-헬만PFS) 와 같이 완벽한 순방향 기밀성 DHE () 을 갖춘 암호 제품군. ECDHE Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

아마존 시작하기 WorkMail

작업을 필수 조건 완료했으면 Amazon을 시작할 준비가 된 WorkMail 것입니다. 자세한 설명은 아마존 시작하기 WorkMail 섹션을 참조하세요.

다음 섹션에서 기존 메일박스를 Amazon으로 마이그레이션하는 방법 WorkMail, Microsoft Exchange와의 상호 운용성 및 WorkMail Amazon 할당량에 대해 자세히 알아볼 수 있습니다.

주제

아마존 시작하기 WorkMail

새 Amazon WorkMail 사용자이든 Amazon 또는 Amazon의 기존 사용자이든 관계없이 다음 단계를 WorkMail 완료하여 Amazon을 시작하십시오. WorkDocs WorkSpaces

> **Note**
>
> 시작하기 전에 필수 조건 단원을 완료하십시오.

주제

1단계: Amazon WorkMail 콘솔에 로그인

사용자를 추가하고 계정 및 사서함을 관리하려면 먼저 Amazon WorkMail 콘솔에 로그인해야 합니다.

Amazon WorkMail 콘솔에 로그인하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.
2. 필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 리전에 대한 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.

2단계: 아마존 WorkMail 사이트 설정

1. Amazon WorkMail 콘솔에 로그인한 후 조직을 설정하고 도메인을 추가합니다. Amazon WorkMail 조직의 전용 도메인을 사용하는 것이 좋습니다. 자세한 내용은 조직 생성 및 도메인 추가 섹션을 참조하세요.
2. (선택 사항) Amazon에서 제공하는 무료 테스트 도메인을 사용하도록 선택할 수 WorkMail 있습니다. 이렇게 하려면 4단계로 건너뛰세요.

> **Note**
>
> 테스트 도메인은 *alias*.awsapps.com 형식을 사용합니다. 테스트할 때는 테스트 도메인만 사용해야 한다는 점을 기억하세요. 프로덕션 환경에서는 테스트 도메인을 사용하지 마세요. 또한 Amazon WorkMail 조직에 최소 한 명 이상의 활성화된 사용자가 있어야 합니다. 활성화된 사용자가 없는 경우 다른 고객이 도메인을 등록하여 사용할 수 있게 됩니다.

3. 외부 도메인을 사용하는 경우 도메인 이름 시스템(DNS) 서비스에 적절한 텍스트(TXT) 및 메일 교환(MX) 레코드를 추가하여 해당 도메인을 확인하세요. TXT 레코드를 사용하면 DNS에 대한 메모를 입력할 수 있습니다. MX 레코드는 수신 메일 서버를 지정합니다. 도메인을 조직의 기본 도메인으로 설정해야 합니다. 자세한 내용은 도메인 확인 및 기본 도메인 선택 섹션을 참조하세요.
4. 새 사용자를 생성하거나 Amazon에서 기존 디렉터리 사용자를 활성화하십시오 WorkMail. 자세한 설명은 사용자 추가 섹션을 참조하세요.

5. (선택 사항) 기존 Microsoft Exchange 사서함이 있는 경우 해당 사서함을 WorkMail Amazon으로 마이그레이션하십시오. 자세한 설명은 아마존으로 마이그레이션 WorkMail 섹션을 참조하세요.

Amazon WorkMail 사이트 설정을 완료한 후 웹 애플리케이션 URL을 WorkMail 사용하여 Amazon에 액세스할 수 있습니다.

Amazon WorkMail 웹 애플리케이션 URL을 찾으려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 이렇게 하려면 검색 상자 오른쪽에 있는 리전 선택 목록을 연 다음 원하는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.

   조직 설정 페이지가 나타나고 사용자 로그인 아래에 URL이 표시됩니다. URL은 https://*alias*.awsapps.com/mail과 같은 형식입니다.

3단계: Amazon WorkMail 사용자 액세스 설정

다음 옵션 중에서 선택하여 Amazon WorkMail 사용자 액세스를 설정합니다.

- Microsoft Outlook 클라이언트를 사용하여 기존 데스크톱 클라이언트에서 사용자 액세스를 설정합니다. 자세한 내용은 Microsoft Outlook을 Amazon WorkMail 계정에 연결하기를 참조하십시오.
- Kindle, Android, iPad 또는 iPhone과 같은 모바일 디바이스에서 사용자 액세스를 설정합니다. 자세한 내용은 모바일 디바이스 시작하기를 참조하십시오.
- 사용자 액세스를 설정하려면 IMAP(인터넷 메일 액세스 프로토콜) 프로토콜과 호환되는 모든 클라이언트 소프트웨어를 사용하세요. 자세한 내용은 Amazon WorkMail 계정에 IMAP 클라이언트 연결을 참조하십시오.

추가 리소스

- 아마존으로 마이그레이션 WorkMail
- 아마존과 WorkMail 마이크로소프트 익스체인지 간의 상호 운용성
- 아마존 WorkMail 쿼터

아마존으로 마이그레이션 WorkMail

파트너와 협력하여 Microsoft Exchange, Microsoft Office 365, G Suite Basic (구 Google Apps for Work) 및 기타 플랫폼에서 WorkMail Amazon으로 마이그레이션할 수 있습니다. 파트너에 대한 자세한 내용은 Amazon WorkMail 기능을 참조하십시오.

주제

1단계: Amazon에서 사용자 생성 또는 활성화 WorkMail

사용자를 마이그레이션하기 전에 WorkMail Amazon에 해당 사용자를 추가하여 사서함을 프로비저닝해야 합니다. 자세한 설명은 사용자 추가 섹션을 참조하세요.

2단계: 아마존으로 마이그레이션 WorkMail

모든 AWS 마이그레이션 파트너와 협력하여 Amazon으로 마이그레이션할 수 WorkMail 있습니다. 이러한 공급자에 대한 자세한 내용은 Amazon WorkMail 기능을 참조하십시오.

사서함을 마이그레이션하려면 마이그레이션 관리자 역할을 할 전담 Amazon WorkMail 사용자를 만드십시오. 다음 절차에서는 이 사용자에게 조직의 모든 사서함에 액세스할 수 있는 권한을 부여합니다.

마이그레이션 관리자를 만들려면

1. 다음 중 하나를 수행합니다.
    - Amazon WorkMail 콘솔에서 마이그레이션 관리자로 활동할 새 사용자를 생성합니다. 자세한 설명은 사용자 추가 섹션을 참조하세요.
    - Active Directory에서 마이그레이션 관리자 역할을 할 새 사용자를 만든 다음 Amazon에서 사용자를 WorkMail 활성화합니다. 자세한 설명은 사용자 활성화 섹션을 참조하세요.
2. Amazon WorkMail 콘솔 탐색 창에서 Organizations를 선택한 다음 조직 이름을 선택합니다.
3. 조직 설정을 선택하고 마이그레이션을 선택한 다음 편집을 선택합니다.
4. 마이그레이션 활성화됨 슬라이더를 켜짐 위치로 이동합니다.
5. 마이그레이션 관리자를 열고 사용자를 선택합니다.
6. 저장을 선택합니다.

3단계: Amazon으로 마이그레이션 완료 WorkMail

이메일 계정을 WorkMail Amazon으로 마이그레이션한 후에는 DNS 레코드를 확인하고 데스크톱 및 모바일 클라이언트를 구성할 수 있습니다.

Amazon으로 마이그레이션을 완료하려면 WorkMail

1. 모든 DNS 레코드가 업데이트되었고 이 레코드가 Amazon을 가리키는지 확인합니다 WorkMail. 필수 DNS 레코드에 대한 자세한 내용은 도메인 추가 단원을 참조하십시오.

   > **Note**
   >
   > DNS 레코드 업데이트 프로세스에는 몇 시간이 걸릴 수 있습니다. MX 레코드가 변경되는 동안 소스 사서함에 새 항목이 나타나면 DNS 레코드가 업데이트된 후 마이그레이션 도구를 다시 실행하여 새 항목을 마이그레이션합니다.

2. Amazon을 사용하도록 데스크톱 또는 모바일 클라이언트를 구성하는 방법에 대한 자세한 내용은 Amazon WorkMail 사용 WorkMail 설명서의 Microsoft Outlook을 Amazon WorkMail 계정에 연결 섹션을 참조하십시오.

아마존과 WorkMail 마이크로소프트 익스체인지 간의 상호 운용성

Amazon과 WorkMail Microsoft Exchange Server 간의 상호 운용성을 통해 사서함을 Amazon으로 마이그레이션하거나 WorkMail Amazon을 회사 사서함의 하위 집합으로 마이그레이션할 때 사용자에게 미치는 영향을 최소화할 수 있습니다. WorkMail

이러한 상호 운용성 덕분에 동일한 회사 도메인을 두 환경의 사서함에 모두 사용할 수 있습니다. 이 방법으로 사용자는 약속 없음/있음 일정 상태 정보를 양방향으로 공유하여 회의를 예약할 수 있습니다.

사전 조건

Microsoft Exchange와 상호 운용성을 활성화하기 전에 다음 작업을 수행합니다.

- 최소 한 명 이상의 사용자가 Amazon을 사용하도록 설정했는지 확인하십시오. WorkMail 이는 Microsoft Exchange의 가용성 설정을 구성하는 데 필요합니다. 사용자를 활성화하려면 사용자에 대해 이메일 라우팅 활성화 단원의 단계를 따릅니다.
- AD(Active Directory) 커넥터를 설정합니다. 온프레미스 디렉터리를 사용해 AD 커넥터를 설정하면 사용자는 계속해서 기존 회사 자격 증명을 사용할 수 있습니다. 자세한 내용은 AD Connector 생성 및 Amazon을 온프레미스 WorkMail 디렉터리와 통합을 참조하십시오.

- Amazon WorkMail 조직을 설정하세요. 설정한 AD Connector를 사용하는 Amazon WorkMail 조직을 만드십시오.
- Amazon WorkMail 조직에 회사 도메인을 추가한 다음 Amazon WorkMail 콘솔에서 확인합니다. 그렇지 않으면 이 별칭으로 보낸 이메일이 반송됩니다. 자세한 내용은 도메인 작업을 참조하십시오.
- 사서함을 WorkMail Amazon으로 마이그레이션. 사용자가 온프레미스 환경에서 Amazon으로 사서함을 프로비저닝하고 마이그레이션할 수 있도록 합니다. WorkMail 자세한 내용은 기존 사용자 활성화 및 WorkMailAmazon으로 마이그레이션을 참조하십시오.

> **Note**
>
> Amazon을 가리키도록 DNS 레코드를 업데이트하지 마십시오 WorkMail. 그러면 두 환경 간에 상호 운용성이 필요한 동안 Microsoft Exchange가 수신 이메일의 주 서버로 유지됩니다.

- Active Directory의 UPN(사용자 보안 주체 이름)이 사용자의 기본 SMTP 주소와 일치하는지 확인합니다.

WorkMail Amazon은 Microsoft Exchange의 EWS (Exchange 웹 서비스) URL에 HTTPS 요청을 보내 일정 휴무/휴무 정보를 얻습니다.

EWS 기반 가용성 공급자의 경우 WorkMail Amazon은 Microsoft Exchange의 EWS (Exchange 웹 서비스) URL에 HTTPS 요청을 보내 일정 휴무/휴무 정보를 얻습니다. 따라서 다음 사전 요구 사항은 EWS 기반 가용성 공급자에만 적용됩니다.

- 인터넷에서의 액세스를 허용하도록 관련 방화벽 설정이 지정되어 있는지 확인합니다. HTTPS의 기본 포트는 포트 443입니다.
- Amazon은 Microsoft Exchange 환경에서 유효한 인증 기관 (CA) 이 서명한 인증서를 사용할 WorkMail 수 있는 경우에만 Microsoft Exchange의 EWS URL에 대해 성공적인 HTTPS 요청을 할 수 있습니다. 자세한 내용은 Microsoft Exchange 설명서 웹 사이트에서 인증 기관에 대한 Exchange Server 인증서 요청 만들기를 참조하세요.
- Microsoft Exchange에서 EWS에 대해 기본 인증을 활성화해야 합니다. 자세한 내용은 Microsoft MVP Award Program 블로그에서 Virtual directories: Exchange 2013을 참조하십시오.

도메인 추가 및 사서함 활성화

기업 도메인을 이메일 주소에 사용할 수 WorkMail 있도록 Amazon에 추가합니다. Amazon에 추가된 도메인이 WorkMail 확인되었는지 확인한 다음 사용자 및 그룹이 WorkMail Amazon에서 사서함을 프

로비저닝할 수 있도록 하십시오. 상호 운용성 WorkMail 모드에서는 Amazon에서 리소스를 활성화할 수 없으므로 상호 운용성 모드를 비활성화한 WorkMail 후 Amazon에서 리소스를 다시 생성해야 합니다. 그러나 이러한 리소스를 사용하여 상호 운용성 모드에서 회의를 예약할 수는 있습니다. Microsoft Exchange의 리소스는 항상 Amazon의 사용자 탭에 표시됩니다 WorkMail.

- 자세한 내용은 도메인 추가, 기존 사용자 활성화 및 기존 그룹 활성화를 참조하십시오.

> **Note**
>
> Microsoft Exchange와의 상호 운용성을 보장하려면 Amazon WorkMail 레코드를 가리키도록 DNS 레코드를 업데이트하지 마십시오. 그러면 두 환경 간에 상호 운용성이 필요한 동안 Microsoft Exchange가 수신 이메일의 주 서버로 유지됩니다.

상호 운용성 활성화

Amazon WorkMail 조직을 생성하지 않은 경우 공개 API를 사용하여 상호 운용성 모드가 활성화된 새 WorkMail 조직을 생성할 수 있습니다.

Active Directory에 연결된 AD Connector를 사용하는 Amazon WorkMail 조직이 이미 있고 Microsoft Exchange도 보유하고 있는 경우, 기존 Amazon WorkMail 조직에 대한 Microsoft Exchange 상호 운용성을 활성화하는 데 대한 지원을 받으려면 AWS Support에 문의하십시오.

마이크로소프트 익스체인지 및 아마존에서 서비스 계정 생성 WorkMail

> **Note**
>
> Exchange를 사용자 지정 가용성 공급자의 백엔드로 사용하지 않는 경우에는 Exchange에서 서비스 계정을 생성할 필요가 없습니다.

일정 휴무/휴무 정보에 액세스하려면 Microsoft Exchange와 Amazon 모두에서 서비스 계정을 만드세요. WorkMail Microsoft Exchange 서비스 계정은 다른 Exchange 사용자의 약속 없음/있음 일정 정보에 액세스할 수 있는 Microsoft Exchange의 사용자입니다. 액세스 권한이 기본적으로 부여되므로 특별 권한은 필요하지 않습니다.

마찬가지로 Amazon WorkMail 서비스 계정은 다른 Amazon 사용자의 캘린더 휴무/휴무 정보에 액세스할 수 WorkMail 있는 WorkMail Amazon의 모든 사용자입니다. 이 권한도 기본적으로 부여됩니다. 온프

레미스 디렉터리에 Amazon WorkMail 사용자를 생성한 다음 Amazon에서 해당 사용자를 활성화하여 WorkMail WorkMail Amazon과 AD Connector를 디렉터리에 통합할 수 있도록 해야 합니다.

상호 운용성 모드에서의 제한 사항

조직이 상호 운용성 모드이면 Exchange Admin Center를 사용하여 모든 사용자, 그룹 및 리소스를 관리해야 합니다. Amazon WorkMail 사용자 및 그룹을 활성화하려면 를 사용하십시오AWS Management Console. 자세한 내용은 기존 사용자 활성화 및 기존 그룹 활성화를 참조하십시오.

WorkMailAmazon에서 사용자 또는 그룹을 활성화하는 경우 해당 사용자 및 그룹의 이메일 주소 또는 별칭을 편집할 수 없습니다. 또한 Exchange 관리 센터를 통해 구성해야 합니다. Amazon은 4시간마다 디렉터리의 변경 내용을 WorkMail 동기화합니다.

상호 운용성 WorkMail 모드에서는 Amazon에서 리소스를 생성하거나 활성화할 수 없습니다. 하지만 모든 Exchange 리소스는 Amazon WorkMail 주소록에서 사용할 수 있으며 평소와 같이 회의 일정을 잡는 데 사용할 수 있습니다.

Amazon에서 가용성 설정을 구성합니다. WorkMail

Amazon에서 가용성 설정을 WorkMail 구성하여 외부 시스템을 쿼리하고, 일정 기능을 제공하고, 일정 휴무/휴무 정보를 가져올 수 있습니다. WorkMail Amazon은 원격 시스템에서 여유/바쁜 정보를 가져오는 두 가지 모드를 지원합니다.

- EWS (Exchange 웹 서비스) — 이 구성에서 WorkMail Amazon은 EWS 프로토콜을 사용하여 Exchange 서버 또는 다른 WorkMail 조직에 가용성 정보를 쿼리합니다. 이는 가장 간단한 구성이지만 공용 인터넷을 통해 Exchange 서버의 EWS 엔드포인트에 액세스할 수 있어야 합니다.
- 사용자 지정 가용성 공급자(CAP) - 이 구성에서 관리자는 지정된 이메일 도메인에 대한 사용자 가용성 정보를 가져오도록 AWS Lambda 함수를 구성할 수 있습니다. 이메일 서버 플랫폼에 따라 WorkMail Amazon에서 CAP를 사용하면 다음과 같은 이점이 있습니다.
  - 방화벽을 열 필요 없이 내부 EWS에서 사용자 가용성을 확보할 수 있습니다. WorkMail
  - Google Workspace(이전의 G Suite) 와 같이 Exchange가 아니거나 EWS가 아닌 시스템에서 사용자 가용성을 확보할 수 있습니다.

주제

EWS 기반 가용성 공급자 구성

콘솔에서 EWS 기반 가용성 설정을 구성하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 이렇게 하려면 검색 상자 오른쪽에 있는 리전 선택 목록을 연 다음 원하는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 조직 설정, 상호 운용성 탭을 선택합니다.
4. 가용성 구성 추가를 선택하고 다음 정보를 입력합니다.

   - 유형 - EWS를 선택합니다.
   - 도메인 - 이 구성을 사용하여 가용성 정보를 쿼리하려고 WorkMail 시도할 도메인입니다.
   - EWS URL — WorkMail 아마존은 이 URL을 EWS 엔드포인트에 쿼리합니다. 이 안내서의 EWS URL 가져오기 섹션을 참조하세요.
   - 사용자 이메일 주소 — EWS 엔드포인트 인증에 사용할 사용자의 이메일 주소입니다. WorkMail
   - 비밀번호 - EWS WorkMail 엔드포인트를 인증하는 데 사용할 비밀번호입니다.
5. 저장을 선택합니다.

EWS URL 가져오기

Microsoft Outlook을 사용하여 Exchange용 EWS URL을 가져오려면 다음 절차를 완료하세요.

1. Exchange 환경에서 아무 사용자로나 Windows Microsoft Outlook에 로그인합니다.
2. Ctrl 키를 누른 상태에서 작업 표시줄에 있는 Microsoft Outlook 아이콘의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 엽니다.
3. [테스트 이메일] 을 선택합니다. AutoConfiguration
4. Microsoft Exchange 사용자의 이메일 주소와 암호를 입력하고 [테스트]를 선택합니다.
5. [결과] 창에서 [가용성 서비스 URL]의 값을 복사합니다.

를 사용하여 PowerShell 교환할 EWS URL을 가져오려면 PowerShell 프롬프트에서 다음 명령을 실행합니다.

```
Get-WebServicesVirtualDirectory |Select name, *url* | fl
```

아마존용 EWS URL을 가져오려면 먼저 아마존 WorkMail WorkMail 엔드포인트 및 할당량 아래에서 EWS 도메인을 찾으십시오. EWS URL - `https://"EWS domain"/EWS/Exchange.asmx`을 입력하고 “EWS 도메인”을 EWS 도메인으로 바꾸세요.

사용자 지정 가용성 공급자 구성

CAP(사용자 지정 가용성 공급자)를 구성하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 이렇게 하려면 검색 상자 오른쪽에 있는 리전 선택 목록을 연 다음 원하는 리전을 선택합니다.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 조직 설정, 상호 운용성 설정을 선택합니다.
4. 가용성 구성 추가를 선택하고 다음 정보를 입력합니다.

   - 유형 - CAP Lambda를 선택합니다.
   - 도메인 - 이 구성을 사용하여 가용성 정보를 쿼리하려고 WorkMail 시도할 도메인입니다.
   - ARN - 가용성 정보를 제공하는 Lambda 함수의 ARN입니다.

CAP Lambda 함수를 구축하려면 사용자 지정 가용성 공급자 Lambda 함수 구축을 참조하세요.

사용자 지정 가용성 공급자 Lambda 함수 구축

사용자 지정 가용성 공급자(CAP)는 잘 정의된 JSON 스키마로 작성된 JSON 기반 요청 및 응답 프로토콜로 구성됩니다. Lambda 함수는 요청을 파싱하여 유효한 응답을 제공합니다.

주제

- 요청 및 응답 요소
- 액세스 권한 부여
- CAP Lambda 함수를 WorkMail 사용하는 아마존의 예

요청 및 응답 요소

요청 요소

다음은 Amazon WorkMail 사용자의 CAP를 구성하는 데 사용되는 샘플 요청입니다.

```
{
    "requester": {
        "email": "user1@internal.example.com",
        "userName": "user1",
        "organization": "m-0123456789abcdef0123456789abcdef",
        "userId": "S-1-5-18",
        "origin": "127.0.0.1"
    },
    "mailboxes": [
        "user2@external.example.com",
        "unknown@internal.example.com"
    ],
    "window": {
        "startDate": "2021-05-04T00:00:00.000Z",
        "endDate": "2021-05-06T00:00:00.000Z"
    }
}
```

요청은 요청자, 사서함, 창의 세 섹션으로 구성됩니다. 이러한 정보는 이 설명서의 요청자, 사서함 및 창 섹션에 설명되어 있습니다.

요청자

요청자 섹션은 WorkMail Amazon에 원래 요청을 한 사용자에 대한 정보를 제공합니다. CAP는 이 정보를 사용하여 공급자의 행동을 변경합니다. 예를 들어 이 데이터를 사용하여 백엔드 가용성 공급자의 동일한 사용자처럼 위장하거나 응답에서 특정 세부 정보를 생략할 수 있습니다.

필드	설명	필수
`Email`	요청자의 기본 이메일 주소입니다.	예
`Username`	요청자의 사용자 이름입니다.	예
`Organization`	요청자의 조직 ID입니다.	예
`UserID`	요청자 ID입니다.	예
`Origin`	요청자의 원격 주소입니다.	아니요
`Bearer`	추후 사용 예약.	아니요

사서함

사서함 섹션에는 가용성 정보가 요청된 사용자의 이메일 주소를 쉼표로 구분한 목록이 포함되어 있습니다.

창

창 섹션에는 가용성 정보가 요청되는 기간이 포함되어 있습니다. `startDate` 및 `endDate`는 모두 UTC로 지정되며 RFC 3339에 따라 형식이 지정됩니다. 이벤트는 잘릴 것으로 예상되지 않습니다. 즉, 정의된 `StartDate` 전에 이벤트가 시작되면 원래 시작 이벤트가 사용됩니다.

응답 요소

WorkMail 아마존은 CAP Lambda 함수에서 응답을 받을 때까지 25초 동안 기다립니다. 25초 후 WorkMail Amazon은 함수에 장애가 발생한 것으로 간주하고 EWS GetUserAvailability 응답에서 관련 사서함에 대해 오류를 생성합니다. 이렇게 해도 전체 GetUserAvailability 작업이 실패하지는 않습니다.

다음은 이 섹션의 시작 부분에 정의된 구성의 샘플 응답입니다.

```
{
    "mailboxes": [{
        "mailbox": "user2@external.example.com",
        "events": [{
            "startTime": "2021-05-03T23:00:00.000Z",
            "endTime": "2021-05-04T03:00:00.000Z",
            "busyType": "BUSY"|"FREE"|"TENTATIVE",
            "details": {  // optional
                "subject": "Late meeting",
                "location": "Chime",
                "instanceType": "SINGLE_INSTANCE"|"RECURRING_INSTANCE"|"EXCEPTION",
                "isMeeting": true,
                "isReminderSet": true,
                "isPrivate": false
            }
        }],
        "workingHours": {
            "timezone": {
                "name": "W. Europe Standard Time"
                "bias": 60,
                "standardTime": {  // optional (not needed for fixed offsets)
                    "offset": 60,
                    "time": "02:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
```

```
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
                "daylightTime": {  // optional (not needed for fixed offsets)
                    "offset": 0,
                    "time": "03:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
            },
            "workingPeriods":[{
                "startMinutes": 480,
                "endMinutes": 1040,
                "days": ["SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"]
            }]
        }
    },{
        "mailbox": "unknown@internal.example.com",
        "error": "MailboxNotFound"
    }]
}
```

응답은 사서함 목록으로 구성된 단일 사서함 섹션으로 구성됩니다. 가용성이 확보된 각 사서함은 사서함, 이벤트 및 근무 시간의 세 섹션으로 구성됩니다. 가용성 공급자가 사서함의 가용성 정보를 가져오지 못한 경우 섹션은 사서함 및 오류라는 두 섹션으로 구성됩니다. 이러한 정보는 이 설명서의 사서함, 이벤트, 근무 시간, Timezone, 근무 기간 및 오류 섹션에 설명되어 있습니다.

사서함

사서함 섹션은 요청의 사서함 섹션에 있는 사용자의 이메일 주소입니다.

이벤트

이벤트 섹션은 요청된 창에서 발생하는 이벤트 목록입니다. 각 이벤트는 다음 매개변수로 정의됩니다.

필드	설명	필수
`startTime`	이벤트 시작 시간은 UTC 기준이며 RFC 3339에 따라 형식이 지정됩니다.	예

필드	설명	필수
endTime	이벤트 종료 시간은 UTC 기준이며 RFC 3339에 따라 형식이 지정됩니다.	예
busyType	이벤트의 약속 있음 유형입니다. 가능한 값은 Busy, Free 또는 Tentative 입니다.	예
details	이벤트의 세부 정보입니다.	아니요
details.subject	이벤트의 제목입니다.	예
details.location	이벤트의 위치입니다.	예
details.instanceType	이벤트의 인스턴스 유형입니다. 가능한 값은 Single_Instance , Recurring_Instance 또는 Exception 입니다.	예
details.isMeeting	이벤트에 참석자가 있는지 여부를 나타내는 부울입니다.	예
details.isReminderSet	이벤트에 미리 알림이 설정되어 있는지 여부를 나타내는 부울입니다.	예
details.isPrivate	이벤트가 비공개로 설정되었는지 여부를 나타내는 부울입니다.	예

근무 시간

근무 시간 섹션에는 사서함 소유자의 근무 시간에 대한 정보가 포함되어 있습니다. 여기에는 시간대 및 근무 기간라는 두 개의 섹션이 있습니다.

Timezone

시간대 하위 섹션에서는 사서함 소유자의 시간대를 설명합니다. 요청자가 다른 시간대에서 근무할 때는 사용자의 근무 시간을 올바르게 렌더링하는 것이 중요합니다. 가용성 공급자는 이름을 사용하는 대신 시간대를 명시적으로 설명해야 합니다. 표준화된 시간대 설명을 사용하면 시간대 불일치를 방지하는 데 도움이 됩니다.

필드	설명	필수
`name`	시간대의 이름입니다.	예
`bias`	GMT의 기본 오프셋(분 단위)입니다.	예
`standardTime`	지정된 시간대의 표준 시간 시작입니다.	아니요
`daylightTime`	지정된 시간대의 일광 절약 시간 시작입니다.	아니요

`standardTime` 및 `daylightTime` 모두 정의하거나 모두 생략해야 합니다. `standardTime` 및 `daylightTime` 객체의 필드는 다음과 같습니다.

필드	설명	허용된 값
`offset`	기본 오프셋을 기준으로 한 오프셋(분)입니다.	NA
`time`	표준 시간과 서머타임 간의 전환이 발생하는 시간으로, `hh:mm:ss`로 지정됩니다.	NA
`month`	표준 시간과 일광 절약 시간 간의 전환이 발생하는 달입니다.	`JAN`,`FEB`, `MAR`, `APR`, `JUN`, `JUL`, `AUG`, `SEP`, `OCT`, `NOV`, `DEC`
`week`	표준 시간과 일광 절약 시간 간의 전환이 발생하는 지정된 달 내의 주입니다.	`FIRST`, `SECOND`, `THIRD`, `FOURTH`, `LAST`

필드	설명	허용된 값
dayOfWeek	표준 시간과 일광 절약 시간 간의 전환이 발생하는 지정된 주 내의 일입니다.	SUN, MON, TUE, WED, THU, FRI, SAT

근무 기간

근무 기간 섹션에는 하나 이상의 근무 기간 객체가 포함되어 있습니다. 각 기간은 하루 이상의 근무일 시작 및 종료를 정의합니다.

필드	설명	허용된 값
startMinutes	근무일의 시작은 자정부터 분 단위입니다.	NA
endMinutes	근무일의 종료는 자정부터 분 단위입니다.	NA
days	이 기간이 적용되는 일입니다.	SUN, MON, TUE, WED, THU, FRI, SAT

오류

오류 필드에는 임의의 오류 메시지가 포함될 수 있습니다. 다음 표에는 잘 알려진 코드와 EWS 오류 코드의 매핑이 나와 있습니다. 다른 모든 메시지는 ERROR_FREE_BUSY_GENERATION_FAILED에 매핑됩니다.

값	EWS 오류 코드	
MailboxNotFound	ERROR_MAIL_RECIPIENT_NOT_FOUND	
ErrorAvailabilityConfigNotFound	ERROR_AVAILABILITY_CONFIG_NOT_FOUND	
ErrorServerBusy	ERROR_SERVER_BUSY	

값	EWS 오류 코드	
ErrorTimeoutExpired	ERROR_TIMEOUT_EXPIRED	
ErrorFreeBusyGenerationFailed	ERROR_FREE_BUSY_GENERATION_FAILED	
ErrorResponseSchemaValidation	ERROR_RESPONSE_SCHEMA_VALIDATION	

액세스 권한 부여

AWS Command Line Interface(AWS CLI)에서 다음 Lambda 명령을 실행합니다. 이 명령은 CAP를 구문 분석하는 Lambda 함수에 리소스 정책을 추가합니다. 이 함수를 사용하면 Amazon WorkMail 가용성 서비스가 Lambda 함수를 호출할 수 있습니다.

```
aws lambda add-permission \
    --region LAMBDA_REGION \
    --function-name CAP_FUNCTION_NAME \
    --statement-id AllowWorkMail \
    --action "lambda:InvokeFunction" \
    --principal availability.workmail.WM_REGION.amazonaws.com \
    --source-account WM_ACCOUNT_ID \
    --source-arn arn:aws:workmail:WM_REGION:WM_ACCOUNT_ID:organization/ORGANIZATION_ID
```

명령에서 지정된 위치에 다음 파라미터를 추가합니다.

- *LAMBDA_REGION* - CAP Lambda가 배포된 리전의 이름입니다. 예: `us-east-1`.
- *CAP_FUNCTION_NAME* - CAP Lambda 함수의 이름입니다.

> **Note**
>
> 이는 CAP Lambda 함수의 이름, 별칭 또는 일부 또는 전체 ARN일 수 있습니다.

- *WM_REGION* — 아마존 WorkMail 조직이 Lambda 함수를 호출하는 지역의 이름입니다.

> **Note**
>
> 다음 리전만 CAP에서 사용할 수 있습니다.
>
> - 미국 동부(버지니아 북부)
> - US West (Oregon)
> - 유럽(아일랜드)

- *WM_ACCOUNT_ID* - 조직 계정의 ID입니다.
- *ORGANIZATION_ID* - CAP Lambda를 호출하는 조직의 ID입니다. 예를 들어, 조직 ID: m-934ebb9eb57145d0a6cab566ca81a21f입니다.

> **Note**
>
> *LAMBDA_REGION* 및 *WM_REGION*은 리전 간 호출이 필요한 경우에만 달라집니다. 리전 간 호출이 필요하지 않은 경우 모두 동일합니다.

CAP Lambda 함수를 WorkMail 사용하는 아마존의 예

Amazon이 CAP Lambda 함수를 WorkMail 사용하여 EWS 엔드포인트를 쿼리하는 예를 보려면 Amazon용 서버리스 애플리케이션 리포지토리의 AWS이 샘플 애플리케이션을 참조하십시오. WorkMail GitHub

Microsoft Exchange에서 가용성 설정 구성

활성화된 사용자에 대한 모든 일정 약속 있음/없음 정보 요청을 WorkMail Amazon으로 리디렉션하려면 Microsoft Exchange에서 가용성 주소 공간을 설정하십시오.

다음 PowerShell 명령을 사용하여 주소 공간을 생성합니다.

```
$credentials = Get-Credential
```

프롬프트에 Amazon WorkMail 서비스 계정의 자격 증명을 입력합니다. 사용자 이름은 다음과 같이 입력해야 합니다. **domain\username**(즉, ***orgname*.awsapps.com\workmail_service_account_*username***). 여기서는 Amazon WorkMail 조직의 이름을 ***orgname***

나타냅니다. 자세한 설명은 마이크로소프트 익스체인지 및 아마존에서 서비스 계정 생성 WorkMail 섹션을 참조하세요.

```
Add-AvailabilityAddressSpace -ForestName orgname.awsapps.com -AccessMethod OrgWideFB -
Credentials $credentials
```

자세한 내용은 Microsoft Docs AvailabilityAddressSpace 추가 기능을 참조하십시오.

Microsoft Exchange와 Amazon WorkMail 사용자 간의 이메일 라우팅 활성화

Microsoft Exchange Server와 Amazon WorkMail 간의 이메일 라우팅을 통해 사용자는 Amazon으로 마이그레이션한 후에도 기존 이메일 주소를 유지할 수 WorkMail 있습니다. 이메일 라우팅을 사용하면 Microsoft Exchange Server를 조직의 수신 이메일에 대한 기본 SMTP(단순 메일 전송 프로토콜) 서버로 유지할 수 있습니다.

이메일 라우팅을 사용하기 전에 다음 사전 조건을 충족해야 합니다.

- 조직에 대해 상호 운용성 모드를 활성화합니다. 자세한 설명은 상호 운용성 활성화 섹션을 참조하세요.
- Amazon WorkMail 콘솔에 도메인이 표시되는지 확인하십시오.
- Microsoft Exchange Server가 인터넷으로 이메일을 보낼 수 있는지 확인합니다. 전송 커넥터를 구성해야 할 수 있습니다. 전송 커넥터에 대한 자세한 내용은 Microsoft 설명서의 Exchange Server에서 인터넷으로 메일 보내기를 위한 송신 커넥터 만들기를 참조하세요.

사용자에 대해 이메일 라우팅 활성화

조직에 변경 사항을 적용하기 전에 테스트 사용자에 대해 다음 단계를 먼저 완료해 보는 것이 좋습니다.

1. WorkMailAmazon으로 마이그레이션하려는 사용자 계정을 활성화합니다. 자세한 내용은 기존 사용자 활성화를 참조하십시오.
2. Amazon WorkMail 콘솔에서 활성화된 사용자와 연결된 이메일 주소가 두 개 이상 있는지 확인합니다.
   - <*workmailuser*@*orgname*.awsapps.com>(자동으로 추가되며 Microsoft Exchange 없이 테스트용으로 사용할 수 있음)

- <*workmailuser*@*yourdomain*.com>(자동으로 추가되며 기본 Microsoft Exchange 주소임)

  자세한 내용은 사용자 이메일 주소 편집을 참조하십시오.

3. Microsoft Exchange의 사서함에 있는 모든 데이터를 Amazon의 사서함으로 마이그레이션해야 WorkMail 합니다. 자세한 내용은 WorkMailAmazon으로 마이그레이션을 참조하십시오.
4. 모든 데이터를 마이그레이션한 후에는 Microsoft Exchange에서 해당 사용자의 사서함을 사용하지 않도록 설정합니다. 그런 다음 Amazon을 가리키는 외부 SMTP 주소를 가진 메일 사용자 (또는 메일 사용 가능 사용자) 를 생성합니다. WorkMail 이렇게 하려면 Exchange 관리 쉘에서 다음 명령을 사용합니다.

> **Important**
>
> 다음 단계는 사서함의 내용을 지웁니다. 이메일 라우팅을 WorkMail 활성화하기 전에 데이터가 Amazon으로 마이그레이션되었는지 확인하십시오. 일부 메일 클라이언트는 이 명령을 실행할 WorkMail 때 Amazon으로 원활하게 전환되지 않습니다. 자세한 설명은 메일 클라이언트 구성 섹션을 참조하세요.

```
$old_mailbox = Get-Mailbox exchangeuser
```

```
Disable-Mailbox $old_mailbox
```

```
$new_mailuser = Enable-MailUser $old_mailbox.Identity -
ExternalEmailAddress workmailuser@orgname.awsapps.com -PrimarySmtpAddress
 $old_mailbox.PrimarySmtpAddress
```

```
Set-MailUser $new_mailuser -EmailAddresses $old_mailbox.EmailAddresses -
HiddenFromAddressListsEnabled $old_mailbox.HiddenFromAddressListsEnabled
```

위 명령에서 *orgname#* 아마존 WorkMail 조직의 이름을 나타냅니다. 자세한 내용은 TechNet Microsoft에서 사서함 비활성화 및 메일 사용자 활성화를 참조하십시오.

5. 사용자에게 테스트 이메일을 보냅니다(위의 예에서는 **workmailuser@yourdomain.com**). 이메일 라우팅이 올바르게 활성화된 경우 사용자는 Amazon WorkMail 메일박스에 로그인하여 이메일을 수신할 수 있어야 합니다.

> **Note**
>
> 그래야 두 환경 간의 상호 운용성을 유지하려는 한 Microsoft Exchange가 수신 이메일의 기본 서버로 남아 있습니다. Microsoft Exchange와의 상호 운용성을 보장하려면 WorkMail 나중에야 Amazon을 가리키도록 DNS 레코드를 업데이트해야 합니다.

후속 설정 구성

위 단계는 사용자 사서함을 Microsoft Exchange 서버에서 WorkMail Amazon으로 이동하고 사용자는 Microsoft Exchange에 연락처로 유지합니다. 마이그레이션된 사용자는 이제 외부 메일 사용자이기 때문에 Microsoft Exchange Server는 추가 제약을 적용합니다. 마이그레이션을 완료하기 위한 추가 구성 요구 사항이 있을 수도 있습니다.

- 사용자가 기본적으로 그룹에 이메일을 보내지 못할 수 있습니다. 이 기능을 활성화하기 위해서는 모든 그룹에 대한 안전한 발신자 목록에 사용자를 추가해야 합니다. 자세한 내용은 Microsoft의 배달 관리를 참조하십시오 TechNet.
- 사용자가 리소스를 예약하지 못할 수 있습니다. 이 기능을 활성화하려면 사용자가 액세스해야 하는 모든 리소스의 `ProcessExternalMeetingMessages`를 설정해야 합니다. 자세한 내용은 CalendarProcessing Microsoft에서 설정하기 항목을 참조하십시오 TechNet.

메일 클라이언트 구성

일부 메일 클라이언트는 WorkMail Amazon으로 원활하게 전환되지 않습니다. 이러한 클라이언트는 사용자가 추가 설정 단계를 수행해야 합니다. 메일 클라이언트마다 다른 조치를 취해야 할 수 있습니다.

- Windows의 Microsoft Outlook – Outlook을 다시 시작해야 합니다. 시작할 때 이전 사서함을 계속 사용할지 아니면 임시 사서함을 사용할지 선택해야 합니다. 임시 사서함 옵션을 선택합니다. 그런 다음 Microsoft Exchange 사서함을 다시 구성합니다.
- MacOS의 Microsoft Outlook – Outlook이 다시 시작되면 Outlook이 서버 ***orgname***.awsapps.com으로 리디렉션되었습니다. 이 서버가 설정을 구성하도록 하시겠습니까?라는 메시지를 받게 됩니다. 제안을 수락합니다.
- iOS의 메일 – 메일 앱이 이메일 수신을 중지하고 메일을 받을 수 없음 오류를 생성합니다. Microsoft Exchange 사서함을 다시 생성하고 다시 구성합니다.

상호 운용성 모드 비활성화 및 메일 서버 폐기

WorkMailAmazon용 Microsoft Exchange 사서함을 구성한 후 상호 운용성 모드를 비활성화할 수 있습니다. 사용자 또는 레코드를 마이그레이션하지 않은 경우에는 상호 운용성 모드를 비활성화하더라도 구성에는 아무런 영향을 미치지 않습니다.

> **Warning**
>
> 상호 운용성 모드를 비활성화하기 전에 필수 단계를 모두 완료해야 합니다. 완료하지 않으면 이메일이 반송되거나 예상치 못한 동작으로 이어집니다. 마이그레이션을 완료하지 않은 경우 상호 운용성을 비활성화하면 조직의 사용이 중단될 수 있습니다. 이 작업은 실행 취소할 수 없습니다.

상호 운용성 모드 지원을 비활성화하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 상호 운용성 모드를 비활성화하려는 조직을 선택합니다.
3. 조직 설정에서 상호 운용성 모드 비활성화를 선택합니다.
4. 상호 운용성 모드 비활성화 대화 상자에서 조직의 이름을 입력하고 상호 운용성 모드 비활성화를 선택합니다.

상호 운용성 지원을 비활성화하면 Amazon을 사용할 수 없는 사용자 및 그룹이 주소록에서 WorkMail 제거됩니다. Amazon WorkMail 콘솔을 사용하여 누락된 사용자 또는 그룹을 활성화할 수 있으며 주소록에 추가됩니다. Microsoft Exchange의 리소스는 활성화할 수 없으며 아래의 단계를 완료해야 주소록에 표시됩니다.

- Amazon에서 리소스 생성 WorkMail — WorkMail Amazon에서 리소스를 생성한 다음 이러한 리소스에 대한 대리자 및 예약 옵션을 구성할 수 있습니다. 자세한 내용은 리소스 작업을 참조하십시오.
- AutoDiscover DNS 레코드 생성 - 조직의 모든 메일 도메인에 대한 AutoDiscover DNS 레코드를 구성합니다. 이를 통해 사용자는 Microsoft Outlook 및 모바일 클라이언트에서 Amazon WorkMail 사서함에 연결할 수 있습니다. 자세한 내용은 엔드포인트 구성에 사용을 AutoDiscover 참조하십시오.

- MX DNS 레코드를 Amazon으로 전환 WorkMail — 모든 수신 이메일을 WorkMail Amazon으로 전송하려면 MX DNS 레코드를 Amazon으로 전환해야 합니다. WorkMail DNS 레코드 변경을 모든 DNS 서버로 전파하는 데 최대 72시간이 걸릴 수 있습니다.
- 메일 서버 사용 중지 — 모든 이메일이 WorkMail Amazon으로 직접 라우팅되고 있음을 확인한 후 앞으로 사용하지 않으려는 경우 메일 서버를 사용 중지할 수 있습니다.

문제 해결

가장 흔히 발생하는 Amazon WorkMail 상호 운용성 및 마이그레이션 오류에 대한 해결 방법은 다음과 같습니다.

EWS(Exchange Web Services) URL이 잘못되었거나 이 URL에 연결할 수 없음 - EWS URL이 올바른지 확인합니다. 자세한 설명은 Amazon에서 가용성 설정을 구성합니다. WorkMail 섹션을 참조하세요.

EWS 평가 중 연결 실패 - 이 문제는 일반적인 오류로, 원인은 다음과 같을 수 있습니다.

- Microsoft Exchange에서 인터넷에 연결되지 않음
- 인터넷에서 액세스할 수 있도록 방화벽이 구성되지 않았습니다. 포트 443(HTTPS 요청의 기본 포트)이 열려 있는지 확인합니다.

인터넷 연결과 방화벽 설정을 확인한 후에도 오류가 지속되면 AWS Support에 문의하세요.

Microsoft Exchange 상호 운용성을 구성할 때 사용자 이름 및 암호가 잘못됨 - 이 문제는 일반적인 오류로, 원인은 다음과 같을 수 있습니다.

- 사용자 이름이 예상 형식이 아닙니다. 다음 패턴을 사용합니다.

```
DOMAIN\username
```

- Microsoft Exchange Server가 EWS에 대한 기본 인증에 맞춰 구성되어 있지 않습니다. 자세한 내용은 Microsoft MVP Award Program 블로그에서 Virtual directories: Exchange 2013을 참조하십시오.

사용자가 winmail.dat 첨부 파일이 포함된 이메일을 수신함 — 암호화된 S/MIME 이메일을 Exchange에서 WorkMail Amazon으로 보내고 Mac용 Outlook 2016 또는 IMAP 클라이언트에서 수신한 경우 이 문제가 발생할 수 있습니다. 이 문제는 Exchange 관리 쉘에서 다음 명령을 실행하면 해결됩니다.

Set-RemoteDomain -Identity "Default" -TNEFEnabled $false

위의 항목을 확인한 후에도 오류가 지속되면 AWS Support에 문의하십시오.

아마존 WorkMail 쿼터

Amazon은 기업 고객과 소규모 비즈니스 소유자 모두가 사용할 WorkMail 수 있습니다. 할당량에 대한 변경을 구성하지 않아도 대부분의 사용 사례를 지원하긴 하지만 제품 침해로부터 사용자 및 인터넷도 보호합니다. 따라서 일부 고객은 사전 설정된 할당량에 걸릴 수 있습니다. 이 단원에서는 이러한 할당량과 할당량을 변경하는 방법을 설명합니다.

일부 할당량 값은 변경할 수 있으며 일부는 변경할 수 없는 하드 할당량입니다. 할당량 증가 요청에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS 서비스 할당량을 참조하세요.

Amazon WorkMail 조직 및 사용자 할당량

30일 무료 평가판을 통해 Amazon WorkMail 조직에 최대 25명의 사용자를 추가할 수 있습니다. 이 기간이 끝나면 활성 사용자를 제거하거나 Amazon WorkMail 계정을 폐쇄하지 않는 한 모든 활성 사용자에 대해 요금이 부과됩니다.

이러한 할당량을 평가할 때 다른 사용자에게 보낸 메시지가 모두 고려됩니다. 여기에는 이메일, 회의 요청, 회의 응답, 작업 요청과 규칙의 결과로 자동으로 전달 또는 리디렉션된 메시지가 모두 포함됩니다.

> **Note**
>
> 특정 조직에 대한 할당량 증가를 요청하는 경우에는 요청에 해당 조직의 이름을 포함해야 합니다.

Resource	기본 할당량	요청 변경에 대한 상한
AWS계정당 아마존 WorkMail 조직 수	100	조직의 디렉터리 유형에 따라 늘릴 수 있습니다. AWS Directory Service 콘솔에서 AWS Directory Service 할당량을 확인하고 증가를 요청할 수 있습니다. 자세한 내용은 AWS 일반 참조의 서비스 할당량을 참조하세요.

Resource	기본 할당량	요청 변경에 대한 상한
Amazon WorkMail 조직당 사용자 수	1,000	조직의 디렉터리 유형에 따라 증가할 수 있습니다. • Amazon WorkMail 디렉터리: 최대 1천만 명의 사용자 • Simple AD 또는 AD 커넥터, 대형: 최대 5,000명* • Simple AD 또는 AD 커넥터, 소형: 최대 500명* • Microsoft AD, AWS Directory Service에서 호스팅: 설정 및 구성에 따라 최대 1천만 명. *Simple AD 또는 AD 커넥터를 사용하는 경우 자세한 내용은 AWS Directory Service를 참조하십시오.
무료 평가판의 사용자 수	처음 30일 동안 최대 25명	무료 평가판 사용 기간은 모든 조직에서 처음 25명의 사용자에게만 적용됩니다. 그 외의 추가 사용자는 무료 평가판에 포함되지 않습니다.
1일간 AWS 계정당 주소 지정된 수신자	100,000명의 조직 외부 수신자 (조직 내부 수신자에 대한 하드 할당량 없음)	상한이 없습니다. 하지만 WorkMail Amazon은 비즈니스 이메일 서비스이므로 대량 이메일 서비스에는 사용할 수 없습니다. 대량 이메일 서비스는 Amazon SES 또는 Amazon Pinpoint를 참조하십시오.

Resource	기본 할당량	요청 변경에 대한 상한
테스트 도메인을 사용하여 1일 간 AWS 계정에 주소 지정된 수신자	수신자 200명(대상과 상관없음)	테스트 메일 도메인은 장기간 사용할 수 없습니다. 고유한 도메인을 추가해 기본 도메인으로 사용하는 것이 좋습니다.

그룹에 대한 할당량은 기본 디렉터리에서 설정됩니다.

WorkMail 조직: 할당량 설정

Resource	기본 할당량
Amazon WorkMail 조직당 도메인 수	1,000 이 수는 하드 할당량이며 변경할 수 없습니다.
규칙당 이메일 흐름 규칙의 발신자 패턴 수	250 이 수는 하드 할당량이며 변경할 수 없습니다.
조직당 이메일 흐름 규칙의 발신자 패턴 수	1,000 이 수는 하드 할당량이며 변경할 수 없습니다.

사용자별 할당량

이러한 할당량을 평가할 때 다른 사용자에게 보낸 메시지가 모두 고려됩니다. 여기에는 이메일, 회의 요청, 회의 응답, 작업 요청과 규칙의 결과로 자동으로 전달 또는 리디렉션된 메시지가 모두 포함됩니다.

Resource	기본 할당량	요청 변경에 대한 상위 할당량
사서함의 최대 크기	50GB 이 수는 하드 할당량이며 변경할 수 없습니다.	해당 사항 없음

Resource	기본 할당량	요청 변경에 대한 상위 할당량
사용자당 최대 별칭 수	100 이 수는 하드 할당량이며 변경할 수 없습니다.	해당 사항 없음
사용자가 소유한 도메인을 사용하여 1일간 사용자당 주소 지정된 수신자	10,000명의 조직 외부 수신자(조직 내부 수신자에 대한 하드 할당량 없음)	상한이 없습니다. 하지만 WorkMail Amazon은 비즈니스 이메일 서비스이므로 대량 이메일 서비스에는 사용할 수 없습니다. 대량 이메일 서비스는 Amazon SES 또는 Amazon Pinpoint를 참조하십시오.

메시지 할당량

이러한 할당량을 평가할 때 다른 사용자에게 보낸 메시지가 모두 고려됩니다. 여기에는 이메일, 회의 요청, 회의 응답, 작업 요청과 규칙의 결과로 자동으로 전달 또는 리디렉션된 메시지가 모두 포함됩니다.

Resource	기본 할당량
수신 메시지의 최대 크기	29MB의 인코딩되지 않은 데이터. 메시지는 MIME 형식으로 수신됩니다. 수신 MIME 메시지의 최대 크기는 40MB입니다. 이 수는 하드 할당량이며 변경할 수 없습니다.
발신 메시지의 최대 크기	29MB의 인코딩되지 않은 데이터. 메시지는 MIME 형식으로 전송됩니다. 발신 MIME 메시지의 최대 크기는 40MB입니다. 이 수는 하드 할당량이며 변경할 수 없습니다.
메시지당 최대 수신자 수	500

Resource	기본 할당량
	이 수는 하드 할당량이며 변경할 수 없습니다.
메시지당 최대 첨부 파일 수	500 이 수는 하드 할당량이며 변경할 수 없습니다.

조직 작업

WorkMailAmazon에서 조직은 회사 내 사용자를 대표합니다. Amazon WorkMail 콘솔에는 사용 가능한 조직 목록이 표시됩니다. 사용할 수 있는 조직이 없는 경우 Amazon을 사용하려면 조직을 만들어야 WorkMail 합니다.

주제

조직 생성

WorkMailAmazon을 사용하려면 먼저 조직을 만들어야 합니다. 하나의 AWS 계정에 여러 Amazon WorkMail 조직이 있을 수 있습니다. 조직을 생성할 때는 조직의 도메인을 선택하고 사용자 디렉터리 및 암호화 설정도 지정합니다.

새 사용자 디렉터리를 만들거나 Amazon을 기존 WorkMail 디렉터리와 통합할 수 있습니다. Amazon은 온프레미스 Microsoft Active Directory, AWS 관리형 Active Directory 또는 Simple WorkMail AD와 함께 사용할 수 있습니다. 온프레미스 디렉터리와 통합하면 Amazon의 기존 사용자 및 그룹을 사용할 수 있으며 사용자는 기존 WorkMail 자격 증명으로 로그인할 수 있습니다. 온프레미스 디렉터리를 사용하는 경우 먼저 AWS Directory Service에서 AD Connector를 설정해야 합니다. AD Connector는 사용자 및 그룹을 Amazon WorkMail 주소록과 동기화하고 사용자 인증 요청을 수행합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Active Directory Connector를 참조하세요.

Amazon에서 사서함 콘텐츠를 암호화하는 데 WorkMail 사용하는 방법을 선택할 수도 있습니다. AWS KMS key WorkMailAmazon의 기본 AWS 관리형 마스터 키를 선택하거나 AWS Key Management Service (AWS KMS) 의 기존 KMS 키를 사용할 수 있습니다. 새 KMS 키 생성에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 생성을 참조하십시오. AWS Identity and Access Management (IAM) 사용자로 로그인한 경우 키의 키 관리자로 등록하세요. KMS 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 활성화 및 비활성화를 참조하세요.

고려 사항

Amazon WorkMail 조직을 만들 때는 다음 사항을 기억하십시오.

- WorkMail Amazon은 현재 여러 계정과 공유하는 관리형 Microsoft Active Directory 서비스를 지원하지 않습니다.
- Microsoft Exchange와 AD Connector를 사용하는 온프레미스 Active Directory를 사용하는 경우 조직의 상호 운용성 설정을 구성하는 것이 좋습니다. 이렇게 하면 사서함을 Amazon으로 마이그레이션하거나 회사 사서함의 일부에 WorkMail 대해 WorkMail Amazon을 사용할 때 사용자에게 미치는 영향을 최소화할 수 있습니다. 자세한 내용은 아마존과 WorkMail 마이크로소프트 익스체인지 간의 상호 운용성 단원을 참조하십시오.
- 무료 테스트 도메인 옵션을 선택하면 제공된 테스트 도메인으로 Amazon WorkMail 조직을 사용할 수 있습니다. 테스트 도메인은 다음 형식을 사용합니다.*example*.awsapps.com. Amazon WorkMail 조직에 활성화된 사용자를 유지하는 한 Amazon WorkMail 및 기타 지원 AWS 서비스에서 테스트 메일 도메인을 사용할 수 있습니다. 하지만 테스트 도메인을 다른 용도로는 사용할 수 없습니다. Amazon WorkMail 조직에 최소 한 명 이상의 활성화된 사용자가 없는 경우 다른 고객이 테스트 도메인을 등록하여 사용할 수 있게 될 수 있습니다.
- WorkMail Amazon은 다중 지역 디렉터리를 지원하지 않습니다.

주제

조직 생성

Amazon WorkMail 콘솔에서 새 조직을 생성합니다.

조직을 생성하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.

2. 탐색 모음에서 조직을 선택합니다.

   조직 페이지가 나타나고 조직(있는 경우)이 표시됩니다.

3. 조직 생성을 선택합니다.
4. 이메일 도메인에서 조직의 이메일 주소로 사용할 도메인을 선택합니다.

   - 기존 Route 53 도메인 - Amazon Route 53(Route 53) 호스팅 영역으로 관리하는 기존 도메인을 선택합니다.
   - 새 Route 53 도메인 — Amazon에서 사용할 새 Route 53 도메인 이름을 WorkMail 등록합니다.
   - 외부 도메인 - 외부 도메인 이름 시스템 (DNS) 공급자를 통해 관리하는 기존 도메인을 입력합니다.
   - 무료 테스트 도메인 — Amazon에서 제공하는 무료 테스트 도메인을 사용합니다 WorkMail. 테스트 도메인을 WorkMail 사용하여 Amazon을 탐색한 다음 나중에 조직에 도메인을 추가할 수 있습니다.

5. (선택 사항) Amazon Route 53을 통해 도메인을 관리하는 경우 Route 53 호스팅 영역에 대해 Route 53 도메인을 선택합니다.
6. 별칭에 조직의 고유한 별칭을 입력합니다.
7. 고급 설정을 선택하고 사용자 디렉터리에 대해 다음 옵션 중 하나를 선택합니다.

   - 새 Amazon WorkMail 디렉터리 생성 — 사용자를 추가하고 관리하기 위한 새 디렉터리를 생성합니다.
   - 기존 디렉터리 사용 - 온프레미스 Microsoft Active Directory, AWS Managed Active Directory 또는 Simple AD와 같은 기존 디렉터리를 사용하여 사용자를 관리합니다.

8. 암호화에 대해 다음 옵션 중 하나를 선택합니다.

   - Amazon WorkMail 관리 키 사용 — 계정에 새 암호화 키를 생성합니다.
   - 기존 KMS 키 사용 - 이미 생성한 기존 KMS 키를 사용합니다 AWS KMS.

9. 조직 생성을 선택합니다.

외부 도메인을 사용하는 경우 DNS 서비스에 적절한 텍스트 (TXT) 및 메일 교환기 (MX) 레코드를 추가하여 확인하십시오. TXT레코드를 사용하여 DNS 서비스에 대한 메모를 입력할 수 있습니다. MX 레코드는 수신 메일 서버를 지정합니다.

도메인을 조직의 기본 도메인으로 설정해야 합니다. 자세한 내용은 도메인 확인 및 기본 도메인 선택 단원을 참조하세요.

조직이 활성 상태이면 사용자를 추가하고 이메일 클라이언트를 설정할 수 있습니다. 자세한 내용은 Amazon용 이메일 클라이언트 설정을 참조하십시오 사용자 추가 WorkMail.

조직 세부 정보 보기

각 Amazon WorkMail 조직은 조직 세부 정보 페이지를 표시할 수 있습니다. 이 페이지에는 에서 사용할 수 있는 정보를 포함하여 IDs 해당 조직에 대한 정보가 표시됩니다 AWS Command Line Interface. 페이지의 메시지에는 확인되지 않은 도메인이나 사용자 부족과 같이 설정 및 구성을 완료하는 데 필요한 모든 단계가 표시될 수도 있습니다. 메시지에서는 해당 이메일 클라이언트를 설정하기 위해 따라야 하는 첫 번째 단계도 제공합니다.

조직 세부 정보를 확인하려면

1. 탐색 모음에서 조직을 선택합니다.

   조직 페이지가 나타나고 조직이 표시됩니다.
2. 표시할 조직을 선택합니다.

Amazon WorkDocs 또는 WorkSpaces 디렉터리 통합

WorkMail Amazon과 함께 Amazon을 WorkDocs 사용하거나 WorkSpaces, 다음 단계를 사용하여 호환되는 디렉터리를 생성하십시오.

호환되는 Amazon WorkDocs 또는 WorkSpaces 디렉터리를 추가하려면

1. Amazon WorkDocs 또는 을 사용하여 호환 가능한 디렉터리를 WorkSpaces 생성하십시오.
   a. Amazon WorkDocs 지침은 Amazon WorkDocs 관리 안내서의 Quick Start 시작하기를 참조하십시오.
   b. WorkSpaces 지침은 Amazon WorkSpaces 관리 안내서의 Amazon WorkSpaces 빠른 설치 시작하기를 참조하십시오.
2. Amazon WorkMail 콘솔에서 Amazon WorkMail 조직을 생성하고 기존 디렉터리를 사용하도록 선택합니다. 자세한 내용은 조직 생성 단원을 참조하십시오.

조직 상태 및 설명

조직을 생성하면 조직은 다음 상태 중 하나일 수 있습니다.

상태	설명
활성	조직이 정상적인 상태로 사용할 준비가 되어 있습니다.
[생성 중]	조직을 생성하는 워크플로우가 실행 중입니다.
실패	조직을 생성할 수 없습니다.
[Impaired]	조직이 제대로 작동하지 않거나 문제가 감지되었습니다.
비활성	조직이 비활성 상태입니다.
[Requested]	조직 생성 요청이 대기열에 있어 생성 대기 중입니다.
검증	조직에 대한 모든 설정의 상태를 확인 중입니다.

조직 삭제

조직의 이메일에 더 이상 WorkMail Amazon을 사용하지 않으려면 Amazon에서 조직을 삭제하면 WorkMail 됩니다.

> **Note**
>
> 이 작업은 실행 취소할 수 없습니다. 조직 삭제 후에는 사서함 데이터를 복구할 수 없습니다.

조직을 삭제하는 방법

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 조직 화면의 조직 목록에서 제거할 조직을 선택하고 삭제를 선택합니다.
3. 조직 삭제에서 조직의 이름을 입력한 후 기존 사용자 디렉터리를 유지할지 삭제할지 선택합니다.

4. 그런 다음 조직 삭제를 선택합니다.

> **Note**
>
> WorkMailAmazon에 사용할 디렉터리를 제공하지 않은 경우 새로 만들어 드립니다. 조직을 삭제할 때 이 기존 디렉터리를 유지하면 Amazon WorkMail WorkDocs, Amazon 또는 에서 사용하지 않는 한 해당 디렉터리에 대한 요금이 부과됩니다 WorkSpaces. 요금에 대한 자세한 내용은 기타 디렉터리 유형 요금을 참조하십시오.
> 디렉터리를 삭제하려면 다른 AWS 애플리케이션을 활성화할 수 없습니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Simple AD 디렉터리 삭제 또는 AD Connector 디렉터리 삭제를 참조하세요.

조직을 삭제하려고 하면 잘못된 Amazon 심플 이메일 서비스 (AmazonSES) 규칙 세트 오류 메시지가 표시될 수 있습니다. 이 오류가 발생하면 Amazon SES 콘솔에서 Amazon SES 규칙을 편집하고 잘못된 규칙 세트를 제거하십시오. 편집하는 규칙에는 규칙 이름에 Amazon WorkMail 조직 ID가 있어야 합니다. Amazon SES 규칙 편집에 대한 자세한 내용은 Amazon Simple Email Service 개발자 안내서의 수신 규칙 생성을 참조하십시오.

잘못된 규칙 세트를 찾아야 하는 경우 먼저 규칙을 저장합니다. 규칙 세트에 대해 오류 메시지가 표시됩니다.

이메일 주소 찾기

조직에서 이메일 주소를 사용하는지 사용자, 리소스 또는 그룹별로 확인할 수 있습니다.

이메일 주소를 찾으려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 조직 페이지에서 이메일 주소 찾기를 선택합니다.
4. 검색을 선택합니다.

조직 설정 작업

다음 섹션에서는 Amazon WorkMail 조직에 사용할 수 있는 설정을 사용하는 방법을 설명합니다. 선택한 설정은 전체 조직에 적용됩니다.

주제

사서함 마이그레이션 활성화

Microsoft Exchange 또는 G Suite Basic과 같은 소스에서 WorkMail Amazon으로 사서함을 전송하려는 경우 사서함 마이그레이션을 활성화합니다. 대규모 마이그레이션 프로세스의 일환으로 마이그레이션을 활성화합니다. 방법 안내 단계를 포함한 자세한 내용은 이 설명서의 시작하기 섹션에서 아마존으로 마이그레이션 WorkMail을 참조하세요.

저널링 활성화

이메일 통신을 기록하도록 저널링을 활성화할 수 있습니다. 저널링을 사용할 때는 일반적으로 통합된 타사 보관 및 도구를 사용합니다. eDiscovery 저널링은 데이터 스토리지, 개인 정보 보호, 정보 보호를 위한 준수 규정을 충족하도록 보장하는 데 도움이 됩니다.

방법 안내 단계를 포함한 자세한 내용은 이 설명서의 시작하기 섹션에서 Amazon WorkMail을 통해 이메일 저널링 사용을 참조하세요.

상호 운용성 활성화

상호 운용성을 통해 Microsoft Exchange에서 마이그레이션하고 Amazon을 회사 사서함의 하위 WorkMail 집합으로 사용할 수 있습니다. 방법 안내 단계를 포함한 자세한 내용은 이 설명서의 시작하기 섹션에서 Amazon에서 가용성 설정을 구성합니다. WorkMail 을 참조하세요.

게이트웨이 활성화 SMTP

아웃바운드 이메일 흐름 규칙과 함께 사용할 단순 메일 전송 프로토콜 (SMTP) 게이트웨이를 활성화합니다. 아웃바운드 이메일 흐름 규칙을 사용하면 Amazon WorkMail 조직에서 보낸 이메일 메시지를 SMTP 게이트웨이를 통해 라우팅할 수 있습니다. 자세한 내용은 아웃바운드 이메일 규칙 작업 단원을 참조하십시오.

> **Note**
>
> SMTP아웃바운드 이메일 흐름 규칙에 맞게 구성된 게이트웨이는 주요 인증 기관의 인증서를 사용하여 Transport Layer Security (TLS) v1.2를 지원해야 합니다. 기본 인증만 지원됩니다.

게이트웨이를 구성하려면 SMTP

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 조직 설정을 선택합니다.

   조직 설정 페이지가 나타나고 탭 세트가 표시됩니다.
4. SMTP게이트웨이 탭을 선택한 다음 게이트웨이 생성을 선택합니다.
5. 다음을 입력합니다.
   - 게이트웨이 이름 - 고유한 이름을 입력합니다.
   - 게이트웨이 주소 - 게이트웨이의 호스트 이름 또는 IP 주소를 입력합니다.
   - 포트 번호 - 게이트웨이의 포트 번호를 입력합니다.
   - 사용자 이름 - 사용자 이름을 입력합니다.
   - 암호 - 강력한 암호를 입력합니다.
6. 생성(Create)을 선택합니다.

   SMTP게이트웨이는 아웃바운드 이메일 흐름 규칙과 함께 사용할 수 있습니다.

아웃바운드 이메일 흐름 규칙과 함께 사용하도록 SMTP 게이트웨이를 구성하면 아웃바운드 메시지가 규칙을 게이트웨이와 일치시키려고 시도합니다. SMTP 규칙과 일치하는 메시지는 해당 게이트웨이로 라우팅되며, 해당 SMTP 게이트웨이는 나머지 이메일 전송을 처리합니다.

WorkMail Amazon이 SMTP 게이트웨이에 연결할 수 없는 경우 시스템은 이메일 메시지를 발신자에게 반송합니다. 이 경우 이전 단계에 따라 게이트웨이 설정을 수정하세요.

이메일 흐름 관리

이메일 관리에 도움이 되도록 이메일 흐름 규칙을 설정할 수 있습니다. 이메일 흐름 규칙은 주소 또는 도메인을 기반으로 이메일 메시지에 대해 하나 이상의 작업을 수행할 수 있습니다. 발신자 및 수신자 모두의 이메일 주소 또는 도메인에서 이메일 흐름 규칙을 사용할 수 있습니다.

이메일 흐름 규칙을 만들 때는 지정된 규칙 패턴이 일치할 때 이메일에 적용되는 규칙 작업을 지정합니다.

주제

인바운드 이메일 규칙 작업

인바운드 이메일 흐름 규칙은 원치 않는 이메일이 사용자의 사서함에 도착하지 않도록 하는 데 도움이 됩니다. 규칙 조치라고도 하는 인바운드 이메일 흐름 규칙은 Amazon WorkMail 조직 내 누구에게나 전송되는 모든 이메일 메시지에 자동으로 적용됩니다. 이는 개별 사서함에 대한 이메일 규칙과 다릅니다.

> **Note**
>
> 선택적으로 AWS Lambda 함수가 포함된 규칙을 사용하여 수신 이메일을 사용자의 사서함으로 전송하기 전에 처리할 수 있습니다. WorkMailAmazon에서 Lambda를 사용하는 방법에 대한

자세한 내용은 을 참조하십시오. AWS Lambda 아마존을 위한 구성 WorkMail Lambda에 대한 자세한 내용은 AWS Lambda 개발자 안내서를 참조하세요.

규칙 조치라고도 하는 인바운드 이메일 흐름 규칙은 Amazon WorkMail 조직 내 누구에게나 전송되는 모든 이메일 메시지에 자동으로 적용됩니다. 이는 개별 사서함에 대한 이메일 규칙과 다릅니다.

다음 규칙 작업은 인바운드 이메일이 처리되는 방식을 정의합니다. 각 규칙에 대해 다음 작업 중 하나와 함께 발신자 및 수신자 패턴을 지정합니다.

작업	설명
이메일 삭제	이메일 메시지는 무시됩니다. 이메일이 전달되지 않고, 발신자에게 전달되지 않음을 알리지 않습니다.
반송 메일 응답 보내기	이메일 메시지가 전달되지 않고, 반송 메일 메시지를 통해 발신자에게 전달되지 않음을 알립니다.
정크 폴더로 전달	이메일 메시지는 Amazon WorkMail 스팸 탐지 시스템에서 원래 스팸으로 식별되지 않았더라도 사용자의 스팸 또는 정크 폴더로 전달됩니다.
기본값	이메일 메시지는 Amazon WorkMail 스팸 탐지 시스템에서 확인한 후 전달됩니다. 스팸 이메일은 정크 폴더로 전달됩니다. 기타 모든 이메일 메시지는 받은 편지함으로 전달됩니다. 덜 구체적인 발신자 패턴을 사용하는 기타 이메일 흐름 규칙은 무시됩니다. 도메인 기반 이메일 흐름 규칙에 예외를 추가하려면 더 구체적인 발신자 패턴을 사용하여 기본 작업을 구성합니다. 자세한 내용은 발신자 및 수신자 패턴 단원을 참조하십시오.
정크 폴더로 전달 안 함	이메일 메시지는 Amazon WorkMail 스팸 탐지 시스템에서 스팸으로 식별된 경우에도 항상 사용자의 받은 편지함으로 전송됩니다.

작업	설명
	Important 기본 스팸 감지 시스템을 우회하면 지정된 주소의 위험성이 높은 콘텐츠에 사용자가 노출될 수 있습니다.
실행 AWS Lambda	이메일 메시지를 사용자의 받은 편지함으로 전송하기 전에 또는 전송 중에 처리를 위해 Lambda 함수에 전달합니다.

Note

인바운드 이메일은 먼저 SES Amazon으로 전송된 다음 WorkMail Amazon으로 전송됩니다. Amazon이 수신 이메일 메시지를 SES 차단하면 규칙 조치가 적용되지 않습니다. 예를 들어 Amazon은 알려진 바이러스가 탐지되거나 명시적인 IP 필터링 규칙 때문에 이메일 메시지를 SES 차단합니다. Default(기본), Deliver to junk folder(정크 폴더로 전달) 또는 Never deliver to junk folder(정크 폴더로 전달 안 함)와 같은 규칙 작업을 지정하면 아무 영향도 미치지 않습니다.

아웃바운드 이메일 규칙 작업

아웃바운드 이메일 흐름 규칙을 사용하여 SMTP 게이트웨이를 통해 이메일을 보내거나 발신자가 지정된 수신자에게 이메일 메시지를 보내지 못하도록 차단할 수 있습니다. 게이트웨이에 SMTP 대한 자세한 내용은 을 참조하십시오. 게이트웨이 활성화 SMTP

또한 아웃바운드 이메일 흐름 규칙을 사용하여 이메일 메시지가 전송된 후 처리를 위해 AWS Lambda 함수에 이메일을 전달할 수 있습니다. Lambda에 대한 자세한 내용은 AWS Lambda 개발자 안내서를 참조하세요.

다음 규칙 작업은 아웃바운드 이메일이 처리되는 방식을 정의합니다. 각 규칙에 대해 다음 작업 중 하나와 함께 발신자 및 수신자 패턴을 지정합니다.

작업	설명
기본값	이메일 메시지가 정상 흐름을 통해 전송됩니다.
이메일 삭제	이메일 메시지가 삭제됩니다. 이메일이 전송되지 않고, 발신자에게 알리지 않습니다.
반송 메일 응답 보내기	이메일 메시지가 전송되지 않고, 관리자가 이메일 메시지를 차단했다는 메시지를 발신자에게 보냅니다.
게이트웨이로 가는 SMTP 경로	이메일 메시지는 구성된 SMTP 게이트웨이를 통해 전송됩니다.
Lambda 실행	이메일 메시지가 전송되기 전이나 전송 중에 처리를 위해 이메일 메시지를 Lambda 함수에 전달합니다.

발신자 및 수신자 패턴

이메일 흐름 규칙은 특정 이메일 주소나 특정 도메인 또는 도메인 세트의 모든 이메일 주소에 적용할 수 있습니다. 패턴을 정의하여 규칙을 적용할 이메일 주소를 결정합니다.

발신자 및 수신자 패턴은 다음 형식 중 하나입니다.

- 이메일 주소는 단일 이메일 주소와 일치합니다. 예를 들어 다음과 같습니다.

```
mailbox@example.com
```

- 도메인 이름은 도메인의 모든 이메일 주소와 일치합니다. 예를 들어 다음과 같습니다.

```
example.com
```

- 와일드카드 도메인은 해당 도메인과 모든 하위 도메인의 모든 이메일 주소와 일치합니다. 와일드카드는 도메인 앞에만 나타납니다. 예를 들면 다음과 같습니다.

```
*.example.com
```

- 별표는 모든 도메인의 모든 이메일 주소와 일치합니다.

```
*
```

> **Note**
>
> + 기호는 발신자 또는 수신자 패턴 내에서 유효하지 않습니다.

규칙 하나에 대해 여러 패턴을 지정할 수 있습니다. 자세한 내용은 인바운드 이메일 규칙 작업 및 아웃바운드 이메일 규칙 작업 단원을 참조하세요.

인바운드 이메일 메시지의 `Sender` 또는 `From` 헤더가 특정 패턴과 일치하는 경우 인바운드 이메일 흐름 규칙이 적용됩니다. 있는 경우 `Sender` 주소가 먼저 일치됩니다. `Sender` 헤더가 없거나 `Sender` 헤더가 어떠한 규칙과도 일치하지 않는 경우에는 그 다음으로 `From` 주소가 일치됩니다. 다양한 규칙과 일치하는 이메일 메시지에 대해 여러 수신자가 있는 경우 일치된 수신자에 대해 각 규칙이 적용됩니다.

아웃바운드 이메일 메시지의 수신자 및 `Sender` 또는 `From` 헤더가 특정 패턴과 일치하는 경우 아웃바운드 이메일 흐름 규칙이 적용됩니다. 다양한 규칙과 일치하는 이메일 메시지에 대해 여러 수신자가 있는 경우 일치된 수신자에 대해 각 규칙이 적용됩니다.

여러 개의 규칙이 일치하는 경우 가장 구체적인 규칙의 작업이 적용됩니다. 예를 들면 특정 이메일 주소에 대한 규칙이 전체 도메인에 대한 규칙보다 우선합니다. 여러 규칙에 동일한 구체성이 있는 경우 가장 제한적인 작업이 적용됩니다. 예를 들면 Drop(삭제) 작업이 Bounce(반송) 작업보다 우선합니다. 작업에 대한 우선순위 순서는 인바운드 이메일 규칙 작업 및 아웃바운드 이메일 규칙 작업에 나열된 순서와 동일합니다.

> **Note**
>
> 삭제 또는 반송 메일 작업을 사용해 발신자 패턴이 중첩된 규칙을 생성하는 경우 주의해야 합니다. 예기치 않은 우선순위 순서 지정으로 인해 많은 수의 인바운드 이메일 메시지가 전달되지 않을 수 있습니다.

이메일 흐름 규칙 생성

이메일 흐름 규칙은 수신 및 발신 이메일 메시지에 규칙 작업을 적용합니다. 메시지가 지정된 패턴과 일치하는 경우 작업이 적용됩니다. 새 이메일 흐름 규칙은 즉시 적용됩니다.

이메일 흐름 규칙을 생성하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 조직 설정을 선택합니다.

   조직 설정 페이지가 나타나고 탭 세트가 표시됩니다. 이 페이지에서 인바운드 또는 아웃바운드 규칙을 만들 수 있습니다. 다음 단계에서는 두 유형을 모두 생성하는 방법에 대해 설명합니다.

   인바운드 규칙을 만들려면

   1. 인바운드 규칙 탭을 선택한 후 생성을 선택합니다.
   2. 규칙 이름 상자에 고유한 이름을 입력합니다.
   3. 작업에서 목록을 열고 작업을 선택합니다. 목록의 각 항목에는 설명이 포함되며 일부는 자세히 알아보기 링크를 제공합니다.

      > **Note**
      >
      > Run Lambda 작업을 선택하면 추가 컨트롤이 나타납니다. 이러한 컨트롤 사용에 대한 자세한 내용은 다음 섹션인 AWS Lambda 아마존을 위한 구성 WorkMail을 참조하세요.

   4. 발신자 도메인 또는 주소에 규칙을 적용할 발신자 도메인 또는 주소를 입력합니다.
   5. 대상 도메인 또는 주소에서 대상 도메인과 이메일 주소를 원하는 대로 조합하여 입력합니다.
   6. 생성(Create)을 선택합니다.

   아웃바운드 규칙을 만들려면

   1. 아웃바운드 규칙 탭을 선택하고 생성을 선택합니다.
   2. 규칙 이름 상자에 고유한 이름을 입력합니다.
   3. 작업에서 목록을 열고 작업을 선택합니다. 목록의 각 항목에는 설명이 포함되며 일부는 자세히 알아보기 링크를 제공합니다.

> **Note**
>
> Lambda 실행 작업을 선택하면 추가 컨트롤이 나타납니다. 해당 제어에 대한 자세한 내용은 다음 섹션인 AWS Lambda 아마존을 위한 구성 WorkMail을 참조하세요.

4. 발신자 도메인 또는 주소에서 유효한 발신자 도메인과 이메일 주소를 원하는 대로 조합하여 입력합니다.
5. 대상 도메인 또는 주소에서 유효한 대상 도메인과 이메일 주소를 원하는 대로 조합하여 입력합니다.
6. 생성(Create)을 선택합니다.

생성한 새 이메일 흐름 규칙을 테스트할 수 있습니다. 자세한 내용은 이메일 흐름 규칙 테스트 단원을 참조하십시오.

이메일 흐름 규칙 편집

이메일 메시지에 대한 하나 이상의 규칙 작업을 변경해야 할 때마다 이메일 흐름 규칙을 편집합니다. 이 섹션의 단계는 수신 및 발신 이메일 메시지에 적용됩니다.

이메일 흐름 규칙을 편집하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 조직 설정을 선택합니다.

   조직 설정 페이지가 나타나고 탭 세트가 표시됩니다.
4. 인바운드 규칙 또는 아웃바운드 규칙 탭을 선택합니다.
5. 변경할 규칙 옆에 있는 라디오 버튼을 선택한 다음 편집을 선택합니다.
6. 필요에 따라 규칙의 동작을 변경한 다음 저장을 선택합니다.

AWS Lambda 아마존을 위한 구성 WorkMail

인바운드 및 아웃바운드 이메일 흐름 규칙에서 Run Lambda 작업을 사용하여 규칙과 일치하는 이메일 메시지를 처리를 위해 함수에 전달합니다. AWS Lambda

Amazon에서 Lambda 실행 작업을 수행하려면 다음 구성 중에서 선택하십시오. WorkMail

동기식 Lambda 실행 구성

> 흐름 규칙과 일치하는 이메일 메시지는 전송되기 전에 처리를 위해 Lambda 함수로 전달됩니다. 이 구성을 사용하여 이메일 콘텐츠를 수정할 수 있습니다. 또한 다양한 사용 사례에 맞게 인바운드 또는 아웃바운드 이메일 흐름을 제어할 수 있습니다. 예를 들어, Lambda 함수에 전달된 규칙은 민감한 이메일 메시지의 전송을 차단하거나 첨부 파일을 제거하거나 고지 사항을 추가할 수 있습니다.

비동기식 Lambda 실행 구성

> 흐름 규칙과 일치하는 이메일 메시지는 전송되는 동안 처리를 위해 Lambda 함수로 전달됩니다. 이 구성은 이메일 전송에 영향을 주지 않으며 인바운드 또는 아웃바운드 이메일 메시지에 대한 지표 수집과 같은 작업에 사용됩니다.

동기식 구성을 선택하든 비동기식 구성을 선택하든 상관없이 Lambda 함수에 전달된 이벤트 객체에는 인바운드 또는 아웃바운드 이메일 이벤트에 대한 메타데이터가 포함됩니다. 메타데이터의 메시지 ID를 사용하여 이메일 메시지의 전체 콘텐츠에 액세스할 수도 있습니다. 자세한 내용은 를 사용하여 메시지 콘텐츠 검색 AWS Lambda 단원을 참조하십시오. 이메일 이벤트에 대한 자세한 내용은 Lambda 이벤트 데이터 다음을 참조하십시오.

인바운드 및 아웃바운드 이메일 흐름 규칙에 대한 자세한 내용은 이메일 흐름 관리 단원을 참조하십시오. Lambda에 대한 자세한 내용은 AWS Lambda 개발자 안내서를 참조하세요.

> **Note**
>
> 현재 Lambda 이메일 흐름 규칙은 구성 중인 Amazon 조직과 AWS 계정 동일한 AWS 리전에 있는 Lambda 함수만 참조합니다. WorkMail

AWS Lambda 아마존용 시작하기 WorkMail

WorkMailAmazon에서 사용을 시작하려면 에서 WorkMail AWS Serverless Application Repository Hello World Lambda 함수를 사용자 AWS Lambda 계정으로 배포하는 것이 좋습니다. 이 함수에는 필요한 모든 리소스와 사용자를 위해 구성된 권한이 있습니다. 더 많은 예를 보려면 의 리포지토리를 참조하십시오. amazon-workmail-lambda-templates GitHub

Lambda 함수를 직접 생성하기로 선택한 경우 () 를 사용하여 AWS Command Line Interface 권한을 구성해야 합니다.AWS CLI다음 예제 명령에서 사용하려면 다음을 수행합니다.

- `MY_FUNCTION_NAME`을 Lambda 함수의 이름으로 바꿉니다.
- Amazon WorkMail AWS 지역으로 `REGION` 대체하십시오. 사용 가능한 Amazon WorkMail 지역에는 `us-east-1` (미국 동부 (버지니아 북부)), `us-west-2` (미국 서부 (오레곤)), `eu-west-1` (유럽 (아일랜드)) 가 포함됩니다.
- `AWS_ACCOUNT_ID`를 12자리 AWS 계정 ID로 바꿉니다.
- Amazon WorkMail 조직 `WORKMAIL_ORGANIZATION_ID` ID로 바꾸십시오. 조직 페이지의 조직 카드에서 찾을 수 있습니다.

```
aws --region REGION lambda add-permission --function-name MY_FUNCTION_NAME
--statement-id AllowWorkMail
--action "lambda:InvokeFunction"
--principal workmail.REGION.amazonaws.com
--source-arn
 arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID
```

사용에 대한 자세한 내용은 사용 AWS Command Line Interface 설명서를 참조하십시오. AWS CLI

동기식 Lambda 실행 규칙 구성

동기식 Lambda 실행 규칙을 구성하려면 Lambda 실행 작업이 포함된 이메일 흐름 규칙을 생성하고 동기식 실행 확인란을 선택합니다. 메일 흐름 규칙 생성에 대한 자세한 내용은 이메일 흐름 규칙 생성 단원을 참조하십시오.

동기 규칙 생성을 완료하려면 Lambda Amazon 리소스 이름 ARN () 을 추가하고 다음 옵션을 구성합니다.

폴백 작업

Lambda 함수 실행에 실패할 경우 Amazon이 WorkMail 적용하는 작업입니다. 이 작업은 플래그가 설정되지 않은 경우 Lambda 응답에서 생략된 모든 수신자에게도 적용됩니다. allRecipients 폴백 작업은 다른 Lambda 작업이 될 수 없습니다.

규칙 제한 시간(분)

WorkMail Amazon에서 함수를 호출하지 못할 경우 Lambda 함수를 재시도하는 기간입니다. 폴백 작업은 이 기간이 끝날 때 적용됩니다.

> **Note**
>
> 동기식 Lambda 실행 규칙은 * 대상 조건만 지원합니다.

Lambda 이벤트 데이터

Lambda 함수는 다음 이벤트 데이터를 사용하여 트리거됩니다. 데이터 표시는 Lambda 함수에 사용되는 프로그래밍 언어에 따라 다릅니다.

```
{
    "summaryVersion": "2018-10-10",
    "envelope": {
        "mailFrom" : {
            "address" : "from@example.com"
        },
        "recipients" : [
           { "address" : "recipient1@example.com" },
           { "address" : "recipient2@example.com" }
        ]
    },
    "sender" : {
        "address" :  "sender@example.com"
    },
    "subject" : "Hello From Amazon WorkMail!",
    "messageId": "00000000-0000-0000-0000-000000000000",
    "invocationId": "00000000000000000000000000000000",
    "flowDirection": "INBOUND",
    "truncated": false
}
```

JSON이벤트에는 다음 데이터가 포함됩니다.

summaryVersion

LambdaEventData의 버전 번호입니다. LambdaEventData에서 이전 버전과 호환되지 않는 변경을 한 경우에만 업데이트됩니다.

envelope

다음 필드가 포함된 이메일 메시지의 엔벌로프입니다.

mailFrom

보낸 사람 주소 - 일반적으로 이메일 메시지를 보낸 사용자의 이메일 주소입니다. 사용자가 다른 사용자 또는 다른 사용자를 대신하여 이메일 메시지를 보낸 경우 mailFrom필드는 실제 발신자의 이메일 주소가 아니라 이메일 메시지를 대신 보낸 사용자의 이메일 주소를 반환합니다.

recipients

모든 수신자 이메일 주소의 목록입니다. WorkMail Amazon은 To, CC 또는 To를 구분하지 않습니다 BCC.

> **Note**
>
> 인바운드 이메일 흐름 규칙의 경우 이 목록에는 규칙을 생성한 Amazon WorkMail 조직의 모든 도메인에 있는 수신자가 포함됩니다. Lambda 함수는 발신자의 SMTP 각 대화에 대해 개별적으로 호출되며, 수신자 필드에 해당 대화의 수신자가 나열됩니다. SMTP 외부 도메인의 수신자는 포함되지 않습니다.

sender

다른 사용자를 대신하여 이메일 메시지를 전송한 사용자의 이메일 주소입니다. 이 필드는 다른 사용자를 대신하여 이메일 메시지를 전송할 때만 설정됩니다.

subject

이메일 제목줄입니다. 256자 제한을 초과할 경우 잘립니다.

messageId

Amazon WorkMail Message Flow를 사용할 때 이메일 메시지의 전체 콘텐츠에 액세스하는 데 사용되는 고유 SDK ID입니다.

invocationId

고유한 Lambda 호출의 ID입니다. Lambda 함수가 같은 함수에 대해 두 번 이상 호출되는 경우에도 이 ID는 동일하게 유지됩니다. LambdaEventData 재시도를 감지하고 중복을 방지하는 데 사용합니다.

flowDirection

이메일 흐름의 방향 (또는 INBOUND) 을 나타냅니다. OUTBOUND

truncated

제목 행 길이가 아니라 페이로드 크기에 적용됩니다. `true`인 경우 페이로드 크기가 128KB 제한을 초과하면 제한을 충족하기 위해 수신자 목록이 잘립니다.

동기식 Lambda 실행 응답 스키마

동기식 Run Lambda 작업이 포함된 이메일 흐름 규칙이 인바운드 또는 아웃바운드 이메일 메시지와 일치하면 Amazon은 구성된 Lambda 함수를 WorkMail 호출하고 응답을 기다린 후 이메일 메시지에 조치를 취합니다. Lambda 함수는 작업, 작업 유형, 적용 가능한 파라미터 및 작업이 적용되는 수신자를 나열하는 미리 정의된 스키마에 따라 응답을 반환합니다.

다음 예는 동기식 Lambda 실행 응답을 보여줍니다. 응답은 Lambda 함수에 사용되는 프로그래밍 언어에 따라 다릅니다.

```
{
    "actions": [
      {
        "action" : {
          "type": "string",
          "parameters": { various }
        },
        "recipients": [list of strings],
        "allRecipients": boolean
      }
    ]
}
```

응답에는 JSON 다음 데이터가 포함됩니다.

작업

수신자에 대해 수행할 작업입니다.

type

작업 유형입니다. 비동기식 Lambda 실행 작업에 대해 작업 유형이 반환되지 않습니다.

인바운드 규칙 작업 유형에는 BOUNCE,, BYPASS_ SPAM _ DROPDEFAULTCHECK, MOVEJUNK_TO_가 포함됩니다. 자세한 내용은 인바운드 이메일 규칙 작업 단원을 참조하십시오.

아웃바운드 규칙 작업 유형에는,, 등이 BOUNCE있습니다. DROPDEFAULT 자세한 내용은 아웃바운드 이메일 규칙 작업 단원을 참조하십시오.

파라미터

추가 작업 파라미터입니다. 키 bounceMessage및 값 문자열이 있는 JSON 객체로서 BOUNCE작업 유형에 지원됩니다. 이 반송 메일 메시지는 반송 이메일 메시지를 생성하는 데 사용됩니다.

recipients

작업을 수행해야 하는 이메일 주소의 목록입니다. 원래 수신자 목록에 포함되지 않은 경우에도 새 수신자를 응답에 추가할 수 있습니다. 액션에 true인 경우 allRecipients이 필드는 필수가 아닙니다.

> **Note**
>
> 인바운드 이메일에 대해 Lambda 작업이 호출되면 조직의 새 수신자만 추가할 수 있습니다. 새 수신자가 응답에 로 추가됩니다. BCC

allRecipients

true인 경우 Lambda 응답에서 다른 특정 작업이 적용되지 않는 모든 수신자에게 작업을 적용합니다.

동기식 Lambda 실행 작업 제한

Amazon이 동기식 Lambda 실행 작업에 대해 Lambda WorkMail 함수를 호출할 때는 다음과 같은 제한이 적용됩니다.

- Lambda 함수는 15초 내에 응답하거나 실패한 호출로 처리되어야 합니다.

> **Note**
>
> 시스템은 사용자가 지정한 규칙 제한 시간 간격 동안 간접 호출을 재시도합니다.

- 최대 256KB의 Lambda 함수 응답이 허용됩니다.
- 응답에는 최대 10개의 고유 작업이 허용됩니다. 10개 이상의 작업에는 구성된 폴백 작업이 적용됩니다.
- 아웃바운드 Lambda 함수에는 최대 500명의 수신자가 허용됩니다.
- 규칙 제한 시간의 최대값은 240분입니다. 최소값인 0으로 구성된 경우 Amazon에서 폴백 작업을 WorkMail 적용하기 전에 재시도할 필요가 없습니다.

동기식 Lambda 실행 작업 실패

Amazon이 오류, 잘못된 응답 또는 Lambda 시간 초과로 인해 Lambda 함수를 호출할 WorkMail 수 없는 경우 WorkMail Amazon은 지수 백오프를 사용하여 호출을 재시도합니다. 지수 백오프는 규칙 제한 시간이 완료될 때까지 처리 속도를 줄입니다. 그런 다음 이메일 메시지의 모든 수신자에게 폴백 작업이 적용 됩니다. 자세한 내용은 동기식 Lambda 실행 규칙 구성 단원을 참조하십시오.

동기식 Lambda 실행 응답 예

다음 예에서는 일반적인 동기식 Lambda 실행 응답의 구조를 보여줍니다.

Example : 이메일 메시지에서 지정된 수신자 제거

다음 예에서는 이메일 메시지에서 수신자를 제거하기 위한 동기식 Lambda 실행 응답의 구조를 보여줍니다.

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      },
      {
        "action": {
          "type": "DROP"
        },
        "recipients": [
          "drop-recipient@example.com"
        ]
      }
    ]
}
```

Example : 사용자 지정 이메일 메시지가 포함된 반송 메일

다음 예에서는 사용자 지정 이메일 메시지로 반송하기 위한 동기식 Lambda 실행 응답의 구조를 보여줍니다.

```
{
    "actions" : [
```

```
      {
        "action" : {
          "type": 'BOUNCE',
          "parameters": {
            "bounceMessage" : "Email in breach of company policy."
          }
        },
        "allRecipients": true
      }
    ]
}
```

Example : 이메일 메시지에 수신자 추가

다음 예에서는 이메일 메시지에 수신자를 추가하기 위한 동기식 Lambda 실행 응답의 구조를 보여줍니다. 이렇게 해도 이메일 메시지의 받는 사람 또는 CC 필드는 업데이트되지 않습니다.

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
        },
        "recipients": [
          "new-recipient@example.com"
         ]
      },
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      }
    ]
}
```

Lambda 실행 작업을 위한 Lambda 함수를 생성할 때 사용할 추가 코드 예제는 Amazon Lambda 템플릿을 참조하십시오. WorkMail

Amazon에서 Lambda를 사용하는 방법에 대한 추가 정보 WorkMail

Lambda 함수를 트리거하는 이메일 메시지의 전체 콘텐츠에도 액세스할 수 있습니다. 자세한 내용은 를 사용하여 메시지 콘텐츠 검색 AWS Lambda 단원을 참조하십시오.

를 사용하여 메시지 콘텐츠 검색 AWS Lambda

WorkMailAmazon의 이메일 흐름을 관리하는 AWS Lambda 함수를 구성한 후에는 Lambda를 사용하여 처리되는 이메일 메시지의 전체 콘텐츠에 액세스할 수 있습니다. WorkMailAmazon용 Lambda를 시작하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS Lambda 아마존을 위한 구성 WorkMail

이메일 메시지의 전체 콘텐츠에 액세스하려면 Amazon WorkMail Message Flow에서 `GetRawMessageContent` 작업을 사용하십시오API. 호출 시 Lambda 함수로 전달되는 이메일 메시지 ID는 요청을 에 보냅니다. API 그러면 이메일 메시지의 전체 MIME 내용으로 API 응답합니다. 자세한 내용은 Amazon WorkMail API레퍼런스의 Amazon WorkMail 메시지 흐름을 참조하십시오.

다음 예제는 Python 런타임 환경을 사용하는 Lambda 함수로 전체 메시지 콘텐츠를 검색하는 방법을 보여줍니다.

> **Tip**
>
> 에서 AWS Serverless Application Repository Amazon WorkMail Hello World Lambda 함수를 사용자 계정으로 배포하는 것으로 시작하면 시스템에서 필요한 모든 리소스와 권한을 포함하는 Lambda 함수를 사용자 계정에 생성합니다. 그런 다음 사용 사례에 따라 Lambda 함수에 비즈니스 로직을 추가할 수 있습니다.

```
import boto3
import email
import os

def email_handler(event, context):
    workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
    msg_id = event['messageId']
    raw_msg = workmail.get_raw_message_content(messageId=msg_id)

    parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())
    print(parsed_msg)
```

전송 중인 메시지의 콘텐츠를 분석하는 방법에 대한 자세한 예는 의 리포지토리를 참조하십시오. amazon-workmail-lambda-templates GitHub

> **Note**
>
> Amazon WorkMail Message API Flow를 사용하여 전송 중인 이메일 메시지에 액세스할 수 있습니다. 전송 또는 수신 후 24시간 이내에만 메시지에 액세스할 수 있습니다. 사용자 사서함의 메시지에 프로그래밍 방식으로 액세스하려면 WorkMail Amazon에서 지원하는 다른 프로토콜 중 하나 (예: IMAP 또는 Exchange Web Services (EWS) 를 사용하십시오.

AWSLambda를 사용하여 메시지 콘텐츠 업데이트

이메일 흐름을 관리하도록 동기 AWS Lambda 함수를 구성한 후 Amazon Message API Flow의 `PutRawMessageContent` 작업을 사용하여 전송 중인 이메일 WorkMail 메시지의 콘텐츠를 업데이트할 수 있습니다. WorkMailAmazon용 Lambda 함수를 시작하는 방법에 대한 자세한 내용은 을 참조하십시오. 동기식 Lambda 실행 규칙 구성 에 대한 자세한 내용은 API 을 참조하십시오. PutRawMessageContent

> **Note**
>
> boto3 1.17.8이 PutRawMessageContent API 필요합니다. 그렇지 않으면 Lambda 함수에 계층을 추가할 수 있습니다. 올바른 boto3 버전을 다운로드하려면 의 boto 페이지를 참조하십시오. GitHub 계층 추가에 대한 자세한 내용은 계층을 사용하도록 함수 구성을 참조하세요.
> 예제 계층: `"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`. 이 예시에서는 `${AWS::Region}`을 us-east-1과 같은 적절한 AWS 리전으로 대체하세요.

> **Tip**
>
> 먼저 서버리스 AWS 애플리케이션 리포지토리에서 Amazon WorkMail Hello World Lambda 함수를 계정에 배포하면 시스템이 필요한 리소스 및 권한을 포함하는 Lambda 함수를 사용자 계정에 생성합니다. 그런 다음 사용 사례에 따라 Lambda 함수에 비즈니스 로직을 추가할 수 있습니다.

진행하면서 다음 사항을 기억해야 합니다.

- 를 사용하여 원본 메시지 콘텐츠를 검색할 GetRawMessageContentAPI수 있습니다. 자세한 정보는 를 사용하여 메시지 콘텐츠 검색 AWS Lambda 섹션을 참조하세요.

- 원본 메시지를 찾았으면 MIME 내용을 변경하십시오. 작업을 마치면 계정의 Amazon Simple Storage Service(S3) 버킷에 메시지를 업로드합니다. S3 버킷이 Amazon WorkMail 작업과 AWS 계정 동일한 것을 사용하고 API 호출과 동일한 AWS 지역을 사용하는지 확인하십시오.
- Amazon에서 요청을 WorkMail 처리하려면 S3 버킷에 올바른 정책이 있어야 S3 객체에 액세스할 수 있습니다. 자세한 내용은 Example S3 policy 단원을 참조하십시오.
- PutRawMessageContentAPI를 사용하여 업데이트된 메시지 콘텐츠를 Amazon으로 다시 보낼 수 WorkMail 있습니다.

> **Note**
>
> PutRawMessageContentAPI이를 통해 업데이트된 메시지의 MIME 내용이 표준과 RawMessageContent데이터 유형에 언급된 RFC 기준을 충족하는지 확인할 수 있습니다. Amazon WorkMail 조직으로 인바운드되는 이메일이 항상 이러한 표준을 충족하는 것은 아니므로 PutRawMessageContent API 거부될 수 있습니다. 이러한 경우 반환된 오류 메시지를 참조하여 문제 해결 방법에 대한 자세한 내용을 확인할 수 있습니다.

Example 예제 S3 정책

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Service": "workmail.REGION.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::My-Test-S3-Bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS_ACCOUNT_ID"
                },
                "Bool": {
                    "aws:SecureTransport": "true"
                },
                "ArnLike": {
```

```
                    "aws:SourceArn":
 "arn:aws:workmailmessageflow:REGION:AWS_ACCOUNT_ID:message/WORKMAIL_ORGANIZATION_ID/*"
                }
            }
        }
    ]
}
```

다음 예제는 Lambda 함수가 Python 런타임을 사용하여 전송 중인 이메일 메시지의 제목을 업데이트하는 방법을 보여줍니다.

```
    import boto3
    import os
    import uuid
    import email

    def email_handler(event, context):
        workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
        s3 = boto3.client('s3', region_name=os.environ["AWS_REGION"])

        msg_id = event['messageId']
        raw_msg = workmail.get_raw_message_content(messageId=msg_id)
        parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())

        # Updating subject. For more examples, see https://github.com/aws-samples/
amazon-workmail-lambda-templates.
        parsed_msg.replace_header('Subject', "New Subject Updated From Lambda")

        # Store updated email in S3
        key = str(uuid.uuid4());
        s3.put_object(Body=parsed_msg.as_bytes(), Bucket="amzn-s3-demo-bucket",
 Key=key)

        # Update the email in WorkMail
        s3_reference = {
            'bucket': "amzn-s3-demo-bucket",
            'key': key
        }
        content = {
            's3Reference': s3_reference
        }
```

```
        workmail.put_raw_message_content(messageId=msg_id, content=content)
```

전송 중인 메시지의 콘텐츠를 분석하는 방법에 대한 더 많은 예를 보려면 의 리포지토리를 참조하십시오. amazon-workmail-lambda-templates GitHub

Amazon WorkMail 메시지 플로우에 대한 액세스 관리 API

AWS Identity and Access Management (IAM) 정책을 사용하여 Amazon WorkMail 메시지 흐름에 대한 액세스를 관리합니다API.

Amazon WorkMail Message Flow는 단일 리소스 유형인 전송 중인 이메일 메시지와 함께 API 작동합니다. 전송 중인 각 이메일 메시지에는 고유한 Amazon 리소스 이름 (ARN) 이 연결되어 있습니다.

다음 예는 전송 중인 이메일 메시지와 ARN 관련된 구문을 보여줍니다.

```
arn:aws:workmailmessageflow:region:account:message/organization/context/messageID
```

이전 예제에서 변경 가능한 필드는 다음과 같습니다.

- 지역 — Amazon WorkMail 조직의 AWS 지역입니다.
- 계정 — Amazon WorkMail 조직의 AWS 계정 ID입니다.
- 조직 — 아마존 WorkMail 조직 ID.
- 컨텍스트 – 메시지가 `incoming` 사용자 조직으로 전송되는지 또는 `outgoing` 사용자 조직에서 전송되는지 여부를 나타냅니다.
- 메시지 ID – 사용자의 Lambda 함수에 입력으로 전달되는 고유한 이메일 메시지 ID입니다.

다음 IDs 예에는 전송 중인 수신 이메일 메시지와 ARN 관련된 예가 포함되어 있습니다.

```
arn:aws:workmailmessageflow:us-east-1:111122223333:message/m-
n1pq2345678r901st2u3vx45x6789yza/incoming/d1234567-8e90-1f23-456g-hjk7lmnop8q9
```

전송 중인 Amazon WorkMail 메시지에 대한 액세스를 관리하기 위해 IAM 사용자 정책 `Resource` 섹션의 ARNs 리소스로 사용할 수 있습니다.

Amazon WorkMail 메시지 흐름 액세스에 대한 예제 IAM 정책

다음 예제 정책은 조직 내 모든 Amazon WorkMail 조직에 대한 모든 인바운드 및 아웃바운드 메시지에 대한 전체 읽기 액세스 권한을 IAM 엔티티에 부여합니다. AWS 계정

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

여러 조직이 있는 경우 하나 이상의 조직에 대한 액세스를 제한할 수도 있습니다. AWS 계정이 기능은 특정 조직에 특정 Lambda 함수만 사용해야 할 경우에 유용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/*",
            "Effect": "Allow"
        }
    ]
}
```

`incoming` 조직으로 전송되거나 `outgoing` 조직에서 전송되는지에 따라 메시지에 대한 액세스 권한을 부여할 수도 있습니다. 이렇게 하려면 한정어 `incoming` 또는 `outgoing` 를 ARN 사용하십시오.

다음 예제 정책은 조직으로 수신되는 메시지에 대한 액세스 권한만 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
```

```
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/incoming/*",
            "Effect": "Allow"
        }
    ]
}
```

다음 예제 정책은 조직의 모든 Amazon WorkMail 조직에 대한 모든 인바운드 및 아웃바운드 메시지에 대한 전체 읽기 및 업데이트 액세스 권한을 IAM 엔티티에 부여합니다. AWS 계정

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent",
                "workmailmessageflow:PutRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

이메일 흐름 규칙 테스트

현재 규칙 구성을 점검하기 위해 특정 이메일 주소에 대해 구성이 작동하는 방식을 테스트할 수 있습니다.

이메일 흐름 규칙을 테스트하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 Organization settings(조직 설정), Inbound/Outbound rules(인바운드/아웃바운드 규칙)를 선택합니다.

4. Test configuration(구성 테스트) 옆에 테스트할 발신자 및 수신자의 전체 이메일 주소를 모두 입력합니다.
5. 테스트를 선택합니다. 입력한 이메일 주소에 대해 수행할 작업이 표시됩니다.

이메일 흐름 규칙 제거

이메일 흐름 규칙을 제거하면 해당 변경 사항이 즉시 적용됩니다.

이메일 흐름 규칙을 제거하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 Organization settings(조직 설정), Inbound/Outbound rules(인바운드/아웃바운드 규칙)를 선택합니다.
4. 규칙을 선택하고 [Remove]를 선택합니다.
5. 확인 프롬프트에서 제거를 선택합니다.

수신 이메일에 DMARC 정책 적용

이메일 도메인은 보안을 위해 도메인 이름 시스템 () 레코드를 사용합니다. DNS 스푸핑 또는 피싱과 같은 일반적인 공격으로부터 사용자를 보호합니다. DNS레코드에는 대개 이메일을 보내는 도메인 소유자가 설정하는 도메인 기반 메시지 인증, 보고 및 적합성 (DMARC) 레코드가 포함됩니다. DMARC레코드에는 이메일 검사에 실패할 경우 취할 조치를 지정하는 정책이 포함됩니다. DMARC 조직으로 보내는 이메일에 DMARC 정책을 적용할지 여부를 선택할 수 있습니다.

새 Amazon WorkMail 조직에는 기본적으로 DMARC 강제 적용 기능이 켜져 있습니다.

DMARC단속 기능을 켜려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.

2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 조직 설정을 선택합니다. 조직 설정 페이지가 나타나고 탭 세트가 표시됩니다.
4. DMARC탭을 선택한 다음 편집을 선택합니다.
5. DMARC적용 슬라이더를 켜진 위치로 이동합니다.
6. DMARC강제 적용을 켜면 보낸 사람의 도메인 구성에 따라 인바운드 이메일이 삭제되거나 격리될 수 있다는 점을 인정함 옆의 확인란을 선택합니다.
7. 저장(Save)을 선택합니다.

강제 적용을 끄려면 DMARC

- 이전 섹션의 단계를 따르되, DMARC적용 슬라이더를 끄기 위치로 이동하십시오.

이메일 이벤트 로깅을 사용하여 DMARC 단속 추적하기

DMARC강제 적용을 설정하면 보낸 사람이 도메인을 구성한 방식에 따라 인바운드 이메일이 삭제되거나 스팸으로 표시될 수 있습니다. 발신자가 이메일 도메인을 잘못 구성한 경우, 사용자가 적법한 이메일의 수신을 중단할 수 있습니다. 사용자에게 전송되지 않는 이메일이 있는지 확인하려면 Amazon WorkMail 조직에 대한 이메일 이벤트 로깅을 활성화할 수 있습니다. 그런 다음 발신자 정책에 따라 필터링된 인바운드 이메일에 대해 이메일 이벤트 로그를 쿼리할 수 있습니다. DMARC

이메일 이벤트 로깅을 사용하여 DMARC 시행을 추적하기 전에 Amazon WorkMail 콘솔에서 이메일 이벤트 로깅을 활성화하십시오. 로그 데이터를 최대한 활용하려면, 이메일 이벤트가 기록되는 동안 잠시 시간을 보내십시오. 자세한 정보와 지침은 the section called “이메일 이벤트 로깅 켜기”단원을 참조하세요.

이메일 이벤트 로깅을 사용하여 DMARC 집행을 추적하려면

1. CloudWatch Insights 콘솔의 로그에서 Insights를 선택합니다.
2. 로그 그룹 선택에서 Amazon WorkMail 조직의 로그 그룹을 선택합니다. 예: /aws/workmail/events/organization-alias.
3. 쿼리할 기간을 선택합니다.
4. 이벤트별 통계 수 () 쿼리를 실행합니다. dmarcPolicy | 필터 이벤트. dmarcVerdict == "" FAIL
5. 쿼리 실행을 선택합니다.

이러한 이벤트에 대한 사용자 지정 지표를 설정할 수도 있습니다. 자세한 내용은 지표 필터 생성을 참조하십시오.

조직 태깅

Amazon WorkMail 조직 리소스에 태그를 지정하면 다음을 수행할 수 있습니다.

- 콘솔에서 조직을 구분하십시오. AWS Billing and Cost Management
- Amazon WorkMail 조직 리소스를 AWS Identity and Access Management (IAM) 권한 정책 설명의 `Resource` 요소에 추가하여 해당 리소스에 대한 액세스를 제어합니다.

Amazon WorkMail 리소스 수준 권한에 대한 자세한 내용은 을 참조하십시오. 리소스 태그에 기반한 액세스 제어에 대한 자세한 내용은 Amazon WorkMail 태그를 기반으로 한 인증 단원을 참조하십시오.

Amazon WorkMail 관리자는 Amazon WorkMail 콘솔을 사용하여 조직에 태그를 지정할 수 있습니다.

Amazon WorkMail 조직에 태그를 추가하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. [Tags]를 선택합니다.
4. 조직 태그에서 새 태그 추가를 선택합니다.
5. 키에 태그를 식별하는 이름을 입력합니다.
6. (선택 사항) 값에 태그의 값을 입력합니다.
7. (선택 사항) 4~6단계를 반복해 조직에 태그를 추가합니다. 최대 50개의 태그를 추가할 수 있습니다.
8. 저장을 선택하여 변경 사항을 저장합니다.

Amazon WorkMail 콘솔에서 조직 태그를 볼 수 있습니다.

개발자는 AWS SDK 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 조직에 태그를 지정할 수도 있습니다. 자세한 내용은 Amazon WorkMail API 참조 또는 `UntagResource` 명령 참조의 `TagResourceListTagsForResource`, 및 AWS CLI 명령을 참조하십시오.

Amazon WorkMail 콘솔을 사용하여 언제든지 조직에서 태그를 제거할 수 있습니다.

Amazon WorkMail 조직에서 태그를 제거하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. [Tags]를 선택합니다.
4. 조직 태그에서 제거할 태그 옆에 있는 제거를 선택합니다.
5. 제출을 선택하여 변경 사항을 저장합니다.

액세스 제어 규칙 작업

Amazon의 액세스 제어 규칙을 WorkMail 통해 관리자는 조직의 사용자 및 가장한 역할에 Amazon에 대한 액세스 권한을 부여하는 방법을 제어할 수 있습니다. WorkMail 각 Amazon WorkMail 조직에는 사용하는 액세스 프로토콜 또는 IP 주소와 상관없이 모든 사용자에게 사서함 액세스 권한을 부여하는 기본 액세스 제어 규칙이 있으며 조직에 추가된 위장 역할도 있습니다. 관리자는 기본 규칙을 편집하거나 자신의 규칙으로 대체하거나, 새 규칙을 추가하거나, 규칙을 삭제할 수 있습니다.

> **Warning**
>
> 관리자가 조직에 대한 모든 액세스 제어 규칙을 삭제하면 Amazon은 조직의 사서함에 대한 모든 액세스를 WorkMail 차단합니다.

관리자는 다음 기준에 따라 액세스를 허용하거나 거부하는 액세스 제어 규칙을 적용할 수 있습니다.

- 프로토콜 - 사서함에 액세스하는 데 사용되는 프로토콜입니다. 예로는 자동 검색,,,, EWSIMAP, Windows용 Outlook SMTPActiveSync, 웹메일 등이 있습니다.
- IP 주소 - 사서함 액세스에 사용되는 IPv4 CIDR 범위입니다.
- Amazon WorkMail 사용자 - 사서함 액세스에 사용되는 조직 내 사용자입니다.
- 위장 역할 - 사서함에 액세스하는 데 사용되는 조직 내 위장 역할입니다. 자세한 내용은 위장 역할 관리 단원을 참조하십시오.

관리자는 사용자의 사서함 및 폴더 사용 권한 외에 액세스 제어 규칙을 적용합니다. 자세한 내용은 Amazon 사용 WorkMail 설명서의 폴더 및 폴더 권한 공유를 참조하십시오 사서함 권한을 사용한 작업.

> **Note**
>
> - Windows용 Outlook에 대한 액세스를 활성화하는 경우 자동 검색 및 EWS 에 대한 액세스도 활성화하는 것이 좋습니다.
> - 액세스 제어 규칙은 Amazon WorkMail 콘솔 또는 SDK 액세스에는 적용되지 않습니다. 대신 AWS Identity and Access Management (IAM) 역할 또는 정책을 사용하십시오. 자세한 내용은 Amazon의 자격 증명 및 액세스 관리 WorkMail 단원을 참조하십시오.

액세스 제어 규칙 생성

Amazon WorkMail 콘솔에서 새 액세스 제어 규칙을 생성합니다.

새 액세스 제어 규칙을 생성하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. Access control rules(액세스 제어 규칙)를 선택합니다.
4. Create rule을 선택합니다.
5. 설명에 규칙에 대한 설명을 입력합니다.
6. 효과에서 허용 또는 거부를 선택합니다. 이렇게 하면 다음 단계에서 선택하는 조건에 따라 액세스가 허용되거나 거부됩니다.
7. 이 규칙은 다음 요청에 적용됩니다…에서 규칙에 적용할 조건(예: 특정 프로토콜, IP 주소, 사용자 또는 위장 역할 포함 또는 제외 여부)을 선택합니다.
8. (선택 사항) IP 주소 범위, 사용자 또는 위장 역할을 입력할 때 규칙에 추가하려면 추가를 선택합니다.
9. Create rule을 선택합니다.

액세스 제어 규칙 편집

Amazon WorkMail 콘솔에서 새 액세스 제어 규칙 및 기본 액세스 제어 규칙을 편집합니다.

액세스 제어 규칙을 편집하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. Access control rules(액세스 제어 규칙)를 선택합니다.
4. 편집할 규칙을 선택합니다.
5. [Edit rule]을 선택합니다.
6. 필요에 따라 설명, 효과 및 조건을 편집합니다.
7. Save changes(변경 사항 저장)를 선택합니다.

> **Important**
>
> 액세스 규칙을 변경하면 영향을 받는 사서함이 업데이트된 규칙을 따르는 데 5분이 걸릴 수 있습니다. 영향을 받는 사서함에 액세스하는 클라이언트는 그 시간 동안 일관되지 않은 동작을 보일 수 있습니다. 하지만 규칙을 테스트하면 즉시 올바른 동작이 표시됩니다. 테스트 규칙에 대한 자세한 내용은 다음 섹션의 단계를 참조하세요.

액세스 제어 규칙 테스트

조직의 액세스 제어 규칙이 어떻게 적용되는지 확인하려면 Amazon WorkMail 콘솔에서 규칙을 테스트하십시오.

조직의 액세스 제어 규칙을 테스트하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.

2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. Access control rules(액세스 제어 규칙)를 선택합니다.
4. Test rules(규칙 테스트)를 선택합니다.
5. Request context(요청 컨텍스트)에서 테스트할 프로토콜을 선택합니다.
6. Source IP address(소스 IP 주소)에 테스트할 IP 주소를 입력합니다.
7. 다음이 수행하는 요청에 테스트할 사용자 또는 위장 역할을 선택합니다.
8. 테스트할 사용자 또는 위장 역할을 선택합니다.
9. 테스트를 선택합니다.

테스트 결과가 효과 아래에 나타납니다.

액세스 제어 규칙 삭제

Amazon WorkMail 콘솔에서 더 이상 필요하지 않은 액세스 제어 규칙을 삭제합니다.

> **Warning**
>
> 관리자가 조직에 대한 모든 액세스 제어 규칙을 삭제하면 Amazon은 조직의 사서함에 대한 모든 액세스를 WorkMail 차단합니다.

액세스 제어 규칙을 삭제하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. Access control rules(액세스 제어 규칙)를 선택합니다.
4. 삭제할 규칙을 선택합니다.
5. 규칙 삭제를 선택합니다.

6. Delete(삭제)를 선택합니다.

사서함 보존 정책 설정

Amazon WorkMail 조직에 대한 사서함 보존 정책을 설정할 수 있습니다. 보존 정책은 선택한 기간이 지나면 사용자 사서함에서 이메일 메시지를 자동으로 삭제합니다. 보존 정책을 적용할 사서함 폴더를 선택할 수 있습니다. 또한 폴더마다 다른 보존 정책을 설정할지 여부를 선택할 수 있습니다. 사서함 보존 정책은 조직의 모든 사용자 사서함에서 선택한 폴더에 적용됩니다. 사용자는 보존 정책을 재정의할 수 없습니다.

사서함 보존 정책을 설정하려면

1. 에서 Amazon WorkMail 콘솔을 엽니다 https://console.aws.amazon.com/workmail/.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 보존 정책을 선택합니다.
4. 폴더 작업의 경우 정책에 포함할 각 사서함 폴더 옆에 있는 삭제 또는 영구 삭제를 선택합니다.
5. 이메일 메시지를 삭제하기 전에 각 사서함 폴더에 보관할 일 수를 입력합니다.
6. 저장(Save)을 선택합니다.

조직에 보존 정책을 적용하는 데 최대 48시간이 걸릴 수 있습니다. 폴더 삭제 작업을 선택하면 사용자가 Amazon WorkMail 웹 애플리케이션 및 지원되는 클라이언트에서 삭제된 이메일 메시지를 복구할 수 있습니다. 폴더 영구 삭제 작업을 선택하면 이메일 메시지를 삭제한 후 복구할 수 없습니다.

보존 정책에 따른 항목 보관 기간(일)은 항목이 생성, 수정 또는 이동된 날짜를 기준으로 합니다. 예를 들어, 보존 정책에 따라 1년이 지난 후 항목이 삭제되는 경우 정책은 해당 항목을 만들었거나 마지막으로 조치를 취한 날짜로부터 보존 일수를 계산합니다. 보존 정책을 구현한 날짜의 영향을 받지 않습니다.

도메인 작업

Amazon에서 사용자 지정 WorkMail 도메인을 사용하도록 구성할 수 있습니다. 도메인을 조직의 기본 도메인으로 설정하고 Microsoft Outlook에서 AutoDiscover 활성화할 수도 있습니다.

주제

도메인 추가

Amazon WorkMail 조직에 최대 100개의 도메인을 추가할 수 있습니다. 새 도메인을 추가하면 Amazon Simple Email Service(Amazon SES) 보내기 권한 부여 정책이 도메인 자격 증명 정책에 자동으로 추가됩니다. 그러면 WorkMail Amazon에서 도메인의 모든 Amazon SES 전송 작업에 액세스할 수 있고 이메일을 도메인으로 리디렉션할 수 있습니다. 이메일을 외부 도메인으로 리디렉션할 수도 있습니다.

> **Note**
>
> 모든 도메인에 <postmaster@> 및 <abuse@>에 대한 별칭을 추가하는 것이 가장 좋습니다. 조직의 특정 사용자가 이러한 별칭으로 보낸 메일을 수신하도록 하려면 해당 별칭에 대한 배포 그룹을 생성할 수 있습니다.

Amazon WorkMail 조직을 사용자 지정 도메인으로 구성할 때는 도메인의 DNS 레코드에 대해 다음 사항을 기억하십시오.

- MX 및 자동 검색 CNAME 레코드의 경우 TTL(Time to Live) 값을 3600으로 설정하는 것이 좋습니다. TTL을 줄이면 MX 레코드를 업데이트하거나 사서함을 마이그레이션한 후 메일 서버가 오래되거나 잘못된 MX 레코드를 사용하지 않습니다.

- 사용자 및 배포 그룹을 만들고 사서함을 성공적으로 마이그레이션한 후에는 MX 레코드를 업데이트하여 Amazon에 이메일 전달을 시작해야 합니다. WorkMail DNS 레코드 업데이트는 처리에 최대 48시간이 소요될 수 있습니다.
- 일부 DNS 공급자는 DNS 레코드의 끝에 도메인 이름을 자동으로 추가합니다. _amazonses.example.com과 같이 도메인 이름을 이미 포함하고 있는 레코드를 추가하면 도메인 이름이 중복되어 _amazonses.example.com.example.com이 될 수 있습니다. 레코드 이름에서 도메인 이름 중복을 방지하려면 DNS 레코드의 도메인 이름 끝에 마침표를 추가하십시오. 이는 DNS 공급자에게 레코드 이름이 정규화되었으며 더 이상 도메인 이름과는 관련이 없음을 나타냅니다. 또한 DNS 공급자가 추가 도메인 이름을 추가하지 못하도록 합니다.
- 복사된 레코드 이름에는 도메인 이름이 포함됩니다. 사용하는 DNS 서비스에 따라 도메인 이름이 도메인 DNS 레코드에 이미 추가되었을 수도 있습니다.
- DNS 레코드를 생성한 후 Amazon WorkMail 콘솔에서 새로 고침 아이콘을 선택하여 확인 상태 및 레코드 값을 확인합니다. 도메인 확인에 대한 자세한 내용은 도메인 확인 단원을 참조하세요.
- 도메인을 `MAIL FROM` 도메인으로 구성하는 것이 좋습니다. iOS 장치를 AutoDiscover 활성화하려면 도메인을 도메인으로 구성해야 합니다. `MAIL FROM` 콘솔의 전달 능력 향상 섹션에서 `MAIL FROM` 도메인의 상태를 확인할 수 있습니다. 자세한 설명은 사용자 지정 MAIL FROM 도메인 구성 섹션을 참조하세요.

도메인을 추가하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.
2. 필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
3. 탐색 창에서 조직을 선택한 다음 도메인을 추가하려는 조직의 이름을 선택합니다.
4. 탐색 창에서 도메인, 도메인 추가를 차례로 선택합니다.
5. 도메인 추가 화면에서 도메인 이름을 입력합니다. 도메인 이름에는 기본 라틴어(ASCII) 문자만 포함될 수 있습니다.

> **Note**
>
> Amazon Route 53 퍼블릭 호스팅 영역에서 관리되는 도메인이 있을 경우 도메인 이름을 입력할 때 나타나는 드롭다운 메뉴에서 선택할 수 있습니다.

6. 도메인 추가를 선택합니다.

   페이지가 나타나고 새 도메인의 DNS 레코드가 나열됩니다. 이 페이지는 레코드를 다음 섹션으로 그룹화합니다.

   - 도메인 소유권
   - WorkMail 구성
   - 개선된 보안
   - 개선된 이메일 전송

   각 섹션에는 하나 이상의 DNS 레코드가 포함되며 각 레코드에는 상태 값이 표시됩니다. 다음 목록에서는 레코드와 사용 가능한 상태 값을 보여줍니다.

   TXT 소유권

   확인됨 - 레코드가 해결되고 확인되었습니다.

   보류 중 – 레코드가 아직 확인되지 않았습니다.

   실패 - 소유권을 확인할 수 없습니다. 레코드가 일치하지 않거나 연결 불가합니다.

   MX 구성 WorkMail

   확인됨 - 레코드가 해결되고 확인되었습니다.

   누락 - 레코드를 확인할 수 없습니다.

   불일치 - 값이 예상 레코드과 일치하지 않습니다.

   AutoDiscover

   확인됨 - 레코드가 해결되고 확인되었습니다.

   누락 - 레코드를 확인할 수 없습니다.

   불일치 - 값이 예상 레코드과 일치하지 않습니다.

   > **Note**
   >
   > AutoDiscover 검증 프로세스에서는 AutoDiscover 설정이 올바른지도 확인합니다. 이 프로세스는 각 단계의 구성 설정을 확인합니다. 확인이 완료되면 상태 열의 확인됨 옆에 녹색 체크 표시가 나타납니다. 확인됨을 마우스로 가리키면 프로세스에서 어떤 단

계가 검증되었는지 확인할 수 있습니다. AutoDiscover 단계에 대한 자세한 내용은 을 참조하십시오엔드포인트 구성 활성화 AutoDiscover .

DKIM CNAME

확인됨 - 레코드가 해결되고 확인되었습니다.

보류 중 - 레코드가 아직 확인되지 않았습니다.

실패 - 소유권을 확인할 수 없습니다. 레코드가 일치하지 않거나 연결 불가합니다.

자세한 내용은 Amazon Simple Email Service 개발자 가이드에서 Amazon SES에서 DKIM으로 이메일 인증을 참조하세요.

SPF TXT

확인됨 - 레코드가 해결되고 확인되었습니다.

누락 - 레코드를 확인할 수 없습니다.

불일치 - 값이 예상 레코드과 일치하지 않습니다.

SPF 확인에 대한 자세한 내용은SPF를 사용하여 이메일 인증을 참조하십시오.

DMARC TXT

확인됨 - 레코드가 해결되고 확인되었습니다.

누락 - 레코드를 확인할 수 없습니다.

불일치 - 값이 예상 레코드과 일치하지 않습니다.

Amazon의 DMARC 레코드에 대한 자세한 내용은 Amazon WorkMail Simple 이메일 서비스 개발자 안내서의 Amazon SES를 사용한 DMARC 규정 준수를 참조하십시오.

TXT MAIL FROM 도메인

확인됨 - 레코드가 해결되고 확인되었습니다.

보류 중 – 레코드가 아직 확인되지 않았습니다.

실패 - 소유권을 확인할 수 없습니다. 레코드가 일치하지 않거나 연결 불가합니다.

MX MAIL FROM 도메인

확인됨 - 레코드가 해결되고 확인되었습니다.

누락 - 레코드를 확인할 수 없습니다.

불일치 - 값이 예상 레코드과 일치하지 않습니다.

7. 다음 단계에서는 사용하는 DNS 공급자에 따라 적절한 조치를 선택합니다.

   Route 53 도메인을 사용하는 경우

   - 페이지 상단의 Route 53에서 모두 업데이트를 선택합니다.

   다른 DNS 공급자를 사용하는 경우

   - 레코드를 복사하여 DNS 공급자에 붙여넣습니다. 레코드를 대량으로 복사하거나 한 번에 하나씩 복사할 수 있습니다. 레코드를 대량으로 복사하려면 모두 복사를 선택합니다. 그러면 DNS 공급자로 가져올 수 있는 파일 영역이 만들어집니다. 레코드를 한 번에 하나씩 복사하려면 레코드 이름 옆에 있는 겹치는 사각형을 선택한 다음 각 사각형을 DNS 공급자에 붙여넣습니다.

8. 새로 고침 아이콘을 선택하여 각 레코드의 상태를 업데이트합니다. 이를 통해 WorkMail Amazon에서 도메인 소유권과 도메인의 올바른 구성을 확인할 수 있습니다.

도메인 제거

도메인이 더 이상 필요 없으면 삭제할 수 있습니다. 하지만 먼저 도메인을 이메일 주소로 사용하는 개인 또는 그룹을 삭제해야 합니다.

도메인을 제거하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 이름 및 엔드포인트를 참조하세요.

2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 도메인 목록에서 도메인 이름 옆에 있는 확인란을 선택하고 [Remove]를 선택합니다.
4. 도메인 제거 대화 상자에 제거할 도메인의 이름을 입력하고 제거를 선택합니다.

기본 도메인 선택

조직과 관련된 도메인을 해당 조직의 사용자 및 그룹에 대한 기본 도메인으로 설정할 수 있습니다. 도메인을 기본 도메인으로 설정하더라도 기본 이메일 주소가 변경되지는 않습니다.

도메인을 기본 도메인으로 설정하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 이름 및 엔드포인트를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 도메인 목록에서 사용하려는 도메인 이름 옆에 있는 확인란을 선택하고 기본값으로 설정을 선택합니다.

도메인 확인

Amazon WorkMail 콘솔에서 도메인을 추가한 후 도메인을 확인해야 합니다. 도메인을 확인하면 도메인을 소유하고 있으며 Amazon을 도메인의 이메일 서비스로 WorkMail 사용하게 된다는 사실이 확인됩니다.

DNS 서비스에서 TXT 및 MX 레코드를 추가하여 도메인을 확인합니다. TXT 레코드를 사용하면 DNS 서비스에 메모를 추가할 수 있습니다. MX 레코드는 수신 메일 서버를 지정합니다.

Amazon SES 콘솔을 사용하여 TXT 및 MX 레코드를 생성한 다음 Amazon WorkMail 콘솔을 사용하여 DNS 서비스에 레코드를 추가합니다. 단계는 다음과 같습니다.

TXT 및 MX 레코드를 만들려면

1. https://console.aws.amazon.com/ses/에서 Amazon SES 콘솔을 엽니다.
2. 탐색 창에서 도메인, 새 도메인 확인을 차례로 선택합니다.

   새 도메인 확인 대화 상자가 나타납니다.
3. 도메인 상자에 도메인 추가 섹션에서 생성한 도메인의 이름을 입력합니다.
4. (선택 사항) DomainKeys 식별 메일 (DKIM) 을 사용하려면 DKIM 설정 생성 확인란을 선택합니다.

5. [Verify This Domain]을 선택합니다.

   콘솔에 TXT 및 MX 레코드 목록이 표시됩니다.

6. TXT 목록 아래에 있는 레코드 세트를 CSV로 다운로드 링크를 선택합니다.

   다음 이름으로 저장 대화 상자가 나타납니다. 다운로드 위치를 선택한 다음 저장을 선택합니다.

7. 다운로드한 CSV 파일을 열고 내용을 모두 복사합니다.

TXT 및 MX 레코드를 생성한 다음 DNS 공급자에 추가합니다. 다음 단계에서는 Route 53을 사용합니다. 다른 DNS 공급자를 사용하고 있는데 레코드 추가 방법을 모르는 경우 제공자의 설명서를 참조하세요.

1. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다. 그런 다음 확인하려는 도메인 옆의 라디오 버튼을 선택합니다.
3. 도메인의 DNS 레코드 목록에서 영역 파일 가져오기를 선택합니다.
4. Zone 파일에서 복사한 레코드를 텍스트 상자에 붙여넣습니다. 텍스트 상자 아래에 파일 목록이 나타납니다.
5. 목록 끝으로 스크롤하고 가져오기를 선택합니다.

> **Note**
>
> 확인 프로세스를 완료하는 데 최대 72시간이 걸릴 수 있습니다.

DNS 서비스를 통해 TXT 레코드 및 MX 레코드를 확인합니다.

도메인 소유를 확인하는 TXT 레코드가 DNS 서비스에 올바르게 추가되었는지 확인합니다. 이 절차는 Windows 및 Linux에서 사용 가능한 nslookup 도구를 사용합니다. Linux의 경우, dig도 사용할 수 있습니다.

`nslookup` 도구를 사용하려면 먼저 사용자의 도메인에 서비스하는 DNS 서버를 찾아야 합니다. 그런 다음, 이러한 서비스를 쿼리하여 TXT 레코드를 확인합니다. 해당 서버에는 도메인에 대한 up-to-date 정보가 가장 많이 포함되어 있기 때문에 해당 도메인의 DNS 서버를 쿼리할 수 있습니다. 이 정보를 다른 DNS 서버로 전파하는 데 시간이 걸릴 수 있습니다.

nslookup을 사용하여 TXT 레코드가 DNS 서비스에 추가되었는지 확인

1. 도메인의 이름 서버 찾기:

   a. 명령 프롬프트(Windows) 또는 터미널(Linux)을 엽니다.

   b. 다음 명령을 실행하여 사용자의 도메인에 서비스하는 모든 이름 서버를 나열합니다. *example.com*을 도메인으로 바꿉니다.

   ```
   nslookup -type=NS example.com
   ```

   다음 단계에서 이러한 이름 서버 중 하나를 쿼리합니다.

2. Amazon WorkMail TXT 레코드가 올바르게 추가되었는지 확인하십시오.

   a. 다음 명령을 실행하여 *example.com*을 사용자 도메인으로 대체하고 *ns1.name-server.net*을 1단계의 이름 서버로 대체합니다.

   ```
   nslookup -type=TXT _amazonses.example.com ns1.name-server.net
   ```

   b. nslookup의 출력에 표시된 "text =" 문자열을 검토하세요. 이 문자열이 Amazon WorkMail 콘솔의 확인된 발신자 목록에 있는 도메인의 TXT 값과 일치하는지 확인하십시오.

   이 예에서는 값이 fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=인 _amazonses.example.com에 대한 TXT 레코드를 찾습니다. 레코드를 올바르게 업데이트하면 명령에 다음과 같은 출력이 포함됩니다.

   ```
   _amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
   ```

dig를 사용하여 TXT 레코드가 DNS 서비스에 추가되었는지 확인

1. 터미널 세션을 엽니다.
2. 다음 명령을 실행하여 도메인에 대한 TXT 레코드를 나열합니다. *example.com*을 도메인으로 바꿉니다.

   ```
   dig +short example.com txt
   ```

3. 명령 출력 뒤에 TXT 오는 문자열이 Amazon WorkMail 콘솔의 Verified Senders 목록에서 도메인을 선택할 때 표시되는 TXT 값과 일치하는지 확인하십시오.

nslookup을 사용하여 MX 레코드가 DNS 서비스에 추가되었는지 확인하려면

1. 다음과 같이 도메인의 이름 서버를 찾습니다.

   a. 명령 프롬프트를 엽니다.

   b. 다음 명령을 실행하여 사용자의 도메인에 대한 모든 이름 서버를 나열합니다.

   ```
   nslookup -type=NS example.com
   ```

   다음 단계에서 이러한 이름 서버 중 하나를 쿼리합니다.

2. 다음과 같이 MX 레코드가 올바르게 추가되었는지 확인합니다.

   a. 다음 명령을 실행하여 *example.com*을 사용자 도메인으로 대체하고 *ns1.name-server.net*을 이전 단계에서 식별한 이름 서버 중 하나로 대체합니다.

   ```
   nslookup -type=MX example.com ns1.name-server.net
   ```

   b. 명령 출력에서 `mail exchange =` 이하의 문자열이 다음 값 중 하나와 일치하는지 확인합니다.

   미국 동부(버지니아 북부) 리전 – `10 inbound-smtp.us-east-1.amazonaws.com`

   미국 서부(오레곤) 리전 - `10 inbound-smtp.us-west-2.amazonaws.com`

   유럽(아일랜드) - `10 inbound-smtp.eu-west-1.amazonaws.com`

   > **Note**
   >
   > 10은 MX 기본 설정 번호 또는 우선순위를 나타냅니다.

dig를 사용하여 MX 레코드가 DNS 서비스에 추가되었는지 확인

1. 터미널 세션을 엽니다.
2. 다음 명령을 실행하여 도메인에 대한 MX 레코드를 나열합니다.

   ```
   dig +short example.com mx
   ```

3. `MX` 이하의 문자열이 다음 값 중 하나와 일치하는지 확인합니다.

미국 동부(버지니아 북부) 리전 – `10 inbound-smtp.us-east-1.amazonaws.com`

미국 서부(오레곤) 리전 - `10 inbound-smtp.us-west-2.amazonaws.com`

유럽(아일랜드) - `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> 10은 MX 기본 설정 번호 또는 우선순위를 나타냅니다.

도메인 확인과 관련된 문제 해결

도메인 확인과 관련된 일반적인 문제를 해결하려면 다음 제안 사항을 참조하세요.

DNS 서비스는 TXT 레코드 이름에 밑줄을 허용하지 않습니다.

TXT 레코드 이름에서 _amazonses를 생략합니다.

동일한 도메인을 여러 번 확인하고자 하지만 이름이 동일한 여러 TXT 레코드를 만들 수 없습니다.

DNS 서비스가 동일한 이름으로 여러 개의 TXT 레코드를 허용하지 않을 경우 두 가지 차선책 중 하나를 사용하세요.

- (권장) DNS 서비스가 허용할 경우 TXT 레코드에 여러 값을 할당하는 것입니다. 예를 들어 Amazon Route 53에서 사용자의 DNS를 관리하는 경우 사용자는 다음과 같이 동일한 TXT 레코드에 여러 값을 설정할 수 있습니다.
  1. Route 53 콘솔에서 첫 번째 리전에서 도메인을 확인할 때 추가한 _amazonses TXT 레코드를 선택합니다.
  2. 값에서 첫 번째 값을 입력한 후 Enter를 누릅니다.
  3. 다른 리전에도 값을 추가하고 레코드 세트를 저장합니다.
- 도메인을 두 번만 확인해야 하는 경우 이름에 _amazonses가 포함된 TXT 레코드를 만들어 한 번 확인한 다음 레코드 이름에 _amazonses가 포함되지 않은 다른 레코드를 생성할 수 있습니다.

Amazon WorkMail 콘솔에서 도메인 확인이 실패했다고 보고함

Amazon에서 DNS 서비스에 필요한 TXT 레코드를 찾을 WorkMail 수 없습니다. DNS 서비스를 통해 TXT 레코드 및 MX 레코드를 확인합니다.의 절차를 따라 필요한 TXT 레코드가 올바로 DNS 서버에 추가되었는지 확인합니다.

DNS 공급자가 TXT 레코드 끝에 도메인 이름을 추가했습니다.

> _amazonses.example.com과 같이 도메인 이름을 이미 포함하고 있는 TXT 레코드를 추가하면 도메인 이름이 중복되어 _amazonses.example.com.example.com과 같이 될 수 있습니다. 레코드 이름에서 도메인 이름 중복을 방지하려면 TXT 레코드의 도메인 이름 끝에 마침표를 추가하십시오. 이는 DNS 공급자에게 해당 레코드 이름이 완전히 정규화되었으며 TXT 레코드에 이미 도메인 이름이 포함되어 있음을 나타냅니다.

Amazon에서 MX 레코드가 일치하지 않는다고 WorkMail 보고했습니다.

> 기존 메일 서버에서 마이그레이션할 때 MX 레코드는 불일치 상태를 반환할 수 있습니다. 이전 메일 서버를 가리키는 WorkMail 대신 Amazon을 가리키도록 MX 레코드를 업데이트하십시오. 타사 이메일 프록시를 Amazon과 함께 사용하는 경우에도 MX 레코드가 일관성 없음으로 반환됩니다. WorkMail 이 경우 Inconsistent(불일치) 경고를 무시해도 됩니다.

엔드포인트 구성 활성화 AutoDiscover

AutoDiscover 전자 메일 주소와 암호만 사용하여 Microsoft Outlook 및 모바일 클라이언트를 구성할 수 있습니다. 이 서비스는 WorkMail Amazon과의 연결을 유지하고 엔드포인트 또는 설정을 변경할 때마다 로컬 설정을 업데이트합니다. 또한 고객이 오프라인 주소록, AutoDiscover 부재 중 도우미, 캘린더에서 휴무/바쁜 시간을 볼 수 있는 WorkMail 기능 등 Amazon의 추가 기능을 사용할 수 있습니다.

클라이언트는 다음 AutoDiscover 단계를 수행하여 서버 엔드포인트 URL을 탐지합니다.

- 1단계 - 클라이언트가 로컬 Active Directory에 대해 SCP(Secure Copy Protocol) 조회를 수행합니다. 클라이언트가 도메인에 가입되어 있지 않은 경우 이 단계를 건너뛰세요. AutoDiscover
- 2단계 - 클라이언트가 다음 URL로 요청을 보내 결과를 확인합니다. 이러한 엔드포인트에서는 HTTPS만 사용할 수 있습니다.
  - https://*company.tld*/autodiscover/autodiscover.xml
  - https://autodiscover.*company.tld*/autodiscover/autodiscover.xml
- 3단계 - 클라이언트가 autodiscover.company.tld에 대해 DNS 조회를 수행하고 사용자의 이메일 주소에서 추출된 엔드포인트로 미인증 GET 요청을 보냅니다. 서버가 302 리디렉션을 반환하는 경우 클라이언트는 반환된 HTTPS 엔드포인트에 대해 요청을 다시 보냅니다. AutoDiscover

이러한 모든 단계에 실패하면 클라이언트를 자동으로 구성할 수 없습니다. 수동으로 모바일 디바이스를 구성하는 방법에 대한 자세한 내용은 수동으로 디바이스에 연결을 참조하십시오.

Amazon에 도메인을 추가할 때 공급자에 AutoDiscover DNS 레코드를 추가하라는 메시지가 표시됩니다 WorkMail. 이를 통해 클라이언트는 AutoDiscover 프로세스의 3단계를 수행할 수 있습니다. 그러나 stock Android 이메일 앱 등 일부 모바일 디바이스에서는 이러한 단계가 통하지 않습니다. 따라서 AutoDiscover 2단계를 수동으로 설정해야 할 수도 있습니다.

다음 방법을 사용하여 도메인의 AutoDiscover 2단계를 설정할 수 있습니다.

(권장) Route 53 및 아마존 사용 CloudFront

> **Note**
>
> 다음 단계는 https://autodiscover.*company.tld*/autodiscover/autodiscover.xml에 대한 프록시를 만드는 방법을 설명합니다. https://*company.tld*/autodiscover/autodiscover.xml에 대한 프록시를 생성하려면 다음 단계의 도메인에서 `autodiscover.` 접두사를 제거합니다.
> Route CloudFront 53을 사용하면 요금이 부과될 수 있습니다. 해당 요금에 대한 자세한 내용은 Amazon CloudFront 요금 및 Amazon Route 53 요금을 참조하십시오.

Route 53으로 AutoDiscover 2단계를 활성화하려면 CloudFront

1. autodiscover.*company.tld*에 대한 SSL 인증서를 가져와 AWS Identity and Access Management(IAM) 또는 AWS Certificate Manager에 업로드합니다. 자세한 내용은 IAM 사용 설명서의 서버 인증서 작업 또는 AWS Certificate Manager 사용 설명서의 시작하기 단원을 참조하세요.
2. 새 CloudFront 배포판 생성:
    1. 에서 CloudFront 콘솔을 엽니다https://console.aws.amazon.com/cloudfront/v4/home.
    2. 탐색 창에서 Distributions(배포)를 선택합니다.
    3. 배포 생성(Create Distribution)을 선택합니다.
    4. 웹에서 시작하기를 선택합니다.
    5. 오리진 설정에 다음 값을 입력합니다.
        - 오리진 도메인 이름 - 해당 리전의 적절한 도메인 이름입니다.
            - 미국 동부(버지니아 북부) - **`autodiscover-service.mail.us-east-1.awsapps.com`**
            - 미국 서부(오레곤) - **`autodiscover-service.mail.us-west-2.awsapps.com`**
            - 유럽(아일랜드) – **`autodiscover-service.mail.eu-west-1.awsapps.com`**

- 오리진 프로토콜 정책 - 원하는 정책: **`Match Viewer`**

> **Note**
>
> 오리진 경로는 비워 두세요. 오리진 ID의 자동 입력 값을 변경하지 마세요.

6. 기본 캐시 동작 설정에서 나열된 설정에 대해 다음 값을 선택합니다.
   - [Viewer Protocol Policy]: HTTPS만
   - [Allowed HTTP Methods]: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - [Cache Based on Selected Request Headers]: 모두
   - [Forward Cookies]: 모두
   - [Query String Forwarding and Caching]: 없음(캐싱 개선)
   - [Smooth Streaming]: 아니요
   - [Restrict Viewer Access]: 아니요
7. Distribution Settings(배포 설정)에 대해 다음 값을 선택합니다.
   - [Price Class]: 미국, 캐나다 및 유럽만 사용
   - 대체 도메인 이름(CNAME)의 경우 **`autodiscover.`*`company.tld`*** 또는 ***`company.tld`***를 입력합니다. 여기서 *`company.tld`*는 도메인 이름입니다.
   - SSL 인증서: 사용자 지정 SSL 인증서(IAM에 저장되어 있음)
   - Custom SSL Client Support(사용자 지정 SSL 클라이언트 지원): All Clients(모든 클라이언트) 또는 Only Clients that Support Server Name Indication (SNI)(서버 이름 표시(SNI)를 지원하는 클라이언트만)을 선택합니다. 이전 버전의 Android에서는 두 번째 옵션이 작동하지 않을 수 있습니다.

> **Note**
>
> All Clients(모든 클라이언트)를 선택하는 경우 Default Root Object(기본 루트 객체)를 비워 둡니다.

   - Logging(로깅): On(활성) 또는 Off(비활성)를 선택합니다. 켜면 로깅이 활성화됩니다.
   - 설명에 **`AutoDiscover type2 for autodiscover.`*`company.tld`***를 입력합니다.
   - 배포 상태: 활성화됨을 선택합니다.
8. 배포 생성(Create Distribution)을 선택합니다.

3. Route 53 콘솔에서 도메인 이름의 인터넷 트래픽을 CloudFront 배포로 라우팅하는 레코드를 생성합니다.

> **Note**
>
> 이러한 단계에서는 example.com에 대한 DNS 레코드가 Route 53에서 호스팅된다고 가정합니다. Route 53을 사용하지 않는 경우 DNS 공급자의 관리 콘솔에 있는 절차를 따르세요.

1. 콘솔의 탐색 창에서 호스팅 영역을 선택한 다음 도메인을 선택합니다.
2. 도메인 목록에서 사용하려는 도메인 이름을 선택합니다.
3. 레코드에서 레코드 생성을 선택합니다.
4. 빠른 레코드 생성에서 다음 매개변수를 설정합니다.
   - 레코드 이름에서 레코드의 이름을 입력합니다.
   - 라우팅 정책에서 단순 라우팅을 선택합니다.
   - 별칭 슬라이더를 선택하여 켭니다. 켜진 상태에서는 슬라이더가 파란색으로 바뀝니다.
   - 레코드 유형 목록에서 A - 주소 및 일부 AWS 리소스로 트래픽 라우팅을 선택합니다.
   - 트래픽 라우팅 대상 목록에서 CloudFront 배포할 Alias를 선택합니다.
   - 트래픽 라우팅 대상 목록 아래에 검색 상자가 나타납니다. 텍스트 상자에 CloudFront 배포 이름을 입력합니다. 검색 상자를 선택할 때 나타나는 목록에서 배포를 선택할 수도 있습니다.
5. Create Record Set(레코드 세트 생성)를 선택합니다.

Apache 웹 서버 사용

다음 단계는 Apache 웹 서버를 사용하여 https://autodiscover.*company.tld*/autodiscover/autodiscover.xml에 대한 프록시를 만드는 방법을 설명합니다. https://*company.tld*/autodiscover/autodiscover.xml 프록시를 만들려면 “자동 검색”을 삭제하세요. 다음 단계에 따라 도메인의 접두사를 입력합니다.

Apache 웹 서버에서 AutoDiscover 2단계를 활성화하려면

1. SSL 지원 Apache 서버에 대해 다음 명령을 실행합니다.

```
SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-
service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
```

2. 필요에 따라 다음 Apache 모듈을 활성화합니다. 방법을 모르는 경우 Apache 도움말을 참조하세요.

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

테스트 및 문제 AutoDiscover 해결에 대한 자세한 내용은 다음 섹션을 참조하십시오.

AutoDiscover 2단계 문제 해결

DNS 공급자를 AutoDiscover 구성한 후에는 AutoDiscover 엔드포인트 구성을 테스트할 수 있습니다. 엔드포인트가 올바르게 구성된 경우 무단 요청 메시지와 함께 응답합니다.

기본 무단 요청을 생성하려면

1. 터미널에서 엔드포인트에 대한 인증되지 않은 POST 요청을 생성합니다. AutoDiscover

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ```

   엔드포인트가 올바르게 구성된 경우 다음 예시에서 표시된 것과 같이 `401 unauthorized` 메시지를 반환해야 합니다.

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ...
   HTTP/1.1 401 Unauthorized
   ```

2. 다음으로 실제 AutoDiscover 요청을 테스트해 보세요. 다음 XML 콘텐츠가 포함된 `request.xml` 파일을 생성합니다.

   ```
   <?xml version="1.0" encoding="utf-8"?>
   ```

```
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
requestschema/2006">
    <Request>
        <EMailAddress>testuser@company.tld</EMailAddress>
        <AcceptableResponseSchema>
            http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006
        </AcceptableResponseSchema>
    </Request>
</Autodiscover>
```

3. 생성한 `request.xml` 파일을 사용하여 엔드포인트에 인증된 AutoDiscover 요청을 합니다. *testuser@company.tld*을 유효한 이메일 주소로 대체하는 것을 잊지 마세요.

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

엔드포인트가 올바르게 구성된 경우 응답은 다음 예제와 비슷합니다.

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml

Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/
responseschema/2006" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006">
    <Culture>en:us</Culture>
    <User>
        <DisplayName>User1</DisplayName>
        <EMailAddress>testuser@company.tld</EMailAddress>
    </User>
    <Action>
        <Settings>
            <Server>
                <Type>MobileSync</Type>
                <Url>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Url>
                <Name>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Name>
            </Server>
```

```
        </Settings>
    </Action>
</Response>
```

도메인 자격 증명 정책 편집

이메일 리디렉션과 같은 도메인 자격 증명 정책은 이메일 작업에 대한 권한을 지정합니다. 예를 들어 Amazon WorkMail 조직의 모든 이메일 주소로 이메일을 리디렉션할 수 있습니다.

> **Note**
>
> 2022년 4월 1일부터 Amazon은 권한 부여를 위해 AWS 계정 보안 주체 대신 서비스 보안 주체를 사용하기 WorkMail 시작했습니다. 2022년 4월 1일 이전에 도메인을 추가한 경우 권한 부여를 위해 AWS 계정 보안 주체를 사용하는 이전 정책이 있을 수 있습니다. 그렇다면 최신 정책으로 업데이트하는 것이 좋습니다. 이 섹션의 단계에서는 방법을 설명합니다. 업데이트 중에도 조직은 계속해서 이메일을 정상적으로 전송합니다.

사용자 지정 Amazon SES 정책을 사용하지 않는 경우에만 다음 단계를 따르세요. 사용자 지정 Amazon SES 정책을 사용하는 경우 직접 업데이트해야 합니다. 자세한 내용은 이 단원 후반부의 사용자 지정 Amazon SES 서비스 원칙 정책을 참조하십시오.

> **Important**
>
> 기존 도메인을 제거하지 마세요. 그렇게 하면 메일 서비스가 중단될 수 있습니다. 기존 도메인을 다시 입력하기만 하면 됩니다.

도메인 자격 증명 정책을 업데이트하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 이렇게 하려면 검색 상자 오른쪽에 있는 리전 선택 목록을 연 다음 원하는 리전을 선택합니다. 리전에 대한 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 도메인을 선택합니다.

4. 다시 입력할 도메인의 이름을 강조 표시하고 복사한 다음 도메인 추가를 선택합니다.

   도메인 추가 대화 상자가 나타납니다.
5. 복사한 이름을 도메인 이름 상자에 붙여넣은 다음 도메인 추가를 선택합니다.
6. 조직의 나머지 도메인에 대해 3~5단계를 반복합니다.

사용자 지정 Amazon SES 서비스 원칙 정책

사용자 지정 Amazon SES 정책을 사용하는 경우 이 예제를 도메인에서 사용할 수 있도록 조정하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuthorizeWorkMail",
      "Effect": "Allow",
      "Principal": {
        "Service": "workmail.REGION.amazonaws.com"
      },
      "Action": [
        "ses:*"
      ],
      "Resource": "arn:aws:ses:REGION:AWS_ACCOUNT_ID:identity/WORKMAIL-DOMAIN-NAME",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn":
 "arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID"
        }
      }
    }
  ]
}
```

SPF를 사용하여 이메일 인증

Sender Policy Framework(SPF)는 이메일 스푸핑 방지를 위해 마련된 이메일 검증 표준입니다. 스푸핑은 악의적인 공격자가 보낸 이메일을 실제 사용자가 보낸 이메일처럼 보이게 만드는 행위입니다. Amazon WorkMail 지원 도메인의 SPF 구성에 대한 자세한 내용은 Amazon SES에서 SPF를 사용한 이메일 인증을 참조하십시오.

사용자 지정 MAIL FROM 도메인 구성

기본적으로 Amazon은 amazonses.com의 하위 도메인을 발신 이메일의 `MAIL FROM` 도메인으로 WorkMail 사용합니다. 이로 인해 도메인의 DMARC 정책이 SPF에 대해서만 설정된 경우 전송이 실패할 수 있습니다. 이 문제를 해결하려면 자체 도메인을 `MAIL FROM` 도메인으로 구성하세요. 이메일 도메인을 `MAIL FROM` 도메인으로 설정하는 방법을 알아보려면 Amazon Simple Email Service 개발자 안내서의 사용자 지정 MAIL FROM 도메인 설정을 참조하세요.

> **Important**
>
> iOS 장치에서 AutoDiscover 활성화하려면 사용자 지정 MAIL FROM 도메인이 필요합니다.

사용자 지정 `MAIL FROM` 도메인에 대한 자세한 내용은 Amazon SES가 이제 사용자 지정 MAIL FROM 도메인을 지원함을 참조하세요.

사용자 작업

Amazon에서 사용자를 생성하고 제거할 수 WorkMail 있습니다. 또한 이메일 암호를 재설정하고, 사서함 할당량 및 디바이스 액세스를 관리하고, 사서함 권한을 제어할 수 있습니다.

주제

사용자 목록 보기

사용자 목록을 보려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택합니다.
4. 또한 사용자 이름, 표시 이름 또는 기본 이메일 주소를 기준으로 사용자를 필터링할 수 있습니다.

> **Note**
>
> 검색은 대소문자를 구분합니다.

사용자 추가

사용자를 추가하면 Amazon에서 WorkMail 자동으로 해당 사용자를 위한 사서함을 생성합니다. 사용자는 Amazon WorkMail 웹 애플리케이션, 모바일 장치 또는 macOS 또는 PC의 Microsoft Outlook을 사용하여 로그인하고 메일에 액세스할 수 있습니다.

사용자를 추가하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 사용자를 추가하려는 조직을 선택합니다.
3. 탐색 창에서 [사용자] 를 선택한 다음 [사용자 추가] 를 선택합니다.

   사용자 추가 화면이 나타납니다.
4. 사용자 세부 정보의 사용자 이름 필드에 사용자의 이름을 입력합니다. 이름은 이메일 주소 상자에도 표시됩니다. 사용자가 자신의 사용자 이름과 다른 이메일 주소를 가지도록 하려면 이메일 주소 필드를 편집할 수 있습니다.
5. (선택 사항) 이름 및 성 상자에 사용자의 성과 이름을 입력합니다.
6. 표시 이름 상자에 사용자의 표시 이름을 입력합니다.
7. 이메일 주소 상자에 이메일 별칭을 수락하거나 다른 별칭을 입력합니다.
8. 기본적으로 사용자는 전체 주소 목록에 표시됩니다. 전체 주소 목록에서 사용자를 숨기려면 전체 주소 목록에 표시 확인란의 선택을 취소합니다.
9. 사용자를 조직에 원격 사용자로 추가하려면 원격 사용자를 선택합니다.
10. 암호 설정에서 암호 및 반복 암호 상자에 사용자 암호를 입력합니다.
11. 사용자 추가(Add user)를 선택합니다.

사용자 활성화

Amazon을 기업 Active WorkMail Directory와 통합하거나 Simple AD 디렉터리에 이미 사용 가능한 사용자가 있는 경우 Amazon에서 해당 사용자를 활성화할 수 WorkMail 있습니다. 또한 다음 단계에 따라 계정이 비활성화된 사용자를 다시 활성화할 수 있습니다.

사용자를 활성화하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 사용자를 활성화하려는 조직을 선택합니다.
3. 탐색 창에서 사용자를 선택합니다.

   사용자 목록이 나타납니다. 활성화, 비활성화 및 시스템 사용자 상태의 사용자 계정이 목록에 표시됩니다.
4. 계정이 비활성화된 사용자 목록에서 활성화하려는 사용자의 확인란을 선택한 다음 활성화를 선택합니다.

   사용자 활성화 대화 상자가 나타납니다.
5. 필요에 따라 각 사용자의 기본 이메일 주소를 검토 및 변경한 다음 활성화를 선택합니다.

사용자 별칭 관리

사용자에게 이메일 별칭을 추가하거나 제거할 수 있습니다.

사용자에게 이메일 별칭을 추가하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 사용자를 추가할 조직의 이름을 선택합니다.
3. 탐색 창에서 [Users] 를 선택한 다음 별칭을 추가할 사용자 이름을 선택합니다.
4. 사용자 세부 정보 섹션에서 별칭 탭을 선택합니다.
5. 별칭 탭에서 별칭 추가를 선택합니다.
6. 별칭 상자에 별칭을 입력합니다.
7. 별칭으로 사용할 도메인을 선택합니다.
8. 추가를 선택합니다.

사용자로부터 이메일 별칭을 제거하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 사용자를 제거하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택한 다음 별칭을 제거하려는 사용자 이름을 선택합니다.
4. 사용자 세부 정보 섹션에서 별칭 탭을 선택합니다.
5. 별칭 탭에서 제거하려는 별칭의 확인란을 선택합니다.
6. 제거될 별칭을 확인합니다.
7. 별칭 제거 창에서 제거를 선택합니다.

사용자 비활성화

언제든지 조직의 모든 사용자를 비활성화할 수 있습니다. 사용자를 비활성화하면 즉시 액세스할 수 없게 됩니다. 30일 이상 비활성화된 사용자는 WorkMail Amazon에서 받은 편지함이 삭제됩니다.

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 비활성화하려는 사용자가 있는 조직을 선택합니다.
3. 탐색 창에서 사용자를 선택합니다.

   사용, 사용 안 함, 시스템 사용자 상태의 계정을 보여 주는 모든 사용자 목록이 나타납니다.
4. 활성화된 사용자 목록에서 비활성화하려는 계정의 확인란을 선택한 다음 비활성화를 선택합니다.

   사용자 비활성화 대화 상자가 나타납니다.
5. 비활성화를 선택합니다.

사용자 세부 정보 편집

사용자 세부 정보를 편집할 때 다음을 변경할 수 있습니다.

- 개인 데이터 — 이름, 이메일 주소, 전화번호 및 기타 개인 세부 정보.
- 사서함 할당량(크기) - 할당량은 1MB에서 51,200MB(50GB) 사이입니다. Amazon은 할당량의 90%에 도달하면 사용자에게 WorkMail 알립니다. 또한 사용자의 메일박스 할당량을 변경해도 요금에는 영향을 주지 않습니다. 요금에 대한 자세한 내용은 Amazon WorkMail 요금을 참조하십시오.
- 모바일 디바이스 액세스 - 디바이스를 제거 및 삭제하고 디바이스 세부 정보를 확인합니다.
- 사서함 액세스 권한 - 사용자에게 사서함 사용 권한을 부여하고 사용자에게 사서함에 대한 다양한 수준의 액세스 권한을 부여합니다.

> **Note**
>
> WorkMail Amazon을 AD Connector 디렉터리와 통합하는 경우 에서 이러한 세부 정보를 편집할 수 없습니다AWS Management Console. 대신 Active Directory 관리 도구를 사용하여 편집해야 합니다. 조직이 상호 운용성 모드에 있는 경우 제한 사항이 적용됩니다. 자세한 설명은 상호 운용성 모드에서의 제한 사항 섹션을 참조하세요.

사용자 세부 정보를 편집하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 사용하려는 조직을 선택합니다.
3. 탐색 창에서 사용자를 선택한 다음 편집하려는 사용자의 이름을 선택합니다.

개인 데이터를 편집하려면

1. 사용자 세부 정보 섹션에서 편집을 선택합니다.
2. 사용자 세부 정보에서 필요에 따라 사용자의 개인 정보를 입력하거나 변경합니다.
3. 작업을 마쳤으면 변경 사항 저장을 선택합니다.

사서함 할당량을 편집하려면

1. 사용자 세부 정보에서 할당량 탭을 선택한 다음 편집을 선택합니다.

2. 사서함 할당량 업데이트 상자에 사서함 크기를 입력합니다. **1~51200**의 값을 입력할 수 있습니다.
3. 변경 사항 저장을 선택합니다.

모바일 디바이스 데이터를 관리하려면

> **Note**
>
> 모바일 디바이스를 관리하려면 사용자가 먼저 디바이스를 Amazon 인스턴스에 연결해야 WorkMail 합니다. 모바일 장치 연결에 대한 자세한 내용은 Amazon용 모바일 장치 클라이언트 설정을 참조하십시오 WorkMail.

1. 사용자 세부 정보에서 모바일 디바이스 탭을 선택합니다.
2. 현재 디바이스 목록을 보려면 새로 고침을 선택합니다.
3. 디바이스의 세부 정보를 보려면 디바이스 ID 열에서 디바이스 이름을 선택합니다.
4. 디바이스를 제거하거나 초기화하려면 디바이스 이름 옆의 라디오 버튼을 선택한 다음 필요에 따라 제거 또는 지우기를 선택합니다.
5. 표시되는 대화 상자에서 제거 또는 지우기 작업을 확인합니다. 디바이스를 Amazon과 다시 동기화하면 사용자가 WorkMail 다시 표시된다는 점을 기억하십시오.

사서함 권한을 편집하려면

1. 권한 탭을 선택합니다.
2. 다음 중 하나를 수행하세요.

    1. 권한을 추가하려면 권한 추가를 선택합니다. 새 권한 추가 목록을 열고 사용자 또는 그룹을 선택하고 사용자 또는 그룹의 권한 설정을 선택한 다음 저장을 선택합니다.
    2. 사용자 권한을 편집하려면 사용자 이름 옆에 있는 버튼을 선택하십시오. 편집을 선택하고 원하는 옵션을 선택한 후 저장을 선택합니다.

    권한 옵션에 대한 자세한 내용은 사서함 권한을 사용한 작업 부분을 참조하세요.
3. 모든 권한을 제거하려면 제거를 선택한 다음 제거를 확인합니다.

사용자 암호 재설정

사용자가 비밀번호를 잊어버렸거나 WorkMail Amazon에 로그인하는 데 문제가 있는 경우 비밀번호를 재설정할 수 있습니다.

> **Note**
>
> Amazon을 AD Connector WorkMail 디렉터리와 통합한 경우 Active Directory에서 사용자 암호를 재설정해야 합니다.

사용자 암호를 재설정하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택합니다.
4. 사용자 목록에서 사용자 이름 옆의 확인란을 선택한 다음 비밀번호 재설정을 선택합니다.
5. 암호 재설정 대화 상자에서 새 암호를 입력하고 재설정을 선택합니다.

Amazon WorkMail 암호 정책 문제 해결

암호 재설정이 성공하지 못하면 새 암호가 암호 정책 요구 사항을 충족하는지 확인합니다.

암호 정책 요구 사항은 Amazon WorkMail 조직에서 사용하는 디렉터리 유형에 따라 다릅니다.

Amazon WorkMail 디렉터리 및 Simple AD 디렉터리 암호 정책

기본적으로 Amazon WorkMail 디렉터리 또는 Simple AD 디렉터리의 비밀번호는 다음과 같아야 합니다.

- 비어 있지 않음
- 최소 8자

- 64자 미만
- 기본 라틴어 또는 라틴어-1 보완 문자로 구성됨

또한 암호는 다음 5개 그룹 중 3개에서 나온 문자를 포함해야 합니다.

- 대문자
- 소문자
- 숫자(0~9)
- 특수 문자(예: <, ~ 또는 !)
- 라틴어-1 보완 문자(예: é, ü 또는 ñ)

Amazon WorkMail 디렉터리 암호 정책은 변경할 수 없습니다.

Simple AD 암호 정책을 변경하려면 Simple AD 디렉터리의 Amazon Elastic Compute Cloud(Amazon EC2) Windows 인스턴스에서 AD 관리 도구를 사용하세요. 자세한 내용은 AWS Directory Service 관리 안내서의 Active Directory 관리 도구 설치를 참조하세요.

AWS Managed Microsoft AD 디렉터리 암호 정책

AWS Managed Microsoft AD 디렉터리의 기본 암호 정책에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 AWS Managed Microsoft AD에 대한 암호 정책 관리를 참조하세요.

AD Connector 암호 정책

AD Connector는 연결된 Active Directory 도메인의 암호 정책을 사용합니다. 암호 정책 설정에 대한 자세한 내용은 Active Directory 도메인 설명서를 참조하세요.

알림 작업

Amazon WorkMail 푸시 알림 API를 사용하면 새 이메일 및 캘린더 업데이트를 포함하여 사서함의 변경 사항에 대한 푸시 알림을 받을 수 있습니다. 또한 알림 메시지를 수신할 URL(또는 푸시 알림 수신인)을 등록해야 합니다. 이 기능을 통해 개발자는 Amazon WorkMail 사용자를 위한 반응형 애플리케이션을 만들 수 있습니다. 애플리케이션은 사용자 사서함에서 변경 내용을 신속하게 통보받기 때문입니다.

자세한 내용은 Notification subscriptions, mailbox events, and EWS in Exchange를 참조하십시오.

사서함 변경 이벤트(새 메일, 생성됨, 수정됨)에 따라 특정 폴더(받은 편지함, 일정 등) 또는 모든 폴더를 구독할 수 있습니다.

EWS Java API 또는 Managed EWS C# API 같은 클라이언트 라이브러리를 사용하면 이러한 기능에 접근할 수 있습니다. AWS Lambda 및 API Gateway (AWS 서버리스 프레임워크 사용) 를 사용하여 개발된 푸시 응답기의 전체 샘플 애플리케이션은 이 페이지에서 제공됩니다. AWS GitHub 이 애플리케이션은 EWS Java API를 사용합니다.

다음은 푸시 구독 요청을 나타내는 샘플입니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://
schemas.microsoft.com/exchange/services/2006/types">
   <soap:Body>
      <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages">
         <m:PushSubscriptionRequest>
            <t:FolderIds>
               <t:DistinguishedFolderId Id="inbox" />
            </t:FolderIds>
            <t:EventTypes>
               <t:EventType>NewMailEvent</t:EventType>
               <t:EventType>CopiedEvent</t:EventType>
               <t:EventType>CreatedEvent</t:EventType>
               <t:EventType>DeletedEvent</t:EventType>
               <t:EventType>ModifiedEvent</t:EventType>
               <t:EventType>MovedEvent</t:EventType>
            </t:EventTypes>
            <t:StatusFrequency>1</t:StatusFrequency>
            <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
         </m:PushSubscriptionRequest>
      </m:Subscribe>
   </soap:Body>
</soap:Envelope>
```

다음은 성공적인 구독 요청 결과입니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
   <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
```

```
      <ServerVersionInfo xmlns="http://schemas.microsoft.com/exchange/
services/2006/types" MajorVersion="14" MinorVersion="2" MajorBuildNumber="390"
 Version="Exchange2010_SP2" MinorBuildNumber="3" />
   </Header>
   <soap:Body>
      <m:SubscribeResponse xmlns:m="http://schemas.microsoft.com/exchange/
services/2006/messages" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types">
         <m:ResponseMessages>
            <m:SubscribeResponseMessage ResponseClass="Success">
               <m:ResponseCode>NoError</m:ResponseCode>
               <m:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</m:SubscriptionId>
               <m:Watermark>AAAAAAA=</m:Watermark>
            </m:SubscribeResponseMessage>
         </m:ResponseMessages>
      </m:SubscribeResponse>
   </soap:Body>
</soap:Envelope>
```

그런 다음 알림 메시지가 구독 요청에서 지정한 URL로 전송됩니다. 다음은 알림 샘플입니다.

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <t:RequestServerVersion
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
 Version="Exchange2010_SP2">
        </t:RequestServerVersion>
    </soap:Header>
    <soap:Body>
        <m:SendNotification
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
            <m:ResponseMessages>
                <m:SendNotificationResponseMessage ResponseClass="Success">
                    <m:ResponseCode>NoError</m:ResponseCode>
                    <m:Notification>
                        <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</
t:SubscriptionId>
                        <t:PreviousWatermark>ygwAAAAAAAA=</t:PreviousWatermark>
                        <t:MoreEvents>false</t:MoreEvents>
                        <t:ModifiedEvent>
```

```
                            <t:Watermark>ywwAAAAAAAA=</t:Watermark>
                            <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
                            <t:FolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></
t:FolderId>
                            <t:ParentFolderId Id="AAB2L089bS1kNDgxOGYwOGE="></
t:ParentFolderId>
                        </t:ModifiedEvent>
                    </m:Notification>
                </m:SendNotificationResponseMessage>
            </m:ResponseMessages>
        </m:SendNotification>
    </soap:Body>
</soap:Envelope>
```

푸시 알림 응답자가 알림 메시지를 수신하였다고 알려주려면 다음과 같이 응답해야 합니다.

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>OK</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

클라이언트가 푸시 알림 메시지 수신을 구독 해제하려면 다음과 유사한 방법으로 SubscriptionStatus 필드에 구독 해제 응답 메시지를 전송해야 합니다.

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

푸시 알림 응답자의 상태를 확인하기 위해 Amazon은 “하트비트" (a라고도 함) 를 WorkMail 전송합니다. StatusEvent 전송 주기는 초기 구독 요청에서 입력한 StatusFrequency 파라미터에 따라

결정됩니다. 예를 들어 StatusFrequency가 **1**이면 StatusEvent가 1분마다 전송됩니다. 이 값은 1~1440분까지 설정할 수 있습니다. StatusEvent의 모습은 다음과 같습니다.

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
    <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
    <m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
    <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
            <m:ResponseCode>NoError</m:ResponseCode>
            <m:Notification>
                <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
                <t:PreviousWatermark>AAAAAAAAAAA=</t:PreviousWatermark>
                <t:MoreEvents>false</t:MoreEvents>
                <t:StatusEvent>
                    <t:Watermark>AAAAAAAAAAA=</t:Watermark>
                </t:StatusEvent>
            </m:Notification>
        </m:SendNotificationResponseMessage>
    </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

클라이언트 푸시 알림 응답자가 이전과 같은 OK 상태로 응답하지 않을 경우에는 최대 StatusFrequency분 동안 알림이 재시도됩니다. 예를 들어 StatusFrequency가 5이고, 첫 번째 알림 메시지가 전송되지 않은 경우에는 각 재시도 사이에 지수 백오프를 사용하여 최대 5분 동안 재시도됩니다. 재시도 시간이 지난 후에도 알림 메시지가 전송되지 않으면 구독 유효성이 무효화되고 새로운 알림 메시지가 전송되지 않습니다. 메일박스 이벤트에 대한 알림을 계속 수신하려면 새 구독을 생성해야 합니다. 현재는 메일박스 1개당 최대 3개까지 구독이 가능합니다.

서명되거나 암호화된 이메일 활성화

S/MIME를 사용하여 사용자가 조직 내부 및 외부 둘 다에서 서명 또는 암호화된 이메일을 보내도록 설정할 수 있습니다.

> **Note**
>
> GAL(전체 주소 목록)의 사용자 인증서는 연결된 Active Directory 설정에서만 지원됩니다.

서명 또는 암호화된 이메일을 보내도록 사용자를 설정하려면

1. AD(Active Directory) 커넥터를 설정합니다. 온프레미스 디렉터리를 사용해 AD 커넥터를 설정하면 사용자는 계속해서 기존 회사 자격 증명을 사용할 수 있습니다.
2. Active Directory에서 사용자 인증서를 자동으로 발급 및 저장하도록 인증서 자동 등록을 구성합니다. Amazon은 Active Directory로부터 사용자 인증서를 WorkMail 받아 GAL에 게시합니다. 자세한 내용은 인증서 자동 등록 구성을 참조하십시오.
3. Microsoft Exchange를 실행하는 서버에서 인증서를 가져와 메일을 통해 전송하여 사용자에게 생성된 인증서를 배포합니다.
4. 각 사용자는 자신의 이메일 프로그램(예: Windows Outlook) 및 모바일 디바이스에 인증서를 설치합니다.

그룹 작업

WorkMail Amazon에서 그룹을 배포 목록으로 사용하여 <sales@example.com> 또는 <support@example.com> 같은 일반 이메일 주소로 이메일을 수신할 수 있습니다. 하나의 그룹에 대해 이메일 별칭을 여러 개 생성할 수 있습니다.

또한 그룹을 보안 그룹으로 사용하여 특정 팀과 사서함 또는 일정을 공유할 수도 있습니다.

그룹에는 자체 사서함이 없으며, 이는 그룹에 부여할 수 있는 사서함 권한에 영향을 줍니다. 그룹 권한 설정에 대한 자세한 내용은 그룹에 대한 사서함 권한 관리 단원을 참조하세요.

> **Note**
>
> 새로 추가한 그룹이 Microsoft Outlook 오프라인 주소록에 나타나려면 최대 2시간이 걸릴 수 있습니다.

주제

그룹 목록 보기

그룹 목록을 보려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.

2. 탐색 창에서 Organizations를 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택합니다.
4. 또한 그룹 이름 또는 기본 이메일 주소를 기준으로 그룹을 필터링할 수 있습니다.

> **Note**
>
> 검색은 대소문자를 구분합니다.

그룹 추가

Amazon WorkMail 콘솔에서 그룹을 추가할 수 있습니다.

그룹을 추가하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경하세요. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택한 다음 그룹 추가를 선택합니다.

   그룹 추가 페이지가 나타납니다.
4. 그룹 이름에 그룹 이름을 입력합니다.
5. 이메일 주소에 그룹의 기본 이메일 주소를 입력합니다.
6. 그룹의 이메일 주소를 확인하고 필요에 따라 업데이트하십시오.
7. 기본적으로 그룹은 전체 주소 목록에 표시됩니다. 전체 주소 목록에서 그룹을 숨기려면 전체 주소 목록에 표시 확인란의 선택을 취소합니다.
8. 그룹 추가를 선택합니다.

그룹 활성화

Amazon을 기업 Active WorkMail Directory와 통합하거나 간단한 Active Directory에 그룹이 이미 있는 경우 이러한 그룹을 Amazon의 보안 그룹 또는 배포 목록으로 사용할 수 WorkMail 있습니다.

기존 디렉터리 그룹을 활성화하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택합니다.
4. 활성화하려는 그룹 옆의 확인란을 선택한 다음 활성화를 선택합니다.

   그룹 활성화 대화 상자가 나타나고 작업을 확인하라는 메시지가 표시됩니다.
5. 필요에 따라 각 그룹의 기본 이메일 주소를 검토 및 변경한 다음 활성화를 선택합니다.

그룹에 구성원 추가

Amazon WorkMail 그룹을 생성하고 활성화한 후 Amazon WorkMail 콘솔을 사용하여 해당 그룹에 구성원을 추가합니다.

> **Note**
>
> WorkMail Amazon이 연결된 Active Directory 서비스 또는 Microsoft Active Directory와 통합되어 있는 경우 Active Directory를 사용하여 그룹 구성원을 관리할 수 있습니다. 그러나 변경 사항이 WorkMail Amazon으로 전파되는 데 시간이 더 오래 걸릴 수 있습니다.

그룹에 구성원을 추가하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.

2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택합니다.
4. 그룹의 이름을 선택합니다.
5. 그룹 세부 정보 페이지에서 구성원 탭을 선택합니다.
6. 그룹 또는 사용자에서 추가할 그룹 또는 사용자를 선택합니다.
7. 드롭다운에서 사용자 또는 그룹을 선택합니다.
8. 저장을 선택합니다.

변경 사항을 전파하는 데 몇 분 정도 걸릴 수 있습니다.

그룹 세부 정보 편집

그룹의 세부 정보를 편집할 수 있습니다.

그룹 세부 정보를 편집하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 [그룹] 을 선택한 다음 편집할 그룹을 선택합니다.
4. 그룹 세부 정보 페이지에서 필요에 따라 이메일 주소를 업데이트합니다.
5. 기본적으로 그룹은 전체 주소 목록에 표시됩니다. 전체 주소 목록에서 그룹을 숨기려면 전체 주소 목록에 표시 확인란의 선택을 취소합니다.
6. 변경 사항 저장을 선택합니다.

그룹에서 구성원 제거하기

Amazon WorkMail 콘솔을 사용하여 그룹에서 구성원을 제거합니다.

> **Note**
>
> WorkMail Amazon이 연결된 액티브 디렉터리 또는 Microsoft Active Directory와 통합되어 있는 경우 Active Directory를 사용하여 그룹 구성원을 관리할 수 있습니다. 하지만 이렇게 하면 WorkMail Amazon에 변경 사항을 전파하는 데 필요한 시간이 늘어날 수 있습니다.

그룹에서 구성원을 제거하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택한 다음 그룹 이름을 선택합니다.
4. 그룹 세부 정보 페이지에서 구성원 탭을 선택합니다.
5. 그룹에서 제거할 구성원을 선택합니다.
6. 제거(Remove)를 선택합니다.

변경 사항을 전파하는 데 몇 분 정도 걸릴 수 있습니다.

그룹 별칭 관리

그룹에 이메일 별칭을 추가하거나 제거할 수 있습니다.

그룹에 이메일 별칭을 추가하려면.

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 별칭을 추가하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 [그룹] 을 선택한 다음 별칭을 추가하려는 그룹의 이름을 선택합니다.
4. 그룹 세부 정보 섹션에서 별칭을 선택합니다.

5. 별칭에서 별칭 추가를 선택합니다.
6. 별칭 상자에 별칭을 입력합니다.
7. 별칭으로 사용할 도메인을 선택합니다.
8. 추가를 선택합니다.

그룹에서 이메일 별칭을 제거하려면.

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 별칭을 제거하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 [그룹] 을 선택한 다음 별칭을 제거하려는 그룹의 이름을 선택합니다.
4. 그룹 세부 정보 섹션에서 별칭을 선택합니다.
5. 별칭에서 제거하려는 별칭의 확인란을 선택합니다.
6. 제거(Remove)를 선택합니다.
7. 제거될 별칭을 확인합니다.
8. 별칭 제거 창에서 제거를 선택합니다.

그룹 비활성화

더 이상 필요 없는 그룹을 비활성화할 수 있습니다.

그룹을 비활성화하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택합니다.
4. 그룹 이름에서 비활성화할 그룹을 선택한 다음 비활성화를 선택합니다.
5. Disable group(s)(그룹 비활성화) 대화 상자에서 비활성화를 선택합니다.

그룹 삭제

그룹을 삭제하려면 먼저 그룹을 비활성화해야 합니다. 그룹을 비활성화하는 데 대한 정보는 그룹 비활성화 부분을 참조하세요.

그룹을 삭제하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택합니다.
4. 삭제하려는 비활성화된 그룹 옆의 확인란을 선택하고 삭제를 선택합니다.

   삭제 대화 상자가 나타납니다.
5. 삭제를 확인할 그룹 이름 입력 상자에 그룹 이름을 입력한 다음 삭제를 선택합니다.

> **Note**
>
> 그룹을 영구적으로 삭제하려면 Amazon용 `DeleteGroup` API 작업을 사용하십시오 WorkMail. 자세한 내용은 Amazon WorkMail API 참조를 참조하십시오 DeleteGroup.

리소스 작업

WorkMail Amazon은 사용자가 리소스를 예약하도록 지원할 수 있습니다. 예를 들어, 사용자는 회의실이나 프로젝터, 전화 또는 자동차와 같은 장비를 예약할 수 있습니다. 리소스를 예약하려면 사용자는 회의 초대에 리소스를 추가합니다.

주제

리소스 목록 보기

리소스 목록을 보려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 리소스를 선택합니다.
4. 또한 리소스 이름 또는 기본 이메일 주소를 기준으로 리소스를 필터링할 수 있습니다.

> **Note**
>
> 검색은 대소문자를 구분합니다.

리소스 추가

조직에 새 리소스를 추가하고 사용자가 해당 리소스를 예약할 수 있도록 합니다.

리소스를 추가하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 리소스를 선택한 다음 리소스 추가를 선택합니다.

   리소스 추가 페이지가 나타납니다.
4. 리소스 이름 상자에 리소스의 이름을 입력합니다.
5. 리소스 설명 상자에 리소스에 대한 설명을 입력할 수도 있습니다.
6. 리소스 유형에서 옵션을 선택합니다.
7. 리소스의 이메일 주소를 확인하고 필요에 따라 업데이트하세요.
8. 기본적으로 리소스는 전체 주소 목록에 표시됩니다. 전체 주소 목록에서 리소스를 숨기려면 전체 주소 목록에 표시 확인란의 선택을 취소합니다.
9. 리소스 추가를 선택합니다.

리소스 세부 정보 편집

이름, 설명, 유형, 이메일 주소, 예약 옵션, 대리인 등 리소스의 일반 세부 정보를 편집할 수 있습니다.

일반 리소스 세부 정보를 편집하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 [Resources]를 선택하고 편집하려는 리소스를 선택합니다.

4. 리소스 세부 정보 페이지에서 필요에 따라 리소스 이름, 설명, 리소스 유형 또는 이메일 주소를 업데이트합니다.
5. 기본적으로 리소스는 전체 주소 목록에 표시됩니다. 전체 주소 목록에서 리소스를 숨기려면 전체 주소 목록에 표시 확인란의 선택을 취소합니다.
6. 변경 사항 저장을 선택합니다.

예약 요청을 자동으로 허용 또는 거부하도록 리소스를 구성할 수 있습니다.

리소스의 예약 옵션을 편집할 수 있습니다.

리소스의 예약 옵션을 변경하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 [Resources]를 선택하고 편집하려는 리소스를 선택합니다. 페이지가 나타나고 리소스 세부 정보가 표시됩니다.
4. 예약 옵션에서 편집을 선택합니다.
5. 필요에 따라 옵션 옆의 확인란을 선택하거나 선택 취소하여 옵션을 활성화하거나 비활성화합니다.

> **Note**
>
> 자동 예약 옵션을 사용하지 않도록 설정하는 경우 예약 요청을 처리할 대리인을 만들어야 합니다. 다음 단계에서는 대리인을 생성하는 방법을 설명합니다.

자동 예약 옵션이 구성되어 있지 않은 리소스에 대한 예약 요청을 제어하는 대리인을 추가할 수 있습니다. 리소스 대리인은 모든 예약 요청의 복사본을 자동으로 수신하고 리소스 일정에 대한 모든 권한을 갖습니다. 또한 리소스에 대한 모든 예약 요청을 허용해야 합니다.

리소스 대리인을 추가하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.

2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 리소스를 선택하고 대리인을 추가하려는 리소스의 이름을 선택합니다.
4. (선택 사항) 예약 옵션 탭에서 편집을 선택하고 모든 리소스 요청 자동 수락 확인란의 선택을 취소한 다음 저장을 선택합니다.
5. 대리인 탭을 선택한 다음 대리인 추가를 선택합니다.

   대리인 추가 대화 상자가 나타납니다.
6. 대리인 검색 목록을 열고 대리인을 선택한 다음 저장을 선택합니다.

리소스 대리인을 제거하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 대리인을 제거하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 리소스를 선택한 다음 대리인을 제거하려는 리소스의 이름을 선택합니다.
4. 대리자를 선택한 다음 제거할 대리인을 선택합니다.
5. 제거를 선택합니다.

리소스 별칭 관리

리소스에 이메일 별칭을 추가하거나 제거할 수 있습니다.

리소스에 이메일 별칭을 추가하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.

2. 탐색 창에서 Organizations를 선택한 다음 별칭을 추가할 조직의 이름을 선택합니다.
3. 탐색 창에서 [Resources] 를 선택한 다음 별칭을 추가하려는 리소스의 이름을 선택합니다.
4. 리소스 세부 정보 섹션에서 별칭을 선택합니다.
5. 별칭에서 별칭 추가를 선택합니다.
6. 별칭 상자에 별칭을 입력합니다.
7. 별칭으로 사용할 도메인을 선택합니다.
8. 추가를 선택합니다.

리소스에서 이메일 별칭을 제거하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 Organizations를 선택한 다음 별칭을 제거하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 [Resources] 를 선택한 다음 별칭을 제거하려는 리소스의 이름을 선택합니다.
4. 리소스 세부 정보 섹션에서 별칭을 선택합니다.
5. 별칭에서 제거하려는 별칭의 확인란을 선택합니다.
6. 제거(Remove)를 선택합니다.
7. 제거될 별칭을 확인합니다.
8. 별칭 제거 창에서 제거를 선택합니다.

리소스 활성화

기본적으로 WorkMail Amazon은 리소스를 생성합니다. 본인 또는 다른 사람이 리소스를 비활성화한 경우 30일 이내에 리소스를 다시 활성화할 수 있습니다.

리소스를 활성화하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 리전에 대한 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.

2. 탐색 창에서 조직을 선택한 다음 활성화하려는 리소스가 있는 조직을 선택합니다.
3. 탐색 창에서 리소스를 선택합니다.
4. 리소스 목록에서 활성화하려는 리소스 옆에 있는 버튼을 선택한 다음 활성화를 선택합니다.

   리소스 활성화 대화 상자가 나타납니다.
5. 활성화를 선택합니다.

리소스 비활성화

리소스를 비활성화하면 예약할 수 없게 됩니다. 예를 들어, 리모델링하는 동안에는 회의실을 비활성화했다가 회의실이 사용 가능해지면 활성화할 수 있습니다.

리소스를 비활성화하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 리전에 대한 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 비활성화하려는 리소스가 있는 조직을 선택합니다.
3. 탐색 창에서 리소스를 선택합니다.
4. 리소스 목록에서 비활성화하려는 리소스 옆에 있는 버튼을 선택한 다음 비활성화를 선택합니다.

   리소스 비활성화 대화 상자가 나타납니다.
5. 비활성화를 선택합니다.

리소스 삭제

리소스를 더 이상 사용할 필요가 없는 경우 삭제할 수 있습니다. 그러나 먼저 리소스를 비활성화해야 합니다. 리소스 비활성화에 대한 자세한 내용은 이전 섹션의 단계를 참조하세요.

리소스를 제거하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 리전에 대한 자세한 내용은 Amazon Web Services 일반 참조의 리전 및 엔드포인트를 참조하세요.

2. 탐색 창에서 조직을 선택한 다음 원하는 조직을 선택합니다.
3. 탐색 창에서 리소스를 선택합니다.
4. 리소스 목록에서 제거하려는 비활성화된 리소스 옆에 있는 버튼을 선택한 다음 삭제를 선택합니다.

   리소스 삭제 대화 상자가 나타납니다.
5. 삭제를 확인하려는 리소스 이름 입력 상자에 삭제하려는 리소스의 이름을 입력한 다음 리소스 삭제를 선택합니다.

모바일 디바이스 작업

이 섹션의 항목에서는 Amazon에 연결된 모바일 디바이스를 관리하는 방법을 설명합니다 WorkMail.

주제

조직의 모바일 디바이스 정책 편집

조직의 모바일 장치 정책을 편집하여 모바일 장치가 Amazon과 상호 작용하는 방식을 변경할 수 WorkMail 있습니다.

조직의 모바일 디바이스 정책을 편집하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 이름 및 엔드포인트를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 Mobile Policies(모바일 정책)을 선택한 다음 Mobile policy(모바일 정책) 화면에서 편집을 선택합니다.
4. 필요에 따라 다음 중 일부를 업데이트합니다.

   a. Require encryption on device(디바이스에서 암호화 필요): 모바일 디바이스에서 이메일 데이터를 암호화합니다.

   b. Require encryption on storage card(스토리지 카드에서 암호화 필요): 모바일 디바이스의 이동식 스토리지에서 이메일 데이터를 암호화합니다.

   c. 암호 필요: 모바일 디바이스를 잠그려면 암호가 필요합니다.

   d. 간단한 암호 허용: 디바이스의 PIN을 암호로 사용합니다.

   e. 최소 암호 길이: 유효한 암호에 필요한 문자 수를 설정합니다.

f. 영숫자 암호 요구: 암호가 문자 및 숫자로 구성되어야 합니다.

g. 허용 실패 시도 횟수: 사용자 디바이스가 초기화되기 전에 허용되는 디바이스 잠금 해제 실패 횟수를 지정합니다. 장치를 초기화하면 개인 파일을 포함한 모든 데이터가 삭제됩니다.

h. [Password expiration]: 암호가 만료되어 변경해야 하기 전에 남은 일수를 지정합니다.

i. [Enable screen lock]: 사용자 화면을 잠그기 위해 사용자의 입력 없이 경과해야 하는 시간(초)을 지정합니다.

j. Enforce password history(암호 기록 적용): 동일한 암호를 반복하기 전에 입력할 수 있는 암호의 개수를 지정합니다.

5. 저장을 선택합니다.

모바일 디바이스 관리

이 섹션의 항목에서는 모바일 디바이스를 원격으로 초기화하고, 조직에서 디바이스를 제거하고, 디바이스의 세부 정보를 보는 방법을 설명합니다. 조직의 모바일 디바이스 정책 활성화에 대한 자세한 내용은 조직의 모바일 디바이스 정책 편집 단원을 참조하십시오.

주제

- 원격으로 모바일 디바이스 지우기
- 디바이스 목록에서 사용자 디바이스 제거
- 모바일 디바이스 세부 정보 보기

원격으로 모바일 디바이스 지우기

이 섹션의 단계에서는 모바일 디바이스를 원격으로 지우는 방법을 설명합니다. 다음 사항에 유의하세요.

- 기기는 온라인 상태이고 Amazon에 연결되어 있어야 WorkMail 합니다. 누군가 디바이스 연결을 끊은 경우, 사용자가 디바이스를 다시 연결하면 지우기 작업이 재개됩니다.
- 지우기 작업을 전파하는 데 5분이 걸릴 수 있습니다.

> **Important**
>
> 대부분의 모바일 디바이스에서 원격 지우기를 수행하면 디바이스가 공장 기본값으로 재설정됩니다. 이 절차를 수행하면 개인 파일을 비롯하여 모든 데이터가 제거될 수 있습니다.

사용자의 모바일 디바이스를 원격으로 지우려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 리전 이름 및 엔드포인트를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택한 다음 사용자 목록에서 디바이스를 지울 사용자의 이름을 선택합니다.
4. 모바일 디바이스 탭을 선택합니다.
5. 디바이스 목록에서 디바이스 옆의 버튼을 선택한 다음 지우기를 선택합니다.
6. 개요에서 상태를 확인하고 지우기 요청 여부를 확인합니다.
7. 디바이스를 지운 후 디바이스 목록에서 제거합니다. 다음 섹션의 단계에서는 방법을 설명합니다.

> **Important**
>
> 초기화된 디바이스를 사용자의 디바이스 목록으로 되돌리려면 먼저 디바이스 목록에서 제거해야 합니다. 그렇지 않으면 시스템이 디바이스를 다시 지웁니다.

디바이스 목록에서 사용자 디바이스 제거

누군가가 특정 모바일 디바이스 사용을 중단했거나 원격으로 디바이스를 지운 경우, 디바이스 목록에서 디바이스를 제거할 수 있습니다. 사용자가 해당 디바이스를 다시 구성하면 목록에 표시됩니다.

디바이스 목록에서 사용자의 모바일 디바이스를 제거하려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택하고 편집하려는 사용자의 이름을 선택합니다.
4. 모바일 디바이스 탭을 선택합니다.
5. 디바이스 목록에서 제거하려는 디바이스를 선택하고 디바이스 제거를 선택합니다.

모바일 디바이스 세부 정보 보기

사용자 모바일 디바이스의 세부 정보를 볼 수 있습니다.

> **Note**
>
> 일부 디바이스는 모든 세부 정보를 서버로 전송하지 않습니다. 사용 가능한 모든 디바이스 세부 정보가 표시되지 않을 수 있습니다.

디바이스 세부 정보를 보려면

1. https://console.aws.amazon.com/workmail/ 에서 아마존 WorkMail 콘솔을 엽니다.

   필요한 경우, 지역을 변경합니다. 탐색 모음에서 요구에 맞는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택한 다음 모바일 디바이스 탭을 선택합니다.
4. 디바이스 목록에서 세부 정보를 보려는 디바이스의 ID를 선택합니다.

   다음 표에는 디바이스 상태 코드가 나와 있습니다.

상태	설명
PROVISIONING_REQUIRED	사용자 또는 관리자가 Amazon에서 사용할 수 있도록 디바이스를 프로비저닝하도록 요청했습니다. WorkMail Amazon WorkMail 콘솔에서 해당 디바이스에 대한 현재 정책을 수정하는 경우에도 디바이스는 이 상태로 설정됩니다.
PROVISIONING_SUCCEEDED	디바이스가 성공적으로 프로비저닝되었습니다. 디바이스가 주어진 정책을 적용했습니다.
WIPE_REQUIRED	관리자가 Amazon WorkMail 콘솔에서 삭제를 요청했습니다.
WIPE_SUCCEEDED	디바이스가 성공적으로 지워졌습니다.

모바일 디바이스 액세스 규칙 관리

Amazon WorkMail의 모바일 디바이스 액세스 규칙을 통해 관리자는 특정 유형의 모바일 디바이스에 대한 사서함 액세스를 제어할 수 있습니다. 기본적으로 각 Amazon WorkMail 조직은 유형, 모델, 운영 체제 또는 사용자 에이전트와 상관없이 모든 디바이스에 사서함 액세스 권한을 부여하는 규칙을 사용합니다. 해당 기본 규칙을 편집하거나 자체 규칙으로 바꿀 수 있습니다. 규칙을 추가, 변경 및 삭제할 수도 있습니다.

Warning

조직에 대한 모든 모바일 디바이스 액세스 규칙을 삭제하면 Amazon WorkMail은 모든 모바일 디바이스 액세스를 차단합니다.

다음 디바이스 속성을 기반으로 액세스를 허용하거나 거부하는 규칙을 생성할 수 있습니다.

- 디바이스 유형 - "iPhone", "iPad" 또는 "Android."
- 디바이스 모델 - "iPhone10C1", "iPad5C1" 또는 "HTCOneX."
- 디바이스 운영 체제 - "iOS 12.3.1 16F203" 또는 "Android 8.1.0".
- 디바이스 사용자 에이전트 - "iOS/14.2 (18B92) exchangesyncd/1.0," 또는 "Android-Mail/7.7.16.163886392.release."

AWS 관리 콘솔에서 디바이스 속성을 보려면 모바일 디바이스 세부 정보 보기를 참조하세요.

Note

일부 디바이스 및 클라이언트는 모든 필드의 속성을 보고하지 않을 수 있습니다. 이러한 경우를 해결하는 방법에 대한 자세한 내용은 Dealing with empty fields 부분을 참조하세요.

Important

Amazon WorkMail 모바일 디바이스 액세스 규칙은 Microsoft Exchange ActiveSync 프로토콜을 사용하는 디바이스에만 적용됩니다. IMAP과 같은 다른 프로토콜을 사용하는 모바일 클라이언트는 여기에 나열된 디바이스 속성을 보고하지 않으므로 이러한 규칙은 적용되지 않습니다. 다른 프로토콜을 사용하는 디바이스에 대한 액세스를 제한해야 하는 경우 액세스 제어 규칙을 만들 수 있습니다. 이에 대한 자세한 내용은 액세스 제어 규칙 작업을 참조하세요. 예를 들

어 다른 프로토콜과 웹 메일에 대한 액세스를 회사 IP 주소 범위로만 제한하고 다른 곳에서는 Microsoft ActiveSync를 허용한 다음, 모바일 디바이스 액세스 규칙을 사용하여 허용된 클라이언트의 유형 및 버전을 추가로 제한할 수 있습니다.

주제

모바일 디바이스 액세스 규칙의 작동 방식

모바일 디바이스 액세스 규칙은 Microsoft Exchange ActiveSync 프로토콜을 사용하는 디바이스에만 적용됩니다. 각 규칙에는 규칙이 적용되는 시점을 지정하는 일련의 조건과 함께 디바이스에 대한 `ALLOW` 및 `DENY` 액세스 효과도 있습니다. 규칙은 규칙의 모든 조건이 사용자 모바일 디바이스의 속성과 일치하는 경우에만 액세스 요청에 적용됩니다. 조건이 없는 규칙은 모든 요청에 적용됩니다. 각 조건은 디바이스의 보고된 속성과 대소문자를 구분하지 않는 접두사 일치를 사용합니다.

Amazon WorkMail은 규칙을 다음과 같이 평가합니다.

- 디바이스 속성과 일치하는 `DENY` 규칙이 있는 경우 정책이 디바이스를 차단합니다. `DENY` 규칙이 `ALLOW` 규칙보다 우선합니다.
- 하나 이상의 `ALLOW` 규칙이 일치하고 `DENY` 규칙이 하나도 일치하지 않는 경우, 정책에서 디바이스를 허용합니다.
- 규칙이 적용되지 않으면 디바이스가 차단됩니다.

Important

모바일 디바이스는 규칙이 작동하는 데 사용하는 속성을 보고합니다. 디바이스는 Microsoft ActiveSync 디바이스 프로비저닝 프로세스 중에 속성을 보고합니다. Amazon WorkMail은 모바일 클라이언트가 올바른 정보 또는 최신 정보를 보고하는지 독립적으로 확인할 수 없습니다.

모바일 디바이스 액세스 규칙 사용

API 또는 AWS 명령줄 인터페이스(CLI)를 사용하여 모바일 디바이스 액세스 규칙을 생성하고 관리할 수 있습니다. AWS CLI에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서 섹션을 참조하세요.

> **Important**
>
> Amazon WorkMail 조직의 액세스 규칙을 변경하면 영향을 받는 디바이스가 업데이트된 규칙을 따르는 데 5분이 걸릴 수 있으며, 이 시간 동안 디바이스는 일관되지 않은 동작을 보일 수 있습니다. 하지만 규칙을 테스트하면 즉시 올바른 동작이 표시됩니다. 자세한 내용은 Testing mobile device access rules 섹션을 참조하세요.

모바일 디바이스 액세스 규칙 나열

다음 예제에서는 모바일 디바이스 액세스 규칙을 표시하는 방법을 보여줍니다.

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

모바일 디바이스 액세스 규칙 생성

다음 예제에서는 모든 Android 디바이스가 사서함에 액세스하는 것을 차단하는 규칙을 만듭니다.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

다음 예제에서는 특정 버전의 iOS만 허용하는 규칙을 생성합니다. 기본 `ALLOW-all` 규칙을 제거해야 합니다.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

모바일 디바이스 액세스 규칙 업데이트

다음 예시에서는 식별자를 추가하여 디바이스 규칙을 업데이트합니다.

```
aws workmail update-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d --
name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.4"
```

모바일 디바이스 액세스 규칙 삭제

다음 예시에서는 지정된 식별자를 사용하는 모바일 디바이스 액세스 규칙을 삭제합니다.

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

모바일 디바이스 액세스 규칙 테스트

액세스 규칙을 테스트하려면 GetMobileDeviceAccessEffect API 또는 AWS CLI에서 get-mobile-device-access-effect 명령을 사용할 수 있습니다. AWS CLI에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서 섹션을 참조하세요.

테스트할 때 시뮬레이션된 모바일 디바이스의 속성을 전달하면 API 또는 CLI가 해당 속성을 가진 실제 모바일 디바이스가 받을 액세스 효과(ALLOW 또는 DENY)를 반환합니다. 예를 들어, 이 명령은 iOS 14.2를 실행하는 iPhone과 기본 메일 앱이 사서함에 액세스할 수 있는지 여부를 테스트합니다.

```
aws workmail get-mobile-device-access-effect --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --device-type "iPhone" --device-model "iPhone10C1"
 --device-operating-system "iOS 14.2.1 16F203" --device-user-agent "iOS/14.2 (18B92)
 exchangesyncd/1.0"
```

빈 필드 처리

일부 모바일 디바이스 또는 클라이언트는 하나 이상의 필드에 대한 정보를 보고하지 않아 값을 비워 둘 수 있습니다. 조건에 특수 값 $NONE을 사용하여 규칙을 이러한 디바이스와 일치시킬 수 있습니다. 예를 들어, DeviceTypes=["iphone", "ipad", "$NONE"]이 있는 규칙의 경우 "iphone" 또는 "ipad"의 디바이스 유형을 보고하는 디바이스를 일치시키거나 디바이스 유형을 전혀 보고하지 않습니다.

NotDeviceTypes 또는 NotDeviceUserAgents와 같은 부정적인 조건은 이러한 빈 값과 일치하지 않습니다. 예를 들어, NotDeviceTypes=["android"]가 있는 규칙은 "android" 이외의 디바이스 유형을 보고하는 디바이스를 일치시킵니다. 하지만 디바이스 유형을 전혀 보고하지 않는 디바이스에는 규칙이 적용되지 않습니다.

모바일 디바이스 액세스 재정의 관리

모바일 디바이스 액세스 재정의를 사용하여 모바일 디바이스 액세스 규칙의 결과를 재정의합니다. 재정의는 특정 사용자 및 디바이스에 적용되며 기본 액세스 규칙을 반대로 수행합니다. 또한 재정의를 사용하여 액세스 규칙에 대한 일회성 예외를 만들고 특정 사용자 및 디바이스 쌍을 허용하거나 거부할 수 있습니다. 또한 `DefaultDenyAll` 모바일 디바이스 액세스 규칙에 재정의를 사용할 수 있습니다. 그러면 타사 모바일 디바이스 관리(MDM) 솔루션에 대한 액세스 결정이 연기됩니다. 자세한 내용은 재정의 관리 및 모바일 디바이스 관리 솔루션과 통합 섹션을 참조하세요.

주제

- 모바일 디바이스 액세스 재정의의 작동 방식
- 재정의 관리

모바일 디바이스 액세스 재정의의 작동 방식

특정 사용자 및 디바이스 쌍에 대한 모바일 디바이스 액세스 재정의를 생성합니다. 재정의는 특정 사용자 및 디바이스에 대한 모바일 디바이스 액세스 규칙을 평가할 때 기본 액세스 결과를 반대로 수행합니다. 예를 들어, 액세스 규칙이 일반적으로 액세스를 거부하는 경우 액세스 재정의는 해당 사용자와 디바이스가 이메일을 동기화하도록 허용합니다. 반대로, 액세스 규칙이 일반적으로 액세스를 허용하는 경우 사용자 및 디바이스가 메일을 동기화하지 못하도록 방지하는 재정의를 만들 수 있습니다. 모바일 장치 액세스 재정의를 삭제하면 Amazon은 WorkMail 다시 현재 모바일 장치 액세스 규칙의 결과를 고려하여 해당 사용자 및 장치에 대한 액세스 권한을 부여할지 여부를 결정합니다.

> **Important**
>
> Amazon WorkMail 조직의 모바일 디바이스 액세스 권한 재정의를 변경하는 경우 영향을 받는 디바이스가 업데이트된 재정의를 따르는 데 5분이 걸릴 수 있습니다.

재정의 관리

모바일 디바이스 액세스 재정의는 API 또는 AWS Command Line Interface를 사용하여 생성, 업데이트 또는 삭제할 수 있습니다. 에 AWS CLI대한 자세한 내용은 AWS 명령줄 인터페이스 사용 설명서를 참조하십시오.

디바이스 ID를 찾으려면 AWS Management Console을 사용하세요. 자세한 내용은 모바일 디바이스 세부 정보 보기를 참조하세요.

모바일 디바이스 액세스 재정의 나열

이 예제는 지정된 Amazon WorkMail 조직에 대한 모든 모바일 장치 액세스 재정의를 나열하는 방법을 보여줍니다.

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

모바일 디바이스 액세스 재정의 생성 및 업데이트

그러면 지정된 Amazon WorkMail 조직, 사용자 및 장치 ID에 대한 액세스를 거부하는 모바일 장치 액세스 재정의가 생성됩니다.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect DENY
```

기존 모바일 디바이스 액세스 재정의를 수정하여 다른 효과를 낼 수 있습니다. 이렇게 하면 이전에 만든 모바일 디바이스 액세스 재정의가 업데이트되어 액세스를 거부하는 대신 허용합니다.

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0 --effect ALLOW
```

모바일 디바이스 액세스 재정의 삭제

이렇게 하면 지정된 Amazon WorkMail 조직, 사용자 및 장치 ID에 대한 모바일 장치 액세스 재정의가 삭제됩니다.

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECD0
```

모바일 디바이스 관리 솔루션과 통합

WorkMail Amazon은 모바일 장치 정책 및 모바일 장치 액세스 규칙을 통해 몇 가지 기본적인 모바일 장치 관리 기능을 지원합니다. 그러나 이러한 기능은 Microsoft Exchange ActiveSync (EAS) 프로토콜을 통해서만 모바일 장치와 상호 작용할 수 있으므로 장치 보안 상태를 검사하고 적용하는 기능이 제한적

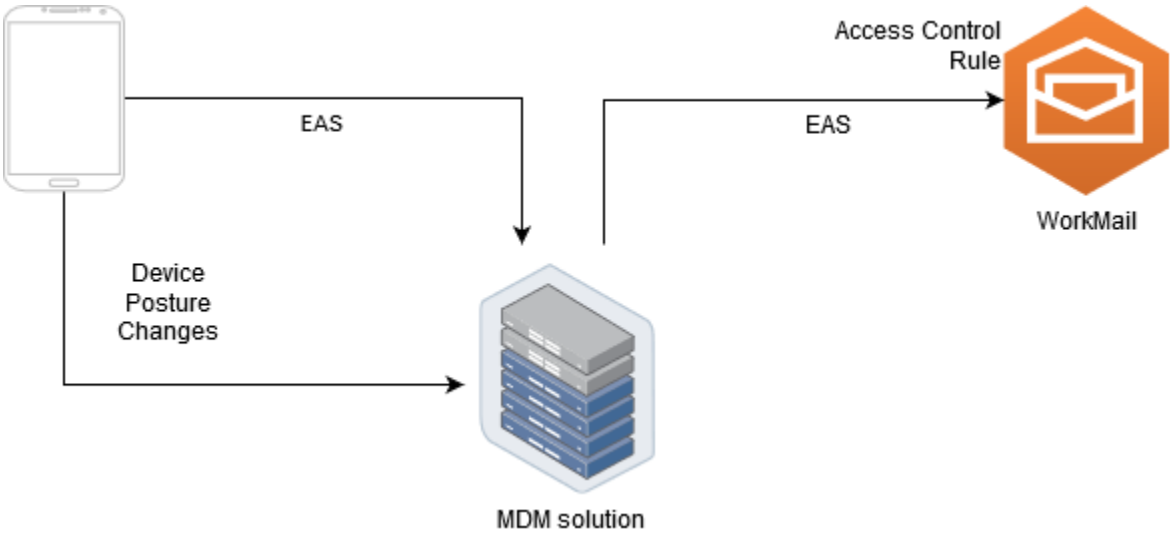
입니다. 디바이스 보안 및 규정 준수에 대한 제어를 강화해야 하는 관리자는 타사 모바일 디바이스 관리(MDM) 솔루션을 사용할 수 있습니다.

모바일 디바이스 관리 솔루션 개요

MDM 솔루션은 프록시 또는 다이렉트의 두 가지 모드로 구성할 수 있습니다. 솔루션이 지원하는 모드를 확인하려면 MDM 설명서를 참조하세요.

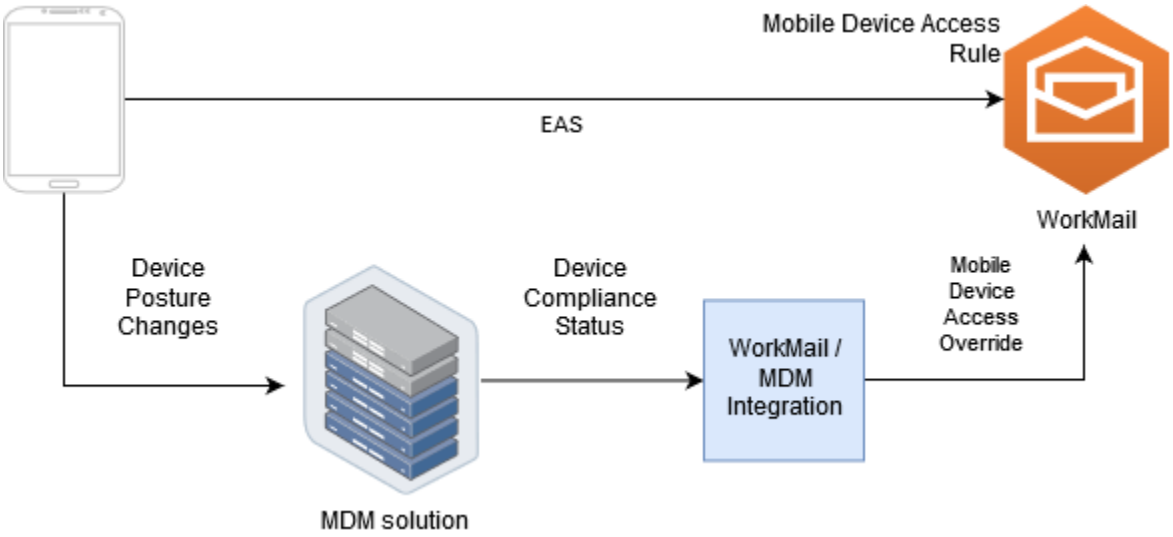
프록시 모드에서 모바일 디바이스는 MDM 솔루션을 통해 Exchange 액티브 싱크 (EAS) 프로토콜을 사용하여 Amazon에 액세스합니다. WorkMail MDM 솔루션은 디바이스 상태를 사용하여 Amazon WorkMail 데이터에 대한 액세스를 허용하거나 거부합니다. Amazon WorkMail 측에서는 MDM 솔루션의 IP 주소 또는 주소에서만 EAS 액세스를 허용하는 액세스 제어 규칙을 사용하십시오. 자세한 내용은 액세스 제어 규칙 작업을 참조하세요.

다음은 일반적인 프록시 모드 구성을 보여줍니다.



다이렉트 모드에서 모바일 디바이스는 EAS를 사용하여 Amazon에 WorkMail 직접 액세스합니다. MDM 솔루션은 디바이스 상태 변경을 수신하고 각 디바이스가 해당 요구 사항을 충족하는지 여부를 지속적으로 평가합니다. MDM 솔루션은 디바이스가 규정을 위반하는 등의 상태 변화를 감지하면 몇 가지 조치를 취할 수 있으며 일반적으로 알림이나 이벤트를 내보냅니다. Amazon WorkMail 관리자는 이러한 규정 준수 상태 이벤트를 수신하도록 시스템을 설정하고 MDM 장치 요구 사항을 준수하거나 준수하지 않을 때 장치에 대한 액세스를 허용하거나 거부하는 모바일 장치 액세스 재정의를 자동으로 생성할 수 있습니다.

다음은 일반적인 직접 모드 구성을 보여줍니다.



직접 모드에서 타사 MDM 솔루션과 통합하도록 WorkMail 조직 구성

직접 모드에서 타사 모바일 디바이스 관리(MDM) 솔루션과 통합하려면 다음 요구 사항을 충족해야 합니다.

- 사용자 장치에 대한 액세스를 ActiveSync 프로토콜로만 제한하는 액세스 제어 규칙을 만드세요.
- 알 수 없거나 관리되지 않는 모든 모바일 장치가 기본적으로 거부되도록 하려면 기본 deny-to-all ""모바일 장치 액세스 규칙을 만드십시오.
- 디바이스가 보안 태세를 변경하는 경우(즉, 규정을 준수하거나 준수하지 않게 됨), 사용자 지정 알림 또는 이벤트를 발생시키는 모바일 디바이스 관리 솔루션을 채택하세요.
- 사용자 지정 소프트웨어 구성 요소를 생성하여 이러한 알림을 수신하고 Amazon WorkMail SDK를 호출하여 모바일 디바이스 액세스 재정의를 생성합니다.

이러한 구성 요소는 모든 사용자 장치가 MDM 규정 준수 요구 사항을 충족하는지 확인한 후 Amazon WorkMail 사서함에 액세스할 수 있도록 합니다.

액세스 제어 규칙을 사용하여 모바일 디바이스 액세스를 다음으로 제한하십시오. ActiveSync

모든 장치가 프로토콜만 사용하는지 확인하고 액세스 제어 규칙을 사용하여 ActiveSync 프로토콜만 사용하도록 해야 합니다. 예를 들어 내부 회사 IP 주소 범위에서만 다른 메일 프로토콜에 대한 액세스 권한을 부여한 다음 회사 방화벽 외부에서 이메일에 액세스하는 ActiveSync 경우에만 허용할 수 있습니다. 디바이스 ID로는 디바이스만 ActiveSync 식별할 수 있으므로 이렇게 해야 합니다. IMAP(인터넷 메시지 액세스 프로토콜) 또는 Exchange 웹 서비스와 같은 프로토콜은 사용할 수 없습니다. 자세한 정보는 액세스 제어 규칙 작업을 참조하세요.

기본 '전체 거부' 액세스 규칙 만들기

모든 모바일 디바이스 액세스 결정을 타사 모바일 디바이스 관리 솔루션에 맡기려면 사용자별 또는 디바이스별로 재정의하지 않는 한 모든 디바이스를 자동으로 거부하는 액세스 규칙을 만드세요. 자세한 정보는 모바일 디바이스 액세스 규칙 관리 단원을 참조하세요.

이 예제에서는 '전체 거부' 규칙을 보여줍니다.

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

디바이스 상태 변화에 대응하고 모바일 디바이스 액세스 재정의를 생성하세요.

디바이스 상태 변경에 대한 알림을 보내도록 MDM 솔루션을 구성해야 합니다. Amazon WorkMail SDK를 사용하여 모바일 디바이스 액세스 재정의를 생성하거나 업데이트할 수 있는 구성 요소가 이러한 알림을 사용해야 합니다. Amazon은 이 주제 앞부분에서 설명한 기본 “전체 WorkMail 거부” 모바일 디바이스 액세스 규칙 때문에 관리되지 않거나 새로 프로비저닝된 디바이스에 대한 액세스를 기본적으로 거부합니다. MDM 솔루션에서 디바이스가 모든 요구 사항을 충족한다고 판단하고 디바이스가 규정을 준수한다는 알림을 보내면 이 구성 요소는 지정된 사용자 및 디바이스에 대해 ALLOW 효과가 있는 모바일 디바이스 액세스 재정의를 생성하여 이 알림에 반응할 수 있습니다. 나중에 디바이스가 규정을 준수하지 않게 되면 모바일 디바이스 관리 솔루션에서 또 다른 알림을 보내며, 액세스 재정의를 삭제하거나 수정하여 해당 디바이스에 대한 액세스를 거부할 수 있습니다. 자세한 정보는 모바일 디바이스 액세스 재정의 관리을 참조하세요.

MDM과 WorkMail 통합된 Amazon의 예는 이 AWS 샘플 애플리케이션을 참조하십시오.

사서함 권한을 사용한 작업

Amazon WorkMail의 사서함 권한을 사용하여 사용자 및 그룹에게 다른 사용자의 사서함에서 작업할 권한을 부여할 수 있습니다. 사서함 권한은 전체 사서함에 적용됩니다. 이를 통해 여러 사용자가 사서함의 자격 증명을 공유하지 않고도 동일한 사서함에 액세스할 수 있습니다. 사서함 권한이 있는 사용자들은 사서함 데이터를 읽고 수정하며 공유 사서함에서 이메일을 보낼 수 있습니다.

> **Note**
>
> 전체 주소 목록에서 숨겨진 사용자의 사서함에 대한 사용 권한이 있는 사용자는 숨겨진 사용자의 사서함에 계속 액세스할 수 있습니다.

다음 목록은 사용자가 부여할 수 있는 권한을 보여줍니다.

- 전체 액세스 - 폴더 수준의 권한을 수정하는 권한을 포함하여 사서함에 대한 전체 읽기 및 쓰기 액세스를 가능하게 해줍니다.

  > **Note**
  >
  > 이 옵션은 사용자만 사용할 수 있습니다. 그룹에는 모든 액세스 권한을 부여할 수 없습니다.

- 대신하여 보내기 - 사용자나 그룹이 다른 사용자를 대신하여 이메일을 보낼 수 있게 해줍니다. 사서함 소유자는 [From:] 헤더에 표시되고 발신자는 [Sender:] 헤드에 표시됩니다.
- 다음으로 보내기 – Amazon WorkMail이 연결된 Active Directory 서비스 또는 Microsoft Active Directory와 통합된 경우 Active Directory를 사용하여 그룹 멤버를 관리할 수 있습니다. 사서함 소유자가 [From:] 헤더와 [Sender:] 헤더에 모두 표시됩니다.
- 없음 - 사용자 또는 그룹이 이메일을 보내지 못하도록 합니다.

> **Note**
>
> 한 그룹에 사서함 권한을 부여하면 그 권한이 중첩된 그룹들의 구성원을 포함하여 그 그룹의 모든 구성원에게 확대됩니다.

사서함 권한을 부여하면 Amazon WorkMail AutoDiscover 서비스가 사용자가 추가한 사용자나 그룹의 그 사서함에 대한 액세스를 자동으로 업데이트합니다.

Windows의 Microsoft Outlook 클라이언트의 경우, 최대 액세스 권한을 가진 사용자는 공유된 사서함에 자동으로 액세스할 수 있습니다. 변경 사항을 전파하는 데 60분 정도 걸릴 수 있으며, 그런 다음 Microsoft Outlook을 다시 시작합니다.

Amazon WorkMail 웹 애플리케이션과 기타 이메일 클라이언트의 경우, 최대 액세스 권한을 가진 사용자가 공유된 사서함을 수동으로 열 수 있습니다. 열린 사서함은 사용자가 닫지 않는 한 다른 세션으로 넘어갈 때도 계속 열려 있습니다.

주제

사서함 및 폴더 권한에 대해

사서함 권한은 사서함 내의 모든 폴더에 적용됩니다. 이 권한은 Amazon WorkMail 관리 API를 호출하도록 승인된 AWS 계정 보유자나 IAM 사용자만이 활성화할 수 있습니다. 사서함 또는 그룹 전체에 대한 권한을 설정하고 변경하려면 AWS Management Console 또는 Amazon WorkMail API를 사용하세요. 콘솔에서 최대 100개의 메일박스 및 그룹 권한을 관리할 수 있습니다. 더 많은 사용자와 그룹에 대한 권한을 관리하려면 Amazon WorkMail API를 사용하세요.

폴더 권한은 하나의 폴더에만 적용됩니다. 최종 사용자는 이메일 클라이언트를 사용하거나 Amazon WorkMail 웹 애플리케이션을 사용하여 폴더 권한을 설정할 수 있습니다. Amazon WorkMail 웹 애플리케이션을 사용하여 폴더를 공유하는 방법에 대한 자세한 내용은 Amazon WorkMail 사용 설명서의 폴더 및 폴더 권한 공유를 참조하세요.

사용자에 대한 사서함 권한 관리

Amazon WorkMail 콘솔을 사용하여 그룹뿐만 아니라 사용자에 대한 사서함 권한을 관리할 수 있습니다. 다음 섹션에서는 사용자에 대한 권한을 관리하는 방법을 설명합니다. 그룹 권한 관리에 대한 자세한 내용은 그룹에 대한 사서함 권한 관리 부분을 참조하세요.

주제

권한 추가

권한을 추가하면 한 사용자에게 다른 사용자의 사서함에서 하나 이상의 작업을 수행할 수 있는 권한을 부여합니다. 예를 들어, 직원 A가 상사인 직원 B를 대신하여 메시지를 보내야 한다고 가정해 보겠습니다. 이 권한을 부여하려면 직원 B의 사서함 설정으로 이동하여 직원 A에게 요청된 작업을 수행할 수 있는 권한을 부여합니다.

사서함 권한을 추가하려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 리전을 변경합니다. 탐색 모음에서 요구에 맞는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 권한을 관리하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택한 다음 권한을 관리하려는 사용자의 이름을 선택합니다.
4. 권한 탭을 선택한 다음 Add permissions(권한 추가)를 선택합니다.

   권한 추가 대화 상자가 나타납니다.
5. 새 권한 추가 목록을 열고 사서함에 액세스해야 하는 사용자 또는 그룹을 선택합니다.
6. 사서함 권한 및 전송 권한에서 원하는 옵션을 선택합니다.
7. 추가(Add)를 선택합니다.

새 권한을 사용자에게 전파하는 데 최대 5분이 걸릴 수 있습니다.

사용자에 대한 사서함 권한 편집

사용자의 사서함 권한을 편집하면 해당 사용자의 사서함에 대한 다른 사용자의 액세스 권한이 변경됩니다. 사서함 권한을 편집해도 사서함의 원래 사용자 액세스 권한은 변경되지 않습니다.

사서함 권한을 편집하려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 리전을 변경합니다. 탐색 모음에서 요구에 맞는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 권한을 관리하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 사용자를 선택한 다음 권한을 편집하려는 사용자의 이름을 선택합니다.

4. 권한(Permissions) 탭을 선택합니다.

   사서함에 액세스할 수 있는 사용자 및 그룹의 목록이 나타납니다.

5. 변경할 사용자 또는 그룹 옆의 라디오 버튼을 선택하고 다음 중 하나를 수행합니다.

   사용자의 권한을 제거하려면

   1. [Remove]를 선택합니다.

      권한 제거 대화 상자가 나타납니다.

   2. 권한 제거 대화 상자에서 제거를 선택합니다.

   사용자의 권한을 편집하려면

   1. 편집(Edit)을 선택합니다.

      권한 편집 대화 상자가 나타납니다.

   2. 필요에 따라 권한을 설정한 다음 저장을 선택합니다.

   사서함에 다른 사용자 권한을 부여하려면

   1. 권한 추가(Add permissions)를 선택합니다.

      권한 추가 대화 상자가 나타납니다.

   2. 새 권한 추가 목록을 열고 추가하려는 사용자를 선택합니다.
   3. 필요에 따라 권한을 설정한 다음 추가를 선택합니다.

권한 변경 사항을 사용자에게 전파하는 데 최대 5분이 걸릴 수 있습니다.

그룹에 대한 사서함 권한 관리

Amazon WorkMail을 위한 그룹 권한을 추가하거나 제거할 수 있습니다.

> **Note**
>
> 그룹은 액세스할 수 있는 사서함이 없으므로 그룹에 모든 액세스 권한을 적용할 수 없습니다.

그룹 권한을 관리하려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경하세요. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 권한을 관리하려는 조직의 이름을 선택합니다.
3. 탐색 창에서 그룹을 선택한 다음 권한을 설정하려는 그룹의 이름을 선택합니다.
4. 권한 탭을 선택한 다음 권한 추가를 선택합니다.

   권한 추가 대화 상자가 나타납니다.
5. 새 권한 추가 목록을 열고 사서함에 대한 권한을 부여하려는 사용자 또는 그룹을 선택합니다.
6. 사서함 권한 및 전송 권한에서 원하는 옵션을 선택합니다.
7. 추가(Add)를 선택합니다.

권한 변경 사항을 사용자에게 전파하는 데 최대 5분이 걸릴 수 있습니다.

사서함에 대한 프로그래밍 방식 액세스

프로그래밍 방식으로 Amazon WorkMail 사서함에 액세스하려면 EWS(Exchange Web Services) 프로토콜을 사용하세요. EWS를 사용하면 사서함의 모든 항목 유형에 액세스할 수 있습니다. Amazon WorkMail과 함께 사용할 수 있는 몇 가지 EWS 라이브러리는 다음과 같습니다.

- Java – EWS Java API
- .Net - EWS 관리형 API
- Python – Exchangelib

Amazon WorkMail은 이메일을 보내고 받는 데 사용할 수 있는 IMAP 및 SMTP 프로토콜도 지원합니다. Amazon WorkMail 엔드포인트 및 할당량에서 Amazon WorkMail 프로토콜이 지원되는 URL을 확인할 수 있습니다.

EWS 프로토콜을 사용하는 경우 Amazon WorkMail은 다음과 같은 인증 방법을 지원합니다.

- 기본 인증 - 기본 인증을 사용하여 이메일 주소와 암호를 입력합니다.
- 위장 역할 - 위장 역할을 사용하면 사용자의 자격 증명을 입력하지 않고도 사용자의 사서함에 액세스할 수 있습니다.

주제

위장 역할 관리

위장 역할을 사용하면 관리자가 사용자의 자격 증명을 입력하지 않고도 사용자 사서함에 프로그래밍 방식으로 액세스할 수 있도록 구성할 수 있습니다. 서비스 및 도구는 사용자 사서함에서 작업을 수행하는 위장 역할을 맡을 수 있습니다. 위장은 EWS 프로토콜에서만 지원됩니다.

위장 역할 개요

위장을 허용하려면 관리자가 다음 속성을 사용하여 위장 역할을 만들어야 합니다.

- 역할 유형 - 모든 액세스 또는 읽기 전용을 선택합니다. 역할 유형은 역할이 수행할 수 있는 작업의 종류를 제한합니다.

- 규칙 - 위장 역할이 위장할 수 있는 사용자를 정의하는 규칙 목록입니다.

Amazon WorkMail은 다음 조건에서 규칙을 평가합니다.

- 거부 규칙이 하나라도 일치하는 경우 정책은 위장을 거부합니다. 거부 규칙은 모든 허용 규칙보다 우선합니다.
- 하나 이상의 허용 규칙이 일치하고 거부 규칙이 하나도 일치하지 않는 경우, 정책에서 위장을 허용합니다.
- 규칙이 적용되지 않는 경우 위장이 거부됩니다.

> **Note**
>
> Amazon WorkMail 조직의 모든 사용자가 위장할 수 있도록 허용하려면 허용 효과가 적용되고 조건 없이 규칙을 생성하세요.

> **Warning**
>
> 위장 역할이 사용자를 위장할 수 있도록 허용하는 규칙을 생성해야 합니다. 규칙을 지정하지 않으면 위장 역할이 사용자의 액세스 권한을 위임할 수 없습니다.

위장 역할을 만든 후에는 이 역할을 사용하여 사용자의 사서함에 액세스할 수 있습니다. 자세한 내용은 위장 역할 사용 섹션을 참조하세요.

보안 고려 사항

위장 역할을 사용하면 Amazon WorkMail 조직 및 AWS 계정 내에서 보안 문제가 발생할 가능성이 있습니다. 위장 역할을 생성할 때 고려해야 할 잠재적인 몇 가지 문제는 다음과 같습니다.

- 전이적 권한 - 사용자 A가 사용자 B의 사서함에 대한 액세스 권한을 갖고 있고 사용자 A를 위장하는 역할을 허용하는 경우 이 위장 역할은 사용자 A의 액세스 권한을 위장하고 사용자 B의 사서함에 액세스할 수 있습니다.
- 액세스 제어 - 액세스 제어 규칙을 사용하여 위장 역할 액세스를 제한할 수 있습니다. 자세한 내용은 액세스 제어 규칙 작업 섹션을 참조하세요.

- IAM 정책 - `workmail:ImpersonationRoleId` 조건을 사용하여 특정 Amazon WorkMail 조직 및 위장 역할에 `AssumeImpersonationRole` 작업을 할당할 수 있습니다. IAM 정책에 대한 예제를 보려면 아마존은 어떻게 WorkMail 협력하나요? IAM 섹션을 참조하세요.

위장 역할 생성

Amazon WorkMail 콘솔에서 위장 역할을 생성할 수 있습니다.

위장 역할을 만들려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 리전을 변경합니다. 탐색 모음에서 요구에 맞는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 위장 역할을 선택한 다음 역할 생성을 선택합니다.
4. 위장 역할 생성 대화 상자가 나타납니다. 역할에서 다음 정보를 입력합니다.
   - 이름 - 역할의 고유한 이름을 입력합니다.
   - (선택 사항) 설명 - 위장 역할에 대한 설명을 입력합니다.
   - 역할 유형 - 읽기 전용 또는 모든 액세스를 선택합니다.
5. 규칙에서 규칙 추가를 선택합니다.
6. 규칙 추가 대화 상자가 나타납니다. 다음 정보를 입력합니다.
   - 이름 – 역할의 고유한 이름을 입력합니다.
   - (선택 사항) 설명 – 규칙에 대한 설명을 입력합니다.
   - 효과에서 허용 또는 거부를 선택합니다. 이렇게 하면 다음 단계에서 선택하는 조건에 따라 액세스가 허용되거나 거부됩니다.
   - (선택 사항) 이 규칙:에서 특정 사용자를 포함하도록 선택한 사용자를 위장하는 요청과 일치을 선택합니다. 선택한 사용자가 아닌 다른 사용자를 위장하는 요청과 일치를 선택하면 선택한 사용자 이외의 사용자를 추가할 수 있습니다.
7. [다른 규칙 추가(Add another rule)]를 선택합니다.

> **Note**
>
> 규칙은 해당 역할을 저장할 때만 저장됩니다.

8. 역할 생성을 선택합니다.

위장 역할 편집

Amazon WorkMail 콘솔에서 위장 역할을 편집할 수 있습니다.

위장 역할을 편집하려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 리전을 변경합니다. 탐색 모음에서 요구에 맞는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 위장 역할을 선택합니다.
4. 편집하려는 위장 역할 이름을 선택한 다음 편집을 선택합니다.
5. 위장 역할 편집 대화 상자가 나타납니다. 역할에서 다음 정보를 입력합니다.

   - 이름 - 역할의 고유한 이름을 입력합니다.
   - (선택 사항) 설명 - 위장 역할에 대한 설명을 입력합니다.
   - 역할 유형 - 위장 역할에 사용자 사서함에 대한 읽기 전용 액세스 권한을 부여하려면 읽기 전용을 선택합니다. 사용자 사서함의 항목을 읽고 수정할 수 있는 권한을 위장 역할에 부여하려면 모든 액세스를 선택합니다.
6. 규칙에서 편집하려는 규칙을 선택하고 편집을 선택합니다.
7. 규칙 편집 대화 상자가 나타납니다. 다음 정보를 입력합니다.

   - 이름 - 규칙의 이름을 편집합니다.
   - (선택 사항) 설명 – 규칙에 대한 설명을 업데이트하거나 입력합니다.
   - 규칙에 설정된 조건이 충족될 때 액세스를 허용하려면 효과에서 허용을 선택합니다. 액세스를 거부하려면 거부를 선택합니다.

- (선택 사항) 이 규칙:에서 특정 사용자를 포함하도록 선택한 사용자를 위장하는 요청과 일치을 선택합니다. 선택한 사용자가 아닌 다른 사용자를 위장하는 요청과 일치를 선택하면 선택한 사용자 이외의 사용자를 추가할 수 있습니다.

8. Save를 선택합니다.
9. Save changes(변경 사항 저장)를 선택합니다.

> **Important**
>
> 위장 규칙을 변경하면 영향을 받는 사서함을 업데이트하는 데 최대 5분이 걸릴 수 있습니다. 규칙 업데이트 프로세스 중에 사서함에서 일관되지 않은 동작이 관찰될 수 있습니다. 하지만 역할을 테스트하는 경우 Amazon WorkMail은 업데이트된 규칙에 따라 예상대로 응답합니다. 자세한 내용은 위장 역할 테스트 섹션을 참조하세요.

위장 역할 테스트

Amazon WorkMail 콘솔에서 위장 역할을 테스트할 수 있습니다.

위장 역할을 테스트하려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 리전을 변경합니다. 탐색 모음에서 요구에 맞는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 위장 역할을 선택합니다.
4. 테스트하려는 위장 역할을 선택합니다.
5. 역할 테스트를 선택합니다.
6. 위장 역할 테스트 대화 상자가 나타납니다. 대상 사용자에서 위장 액세스를 테스트하려는 사용자를 선택합니다.
7. 테스트(Test)를 선택합니다.

위장 역할 삭제

Amazon WorkMail 콘솔에서 위장 역할을 삭제할 수 있습니다.

위장 역할을 삭제하려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 리전을 변경합니다. 탐색 모음에서 요구에 맞는 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 위장 역할을 선택합니다.
4. 삭제하려는 위장 역할 이름을 선택합니다.
5. 삭제를 선택합니다.
6. 역할 삭제 대화 상자가 나타납니다. 삭제를 확인하려면 대화 상자에 역할 이름을 입력하고 삭제를 선택합니다.

위장 역할 사용

사서함 데이터에 액세스하려면 Amazon WorkMail API 작업 `AssumeImpersonationRole`를 사용하세요. Amazon WorkMail API에 대한 자세한 내용은 API 참조를 참조하세요.

`AssumeImpersonationRole`에서 `Token`을 반환합니다. 이 `Token` 정보는 HTTP 헤더 `Authorization`를 통해 15분 이내에 EWS 프로토콜로 전달되어야 합니다.

다음 예제에서는 EWS 프로토콜에서 위장 역할을 사용하는 방법을 보여줍니다. 예제에 사용된 상수는 조직 및 계정에 고유한 다음과 같은 세부 정보를 지정합니다.

- *`WORKMAIL_ORGANIZATION_ID`* - Amazon WorkMail 조직 ID
- *`IMPERSONATION_ROLE_ID`* - 위장 역할 ID
- *`WORKMAIL_EWS_URL`* - Amazon WorkMail 엔드포인트 및 할당량에서 EWS 엔드포인트 사용 가능
- *`EMAIL_ADDRESS`* - 사용자 사서함의 이메일 주소

Example Java – EWS Java API

```
import software.amazon.awssdk.services.workmail.WorkMailClient;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleRequest;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleResponse;

import microsoft.exchange.webservices.data.core.ExchangeService;
import microsoft.exchange.webservices.data.core.enumeration.misc.ExchangeVersion;
```

```
import microsoft.exchange.webservices.data.misc.ImpersonatedUserId;
import microsoft.exchange.webservices.data.core.enumeration.misc.ConnectingIdType;

// ...

AssumeImpersonationRoleResponse response = workMailClient.assumeImpersonationRole(
    AssumeImpersonationRoleRequest.builder()
        .organizationId(WORKMAIL_ORGANIZATION_ID)
        .impersonationRoleId(IMPERSONATION_ROLE_ID)
        .build());

ExchangeService exchangeService = new
 ExchangeService(ExchangeVersion.Exchange2010_SP2);
exchangeService.setUrl(URI.create(WORKMAIL_EWS_URL));
exchangeService.getHttpHeaders().put("Authorization", "Bearer " + response.token());
exchangeService.setImpersonatedUserId(new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS));
```

Example .Net - EWS 관리형 API

```
using Amazon.WorkMail;
using Amazon.WorkMail.Model;

using Microsoft.Exchange.WebServices.Data;

// ...

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSONATION_ROLE_ID;
AssumeImpersonationRoleResponse response =
 workMailClient.AssumeImpersonationRole(request);

ExchangeService service = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
service.Url = new Uri(WORKMAIL_EWS_URL);
service.HttpHeaders.Add("Authorization", "Bearer " + response.Token);
service.ImpersonatedUserId = new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS);
```

Example Python – Exchangelib

```
import boto3
```

```
from requests.auth import AuthBase
from exchangelib.transport import AUTH_TYPE_MAP
from exchangelib import Configuration, Account, Version, IMPERSONATION
from exchangelib.version import EXCHANGE_2010_SP2


work_mail_client = boto3.client("workmail")

class ImpersonationRoleAuth(AuthBase):
    def __init__(self):
         self.token = work_mail_client.assume_impersonation_role(
             OrganizationId=WORKMAIL_ORGANIZATION_ID,
             ImpersonationRoleId=IMPERSONATION_ROLE_ID
        )["Token"]

     def __call__(self, r):
         r.headers["Authorization"] = "Bearer " + self.token
         return r

AUTH_TYPE_MAP["ImpersonationRoleAuth"] = ImpersonationRoleAuth

ews_config = Configuration(
     service_endpoint=WORKMAIL_EWS_URL,
     version=Version(build=EXCHANGE_2010_SP2),
     auth_type="ImpersonationRoleAuth"
)
ews_account = Account(
     config=ews_config,
     primary_smtp_address=EMAIL_ADDRESS,
     access_type=IMPERSONATION
)
```

사서함 콘텐츠 내보내기

Amazon StartMailboxExportJobAPI WorkMail APIReference의 작업을 사용하여 Amazon WorkMail 사서함 콘텐츠를 Amazon Simple Storage Service (Amazon S3) 버킷으로 내보낼 수 있습니다. 이 작업은 지정된 사서함의 모든 이메일 메시지와 캘린더 항목을 Amazon S3 버킷의 `.zip` 파일 MIME 형식으로 내보냅니다. 연락처 및 작업과 같은 다른 항목은 내보낼 수 없습니다.

사서함 내보내기 작업을 완료하는 데 걸리는 시간은 사서함의 항목 크기 및 수에 따라 다릅니다. 사서함 내보내기 작업은 일정 기간 동안 수행되므로 특정 시점의 사서함 콘텐츠 스냅샷을 나타내지 않습니다. 내보내기 작업의 상태를 보려면 Amazon WorkMail API Reference의 DescribeMailboxExportJob또는 ListMailboxExportJobsAPI작업을 사용하십시오.

사서함 내보내기 작업이 완료되면 Amazon S3 버킷의 `.zip` 파일이 사용자가 제공한 대칭 AWS Key Management Service (AWS KMS) 고객 마스터 키 (CMK) 를 사용하여 암호화됩니다. AWS KMS 암호화는 Amazon S3와 통합되어 있기 때문에 사용자가 액세스할 수 있는 한, 데이터를 다운로드하는 사용자가 복호화된 데이터를 볼 수 있습니다. AWS KMS CMK

사전 조건

다음은 사서함 콘텐츠를 내보내는 데 대한 사전 조건입니다.

- 프로그래밍 기능.
- Amazon WorkMail 관리자 계정.
- 퍼블릭 액세스를 허용하지 않는 Amazon S3 버킷. 자세한 내용은 Amazon Simple Storage Service 사용 설명서 및 Amazon Simple Storage Service 사용 설명서의 Amazon S3 퍼블릭 액세스 차단 사용을 참조하세요.
- 대칭형 AWS KMS CMK. 자세한 내용은 AWS Key Management Service 개발자 안내서의 시작하기를 참조하세요.
- Amazon S3 버킷에 쓸 권한을 부여하고 를 사용하여 전송된 파일을 암호화하는 정책을 포함하는 AWS Identity and Access Management (IAM) 역할. AWS KMS CMK 자세한 내용은 아마존은 어떻게 WorkMail 협력하나요? IAM 단원을 참조하십시오.

IAM정책 예제 및 역할 생성

다음 예제는 Amazon S3 버킷에 쓰기 권한을 부여하고 를 사용하여 전송된 파일을 암호화하는 IAM 정책을 보여줍니다. AWS KMS CMK 다음 예: 사서함 콘텐츠 내보내기 절차에서 이 예제 정책을 사용하려면 정책을 JSON 파일 이름이 `mailbox-export-policy.json` 있는 파일로 저장하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetBucketPolicyStatus"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/KEY-ID"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-
bucket/S3-PREFIX*"
                }
            }
        }
    ]
}
```

다음 예는 생성한 IAM 역할에 연결된 IAM 신뢰 정책을 보여줍니다. 다음 예: 사서함 콘텐츠 내보내기 절차에서 이 예제 정책을 사용하려면 정책을 JSON 파일 이름이 있는 파일로 `mailbox-export-trust-policy.json` 저장하십시오.

`aws:SourceArn` 및 `aws:SourceAccount` 조건을 동시에 사용할 필요는 없습니다. 예를 들어 동일한 AWS 계정으로 다른 Amazon WorkMail 조직에서 메시지를 내보내는 데 동일한 역할을 사용해야 하는 경우 `aws:SourceArn` 정책에서 제거할 수 있습니다. 조건 키에 대한 자세한 내용은 AWS IID 및 액세스 관리 사용 설명서에서 AWS 글로벌 조건 컨텍스트 키를 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-east-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
}
```

다음 명령을 AWS CLI 실행하여 를 사용하여 계정에 IAM 역할을 생성할 수 있습니다.

```
aws iam create-role --role-name WorkmailMailboxExportRole --assume-role-policy-
document file://mailbox-export-trust-policy.json --region us-east-1
```

```
aws iam put-role-policy --role-name WorkmailMailboxExportRole --policy-
name MailboxExport --policy-document file://mailbox-export-policy.json
```

에 AWS CLI대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하십시오.

예: 사서함 콘텐츠 내보내기

이전 섹션에서 IAM 역할과 정책을 만든 후 다음 단계를 완료하여 사서함 콘텐츠를 내보내십시오. Amazon WorkMail 조직 ID 및 사용자 ID (개체 ID) 가 있어야 하며, 이 ID는 Amazon WorkMail 콘솔에서 또는 Amazon을 사용하여 액세스할 수 WorkMail API 있습니다.

예: 사서함 콘텐츠를 내보내려면

1. AWS CLI 를 사용하여 사서함 내보내기 작업을 시작합니다.

```
aws workmail start-mailbox-export-job --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56 --entity-
id S-1-1-11-1111111111-2222222222-3333333333-3333 --kms-key-
arn arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn
 arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name amzn-s3-
demo-bucket --s3-prefix S3-PREFIX
```

2. AWS CLI 를 사용하여 Amazon WorkMail 조직의 사서함 내보내기 작업 상태를 모니터링할 수 있습니다.

```
aws workmail list-mailbox-export-jobs --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56
```

   또는 **start-mailbox-export-job** 명령에 의해 생성된 작업 ID를 사용하여 해당 사서함 내보내기 작업의 상태만 모니터링할 수도 있습니다.

```
aws workmail describe-mailbox-export-job --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
```

사서함 내보내기 작업 상태가 COMPLETED인 경우 내보낸 사서함 항목은 지정된 Amazon S3 버킷의 `.zip` 파일에서 사용할 수 있습니다.

다음은 내보낸 사서함의 출력 로그 예제입니다.

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
```

```
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportable항목은 메모나 연락처와 같이 지원되지 않는 항목입니다.

고려 사항

Amazon용 사서함 작업을 내보낼 때는 다음 고려 사항이 적용됩니다 WorkMail.

- 특정 Amazon WorkMail 조직에 대해 최대 10개의 동시 사서함 내보내기 작업을 실행할 수 있습니다.
- 지정된 사서함에 대해 최대 24시간에 한 번씩 사서함 내보내기 작업을 실행할 수 있습니다.
- 다음 리소스는 모두 같은 AWS 지역에 있어야 합니다.
  - 아마존 WorkMail 조직
  - AWS KMS CMK
  - Amazon S3 버킷

문제 해결

이 섹션의 항목에서는 WorkMail Amazon에서 문제를 해결하는 방법을 설명합니다.

주제

이메일 헤더 보기

이메일 헤더의 정보는 일반적인 사용자 이메일 문제를 해결하는 데 도움이 될 수 있습니다. WorkMail Amazon에서는 모든 메시지의 헤더 정보를 볼 수 있습니다.

Amazon에서 이메일 헤더를 보려면 WorkMail

1. Amazon WorkMail 웹 애플리케이션에서 이메일 메시지를 두 번 클릭하여 엽니다.
2. 메시지 오른쪽 상단의 전송 날짜 옆에 있는 메시지 옵션(톱니바퀴 및 봉투 아이콘)을 선택합니다.

이메일 헤더는 인터넷 헤더 아래 나타납니다.

메일 라우팅

사용자가 이메일 수신을 중단하면 Amazon WorkMail 조직에 메일 라우팅 문제가 발생한 것일 수 있습니다. 이 섹션의 단계에서는 전송 및 라우팅 문제를 해결하는 일반적인 방법을 설명합니다.

인바운드 메일 문제:

- Amazon WorkMail 조직과 연결된 도메인의 MX 레코드를 확인합니다. `WorkMail`유일한 항목이어야 하며 우선 순위가 가장 낮아야 합니다. MX 레코드가 여러 개 있으면 잘못된 서비스가 메시지를 수신할 수 있습니다. MX 레코드에 대한 자세한 내용은 도메인 확인 부분을 참조하세요.
- Amazon 콘솔에서 조직의 도메인 기반 메시지 인증, 보고 및 준수 (DMARC) 설정을 확인합니다. WorkMail DMARC 레코드는 사용자의 계정 자격 증명을 손상시킬 수 있는 스푸핑 또는 피싱과 같은 일반적인 공격으로부터 보호하는 데 사용됩니다. DMARC에 대한 자세한 내용은 수신 이메일에 DMARC 정책 적용 부분을 참조하세요.
- Amazon Simple Email Service 인바운드 규칙을 확인합니다. 규칙에 Amazon WorkMail 이외의 작업이 포함된 경우 해당 작업이 실패하여 Amazon에서 메일 WorkMail 수신을 중단할 수 있습니다.

Amazon SES 규칙에 대한 자세한 내용은 Amazon Simple 이메일 서비스 개발자 안내서의 Amazon 과 통합 WorkMail 작업을 참조하십시오.

- WorkMailAmazon에서 메시지 추적을 활성화한 다음 로그에서 전송 문제를 확인합니다. 메시지 추적에 대한 자세한 내용은 이메일 이벤트 로깅 활성화 부분을 참조하세요.

아웃바운드 메일 문제

- SPF 레코드에 Amazon SES가 포함되어 있는지 확인하세요. Amazon WorkMail 콘솔의 도메인 페이지를 확인하여 확인하십시오. SPF에 대한 자세한 내용은 SPF를 사용하여 이메일 인증 부분을 참조하세요.
- Amazon에 도메인 사용 WorkMail 권한이 있는지 확인하십시오. 그렇지 않은 경우 도메인을 다시 추가하세요. 이 가이드의 도메인 추가에서 사용 방법을 단계별로 설명합니다.

Amazon WorkMail을 통해 이메일 저널링 사용

통합된 타사 보관 도구 및 eDiscovery 도구를 사용하여 이메일 통신을 기록하도록 저널링을 설정할 수 있습니다. 이렇게 하면 개인 정보 보호, 데이터 스토리지 및 정보 보호를 위한 이메일 스토리지 준수 규정이 충족됩니다.

저널링 사용

Amazon WorkMail은 지정한 조직 내 모든 사용자에게 전송된 이메일 메시지와 해당 조직의 사용자가 보낸 모든 이메일 메시지를 모두 저널링합니다. 시스템 관리자가 지정한 주소로 모든 이메일 메시지의 복사본이 `journal record` 형식으로 전송됩니다. 이 형식은 Microsoft 이메일 프로그램과 호환됩니다. 이메일 저널링에 따르는 추가 요금은 없습니다.

이메일 저널링에는 저널링 이메일 주소와 보고서 이메일 주소, 이렇게 2개의 이메일 주소가 사용됩니다. 저널링 이메일 주소는 전용 사서함 또는 계정과 통합된 타사 디바이스의 주소입니다. 저널 보고서가 이 디바이스로 전송됩니다. 보고서 이메일 주소는 시스템 관리자의 주소로, 실패한 저널 보고서에 대한 알림이 이 주소로 전송됩니다.

모든 저널 레코드는 도메인에 자동으로 추가된 이메일 주소에서 전송되며 다음과 유사합니다.

```
amazonjournaling@yourorganization.awsapps.com
```

이 주소와 연결된 사서함이 없으므로 이 이름 또는 주소를 사용하여 사서함을 생성할 수 없습니다.

> **Note**
>
> Amazon Simple Email Service(Amazon SES) 콘솔에서 다음 도메인 레코드를 삭제하지 마세요. 그렇지 않으면 이메일 저널링이 작동을 멈춥니다.
>
> ```
> yourorganization.awsapps.com
> ```

수신자 또는 사용자 그룹 수와 관계 없이 모든 수신 또는 발신 이메일 메시지는 저널 레코드 하나를 생성합니다. 저널 레코드를 생성하지 못한 이메일에 대해서는 오류 알림이 생성되고, 이 알림은 보고서 이메일 주소로 전송됩니다.

이메일 저널링을 활성화하려면

1. https://console.aws.amazon.com/workmail/에서 Amazon WorkMail 콘솔을 엽니다.

   필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 자세한 내용은 Amazon Web Services 일반 참조의 Regions and endpoints를 참조하세요.
2. 탐색 창에서 조직을 선택한 다음 조직의 이름을 선택합니다.
3. 탐색 창의 조직 설정에서 저널링 탭을 선택한 다음 편집을 선택합니다.
4. 저널링 상태 슬라이더를 켜짐 위치로 이동합니다.
5. 저널링 이메일 주소 상자에 이메일 저널링 공급자가 제공한 이메일 주소를 입력합니다.

   > **Note**
   >
   > 전용 저널링 공급자를 사용할 것을 권장합니다.

6. 보고 이메일 주소에 이메일 관리자의 주소를 입력합니다.
7. Save를 선택합니다. 변경 사항이 바로 적용됩니다.

문서 기록

다음 표에는 Amazon WorkMail 관리자 안내서의 각 릴리스에서 변경된 주요 내용이 설명되어 있습니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
감사 로깅 지원	감사 로그는 사서함에 대한 사용자의 액세스를 모니터링하고, 의심스러운 활동을 감사하고, 액세스 제어 및 가용성 공급자 구성을 디버깅하는 데 사용할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 WorkMail Amazon에서 감사 로깅 활성화 및 로깅 및 모니터링을 참조하십시오.	2024년 3월 20일
전송 계층 보안 (TLS) 지원	아마존은 전송 계층 보안 (TLS) 1.0 및 1.1에 대한 지원을 WorkMail 중단했습니다. TLS 1.0 또는 1.1을 사용하는 경우 TLS 버전을 1.2로 업그레이드해야 합니다.	2023년 11월 2일
원격 사용자	원격 WorkMail 사용자는 Amazon WorkMail 조직 외부에서 호스팅되거나 다른 이메일 도메인에서 호스팅되는 Amazon 사용자입니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 사용자를 참조하십시오.	2023년 9월 18일
사서함에 대한 프로그래밍 방식 액세스	Amazon은 WorkMail 이제 사서함에 프로그래밍 방식으로 액세스할 수 있는 권한을 부여하	2022년 10월 4일

	는 사칭 역할을 제공합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 사서함에 대한 프로그래밍 방식 액세스를 참조하십시오.	
Amazon에서 사용자 지정 가용성 공급자 구성 WorkMail	Amazon은 사용자 지정 가용성 공급자 (CAP) 사용을 WorkMail 지원합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 사용자 지정 가용성 공급자 구성을 참조하십시오.	2022년 6월 30일
조직 생성을 위한 콘솔 변경 사항	조직 생성을 위한 Amazon WorkMail 콘솔 환경이 업데이트되었습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 조직 생성을 참조하십시오.	2020년 10월 23일
사서함 콘텐츠 내보내기	`StartMailboxExportJob` API 작업을 사용하여 Amazon WorkMail 메일박스 콘텐츠를 Amazon Simple Storage Service (Amazon S3) 버킷으로 내보낼 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 사서함 콘텐츠 내보내기를 참조하십시오.	2020년 9월 22일

사서함 보존 정책	선택한 기간이 지나면 이메일 메시지를 자동으로 삭제하도록 Amazon WorkMail 조직에 대한 사서함 보존 정책을 설정하십시오. 자세한 내용은 Amazon WorkMail 관리자 안내서의 사서함 보존 정책 설정을 참조하십시오.	2020년 5월 28일
동기식 및 비동기식 Lambda 실행 작업	Amazon 이메일 흐름 규칙에서 Lambda 실행 작업에 대한 동기 또는 비동기 구성을 선택합니다. WorkMail 자세한 AWS Lambda 내용은 Amazon WorkMail WorkMail 관리자 안내서의 Amazon 구성을 참조하십시오.	2020년 5월 11일
액세스 제어 규칙 작업	액세스 제어 규칙을 통해 Amazon WorkMail 관리자는 조직의 사서함에 액세스하는 방법을 제어할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 액세스 제어 규칙 사용을 참조하십시오.	2020년 2월 12일
조직 태깅	Amazon WorkMail 조직에 태그를 지정하여 AWS Billing and Cost Management 콘솔에서 조직을 구분하거나 조직 리소스에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 조직 태그 지정을 참조하십시오.	2020년 1월 23일

수신 이메일에 DMARC 정책 적용	자세한 내용은 Amazon WorkMail 관리자 안내서의 수신 이메일에 DMARC 정책 적용을 참조하십시오.	2019년 10월 17일
Lambda를 통해 메시지 콘텐츠 검색	Amazon WorkMail 메시지 흐름 API와 함께 AWS Lambda 사용하여 메시지 콘텐츠를 검색하십시오. 자세한 내용은 Amazon 관리자 안내서의 Lambda를 사용한 메시지 콘텐츠 검색을 참조하십시오. WorkMail	2019년 9월 12일
Amazon WorkMail 이메일 이벤트 로깅	Amazon WorkMail 콘솔에서 이메일 이벤트 로깅을 활성화하여 조직의 이메일 메시지를 추적할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 메시지 추적을 참조하십시오.	2019년 5월 13일
Route 53 DNS 레코드 삽입	Route 53 퍼블릭 호스팅 영역에서 관리되는 도메인을 설정할 때 Amazon은 WorkMail 자동으로 DNS 레코드를 삽입합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 도메인 추가를 참조하십시오.	2019년 2월 13일
인바운드 이메일 규칙 작업을 위한 Lambda 구성	WorkMail Amazon은 인바운드 이메일 흐름 규칙과 함께 사용하도록 Lambda 함수를 구성할 수 있도록 지원합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 이메일 흐름 관리를 참조하십시오.	2019년 1월 24일

아마존용 Lambda 구성 WorkMail	WorkMail Amazon은 아웃바운드 이메일 흐름 규칙과 함께 사용하도록 Lambda 함수를 구성할 수 있도록 지원합니다. 자세한 내용은 WorkMail Amazon 관리자 안내서의 WorkMail Amazon용 Lambda 구성을 참조하십시오.	2018년 11월 19일
SMTP 라우팅	WorkMail Amazon은 아웃바운드 이메일 흐름 규칙과 함께 사용할 SMTP 게이트웨이 구성을 지원합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 SMTP 게이트웨이 구성을 참조하십시오.	2018년 11월 1일
사용자 지정 도메인용 디버깅 도구	WorkMail Amazon은 사용자 지정 도메인을 위한 디버깅 도구를 추가했습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 도메인 추가를 참조하십시오.	2018년 10월 15일
Outlook 2019 지원	아마존은 윈도우와 macOS용 아웃룩 2019를 WorkMail 지원합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 Amazon WorkMail 시스템 요구 사항을 참조하십시오.	2018년 10월 1일
다양한 업데이트	주제 레이아웃과 조직에 대한 다양한 업데이트입니다.	2018년 7월 12일

사서함 권한	WorkMail Amazon에서 사서함 권한을 사용하여 사용자 또는 그룹에 다른 사용자의 사서함에서 작업할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 사서함 권한 사용을 참조하십시오.	2018년 9월 4일
에 대한 지원 AWS CloudTrail	WorkMail Amazon은 과 통합되어 AWS CloudTrail있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 Amazon WorkMail API 호출 로깅을 참조하십시오. AWS CloudTrail	2017년 12월 12일
이메일 흐름 지원	발신자의 이메일 주소 또는 도메인을 기반으로 수신 이메일 처리를 위한 이메일 흐름 규칙을 설정할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 이메일 흐름 관리를 참조하십시오.	2017년 7월 5일
빠른 설정에 대한 업데이트	이제 빠른 설치가 Amazon WorkMail 디렉터리를 자동으로 생성합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 빠른 WorkMail 설정으로 Amazon 설정을 참조하십시오.	2017년 5월 10일

보다 광범위한 이메일 클라이언트 지원	이제 Mac용 Microsoft Outlook 2016 및 IMAP 이메일 클라이언트와 WorkMail 함께 Amazon 을 사용할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 WorkMail Amazon 의 시스템 요구 사항을 참조하십시오.	2017년 1월 9일
SMTP 저널링 지원	이메일 통신을 기록하도록 저널링을 설정할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 WorkMail Amazon에서의 이메일 저널링 사용을 참조하십시오.	2016년 11월 25일
외부 이메일 주소로 이메일 리디렉션 지원	도메인에 대한 Amazon SES 자격 증명 정책을 업데이트하여 이메일 리디렉션 규칙을 설정할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 도메인 ID 정책 편집을 참조하십시오.	2016년 10월 26일
상호 운용성 지원	Amazon과 WorkMail Microsoft Exchange 간의 상호 운용성을 활성화할 수 있습니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 Amazon과 WorkMail Microsoft Exchange 간의 상호 운용성을 참조하십시오.	2016년 10월 25일
정식 출시	Amazon의 일반 공급 WorkMail 릴리스입니다.	2016년 1월 4일

리소스 예약 지원	회의실 및 장비와 같은 리소스 예약에 대한 지원입니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 리소스 사용을 참조하십시오.	2015년 10월 19일
이메일 마이그레이션 도구 지원	이메일 마이그레이션 도구 지원. 자세한 내용은 Amazon WorkMail 관리자 안내서의 WorkMail Amazon으로 마이그레이션을 참조하십시오.	2015년 8월 16일
아마존 프리뷰 출시 WorkMail	Amazon의 프리뷰 릴리즈 WorkMail.	2015년 1월 28일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.