MSP, MSSP 및 다중 조직 고객을 위한 Amazon의 S3 서비스를 사용한 중앙 집중식 Umbrella Log 관리 이해

목차

소개

이 문서에서는 MSP, MSSP 및 다중 조직 고객을 위한 Amazon의 S3 서비스를 사용한 중앙 집중식 Umbrella 로그 관리에 대해 설명합니다.

개요

MSP, MSSP 및 Multi-org 콘솔에는 클라우드 스토리지에 오프라인으로 고객의 DNS, URL 및 IP 로그를 저장할 수 있는 기능이 있습니다. 스토리지는 Amazon S3에 있으며 로그를 업로드한 후에는 규정 준수 또는 보안 분석을 위해 다운로드하고 보관할 수 있습니다.

이 설명서는 이 기능을 이해하고, Umbrella 대시보드와 Amazon S3 콘솔 모두에 설정하고, 로그를 S3에 보관할 기간을 포함한 몇 가지 구성 옵션을 실행하는 데 도움이 됩니다.

MSP, MSSP 및 다중 조직용 Umbrella는 모두 콘솔의 하위 조직에서 트래픽 활동 로그를 업로드하고 클라우드에 저장할 수 있습니다. Amazon의 AWS S3(Simple Storage Service)는 로그를 보관하

는 서비스이며, 이를 오프라인 스토리지 또는 로그 보존이라고 부르기도 합니다.

로그 아카이빙은 필요에 따라 여러 가지 이유로 유용할 수 있습니다. 일부 사용자의 경우 내보내기 및 아카이브된 로그를 데이터 분석 또는 보안 포렌식 툴(예: SIEM)로 가져올 수 있습니다. 다른 사용자의 경우, 작업 로그 아카이브는 보안 사고 발생 시 데이터 포렌식 또는 인사 기록에 유용할 수 있습니다.

AWS S3는 로그를 압축(gzip) 아카이브에 CSV 형식으로 저장합니다. 로그는 10분마다 업로드되므로 네트워크에서 오는 네트워크 트래픽 사이에 최소 10분 정도 지연이 발생하며, Umbrella에서 로깅한 다음 S3에서 다운로드할 수 있습니다.

Console의 orgID 번호

각 고객 조직은 콘솔에서 조직 ID 번호를 사용하여 각 고객을 폴더에 매핑하여 개별적으로 로그를 업로드합니다. 이 기능은 고객별/조직별로 활성화 또는 비활성화할 수도 있습니다.

두 가지 유형의 Umbrella 로그 관리

로그 관리는 AWSit S3 환경 내의 폴더인 isbucketit에 로그를 업로드하여 수행됩니다. Umbrella 로그에 대한 버킷을 호스트하는 방법에는 두 가지가 있습니다.

- 관리, 관리 및 지불은 귀사 관리자(administrator)가 수행합니다.
- Cisco Umbrella에서 관리, 관리 및 지불합니다.

Cisco에서 S3 버킷을 관리하게 하는 데에는 장단점이 있습니다.

버킷을 관리하는 Cisco의 장점:

- 설정이 매우 간편합니다. 단 2분 정도만 소요되며 그 이후에는 관리가 매우 쉽습니다.
- Cisco Bucket-Management는 Umbrella와 함께 라이센스 비용에 포함되어 있으므로 서비스를 효과적으로 무료로 이용할 수 있습니다. 자신의 버킷을 갖는 것은 비싼데 비해, 또 다른 청구서를 관리하는 간접비는 터무니없을 수 있다.

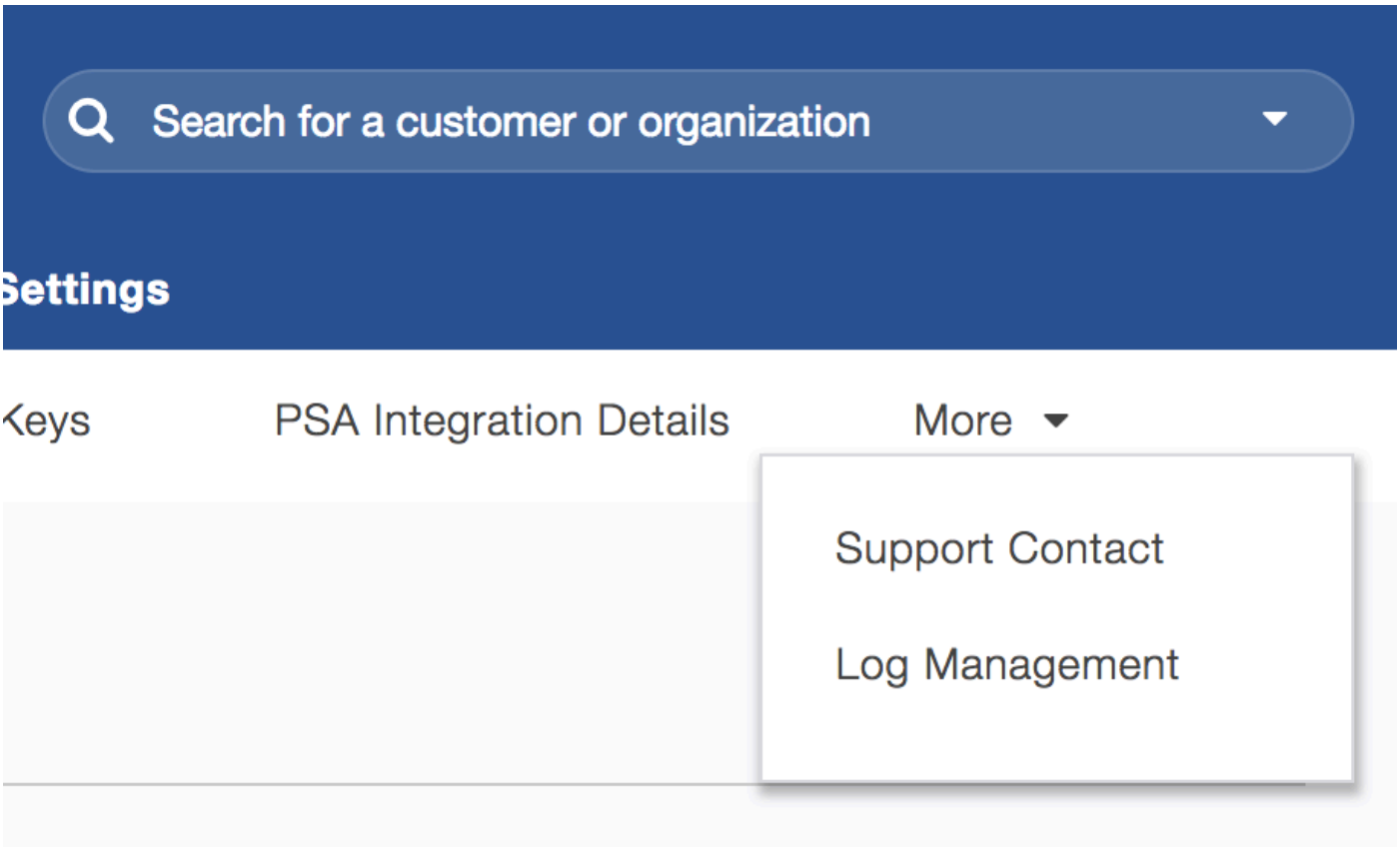
S3 인스턴스를 직접 관리할 때의 장점:

- 오프라인 상에서 데이터를 얼마나 오래 저장할 수 있는가에 대한 제한은 없다. Cisco는 오프라인 스토리지를 최대 30일로 제한합니다.
- Umbrella의 로그 파일을 포함하여 버킷에 무엇이든 추가할 수 있으므로 다른 애플리케이션에서도 버킷을 사용할 수 있습니다.
- 자동화나 명령줄 도움말과 같은 고급 구성 지원을 위해 Amazon에서 직접 지원을 받을 수 있습니다.

대부분의 고객은 버킷 유지 관리 비용이 매우 저렴하지만 번거로울 수 있습니다.

시작하기

로그 관리 기능은 Console의 Settings(설정) > Log Management(로그 관리) 아래에 있습니다(드롭다운 화살표를 누를 수 있음).



115012963103

셀프 관리 S3 버킷 구성

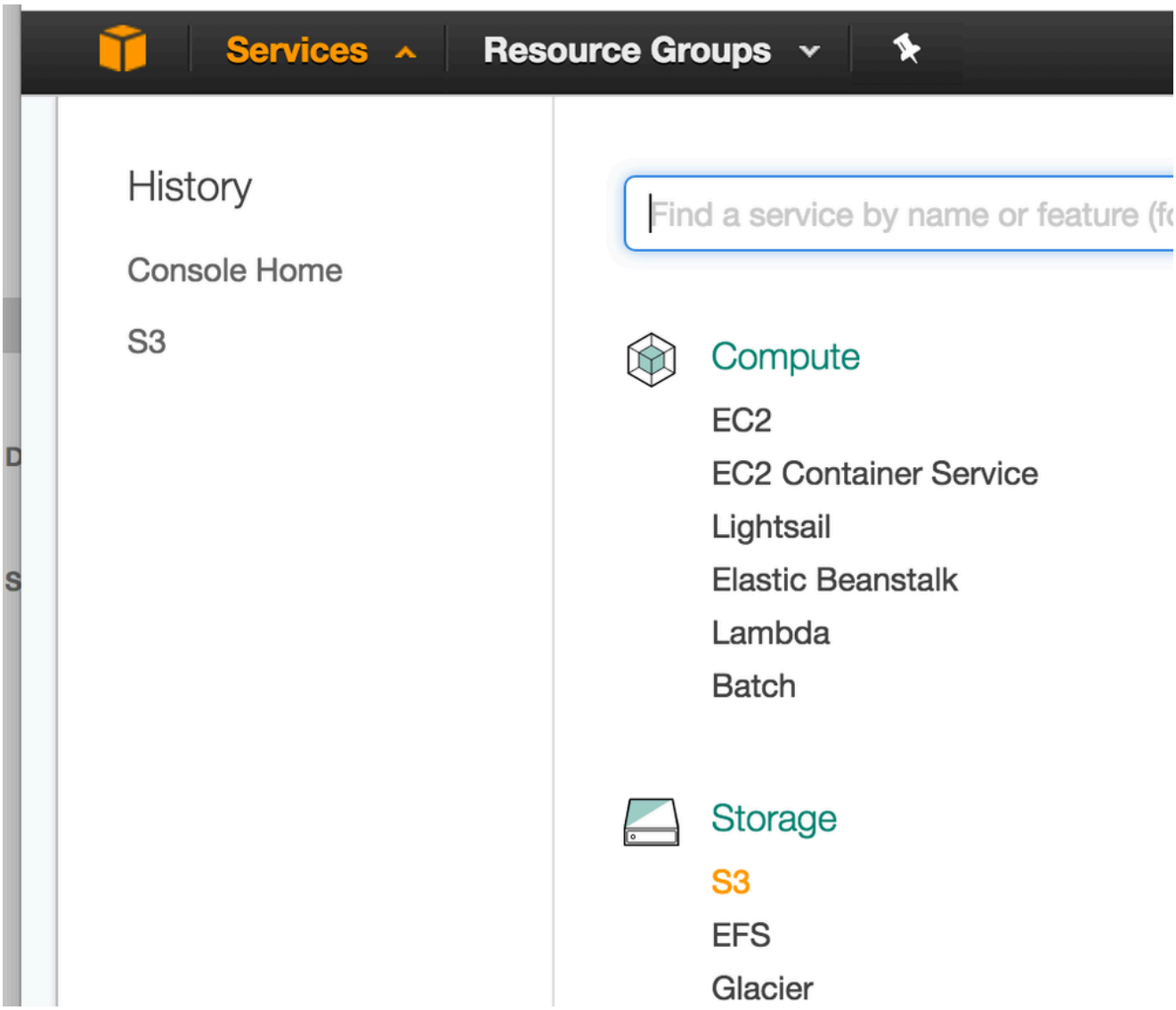
사전 요구 사항

로그를 아카이브하려면 다음 요구 사항을 충족해야 합니다.

- Cisco Umbrella MSP, MSSP 또는 다중 조직 콘솔에 대한 전체 관리 액세스
- Amazon AWS 서비스에 로그인합니다(https://aws.amazon.com/console/). 계정이 있는 경우 Amazon은 S3에 대한 무료 등록을 제공합니다. 하지만, 무료 요금제 사용량을 초과하는 경우 신용 카드가 필요합니다.
- 로그 스토리지용으로 Amazon S3에 구성된 버킷. Amazon S3 버킷 구성 및 설정에 대한 지침은 다음 섹션을 참조하십시오.

Amazon S3 버킷 설정

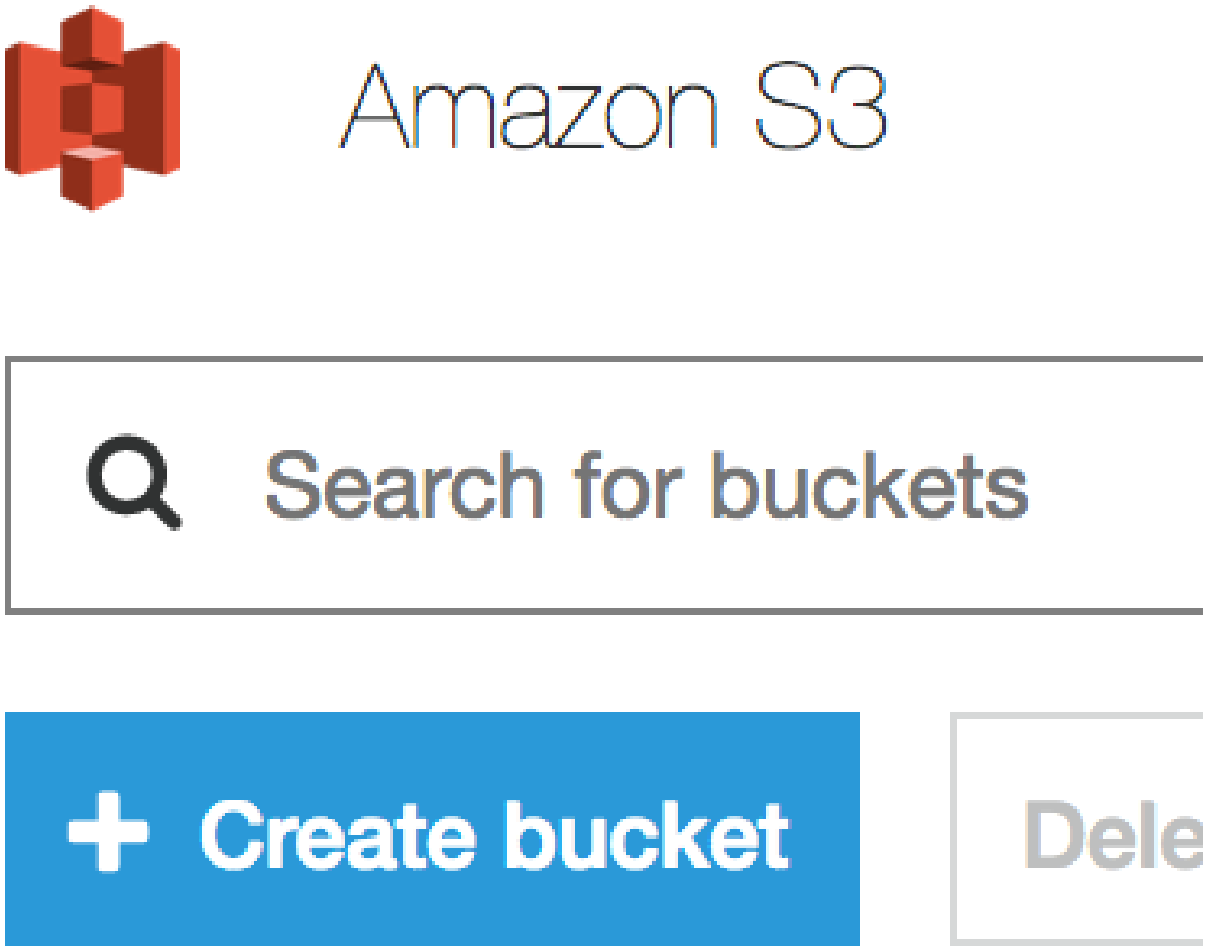
1. AWS Console에 로그인하고 Storage(스토리지) 아래의 옵션 목록에서 "S3"를 선택하여 시작합니다.



115012842106

2. Amazon Simple Storage System 소개 화면이 나타납니다

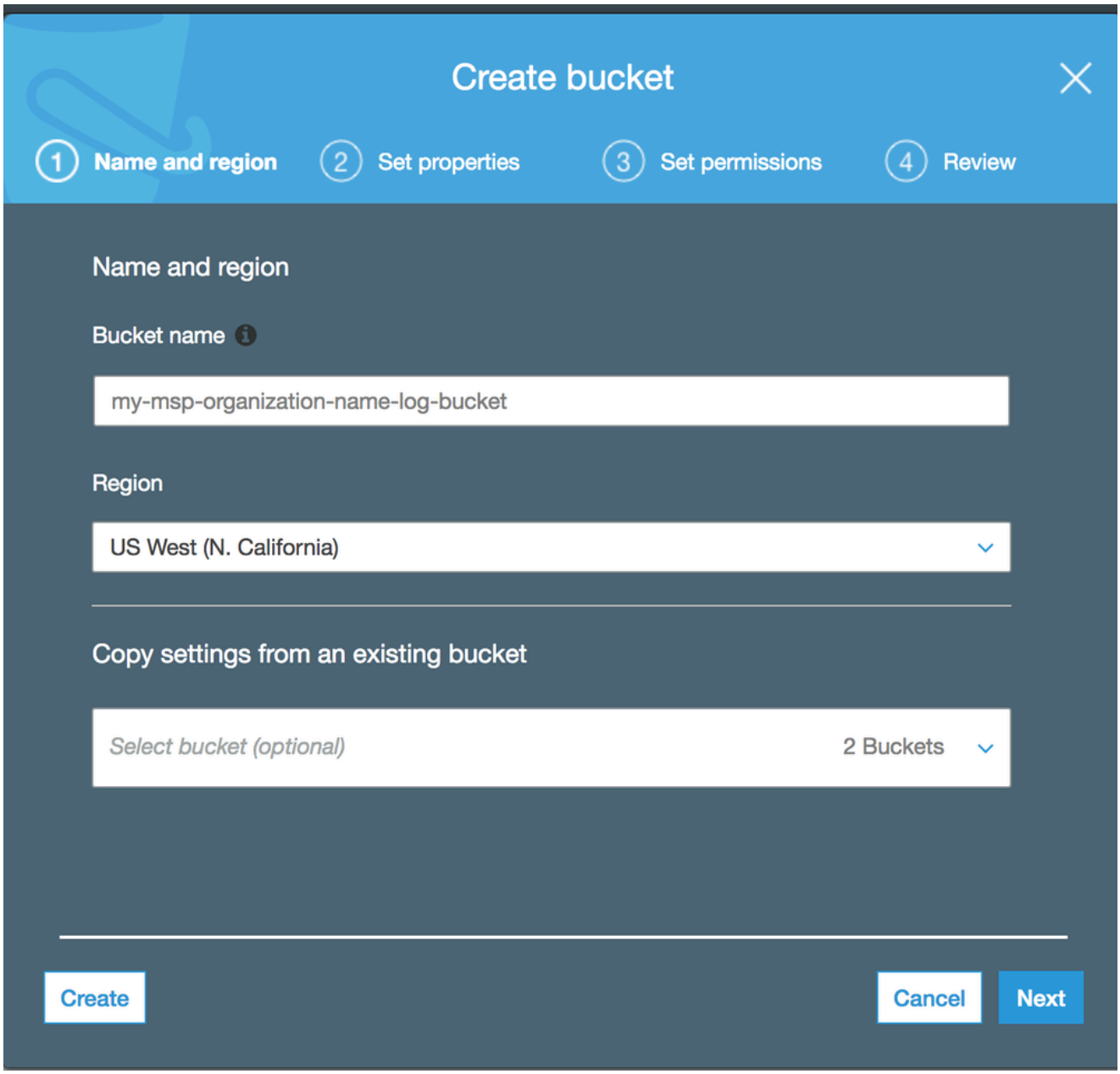
3. 다음으로, 아직 버킷이 없는 경우 버킷을 생성합니다. 을 클릭합니다 버킷 생성



115012842326

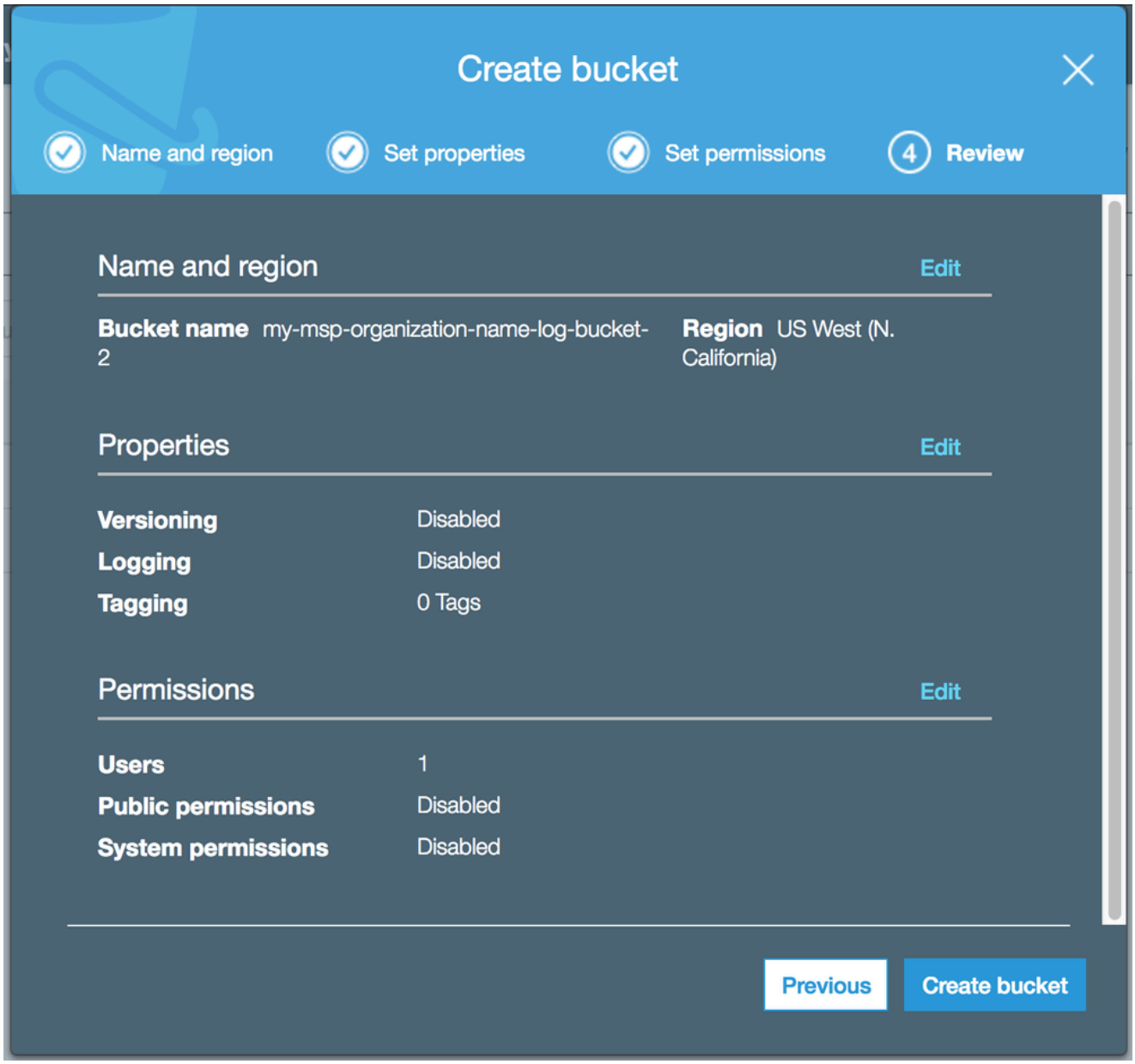
.

4. 버켓 이름을 입력하여 시작합니다.
   버킷 이름은 AWS나 Umbrella뿐만 아니라 모든 Amazon AWS에 대해 고유해야 합니다. "my-organization-name-log-bucket"과 같은 개인적인 것을 사용하면 보편적으로 고유한 버킷 이름에 대한 요구 사항을 우회할 수 있습니다. 버킷 이름은 소문자만 사용해야 하며 공백이나 마침표를 포함할 수 없으며 DNS 명명 규칙을 준수해야 합니다. 이름 제한에 대한 자세한 내용은 여기를 참조하십시오. 이름 지정을 포함하여 버킷 생성에 대한 자세한 내용은 여기를 참조하십시오.



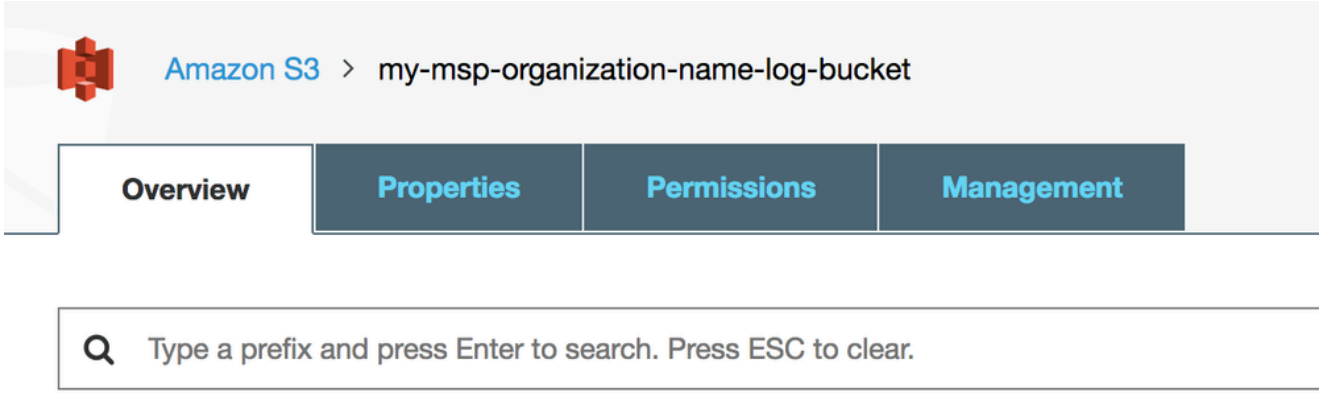
115013010503

5. 해당 위치에 가장 적합한 지역을 선택하고 생성을 누릅니다. 다른 버킷에서 설정을 복사하지 않음
6. "속성 설정" 단계에서 다음을 클릭합니다. 이 값은 나중에 조정할 수 있습니다
7. "권한 설정" 단계에서 다음을 클릭합니다. 나중에 권한을 다시 방문하여 업로드할 버킷을 설정하겠습니다.
8. 검토 프로세스를 마무리하고 버킷 만들기



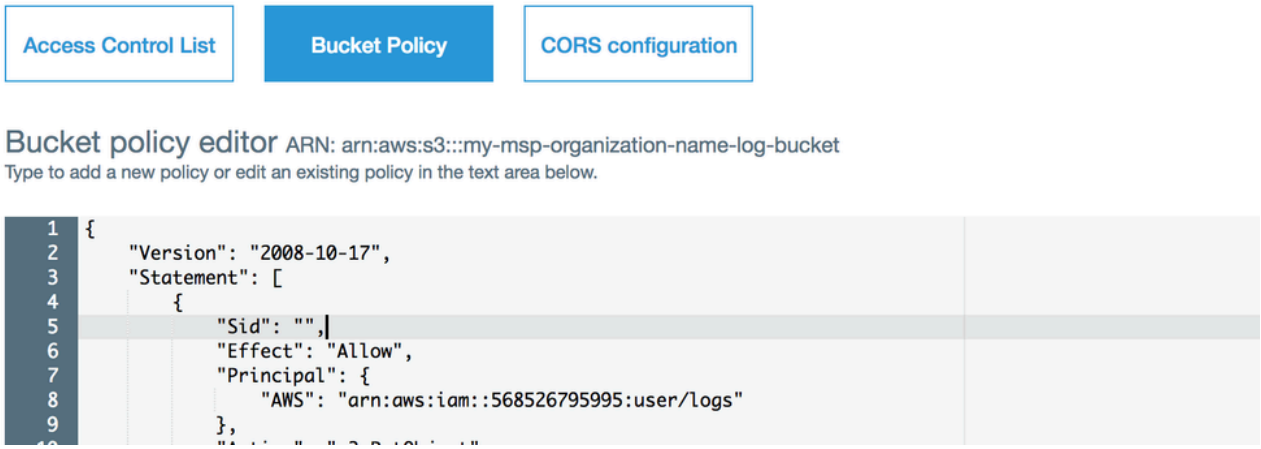
115012842686

9. 그런 다음 Umbrella Service의 업로드를 수락하도록 버킷을 구성해야 합니다. S3에서는 이를 버킷 정책(bucket policy)이라고 한다. 새로 구성된 버킷의 이름을 클릭한 다음 인터페이스 상단에서 Permissions 탭을 선택합니다



115012842906

10. 버킷 정책을 선택한 다음 버킷에 붙여넣으라는 메시지가 표시됩니다



115012843006

11. 버킷 정책이 포함된 아래 JSON 문자열을 복사하여 텍스트 편집기에 붙여넣거나 창에 붙여넣기만 하면 됩니다. 아래에 bucketname이 지정된 정확한 버킷 이름으로 대체합니다. 이 작업을 수행하지 않으면 오류 메시지가 표시됩니다.

{
"버전": "2008-10-17",
"명령문": [
{
"시드": "",
"효과": "허용",
"주도자": {
"AWS": "arn:aws:iam::568526795995:user/logs"
},
"작업": "s3:PutObject",
"리소스": "arn:aws:s3:::bucketname/*"
},
{
"시드": "",
"효과": "거부",
"주도자": {
"AWS": "arn:aws:iam::568526795995:user/logs"
},
"작업": "s3:GetObject",
"리소스": "arn:aws:s3:::bucketname/*"
},

{
"시드": "",
"효과": "허용",
"주도자":

{ "AWS": "arn:aws:iam::568526795995:user/logs" }

,
"작업": "s3:GetBucketLocation",
"리소스": "arn:aws:s3:::bucketname""
},

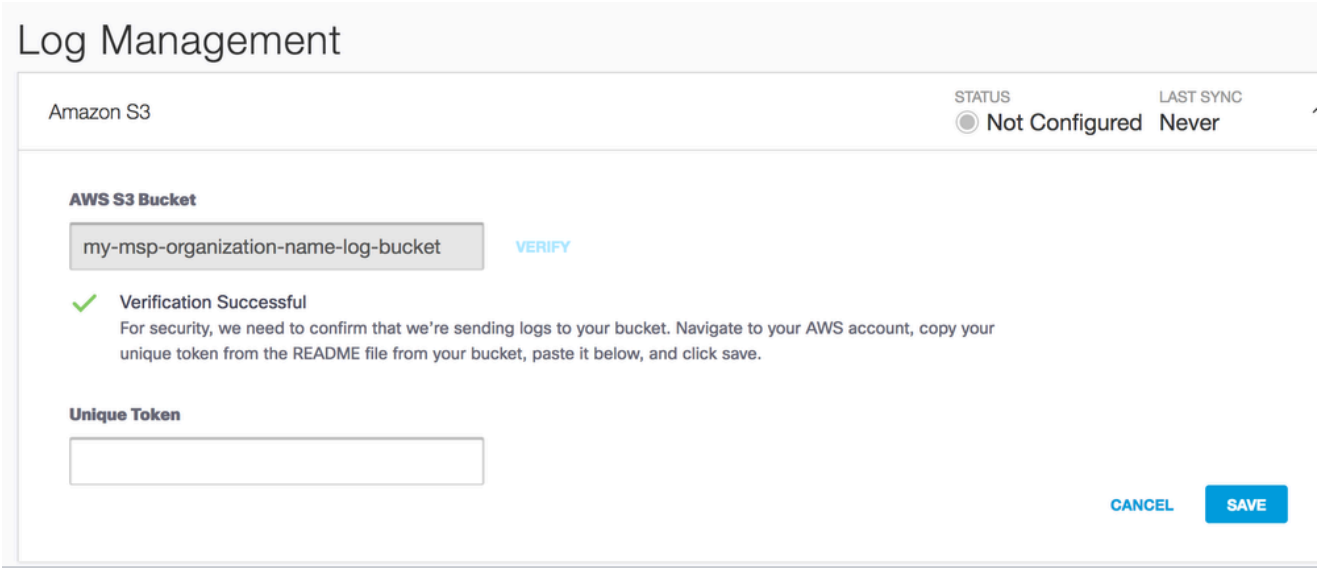
{
"시드": "",
"효과": "허용",
"주도자": {
"AWS": "arn:aws:iam::568526795995:user/logs"
},
"작업": "s3:ListBucket",
"리소스": "arn:aws:s3:::bucketname""
}
]
}

12. 저장을 눌러 이 변경을 확인합니다

Amazon S3 버킷 확인

1단계:

1. Umbrella Console로 돌아가 Settings(설정) > Log Management(로그 관리)로 이동합니다
2. "Amazon S3"를 클릭하여 창을 확장합니다.
3. Bucket Name(버킷 이름) 필드에 S3에서 생성한 정확한 버킷 이름을 입력하거나 붙여넣은 후 Verify(확인)를 클릭합니다
   버킷이 성공적으로 확인되었음을 나타내는 확인 메시지가 대시보드에 표시됩니다.



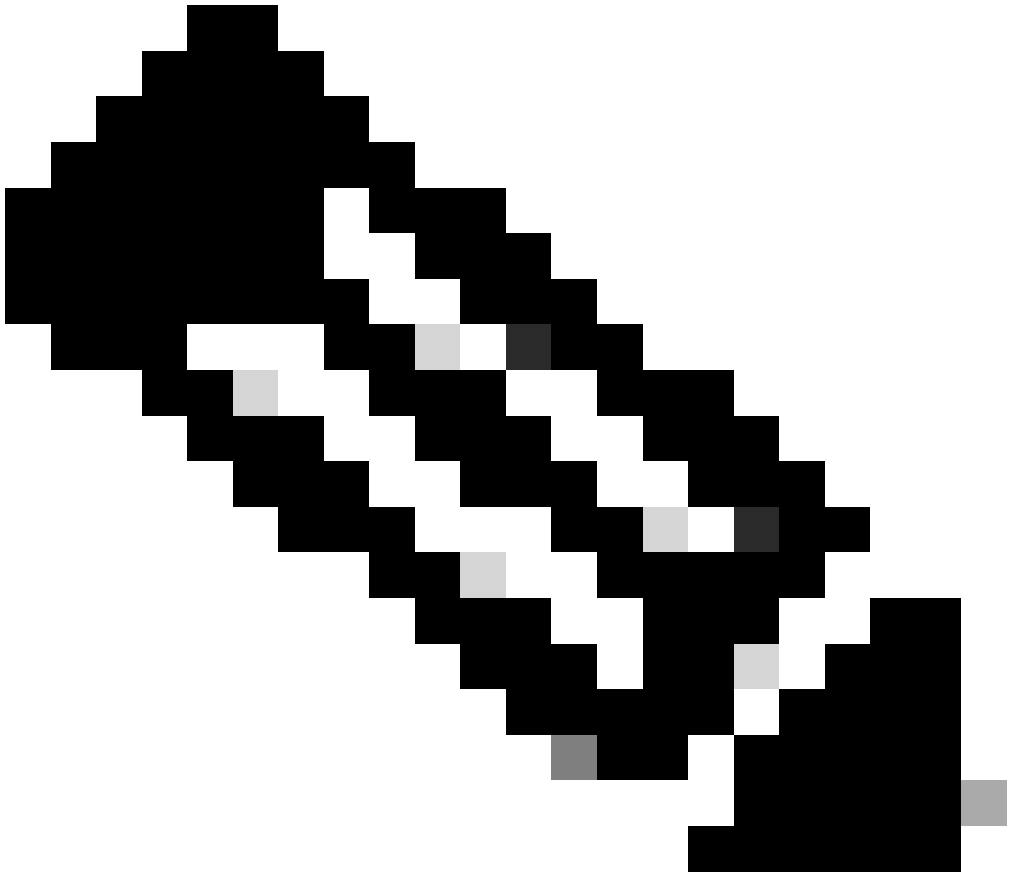
115012847146

버킷을 확인할 수 없다는 오류 메시지가 표시되면 버킷 이름의 구문을 다시 확인하고 컨피그레이션을 검토합니다. 문제가 계속되면 지원 부서에 문의하여 케이스를 여십시오.

2단계:

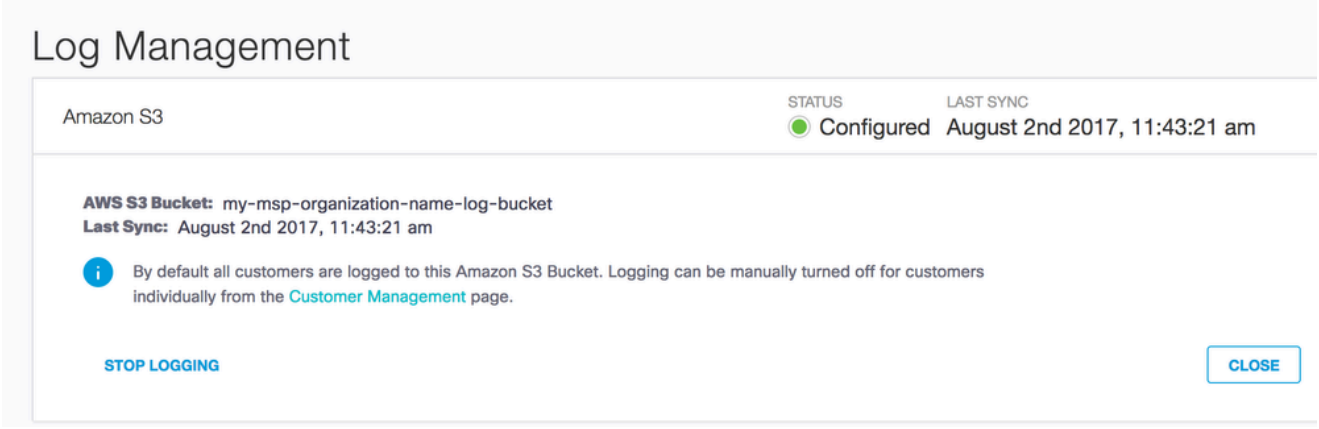
올바른 버킷이 지정되었는지 확인하기 위한 보조 예방 조치로 Umbrella는 고유한 활성화 토큰을 입력하도록 요청합니다. 활성화 토큰은 S3 버킷을 다시 방문하여 얻을 수 있습니다. 확인 프로세스의 일부로 README_FROM_UMBRELLA.txt라는 파일이 Umbrella에서 Amazon S3 버킷으로 업로드되었으며 여기에 표시됩니다.

1. Readme 파일을 두 번 클릭하여 다운로드한 다음 텍스트 편집기에서 엽니다. 파일 내에는 S3 버킷을 Umbrella 대시보드에 연결하는 고유한 토큰이 있습니다



참고: 항목이 업로드된 후 README 파일을 보려면 브라우저에서 S3 버킷을 새로 고쳐야 할 수 있습니다.

2. Umbrella 대시보드로 돌아가 토큰을 "Unique token(고유 토큰)" 필드에 붙여넣고 Save(저장)를 클릭합니다. 이 시점에서 컨피그레이션은
완료. 구성을 검토하려면 Log Management(로그 관리) 섹션에서 Amazon S3 이름을 클릭하면 됩니다



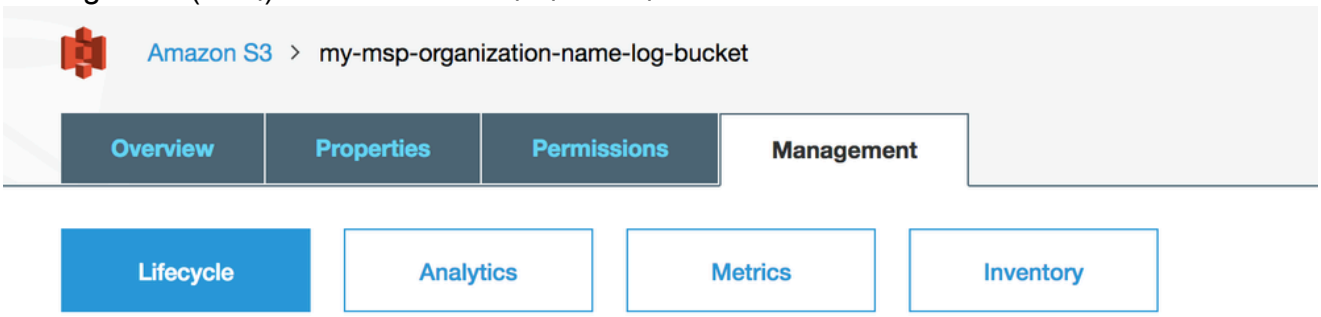
115012848126

로그 라이프사이클 관리

S3를 사용하는 경우 버킷 내에서 데이터의 라이프사이클을 관리하여 로그를 보존하려는 기간을 연장할 수 있습니다. 외부 로그 관리를 사용하는 이유에 따라 기간이 매우 짧거나 매우 길 수 있습니다. 예를 들어, 24시간 후에 S3 버킷에서 로그를 다운로드하여 오프라인에 저장하거나, 클라우드에서 로그를 무기한 유지할 수 있습니다. 기본적으로 Amazon은 데이터를 버킷에 무기한 저장하지만 무제한 저장소는 버킷을 유지 관리하는 비용을 발생시킵니다. S3 주기에 대한 자세한 내용은 여기를 참조하십시오.

버킷의 라이프사이클을 구성하려면

1. Management(관리)를 선택한 다음 라이프사이클



115012848246

2. Add a Rule(규칙 추가)을 클릭한 다음 Apply the Rule to the whole bucket(또는 구성한 경우 하위 폴더)을 클릭합니다.
3. Delete(삭제) 또는 Archive(아카이브)와 같은 객체에 대한 작업을 선택한 다음 기간과 Amazon 비용 절감을 위해 Glacier 스토리지를 사용할지 여부를 선택합니다. (Glacier는 오프라인 스토리지이므로 액세스 속도가 느리지만 비용이 적게 듭니다.)

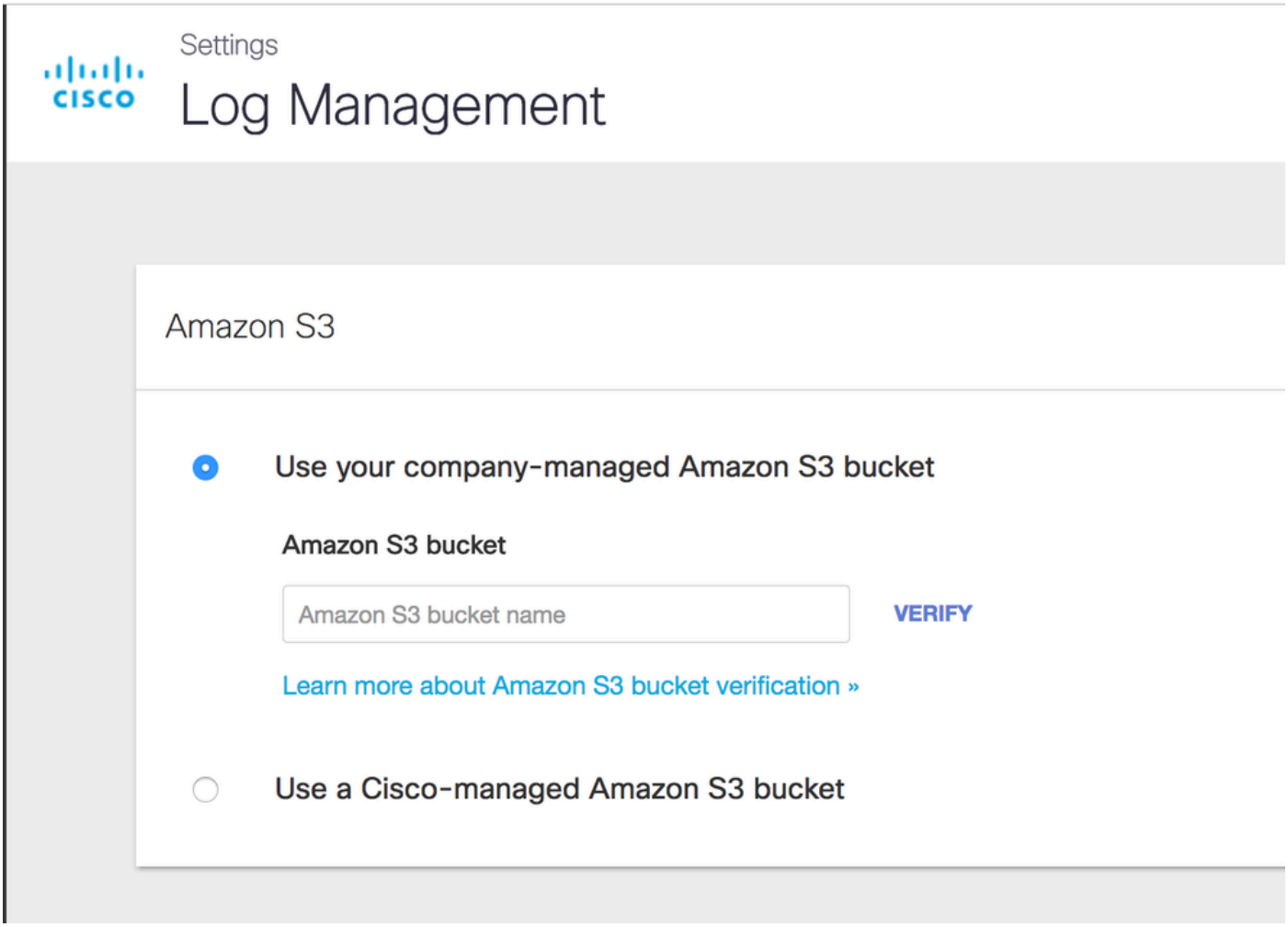
4. 다른 방법(예: 내부 백업 솔루션)으로 로그를 관리하려는 경우 S3에서 로그를 다운로드하고 다른 방법으로 보존한 다음 보존 시간을 며칠로 설정하면 됩니다.

Cisco 관리 S3 버킷 구성

Umbrella 대시보드에서 Settings(설정) > Log Management(로그 관리)로 이동합니다.

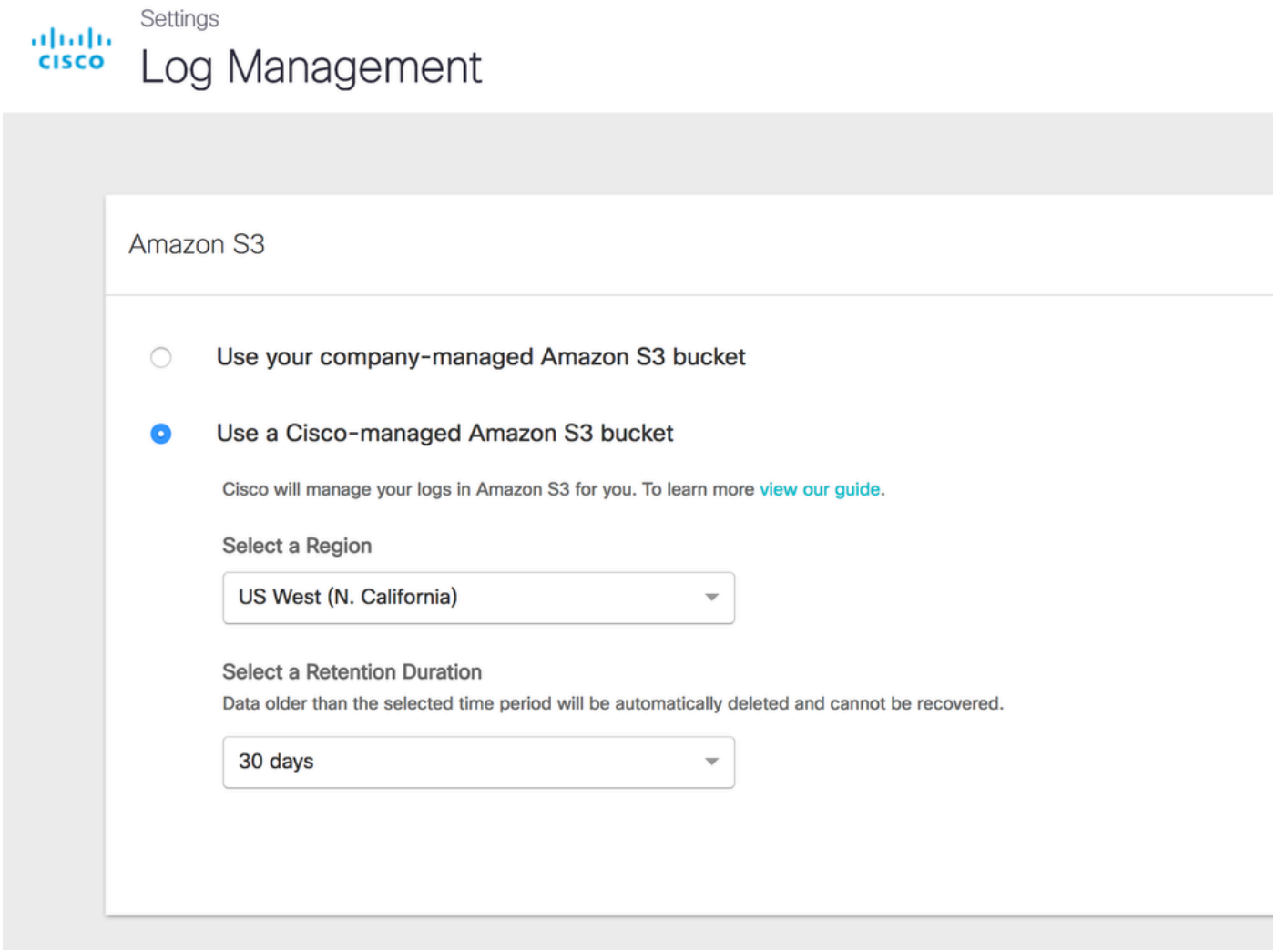
두 가지 옵션이 있습니다.

- 회사에서 관리하는 Amazon S3 버킷 사용
- Cisco 매니지드 Amazon S3 버킷 사용



25231151138964

"Cisco에서 관리하는 Amazon S3 버킷 사용"을 선택하면 두 가지 새로운 옵션이 제공됩니다. "지역 선택" 및 "보존 기간 선택"



252311511158036

지역 선택

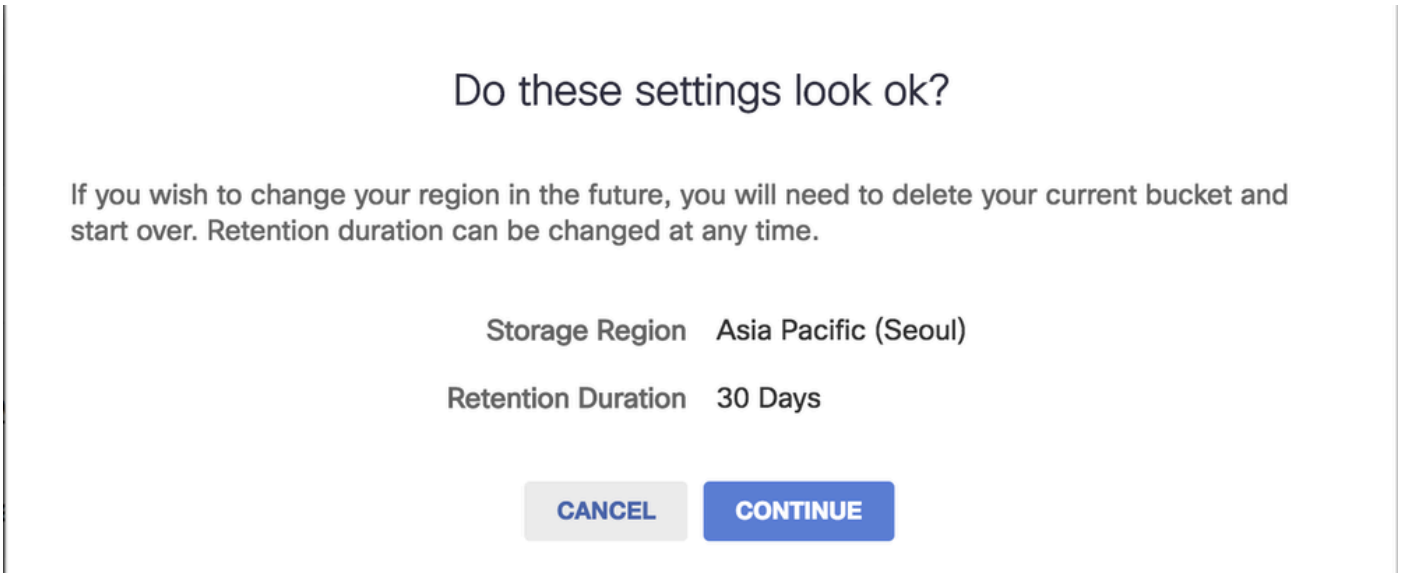
서버에 로그를 다운로드할 때 지연 시간을 최소화하려면 지역별 엔드포인트가 중요합니다. 나열된 리전은 Amazon S3에서 사용할 수 있는 리전과 일치하지만 모든 리전을 사용할 수 있는 것은 아닙니다. 예를 들어, 중국은 목록에 없습니다.

드롭다운에서 가장 가까운 지역을 선택합니다. 나중에 지역을 변경하려면 현재 설정을 삭제하고 다시 시작해야 합니다.

보존 기간 선택

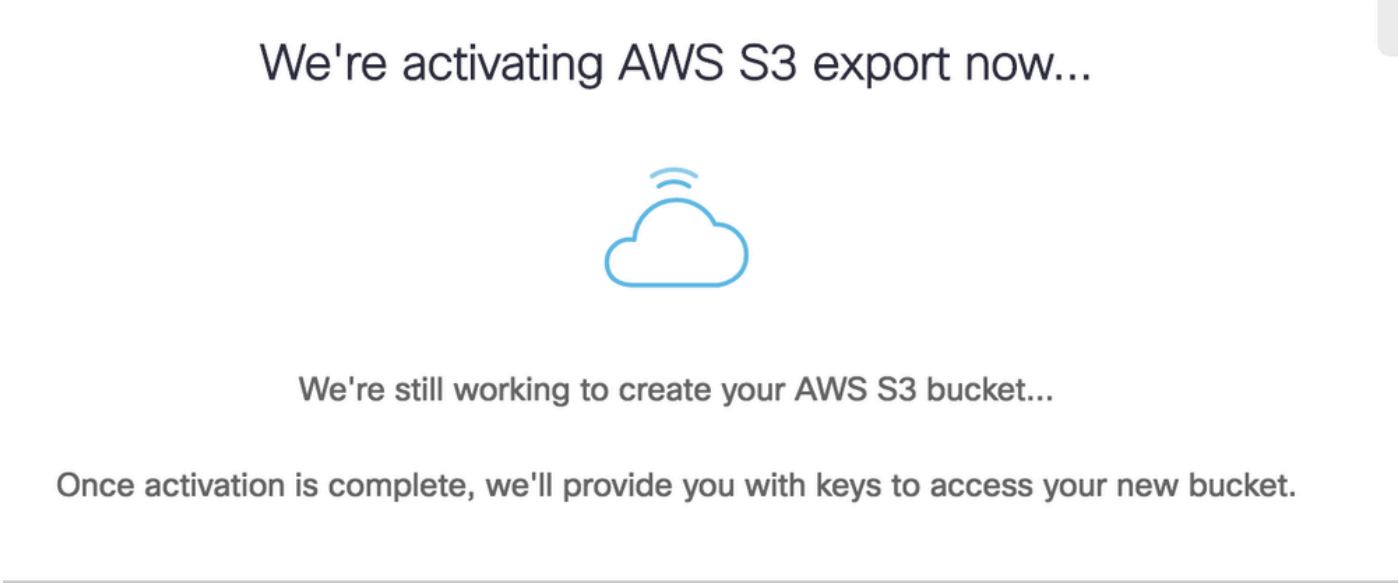
보존 기간은 단순히 7, 14 또는 30일입니다. 선택한 기간이 지나면 모든 데이터가 삭제되고 어떤 경우에도 검색할 수 없습니다. 섭취 주기가 규칙적이라면 좀 더 짧은 기간을 권장한다. 보존 기간은 나중에 변경할 수 있습니다.

선택한 후 다음을 클릭하면 지역 및 기간을 확인하라는 메시지가 표시됩니다



25231181211796

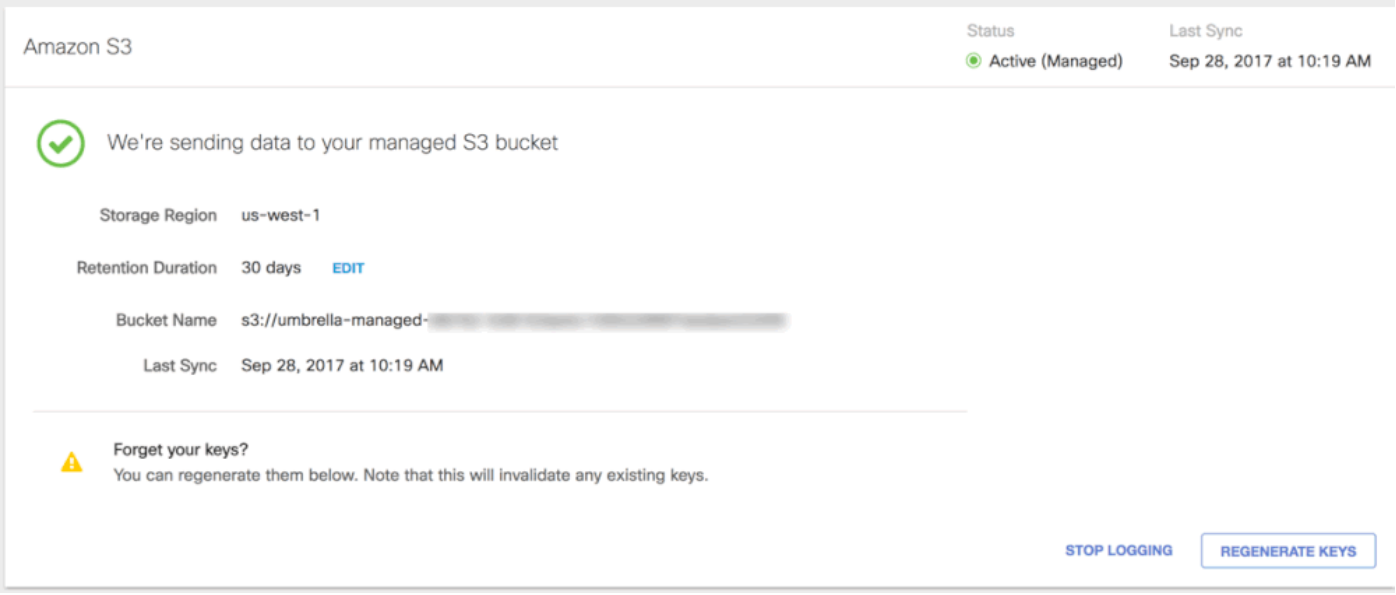
계속하는 데 동의하면 활성화 알림이 전송됩니다.



25231181218708

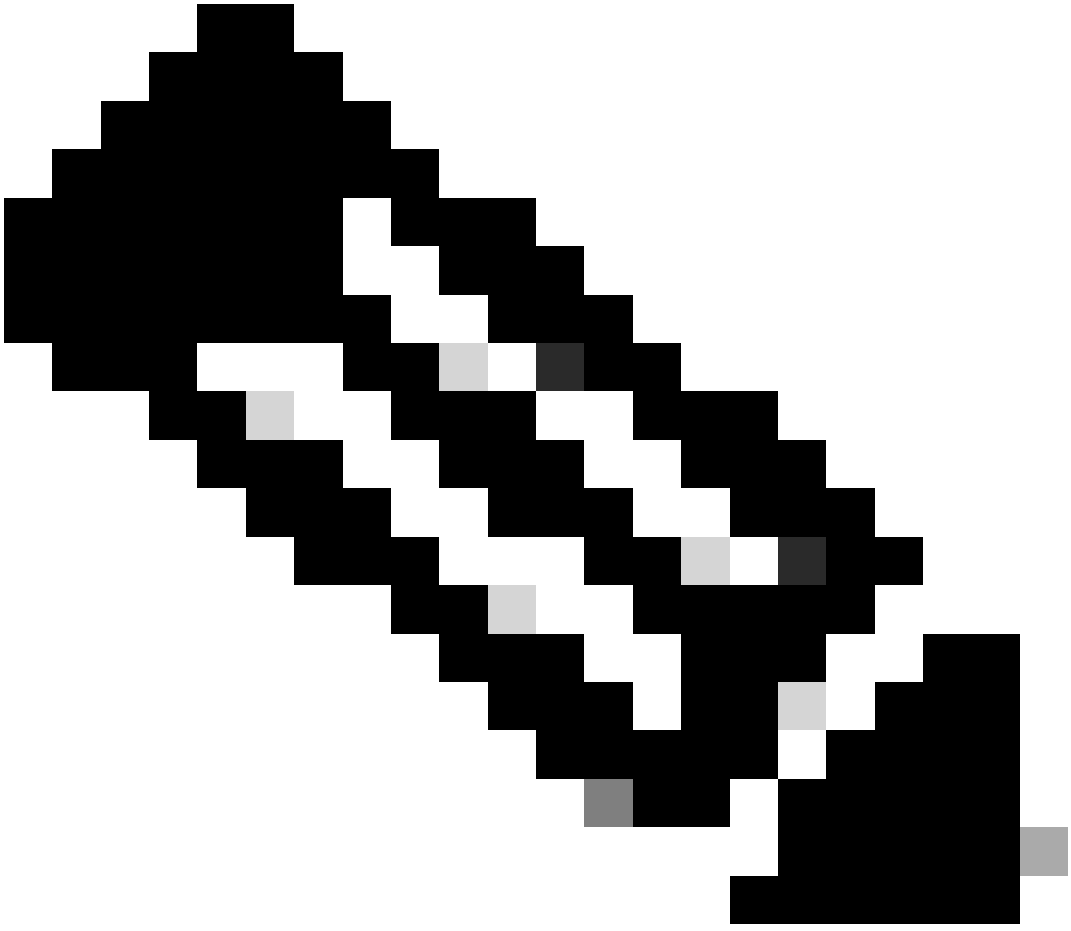
그런 다음 액세스 키와 의 비밀 키를 수신합니다. 이 경우에 유일하게 키 중 하나를 볼 수 있으므로 수락해야 합니다("Got it!" 클릭). 버킷에 액세스하고 로그를 다운로드하려면 액세스 및 비밀 키가 필요합니다.

마지막으로 컨피그레이션 및 가장 중요한 버킷 이름을 보여 주는 요약 화면이 표시됩니다.



25231181228180

편리한 시간에 로깅을 켜거나 끌 수 있습니다.



참고: 로깅이 해제된 경우에도 Cisco는 선택한 보존 기간을 기반으로 로그를 계속 삭제합니다.

사후 컨피그레이션 옵션

로그 업로드 실패

Cisco Umbrella에서 S3 버킷으로 로그를 업로드하지 못할 경우, 서비스가 20분마다 재시도되는 4시간의 유예 기간이 있습니다. 4시간 후 지원 팀과 함께 케이스를 열고 문제의 원인을 조사하고 문제를 사전에 알려드릴 수 있도록 합니다.

업로드된 로그 및 형식 확인

로그는 Umbrella 로그 대기열에서 S3 버킷으로 10분 간격으로 업로드됩니다. 컨피그레이션을 완료한 후, 첫 번째 로그는 2시간 내에 S3 버킷에 업로드됩니다. 단, 프로세스는 대개 즉시 또는 즉시 가까이에 있습니다. 그러나 항목을 업로드하려면 새로 생성된 로그 데이터가 있어야 합니다. 따라서 테스트 환경에서 이 작업을 시도하는 경우 네트워크 데이터가 작업 검색에 기록되고 있는지 확인합니다.

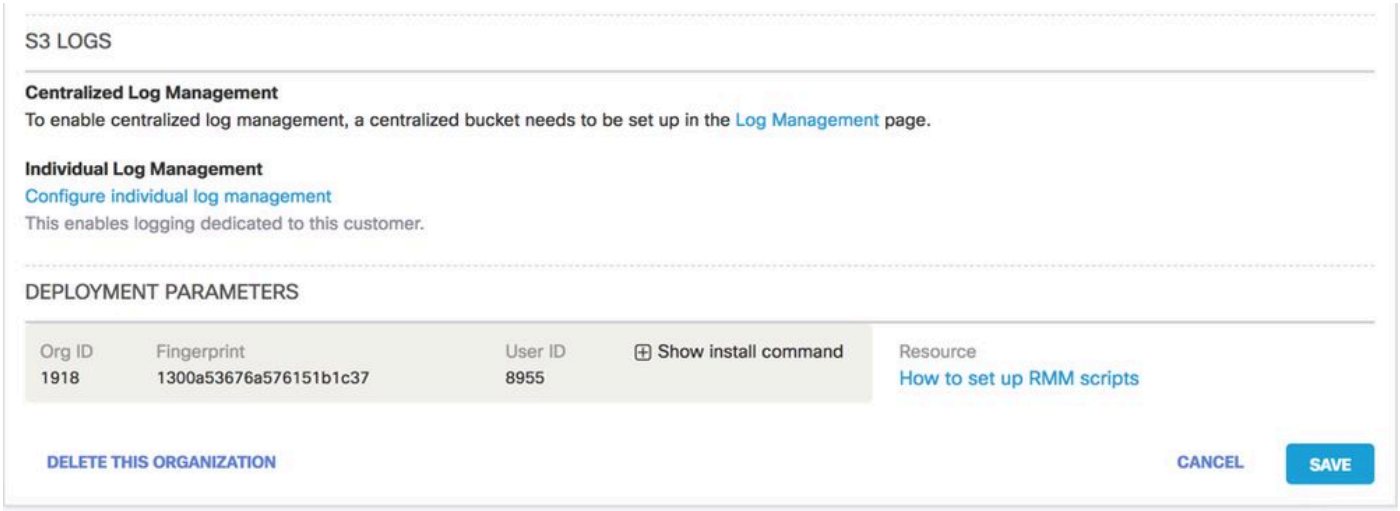
모든 것이 작동하는지 확인하기 위해 Umbrella 대시보드 업데이트 및 로그의 마지막 동기화 시간이 S3 버킷에 나타나기 시작합니다.

버켓 내에서 각 고객 또는 조직은 조직 ID로 레이블이 지정되므로 폴더 구조는 다음과 같습니다.

```
Amazon S3/<bucket-name>/<orgID>/<subfolder>
```

<bucket-name>은(는) 버킷 이름이고, <orgID>는(는) 조직 ID이며, <subfolder>는(는) 내 로그 유형에 따라 dnslogs, proxylogs 또는 iplogs입니다.

MSP 및 MSSP 고객의 경우 orgID는 배포 매개변수 섹션의 각 고객 세부사항 아래에 있는 고객 설정에 있는 것과 일치합니다. 복수 조직 고객은 각 개별 하위 조직에 로그인하고 브라우저 URL에 orgID를 표시하여 orgID를 수집할 수 있습니다. (https://dashboard.umbrella.com/o/######/).



360002271623

현재 MSP, MSSP 및 복수 조직 고객의 로그 형식 버전은 버전 1.1입니다. 로그는 GZIP 형식으로 표시되며 다음과 같은 이름 지정 형식의 해당 하위 폴더에 있는 S3 버킷에 업로드됩니다.

```
<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz
```

<subfolder>는 내부 로그 유형에 따라 dnslogs, proxylogs 또는 iplogs입니다. <xxxx>는 4자의 영숫자로 된 임의의 문자열로서 중복 파일 이름을 덮어쓰지 않도록 합니다.

예를 들면 다음과 같습니다.

```
dnslogs/2019-01-01/2019-01-01-00-00-e4e1.csv.gz
```

10분 내에 버킷에 로그가 표시되지 않으면 지원 팀에 문의하여 지금까지 수행한 단계를 요약해 주십시오.

로그가 표시되면 수신된 처음 몇 개의 로그 업로드의 내용을 압축 해제하여 데이터를 검토하여 텍스트 편집기(또는 Microsoft Excel에서도 종종 .CSV의 기본값)에서 데이터를 볼 수 있도록 하는 것이 좋습니다. 로그의 각 필드가 나타내는 정보에 대해서는 여기를 참조하십시오.

Cisco Umbrella에서 S3 버킷으로의 로그 업로드가 실패하면 서비스가 20분마다 재시도하는 4시간의 유예 기간이 있습니다. 4시간 후 지원 팀 내에서 케이스가 열리며, 지원 팀은 문제의 원인에 대한 조사를 시작하고 문제에 대해 알려드리기 위해 사전에 연락을 드릴 것입니다.

고객별로 로깅 활성화

별도로 명시되지 않는 한 이 기능은 모든 고객에게 기본적으로 제공됩니다. 이 기능은 개별 고객의 경우 해제할 수 있으며, 해당 기능을 보유한 고객의 서비스 수준이 다른 경우 유용합니다. 이것은

Console의 각 사용자 지정 설정에 있습니다. 이전 섹션의 스크린샷은 토글 기능을 해제하여 보여줍니다.

Amazon에서 IAM 사용자를 생성하고 이러한 IAM 사용자를 버킷의 개별 orgit 하위 폴더에 할당할 수도 있습니다. 이렇게 하면 최종 사용자가 자신의 로그에 액세스하도록 허용할 수 있지만 해당 로그만이 허용됩니다.

로그 다운로드, 형식 이해 및 Splunk/QRadar 통합

보존 또는 사용을 위해 로그를 다운로드하려면 S3에서 DNS 로그를 다운로드하는 몇 가지 방법이 있습니다. 이 문제에 대한 몇 가지 방법을 설명하는 문서를 여기에 작성했습니다.

또한 로그 형식 및 Umbrella 대시보드에 표시되는 로그와 어떻게 다른지에 대한 몇 가지 질문이 있을 수 있습니다. 내보낸 로그 형식에 대한 자세한 내용은 이 문서를 참조하십시오.

마지막으로, DNS 로그를 내보내는 주요 용도 중 하나는 SIEM 툴과의 통합입니다. 이와 같은 로그를 처리할 때 SIEM에 대한 컨피그레이션은 관리자에게 전달되는 경우가 종종 있지만, 가장 많이 사용되는 SIEM에 대한 몇 가지 지침이 있습니다.

Amazon AWS S3 및 Umbrella용 Splunk 플러그인 설정에 대한 자세한 내용은 여기를 참조하십시오.

Amazon S3에서 로그를 가져오고 다이제스트하도록 IBM QRadar를 구성하는 방법에 대한 자세한 내용은 여기를 참조하십시오.

S3 로그의 크기는 어느 정도입니까?

S3 로그의 크기는 발생한 이벤트 수에 따라 달라지며, 이는 DNS 트래픽의 볼륨에 따라 달라집니다.

S3 로깅의 로그 형식은 여기에서 확인할 수 있습니다.

예제 항목은 220바이트이지만 각 로그 줄의 크기는 항목 수(도메인 이름 길이, 범주 수 등)에 따라 달라집니다. 각 로그 행이 220바이트라고 가정하면 백만 개의 요청은 220MB가 됩니다.

매일 표시되는 DNS 쿼리 수를 추정하려면

1. Umbrella 대시보드에서 Reporting(보고) > Activity Search(활동 검색)로 이동합니다.
2. Filters(필터)에서 지난 24시간 동안 보고서를 실행한 다음 Export CSV(CSV 내보내기) 아이콘을 클릭합니다.
3. 다운로드한 .csv 파일을 엽니다. 행 수(헤더에 대해 1을 빼기)는 일별 DNS 쿼리 수입니다. 여기에 220바이트를 곱하여 하루 동안의 예상치를 구합니다.

비용 측면에서는 가변적이지만 가장 많은 고객들조차도 한 달에 몇 달러밖에 소비하지 않는다는 것을 알 수 있습니다. 한 가지 비용은 스토리지 시간과 관련이 있으며 다른 한 가지 비용은 S3에서 사용자 환경으로 데이터를 다운로드하는 데 사용됩니다. 자세한 내용은 Amazon에 문의하십시오.

Cisco의 모든 기능과 마찬가지로, 특히 SIEM 통합 또는 이 문서에서 다루는 기타 질문에 대한 여러분의 의견을 알고 싶습니다. 피드백이 있으면 알려 주십시오!

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.