MSP、MSSP、および複数の組織のお客様に対するAmazon S3サービスによる集中Umbrella口グ管理について

内容

はじめに

このドキュメントでは、MSP、MSSP、および複数の組織のお客様に対するAmazon S3サービスでのUmbrella口グの一元管理について説明します。

概要

MSP、MSSP、およびマルチ組織コンソールには、顧客のDNS、URL、およびIP口グをクラウドストレージにオフラインで保存する機能があります。ストレージはAmazon S3にあり、口グがアップロードされた後、コンプライアンス上の理由またはセキュリティ分析のために口グをダウンロードして保持できます。

このドキュメントでは、この機能を理解し、Umbrellaダッシュボードと Amazon S3コンソールの両方で設定し、S3で口グを保持する期間を含む、いくつかの設定オプションを実行するのに役立ちます。

MSP、MSSP、およびマルチ組織のすべてのUmbrellaには、コンソールの子組織からトラフィックアクティビティログをアップロードし、それらのログをクラウドに保存する機能があります。AmazonのAWS S3(Simple Storage Service)はログをアーカイブするサービスで、isoffline storageまたはislog retentionと呼ばれることもあります。

ログのアーカイブは、必要に応じて、いくつかの理由で役立ちます。一部のユーザは、エクスポートおよびアーカイブされたログをSIEMなどのデータ分析またはセキュリティフォレンジックツールにインポートできます。また、セキュリティインシデントの場合にデータフォレンジックや人事記録に役立つアクティビティログのアーカイブもあります。

AWS S3では、ログは圧縮(gzip)アーカイブにCSV形式で保存されます。ログは10分ごとにアップロードされるため、ネットワークからのネットワークトラフィックがUmbrellaによって記録されてからS3からダウンロードできるようになるまでの間に、最低10分の遅延が発生します。

コンソールからのorgID番号

各カスタマー組織は、コンソールのorgID番号を使用して各カスタマーをフォルダにマッピングし、ログを個別にアップロードします。 この機能は、カスタマー単位または組織単位で有効または無効にできます。

2種類のUmbrella口グ管理

口グ管理は、いわゆるit isbucketit is （本質的にAWSit is S3環境内のフォルダ）に口グをアップロードすることによって実行されます。 Umbrella口グのバケットをホストするには、次の2つの方法があります。

- 会社の管理者であるあなたによって管理、管理、および支払われます。
- Cisco Umbrellaによる管理、管理、支払い。

シスコにS3バケットを管理してもらうことには、長所と短所があります。

バケットを管理するシスコの長所：

- 設定が非常に簡単です。数分で済み、その後の管理は非常に簡単です。
- シスコのバケット管理はUmbrellaのライセンスコストに含まれており、実質的にサービスが無料になります。自分のバケットを持つことはコストがかかりますが、別の請求書を管理するための間接費は非常に高額になる可能性があります。

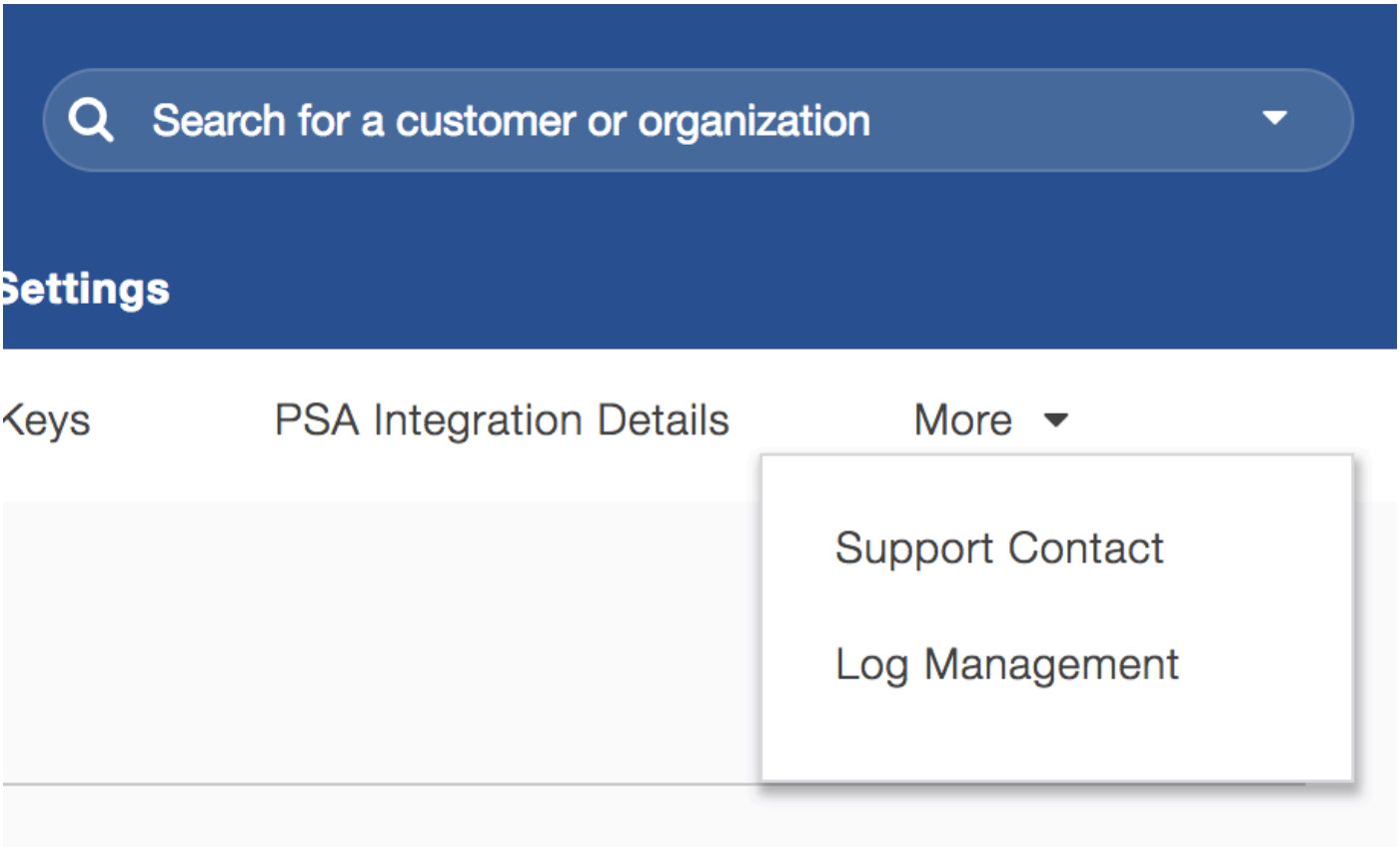
S3インスタンスを自分で管理する長所：

- データをオフラインで保存できる期間に制限はありません。シスコでは、オフラインストレージを最大30日間に制限しています。
- Umbrellaのログファイルを含め、バケットに何でも追加できるため、バケットは他のアプリケーションでも使用できます。
- 自動化やコマンドラインのヘルプなど、高度な設定サポートについては、Amazonから直接サポートを受けることができます。

ほとんどのお客様にとって、バケットの維持コストは非常に安価ですが、手間がかかることがあります。

はじめに

ログ管理機能は、コンソールのSettings > Log Managementにあります（ドロップダウン矢印をクリックします）。



115012963103

自己管理型S3バケットの設定

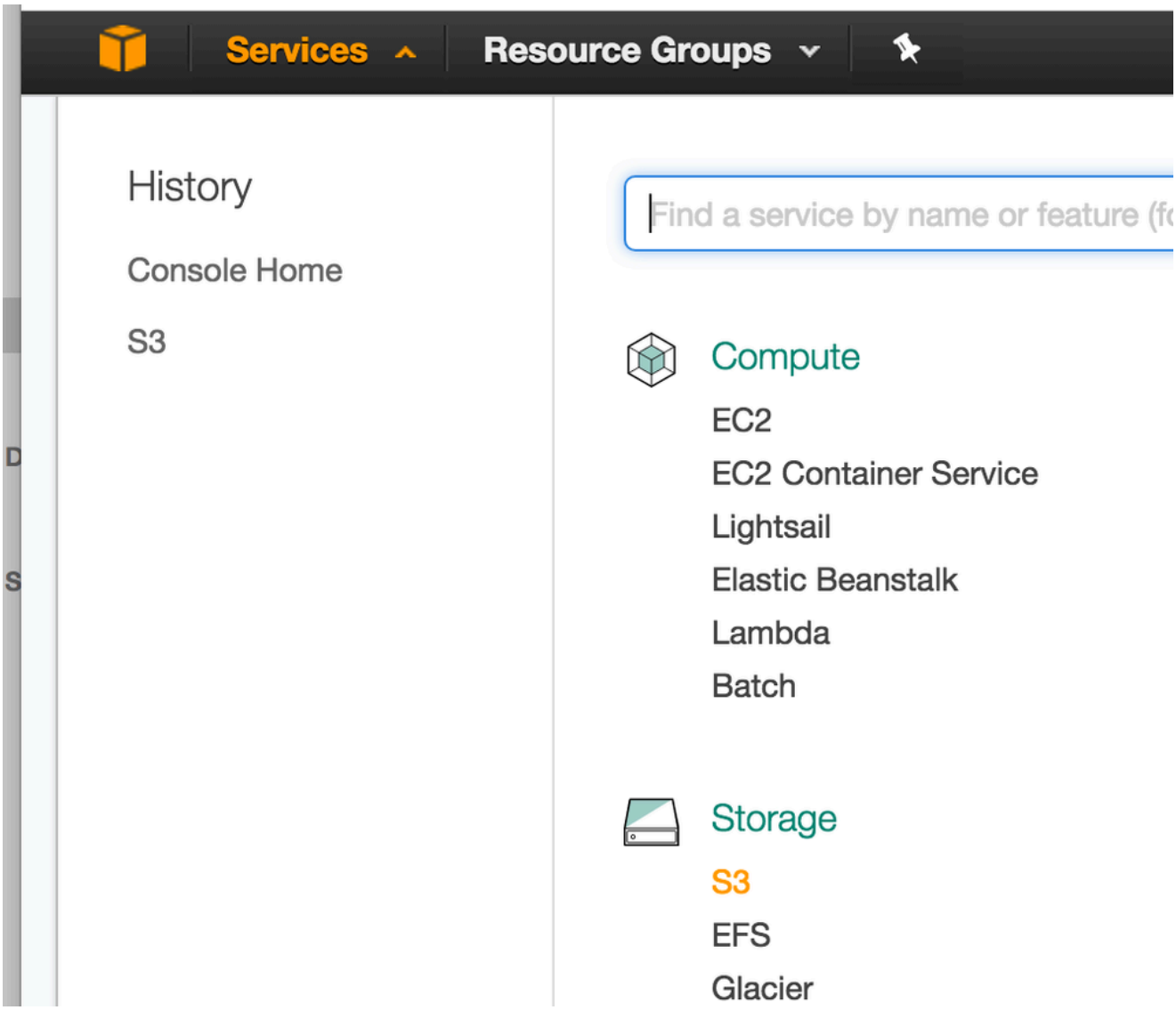
前提条件

ログをアーカイブするには、次の要件を満たす必要があります。

- Cisco Umbrella MSP、MSSP、またはMulti-org Consoleへの完全な管理アクセス。
- Amazon AWSサービス(https://aws.amazon.com/console/)にログインします。 アカウントをお持ちでない場合、AmazonはS3に無料のサインアップを提供します。ただし、無料利用枠を超える場合はクレジットカードが必要です。
- ログストレージ用にAmazon S3で構成されたバケット。Amazon S3バケットの設定とセットアップの手順については、次のセクションを参照してください。

Amazon S3バケットのセットアップ

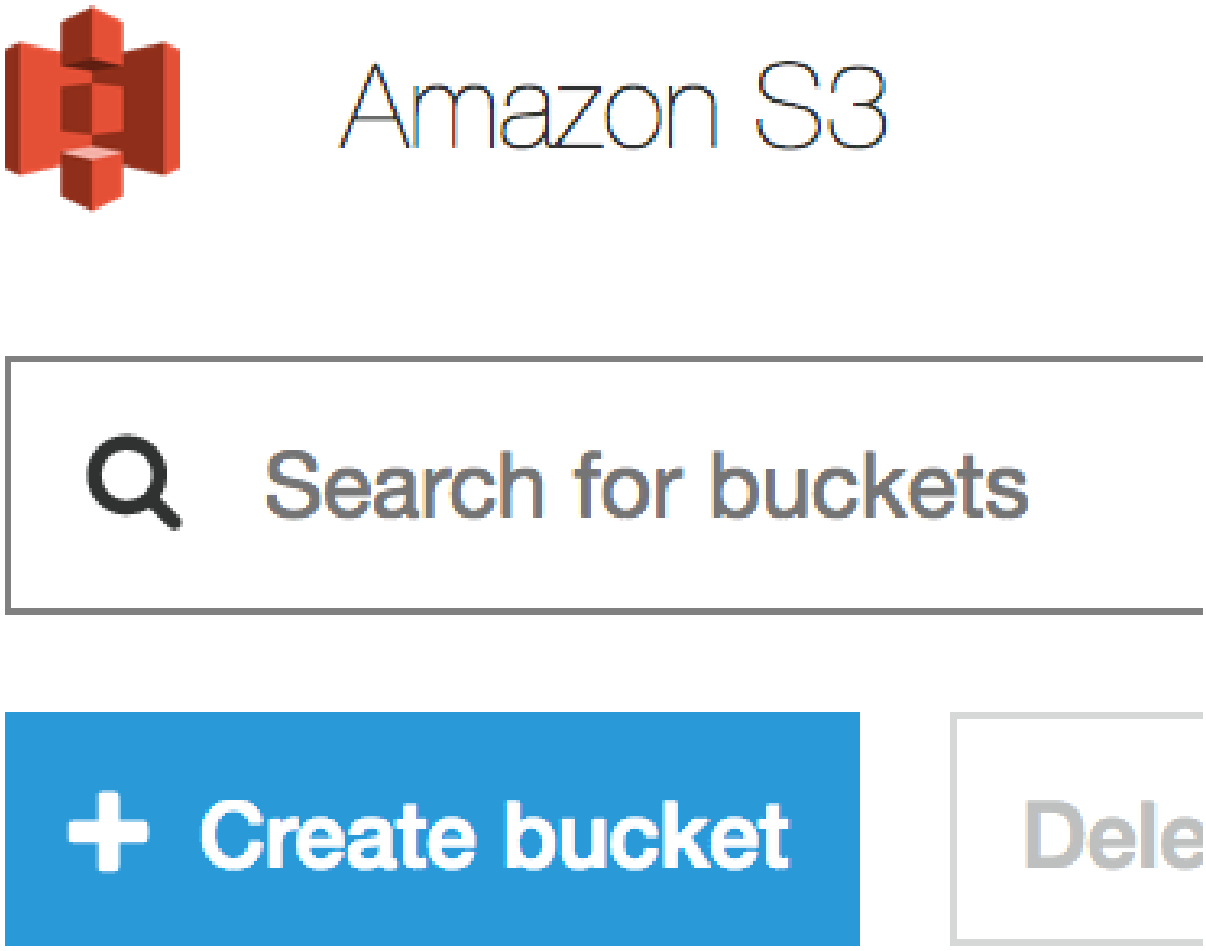
1. 最初にAWSコンソールにサインインし、「ストレージ」の下のオプションのリストから「S3」を選択します。



115012842106

2. Amazon Simple Storage Systemを開始するための概要画面が表示されます

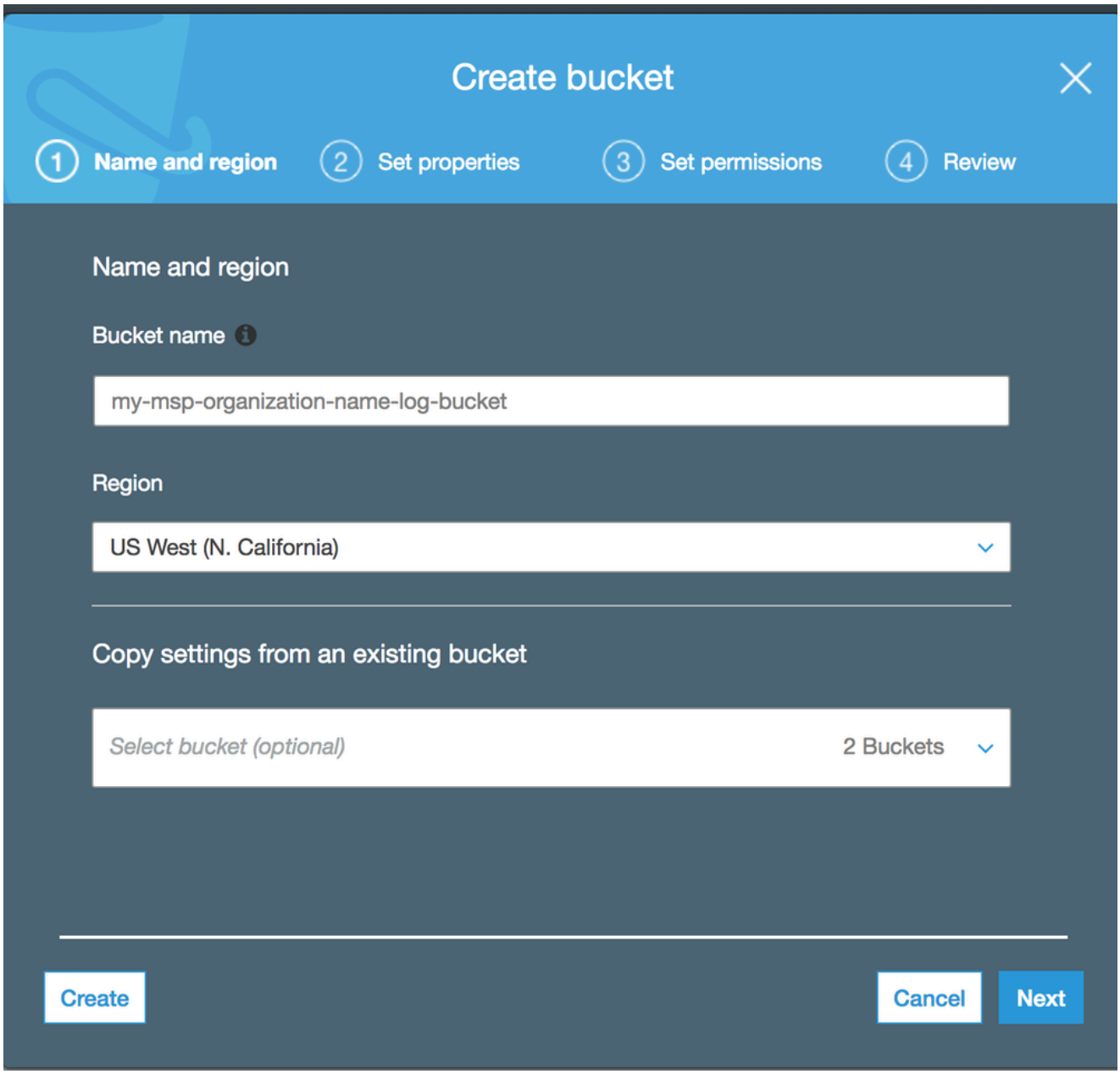
3. 次に、まだバケットがない場合は、バケットを作成します。[保存（ バケットの作成



115012842326

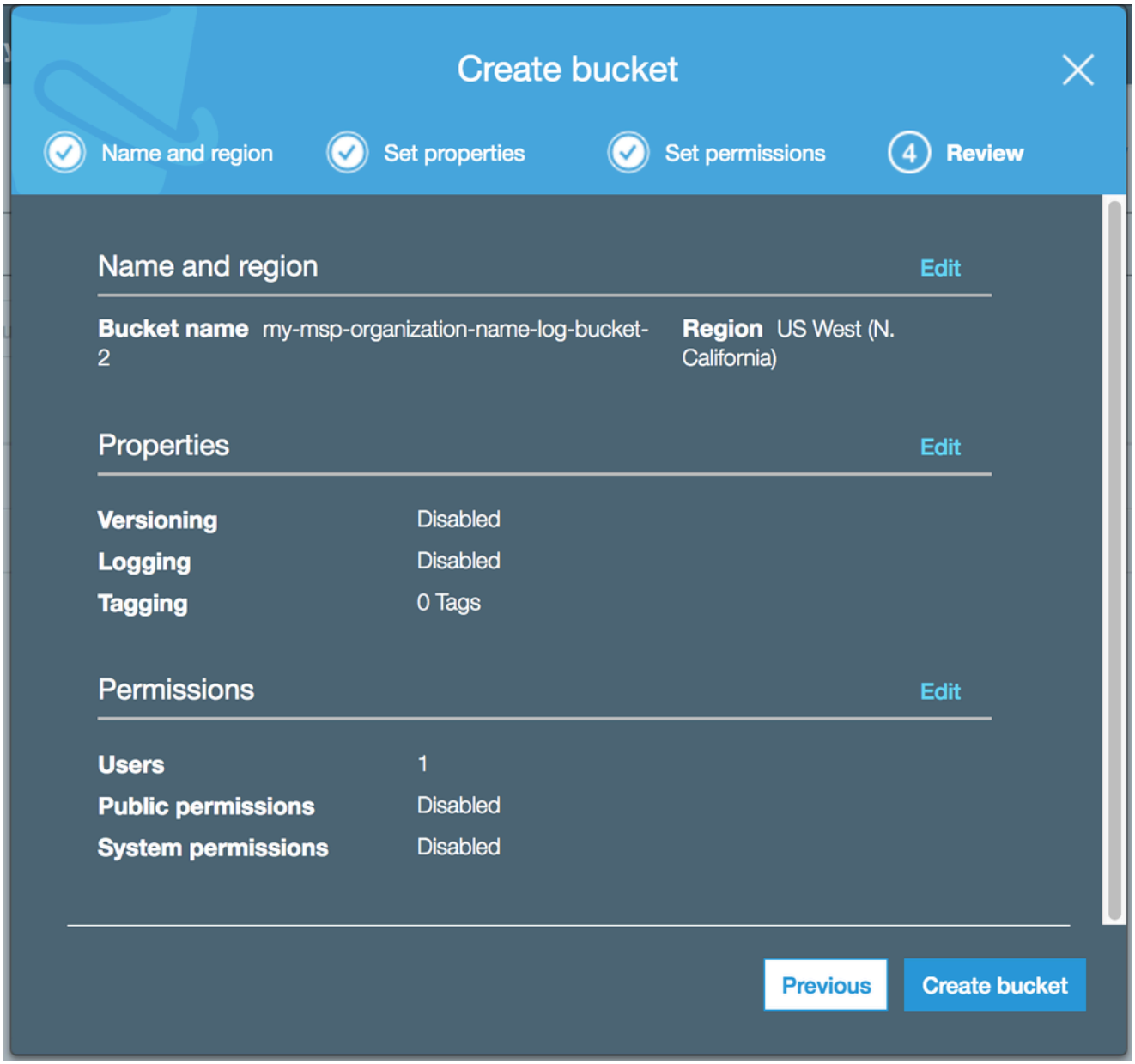
.

4. バケット名の入力から開始します。
   バケット名は、AWSまたはUmbrellaだけでなく、すべてのAmazon AWSに対して普遍的に一意である必要があります。「my-organization-name-log-bucket」などの個人的な名前を使用すると、汎用的に一意なバケット名の要件をバイパスできます。バケット名は小文字だけを使用する必要があり、スペースやピリオドを含めることはできません。また、DNSの命名規則に従う必要があります。 名前の制限の詳細については、ここを参照してください。
   命名を含むバケット作成の詳細については、ここを参照してください。



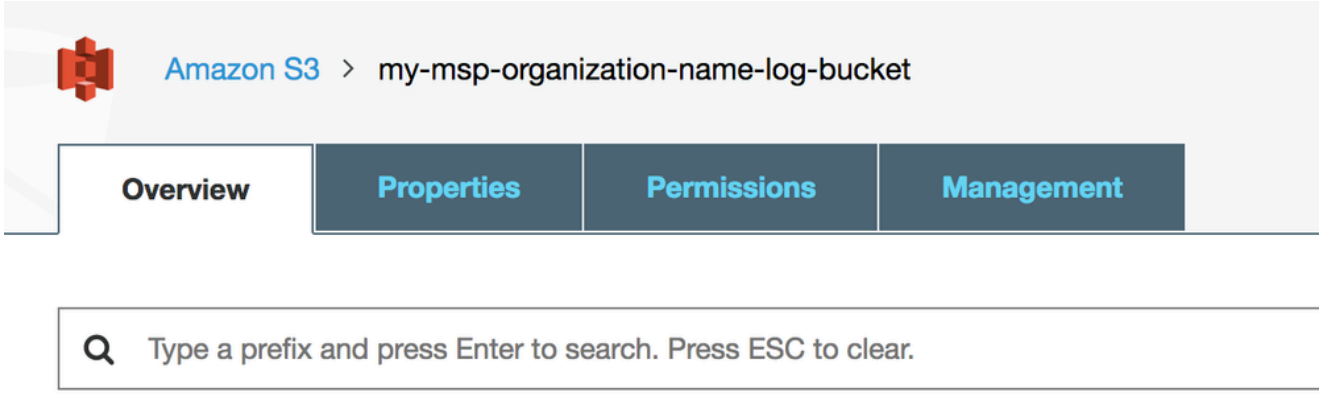
115013010503

5. 場所に最も適したリージョンを選択し、Createをクリックします。別のバケットから設定をコピーしないでください
6. 「プロパティの設定」ステップでは、次へをクリックするだけです。これらは後で調整できます
7. 「権限の設定」ステップで、次へをクリックします。後で権限を再確認して、アップロード用にバケットを設定します
8. レビュープロセスを完了し、 バケットの作成



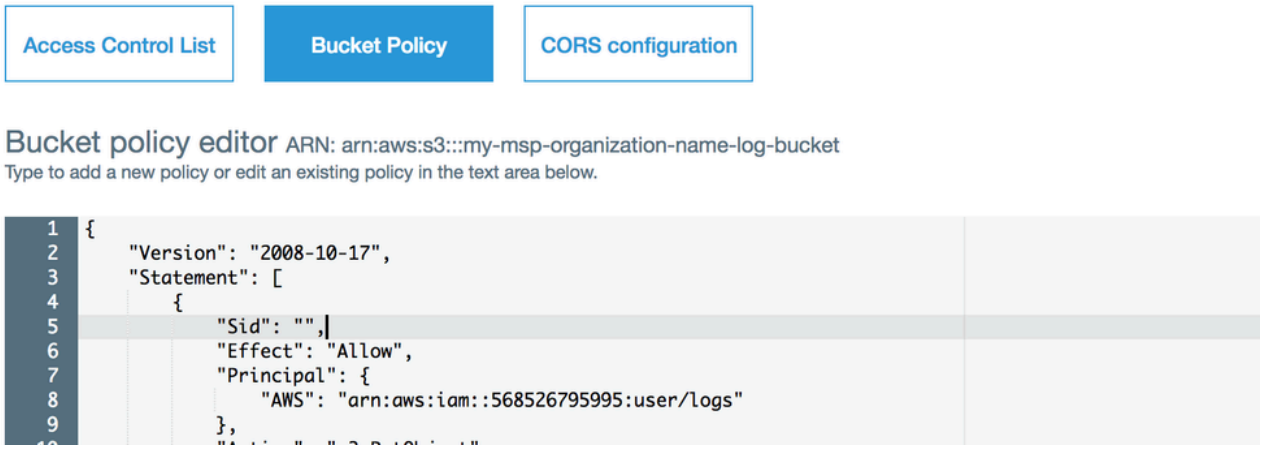
115012842686

9. 次に、Umbrellaサービスからのアップロードを受け入れるようにバケットを設定する必要があります。S3では、これはバケットポリシーと呼ばれます。新しく設定したバケットの名前をクリックし、インターフェイスの上部にあるPermissionsタブを選択します



115012842906

10. Bucket Policyを選択すると、バケットに貼り付けるよう求めるプロンプトが表示されます



115012843006

11. バケットポリシーを含む以下のJSON文字列をテキストエディタにコピーアンドペーストするか、ウィンドウにペーストします。bucketnameを以下に指定する正確なバケット名に置き換えてください。これを行わないと、エラーメッセージが表示されます

{
「バージョン」:「2008-10-17」、
「ステートメント」:[
{
"Sid": "",
"効果": "許可",
「プリンシパル」:{
「AWS」:「arn:aws:iam::568526795995:user/logs」
},
"Action": "s3:PutObject",
"Resource": "arn:aws:s3:::bucketname/*"
},
{
"Sid": "",
"効果": "拒否",
「プリンシパル」:{
「AWS」:「arn:aws:iam::568526795995:user/logs」
},
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::bucketname/*"
},

{
"Sid": "",
"効果": "許可",
「プリンシパル」:

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

、
"アクション": "s3:GetBucketLocation",
"Resource": "arn:aws:s3:::bucketname"
},

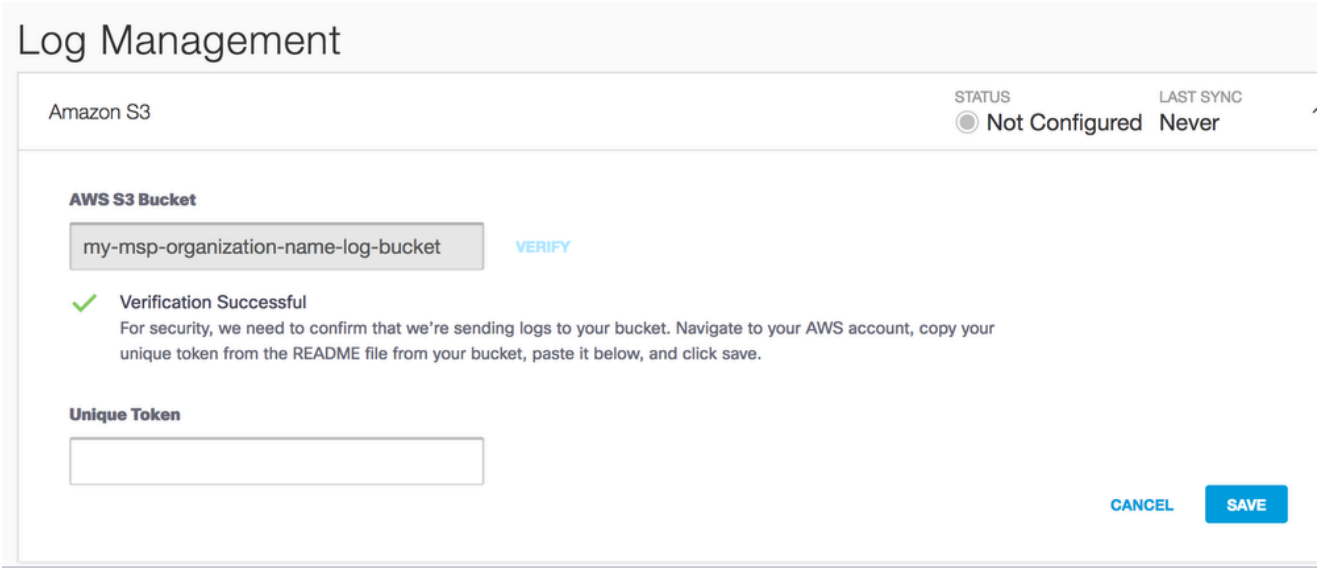
{
"Sid": "",
"効果": "許可",
「プリンシパル」: {
「AWS」: 「arn:aws:iam::568526795995:user/logs」
},
"アクション": "s3:ListBucket",
"Resource": "arn:aws:s3:::bucketname"
}
]
}

12. Saveをクリックしてこの変更を確認します

Amazon S3バケットの検証

ステップ 1：

1. Umbrellaコンソールに戻り、Settings > Log Managementの順に選択します。
2. 「Amazon S3」をクリックしてウィンドウを展開します
3. Bucket Nameフィールドで、S3で作成した正確なバケット名を入力するか貼り付けて、Verifyをクリックします
   バケットが正常に検証されたことを示す確認メッセージがダッシュボードに表示されます。



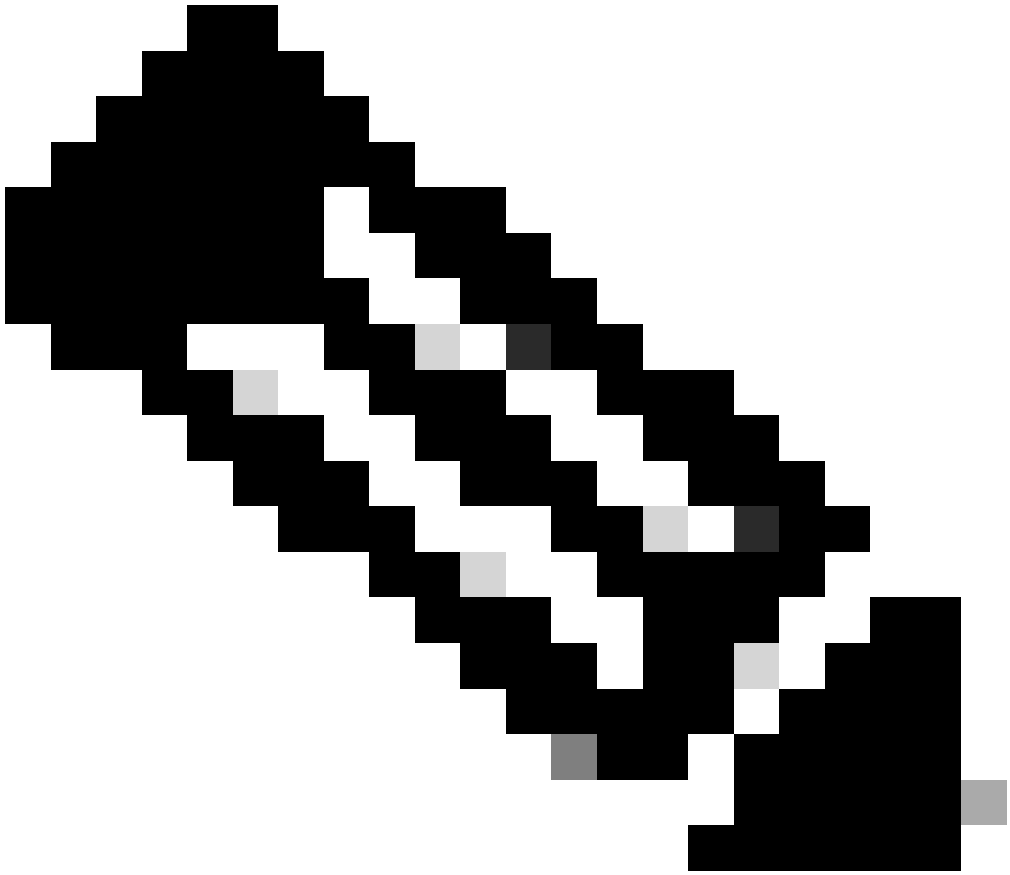
115012847146

バケットを検証できなかったことを示すエラーが表示された場合は、バケット名の構文を再確認し、設定を確認してください。問題が解決しない場合は、サポート部門でケースをオープンしてください

ステップ 2 :

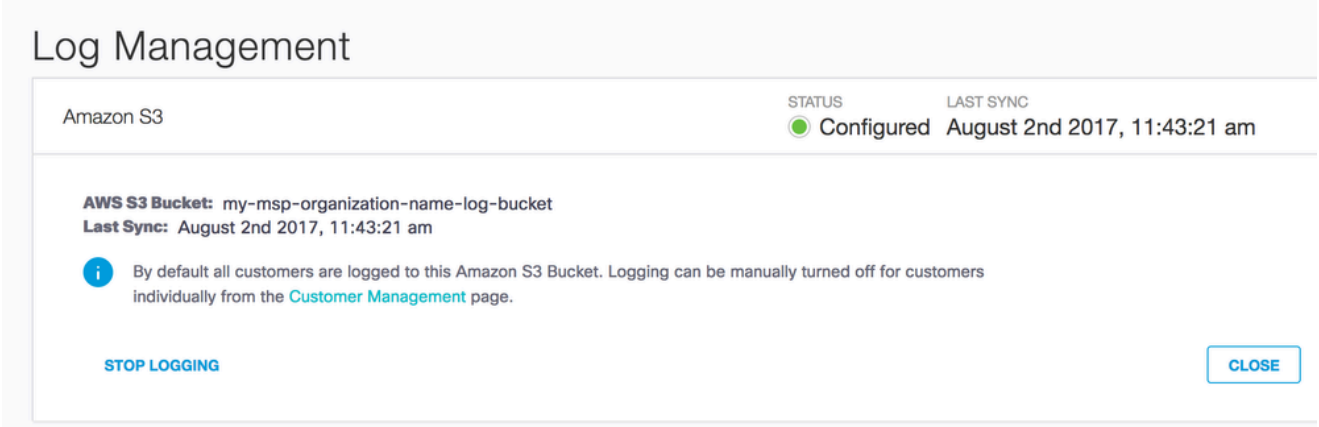
正しいバケットが指定されたことを確認するための二次的な注意事項として、Umbrellaは一意のアクティベーショントークンを入力するように要求します。アクティベーショントークンは、S3バケットを再訪問することで取得できます。検証プロセスの一環として、README_FROM_UMBRELLA.txtという名前のファイルがUmbrellaからAmazon S3バケットにアップロードされ、そこに表示されました。

1. readmeファイルをダブルクリックしてダウンロードし、テキストエディタで開きます。ファイル内には、S3バケットをUmbrellaダッシュボードに結び付ける一意のトークンがあります



注：アップロード後にREADMEファイルを表示するには、ブラウザでS3バケットを更新する必要がある場合があります。

2. Umbrellaダッシュボードに戻り、トークンを「Unique token」というフィールドに貼り付けて、Saveをクリックします。この時点で、設定は次のようになります
完了しました。設定を確認するには、ログ管理セクションでAmazon S3の名前をクリックします



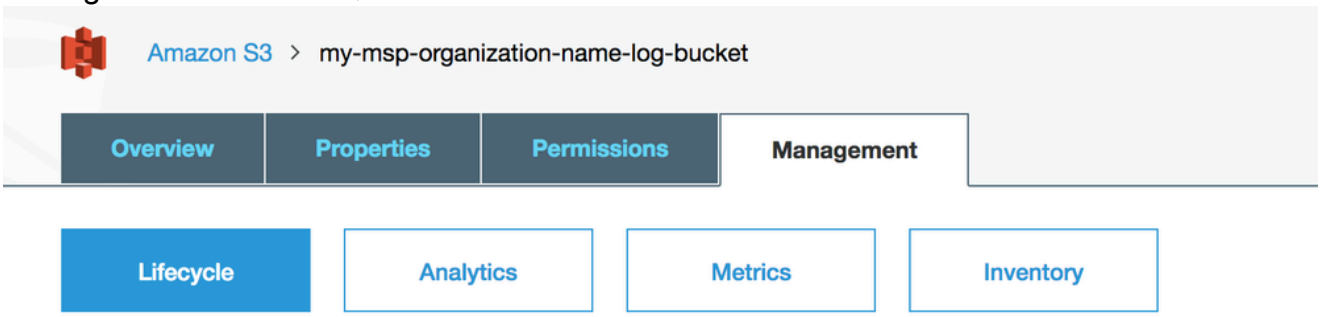
115012848126

ログ・ライフサイクルの管理

S3を使用している場合は、バケット内のデータのライフサイクルを管理して、ログを保持する期間を延長できます。外部ログ管理を使用している理由によっては、期間が非常に短いか、非常に長い可能性があります。たとえば、24時間後にS3バケットからログをダウンロードしてオフラインで保存したり、ログをクラウドに無期限に保持したりできます。 デフォルトでは、Amazonはデータを無期限にバケットに保存しますが、無制限のストレージはバケットの維持コストを上昇させます。S3ライフサイクルの詳細については、ここを参照してください。

バケットのライフサイクルを構成する手順は、次のとおりです。

1. Managementを選択して、 ライフ サイクル



115012848246

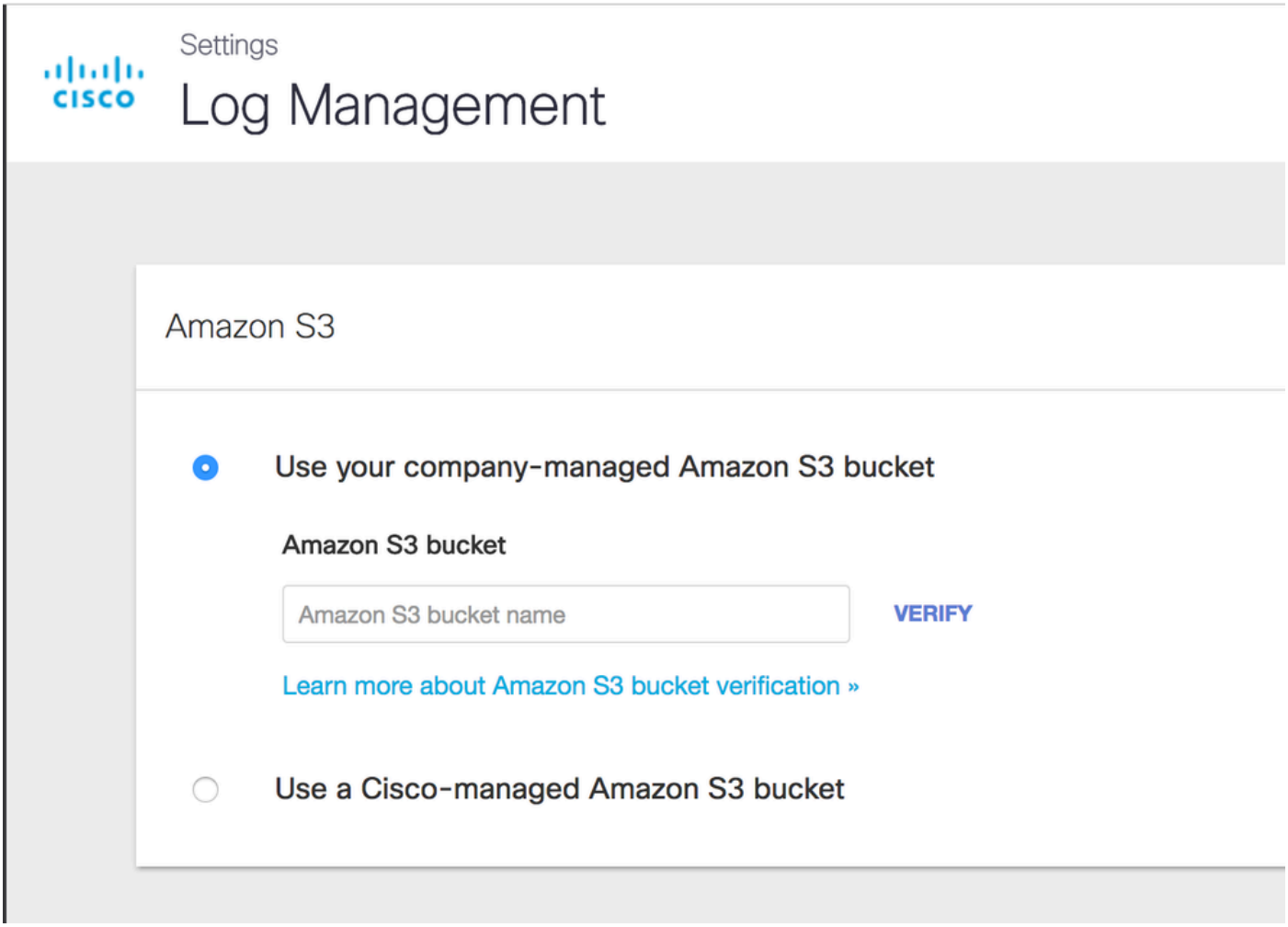
2. Add a Ruleをクリックしてから、Apply the Rule to the Whole bucket（または、サブフォルダを設定済みの場合は、そのサブフォルダ）をクリックします。
3. オブジェクトに対するアクション（削除やアーカイブなど）を選択し、期間と、Glacierストレージを使用してAmazonコストを削減するかどうかを選択します。（Glacierは、iscolditがオフラインのストレージであり、アクセスに時間がかかりますが、安価です）。
4. 別の方法（内部バックアップソリューションなど）でログを管理する場合は、S3からログをダウンロードして別の方法で保存し、保存期間を数日に設定します。

CiscoマネージドS3バケットの設定

Umbrellaダッシュボードで、Settings > Log Managementの順に移動します。

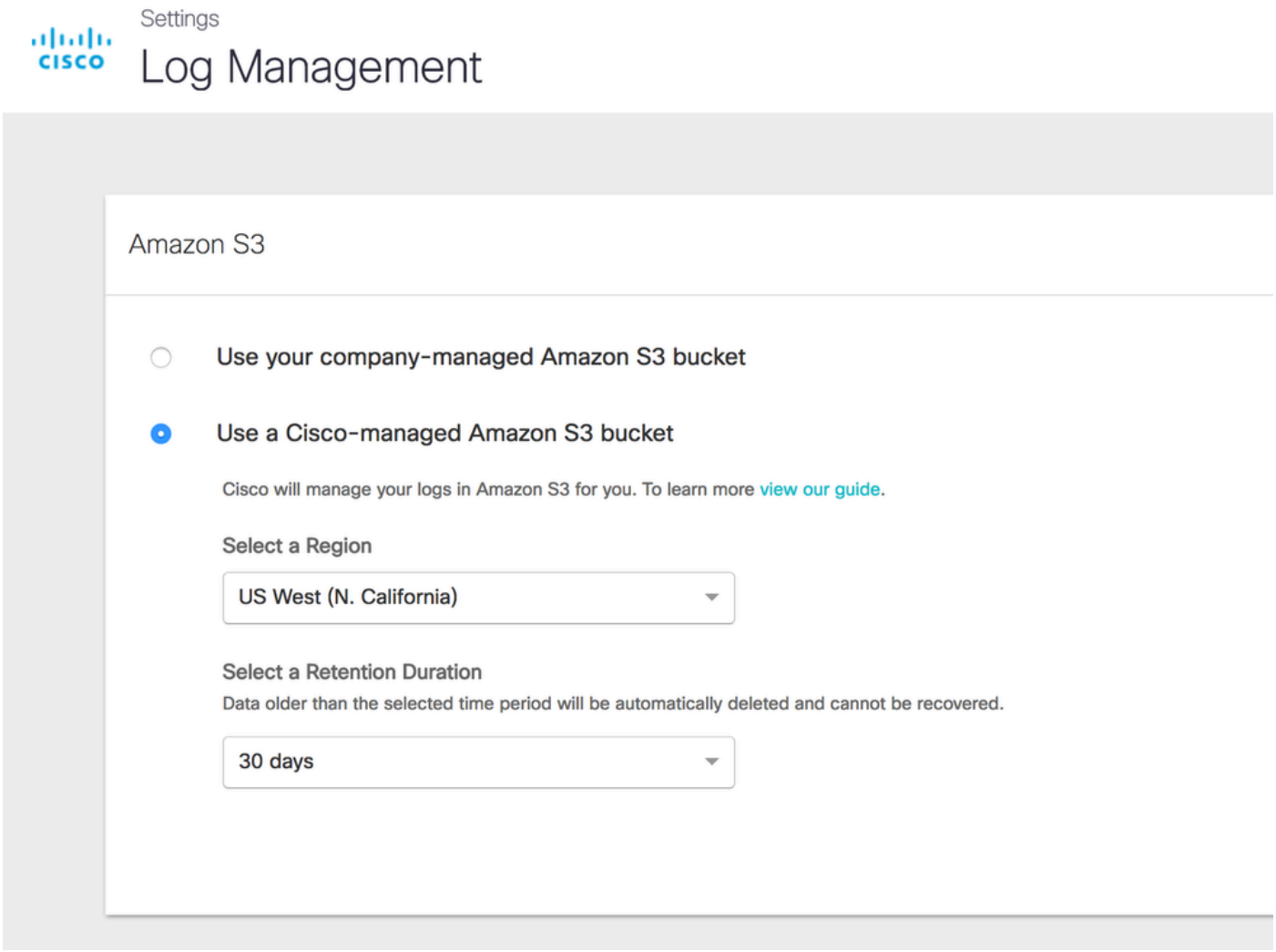
次の2つのオプションがあります。

- 会社管理のAmazon S3バケットを使用する
- シスコが管理するAmazon S3バケットを使用する



25231151138964

「シスコが管理するAmazon S3バケットを使用する」を選択すると、「リージョンの選択」と「保持期間の選択」の2つの新しいオプションが表示されます。



252311511580 36

地域の選択

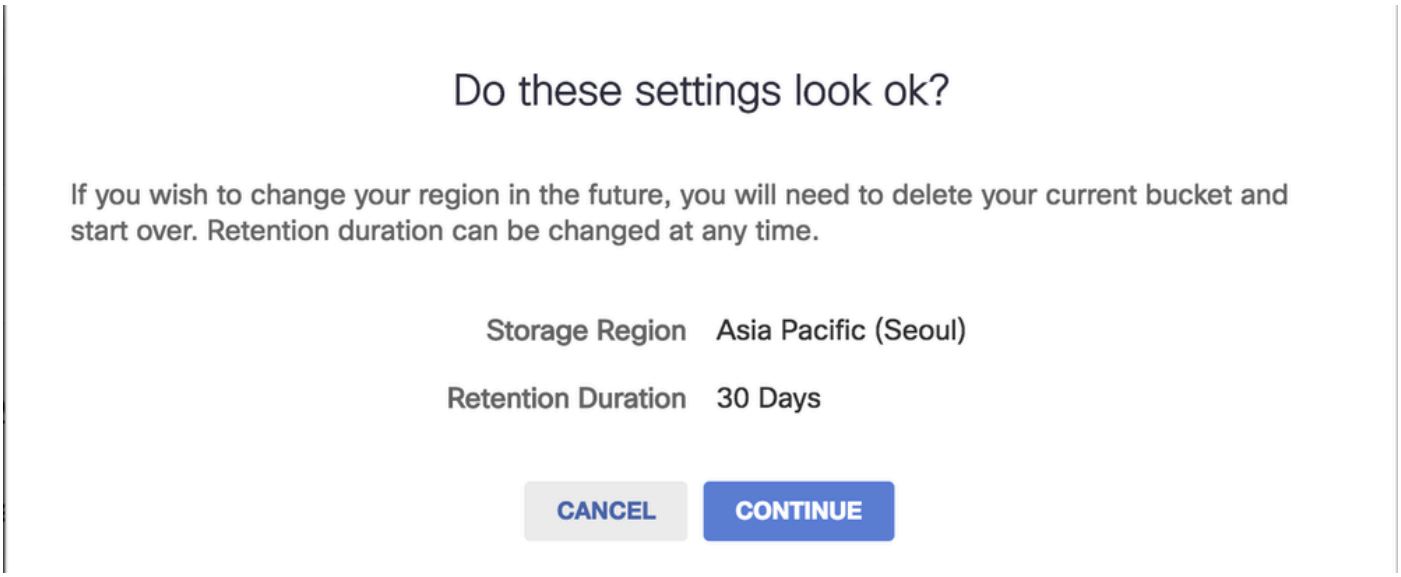
サーバにログをダウンロードする際の遅延を最小限に抑えるには、地域のエンドポイントが重要です。リストされたリージョンはAmazon S3で利用可能なリージョンと一致しますが、すべてのリージョンが利用可能なわけではありません。たとえば、中国はリストされていません。

ドロップダウンから、最も近い地域を選択します。将来リージョンを変更する場合は、現在の設定を削除してやり直す必要があります。

保存期間の選択

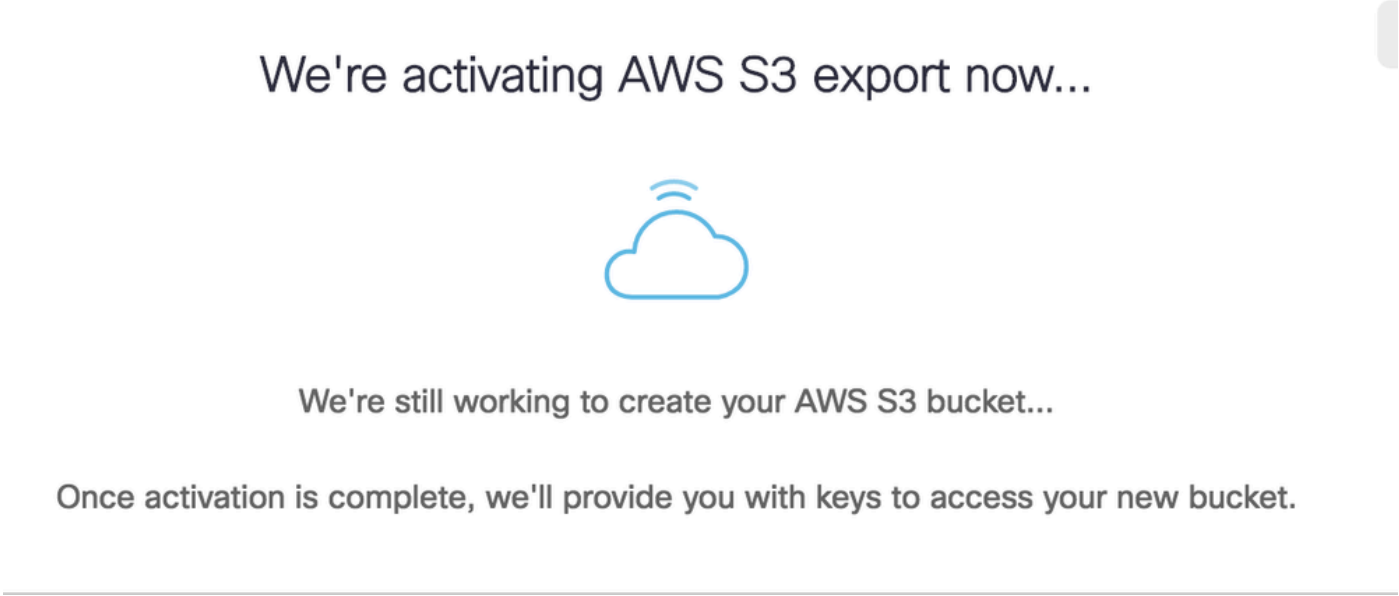
保持期間は単純に7、14、または30日です。選択した期間が経過すると、すべてのデータがパージされ、何があっても取得できなくなります。定期的に摂取する場合は、より短い期間を推奨します。保存期間は後で変更できます。

選択したら、Nextをクリックします。地域と期間の確認が求められます



25231181211796

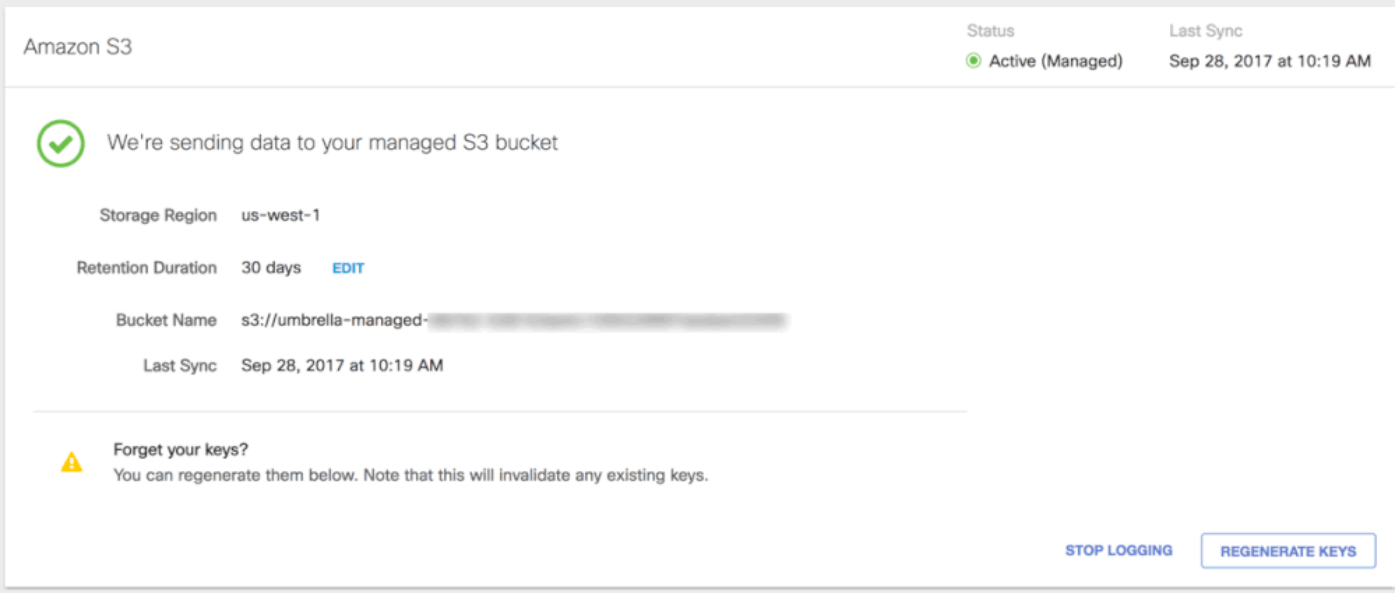
続行に同意すると、アクティベーション通知が届きます。



25231181218708

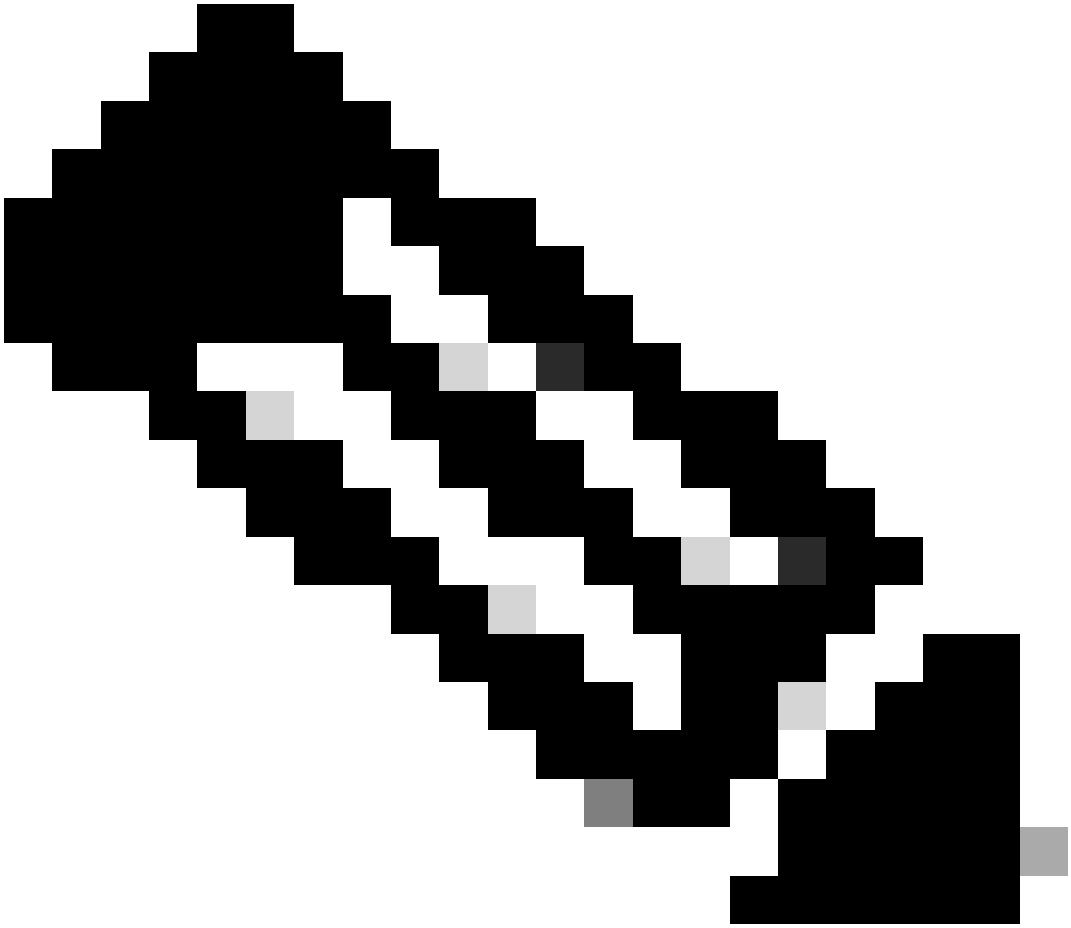
次に、アクセスキーと秘密キーを受信します。キーのいずれかが表示されるのは唯一の時間なので、（クリックして）受け入れる必要があります（「了解！」）をクリック。 バケットにアクセスしてログをダウンロードするには、アクセスキーとシークレットキーが必要です。

最後に、設定と最も重要なバケット名を示すサマリー画面が表示されます。



25231181228180

必要に応じて、ログインのオン/オフを切り替えることができます。



注：シスコは、ロギングがオフになっていても、選択した保存期間に基づいてログを消去し続けます。

構成後のオプション

ログのアップロードエラー

Cisco UmbrellaからS3バケットにログをアップロードできなかった場合は、20分ごとにサービスが再試行される4時間の猶予期間があります。4時間後、サポートチームがケースをオープンします。サポートチームは問題の原因に関する調査を開始し、問題について知らせるために積極的に連絡します。

アップロードされたログと形式の確認

ログは、UmbrellaログキューからS3バケットに10分間隔でアップロードされます。設定が完了すると、最初のログは2時間以内にS3バケットにアップロードされますが、通常は即座に処理されるか、すぐに処理に近づきます。ただし、何かをアップロードするには、新しく生成されたログデータが存在している必要があります。そのため、テスト環境でこれを試みている場合は、ネットワークデータがアクティビティ検索に記録されていることを確認してください。

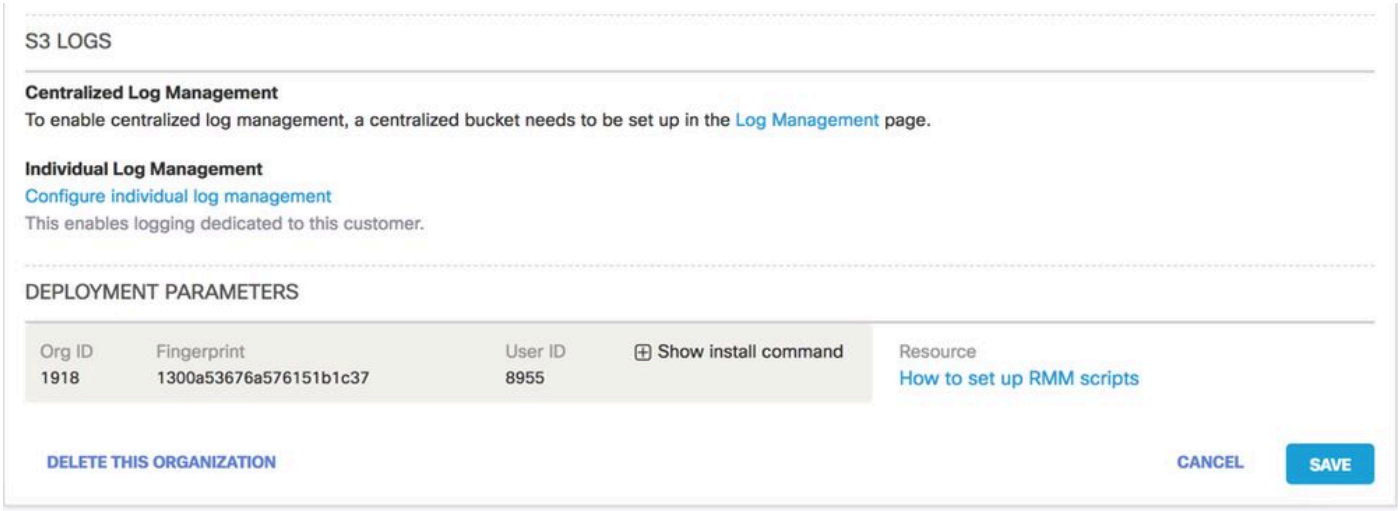
すべてが動作しているかどうかを確認するために、Umbrellaダッシュボードの最終同期時刻が更新され、S3バケットにログが表示され始めます。

バケット内では、各顧客または各組織に組織IDのラベルが付いているため、フォルダ構造は次のようになります。

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

<bucket-name>はバケットの名前、<orgID>は組織のID、<subfolder>は内部のログのタイプに応じてdnslogs、proxylogs、またはiplogのいずれかです。

MSPおよびMSSPのお客様の場合、orgIDは、導入パラメータセクションの各顧客の詳細の下にある顧客設定のorgIDと一致します。複数組織のお客様は、個々のサブ組織にログインし、ブラウザのurl(https://dashboard.umbrella.com/o/#####/)に組織IDを記録することで、組織IDを収集できます。



360002271623

現在、MSP、MSSP、および複数組織のお客様のログ形式のバージョンはバージョン1.1です。 ログはGZIP形式で表示され、次の命名形式で適切なサブフォルダのS3バケットにアップロードされます。

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

<subfolder>は、内部のログのタイプに応じて、dnslogs、proxylogs、またはiplogのいずれかです。<xxxx>は4つの英数字で構成されるランダムな文字列で、重複するファイル名が上書きされるのを防ぎます。

例：

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

10分以内にバケットのログが表示されない場合は、サポートに連絡して、これまでに行った手順の概要を説明してください。

ログが表示されたら、受信した最初のいくつかのログアップロードの内容を解凍してデータを確認し、データをテキストエディタ（またはMicrosoft Excel、通常は.CSVのデフォルト）で表示できるようにすることをお勧めします。 ログの各フィールドが表す情報については、こちらを参照してください。

Cisco UmbrellaからS3バケットへのログアップロードが失敗した場合、サービスは20分ごとに4時間の猶予期間で再試行されます。4時間後、サポートチーム内でサービスリクエストがオープンします。サポートチームは問題の原因に関する調査を開始し、問題について知らせるために積極的に連絡します。

顧客ごとの口ギングの有効化

特別な指定がない限り、この機能はデフォルトですべてのユーザに対して有効になっています。この機能は、個々のお客様に対してオフにできます。これは、この機能を使用するお客様のサービスレベルが異なる場合に役立ちます。これは、各カスタマーの下にあります。コンソールの設定です。前のセクションのスクリーンショットは、オフにする切り替えを示しています。

AmazonでIAMユーザーを作成し、バケットの個々のorgit isサブフォルダにこれらのIAMユーザーを割り当てることもできます。これにより、エンドユーザの口グへのアクセスは許可できますが、口グへのアクセスはのみ許可できます。

口グのダウンロード、フォーマットとSplunk/QRadar統合について

保存または使用する口グをダウンロードするには、S3からDNS口グをダウンロードする方法がいくつかあります。Weitは、この問題に対するいくつかのアプローチの概要を示す記事を作成しました。

また、口グ形式と、Umbrellaダッシュボードに表示される口グとの違いについて、いくつか質問があるかもしれません。エクスポートされた口グ形式の詳細については、この記事を参照してください。

最後に、DNS口グをエクスポートするための主な用途の1つは、SIEMツールとの統合です。このような口グを扱う際のSIEMの設定は、管理者の好みによることが多いですが、最も一般的なSIEMに関するいくつかのガイダンスがあります。

Amazon AWS S3およびUmbrella用のSplunkプラグインのセットアップの詳細については、こちらを参照してください。

IBM QRadarを設定してAmazon S3から口グを取得し、それらをダイジェストする方法については、こちらを参照してください。

S3口グのサイズはどのくらいですか。

S3口グのサイズは、DNSトラフィックのボリュームに応じて発生するイベントの数によって異なります。

S3口ギングの口グ形式については、こちらを参照してください。

エントリの例は220バイトですが、各口グ行のサイズは項目の数（ドメイン名の長さ、カテゴリの数など）によって異なります。 各口グ行が220バイトであると仮定すると、100万件の要求は220 MBになります。

1日に表示されるDNSクエリの数の見積もりを取得するには、次の手順を実行します。

1. Umbrellaダッシュボードで、レポート>アクティビティ検索に移動します。

2. Filtersで、過去24時間のレポートを実行し、Export CSVアイコンをクリックします。
3. ダウンロードした.csvファイルを開きます。行数（ヘッダーのマイナス1）は、1日あたりのDNSクエリ数です。これを220バイトで乗算すると、1日の見積もりが得られます。

コストの面では、変動はありますが、最も多くのお客様でも月に数ドルしかサービスに費やしていないことがわかります。 コストの1つはストレージ時間に関連づけられ、もう1つはS3から環境へのデータのダウンロードに関連づけられます。詳細については、Amazonをご覧ください。

当社の機能と同様に、weitは皆さんの考えを知りたいと思っています。特に、SIEMの統合や、このドキュメントで取り上げている追加の質問に関する意見を知りたいと思っています。ご意見やご感想がありましたら、お知らせください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。