Zentrales Umbrella Log Management mit dem Amazon S3 Service für MSP-, MSSP- und Multi-Org-Kunden

Inhalt

Einleitung

In diesem Dokument wird das zentrale Umbrella Log Management mit dem Amazon S3 Service für MSP-, MSSP- und Multi-Org-Kunden beschrieben.

Überblick

Die MSP-, MSSP- und Multi-Org-Konsolen haben die Möglichkeit, die DNS-, URL- und IP-Protokolle Ihrer Kunden offline in Cloud-Storage zu speichern. Der Speicher befindet sich in Amazon S3. Nachdem die Protokolle hochgeladen wurden, können sie heruntergeladen und aus Compliance-Gründen oder für Sicherheitsanalysen aufbewahrt werden.

Diese Dokumentation hilft Ihnen, diese Funktion zu verstehen, sie sowohl in Ihrem Umbrella Dashboard als auch in Ihrer Amazon S3 Konsole einzurichten und verschiedene Konfigurationsoptionen auszuführen, einschließlich der Zeitdauer, während der die Protokolle in S3 gespeichert werden sollen.

Umbrella for MSP, MSSP und Multi-Org haben alle die Möglichkeit, die Traffic Activity Logs von den untergeordneten Organisationen der Konsole hochzuladen und diese Logs in der Cloud zu speichern. Amazon AWS S3 (Simple Storage Service) ist der Dienst, der Protokolle archiviert und manchmal auch als Offline-Speicher bezeichnet wird.

Archivierungsprotokolle können aus verschiedenen Gründen nützlich sein, je nach Ihren Anforderungen. Bei einigen Personen können die exportierten und archivierten Protokolle in Datenanalysetools oder forensische Sicherheitstools wie SIEMs importiert werden. Für andere kann ein Archiv von Aktivitätsprotokollen für die Datenforensik bei einem Sicherheitsvorfall oder für Personalakten nützlich sein.

AWS S3 speichert Protokolle in einem komprimierten (gzip) Archiv im CSV-Format. Da alle zehn Minuten Protokolle hochgeladen werden, muss der Netzwerkverkehr, der von Umbrella protokolliert und dann vom S3 heruntergeladen wird, mindestens zehn Minuten warten.

Die OrgID-Nummer der Konsole

Jede Kundenorganisation lädt ihre Protokolle einzeln hoch, wobei sie die orgID-Nummer aus der Konsole verwendet, um jeden Kunden einem Ordner zuzuordnen. Die Funktion kann auch für jeden Kunden/jede Organisation aktiviert oder deaktiviert werden.

Zwei Arten von Umbrella Log Management

Die Protokollverwaltung erfolgt durch Hochladen von Protokollen in die so genannte "bucketit" (im Wesentlichen ein Ordner in der AWSit-S3-Umgebung). Es gibt zwei Möglichkeiten, einen Bucket für Ihre Umbrella-Protokolle zu hosten:

- Verwaltet, verwaltet und bezahlt von Ihnen, dem Unternehmensadministrator.
- Verwaltet, verwaltet und bezahlt von Cisco Umbrella

Die Verwaltung Ihres S3-Laufwerks durch Cisco birgt Vor- und Nachteile.

Vorteile von Cisco Lösungen:

- Extrem einfache Einrichtung. Der Vorgang dauert nur wenige Minuten und ist anschließend äußerst einfach zu verwalten.
- Cisco Bucket-Management ist in Ihren Lizenzkosten für Umbrella inbegriffen, wodurch der Service praktisch kostenlos ist. Es ist zwar kostengünstig, einen eigenen Eimer zu haben, aber die Gemeinkosten für die Verwaltung einer anderen Rechnung können unerschwinglich sein.

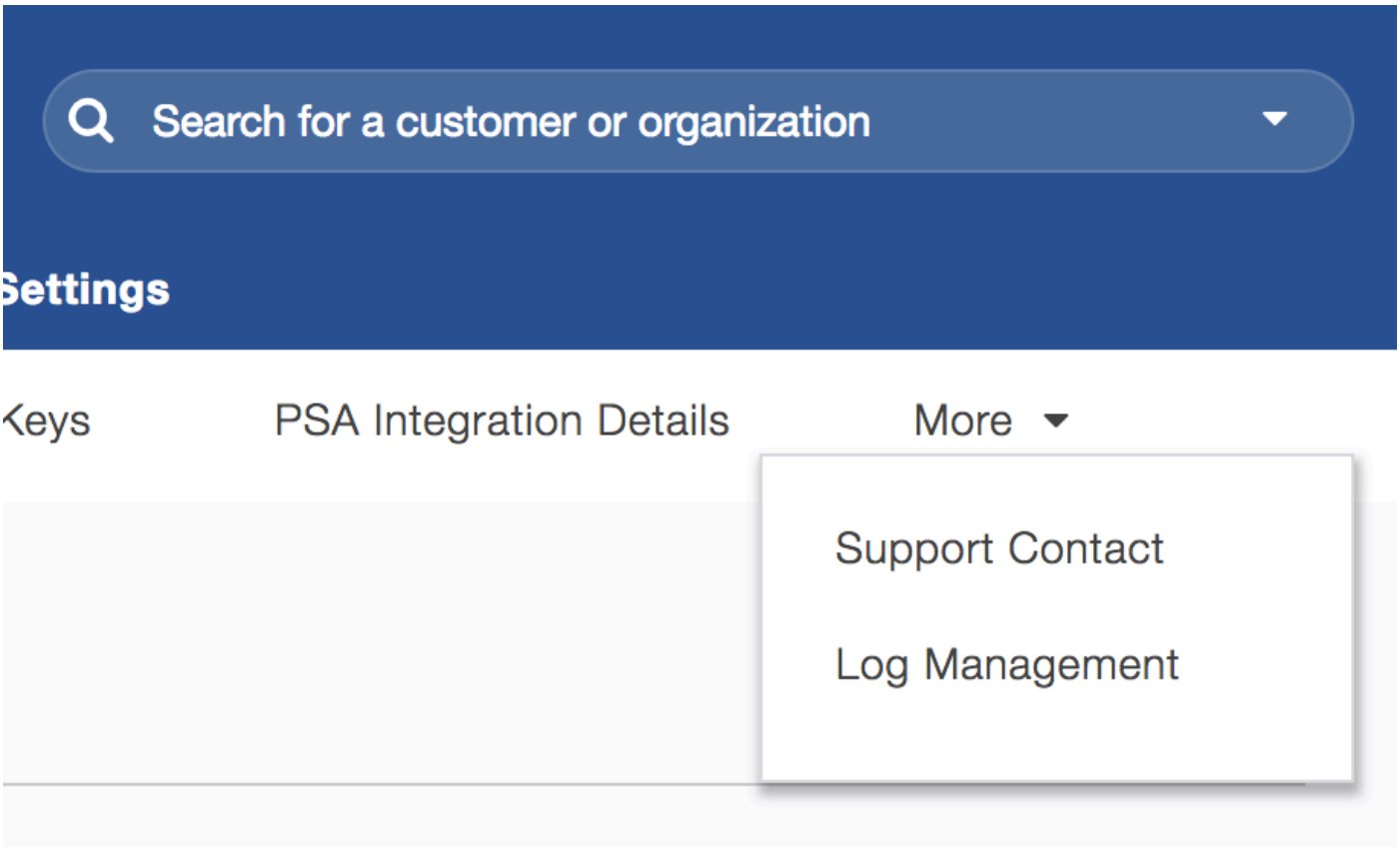
Die Vorteile einer eigenen S3-Instanz:

- Es gibt keine Einschränkung, wie lange Daten offline gespeichert werden können. Cisco begrenzt den Offline-Speicher auf maximal 30 Tage.
- Sie können Ihrem Bucket alles hinzufügen, einschließlich Protokolldateien von Umbrella, sodass der Bucket auch von anderen Anwendungen verwendet werden kann.
- Sie können Support direkt von Amazon für erweiterte Unterstützung bei der Konfiguration erhalten, wie z. B. Automatisierung oder Hilfe bei der Befehlszeile.

Für die meisten Kunden sind die Wartungskosten sehr günstig, können sich aber als lästig erweisen.

Erste Schritte

Die Protokollverwaltungsfunktion finden Sie in der Konsole unter Einstellungen > Protokollverwaltung (Sie können auf den Dropdown-Pfeil klicken).



115012963103

Konfigurieren eines selbst verwalteten S3-Buckets

Voraussetzungen

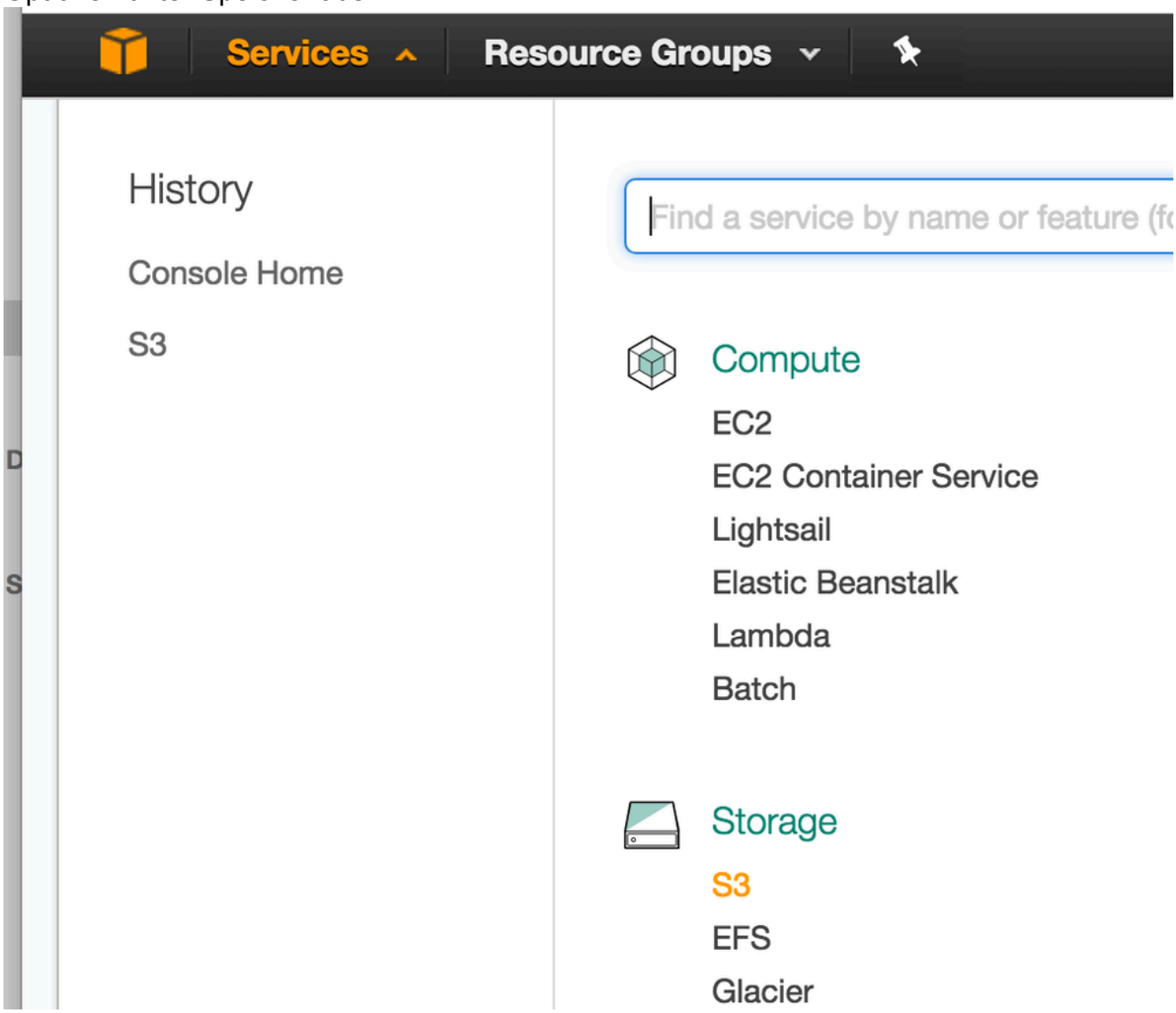
Um Protokolle zu archivieren, müssen Sie folgende Anforderungen erfüllen:

- Vollständiger Administratorzugriff auf Cisco Umbrella MSP, MSSP oder Multi-Org Console
- Eine Anmeldung bei Amazon AWS (https://aws.amazon.com/console/). Wenn Sie ein Konto bei Amazon hinterlassen, können Sie sich kostenlos für S3 anmelden. Falls Ihre Nutzung die Nutzung des kostenlosen Tarifs übersteigt, benötigen Sie jedoch eine Kreditkarte.
- Ein in Amazon S3 konfigurierter Bucket für die Protokollspeicherung. Im nächsten Abschnitt finden Sie Anleitungen zur Konfiguration und Einrichtung der Amazon S3 Bucket.

Einrichten Ihres Amazon S3-Buckets

1. Melden Sie sich zunächst bei der AWS-Konsole an, und wählen Sie "S3" aus der Liste der

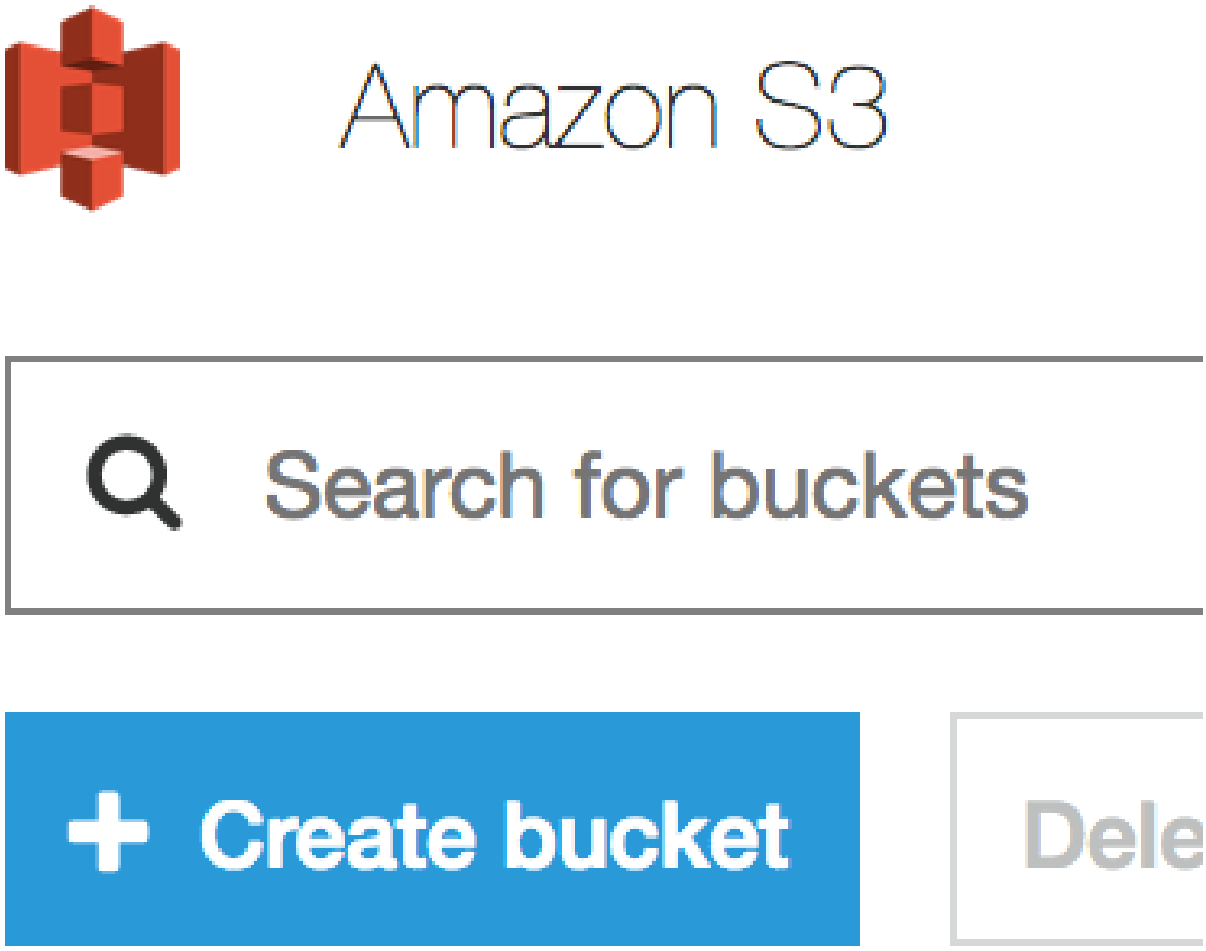
Optionen unter Speicher aus.



115012842106

2. Sie sehen einen Einführungsbildschirm, der Sie zum Amazon Simple Storage System einlädt.

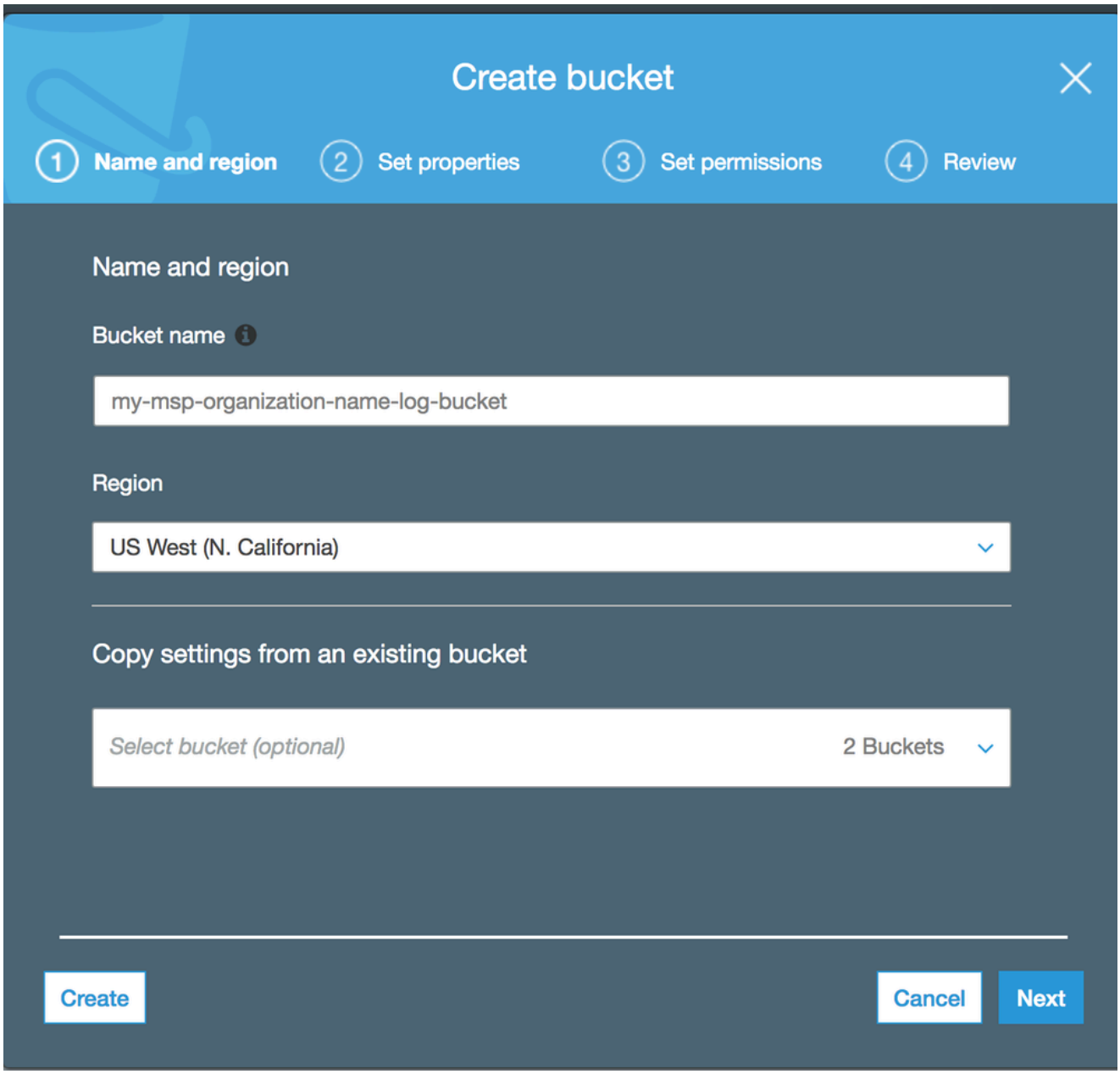
3. Wenn Sie als Nächstes noch keinen Bucket haben, möchten Sie einen erstellen. Klicken Sie auf Bucket erstellen



115012842326

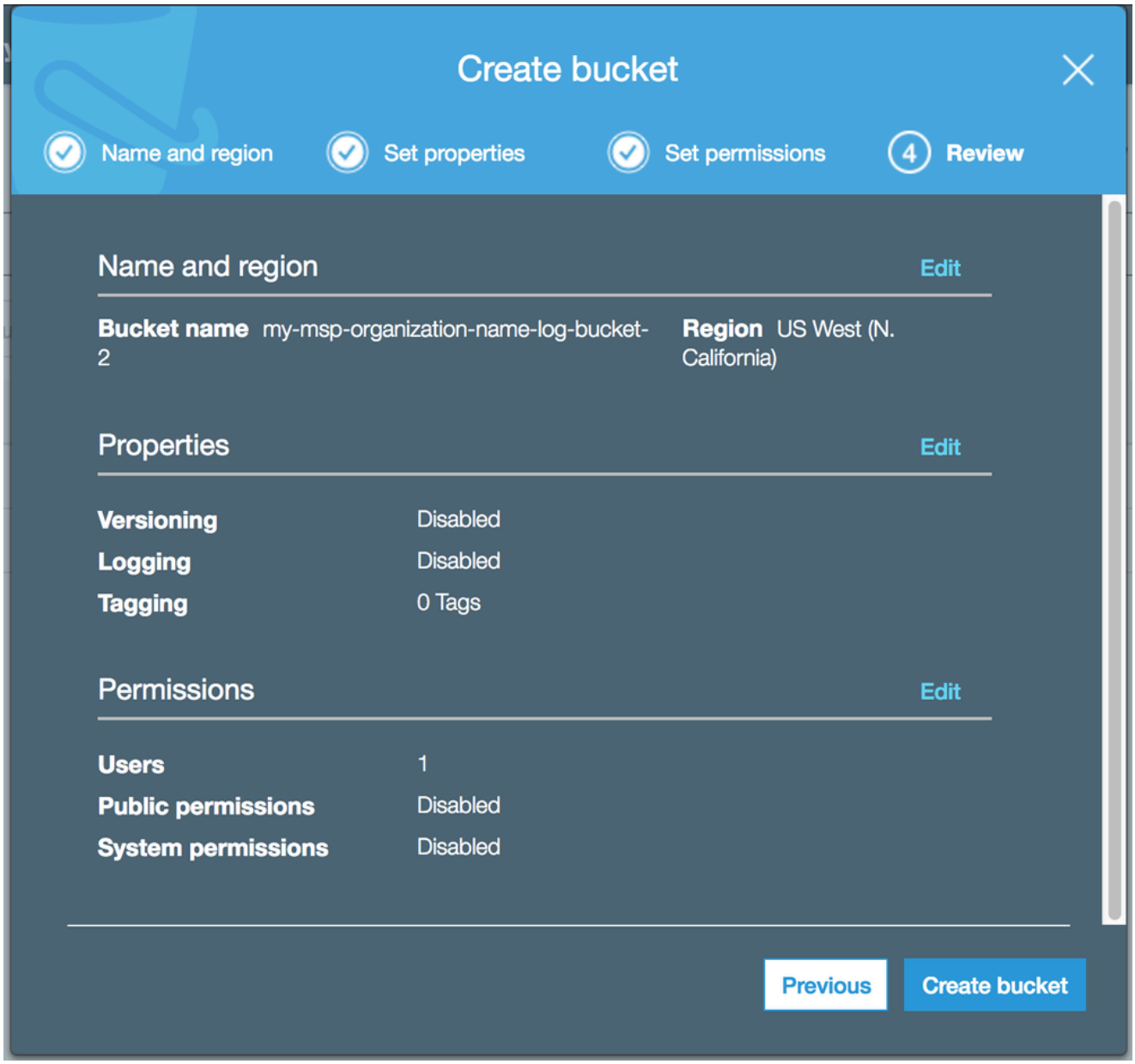
.

4. Beginnen Sie mit der Eingabe eines Bucketnamens
   Der Bucketname muss universell eindeutig sein - nicht nur für Ihren AWS oder Ihren Umbrella, sondern für alle Amazon AWS. Wenn Sie etwas Persönliches wie "my-organisation-name-log-bucket" verwenden, können Sie die Anforderung nach einem universell eindeutigen bucket-Namen umgehen. Der Bucketname darf nur Kleinbuchstaben enthalten und darf keine Leerzeichen oder Punkte enthalten. Er muss den DNS-Namenskonventionen entsprechen. Weitere Informationen zu Namensbeschränkungen finden Sie hier. Weitere Informationen zur Bucketerstellung, einschließlich der Namensvergabe, finden Sie hier.



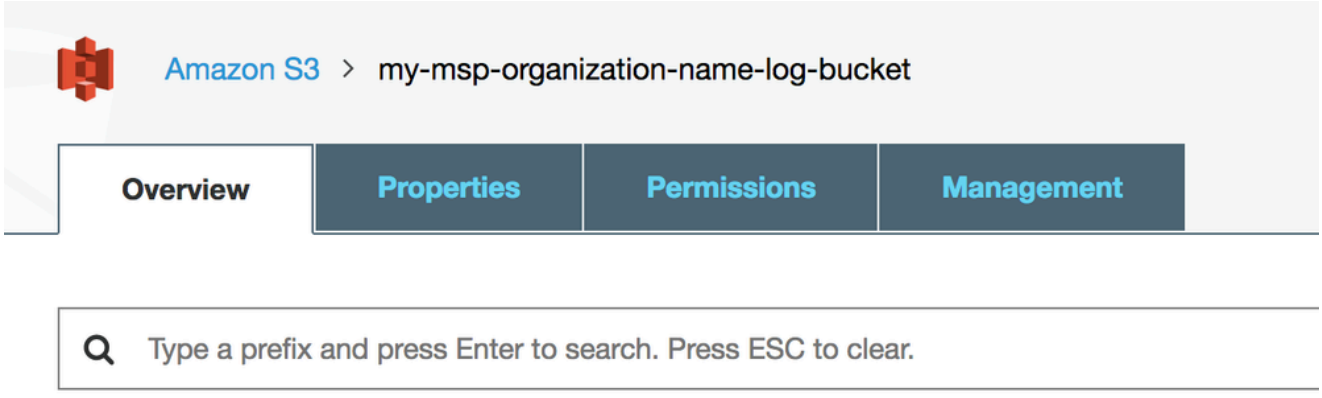
115013010503

5. Wählen Sie die Region aus, die für Ihren Standort am besten geeignet ist, und klicken Sie auf Erstellen. Einstellungen nicht aus einem anderen Bucket kopieren
6. Klicken Sie im Schritt "Eigenschaften festlegen" einfach auf "Weiter". Diese können später angepasst werden.
7. Klicken Sie im Schritt "Berechtigungen festlegen" einfach auf Weiter. Wir werden die Berechtigungen später erneut überprüfen, um den Bucket für das Hochladen einzurichten.
8. Schließen Sie den Prüfprozess ab, und klicken Sie auf Bucket erstellen



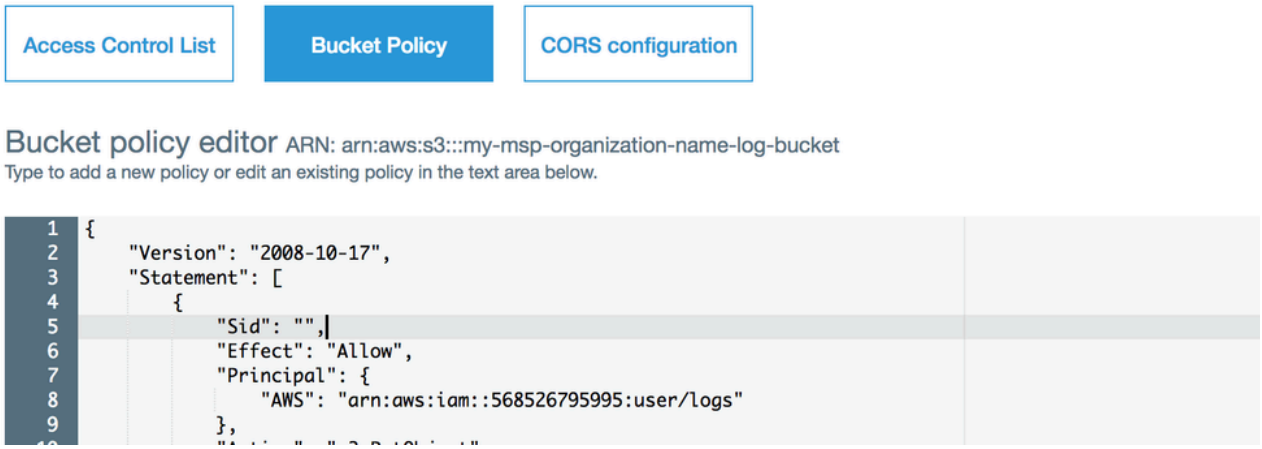
115012842686

9. Als Nächstes müssen Sie den Bucket so konfigurieren, dass er Uploads vom Umbrella Service akzeptiert. In S3 wird dies als Bucket-Richtlinie bezeichnet. Klicken Sie auf den Namen der neu konfigurierten Gruppe, und wählen Sie dann oben auf der Schnittstelle die Registerkarte Permissions aus.



115012842906

10. Wählen Sie Bucket Policy aus, und Sie werden aufgefordert, die Bucket-Policy einzufügen.



115012843006

11. Kopieren Sie den unten stehenden JSON-String, der die Bucket Policy enthält, in einen Texteditor, oder fügen Sie ihn einfach in das Fenster ein. Ersetzen Sie Ihren genauen Bucketnamen, wobei bucketname unten angegeben ist. Andernfalls wird eine Fehlermeldung angezeigt.

{
Version: "2008-10-17",
"Anweisung": [
{
"SID": "",
"Effekt": "Zulassen",
"Auftraggeber": {
AWS: "arn:aws:iam::568526795995:user/logs"
},
"Aktion": "s3:PutObject",
Ressource: "arn:aws:s3:::bucketname/*"
},
{
"SID": "",
"Effekt": "Verweigern",
"Auftraggeber": {
AWS: "arn:aws:iam::568526795995:user/logs"
},
"Aktion": "s3:GetObject",
Ressource: "arn:aws:s3:::bucketname/*"
},

{
"SID": "",
"Effekt": "Zulassen",
"Auftraggeber":

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

,
"Aktion": "s3:GetBucketLocation",
Ressource: "arn:aws:s3:::bucketname"
},

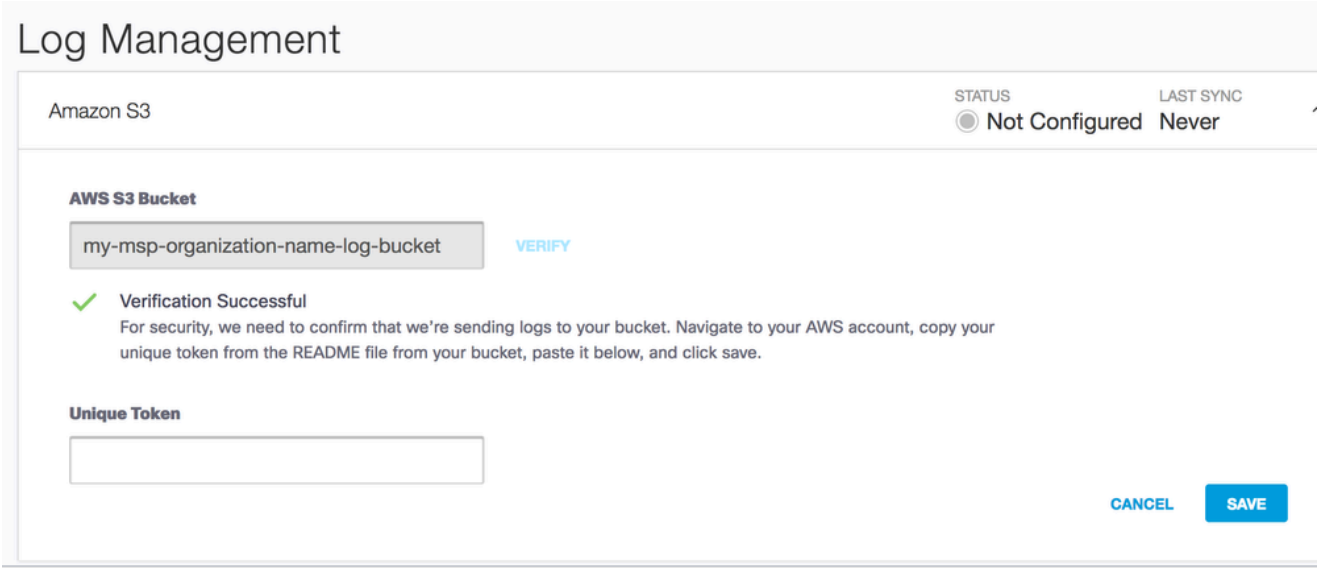
{
"SID": "",
"Effekt": "Zulassen",
"Auftraggeber": {
AWS: "arn:aws:iam::568526795995:user/logs"
},
"Aktion": "s3:ListBucket",
Ressource: "arn:aws:s3:::bucketname"
}
]
}

12. Klicken Sie auf Speichern, um diese Änderung zu bestätigen.

Überprüfen Ihrer Amazon S3 Bucket

Schritt 1:

1. Wechseln Sie zurück zu Ihrer Umbrella Console und navigieren Sie zu Einstellungen > Protokollverwaltung.
2. Klicken Sie auf "Amazon S3", um das Fenster zu erweitern
3. Geben Sie im Feld Bucket-Name den genauen Bucket-Namen ein, den Sie in S3 erstellt haben, oder fügen Sie ihn ein, und klicken Sie auf Verifizieren
   Sie erhalten eine Bestätigungsmeldung in Ihrem Dashboard, dass der Bucket erfolgreich verifiziert wurde.



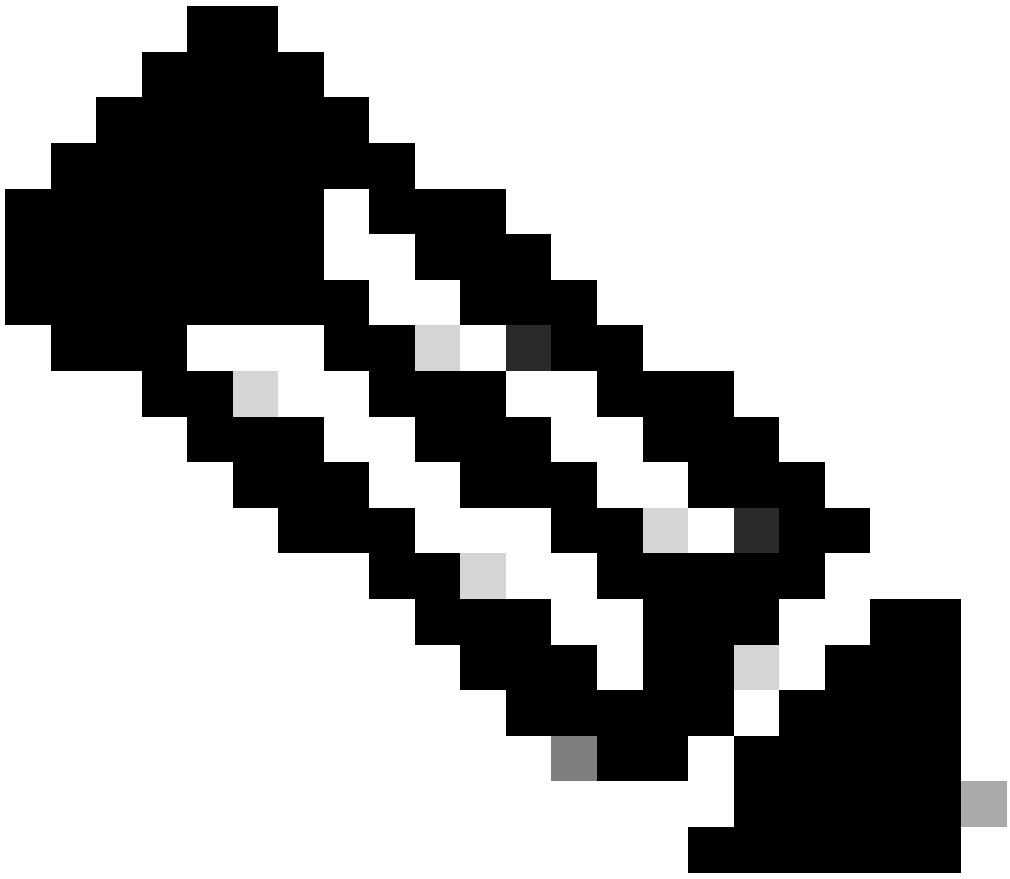
115012847146

Wenn Sie eine Fehlermeldung erhalten, die besagt, dass Ihr Bucket nicht überprüft werden konnte, überprüfen Sie die Syntax des Bucketnamens und überprüfen Sie die Konfiguration. Wenn das Problem weiterhin besteht, wenden Sie sich an unseren Support.

Phase 2:

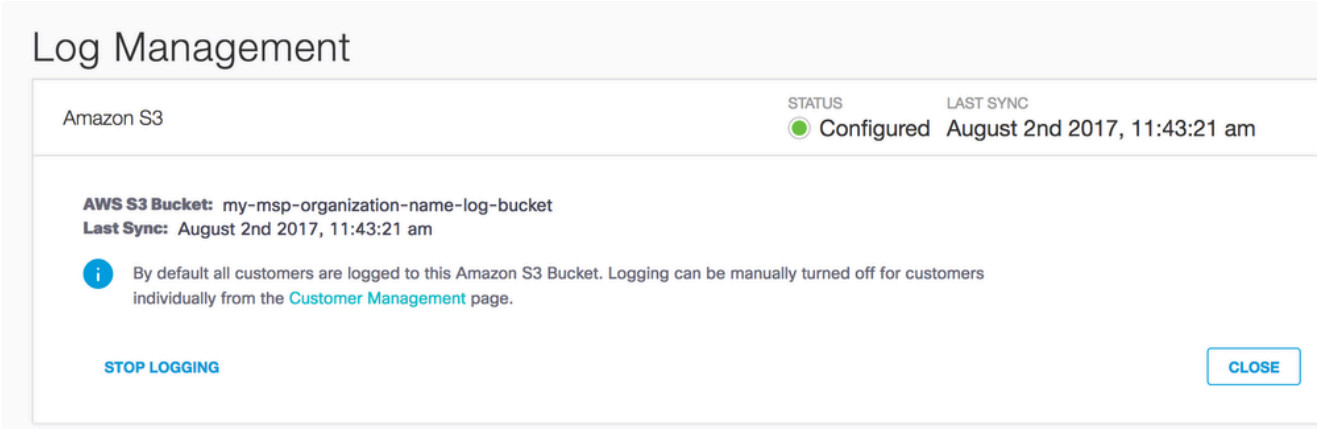
Als sekundäre Vorsichtsmaßnahme, um sicherzustellen, dass der richtige Bucket angegeben wurde, fordert Umbrella Sie auf, ein eindeutiges Aktivierungstoken einzugeben. Das Aktivierungstoken kann durch einen erneuten Besuch Ihres S3-Buckets abgerufen werden. Im Rahmen des Verifizierungsprozesses wurde eine Datei mit dem Namen README_FROM_UMBRELLA.txt von Umbrella auf Ihren Amazon S3-Bucket hochgeladen und erscheint dort.

1. Laden Sie die Readme-Datei herunter, indem Sie darauf doppelklicken und sie dann in einem Texteditor öffnen. In der Datei ist ein eindeutiges Token enthalten, das Ihren S3-Bucket an Ihr Umbrella Dashboard bindet



Anmerkung: Möglicherweise müssen Sie Ihren S3-Bucket im Browser aktualisieren, damit die README-Datei nach dem Hochladen angezeigt wird.

2. Kehren Sie zum Umbrella Dashboard zurück, und fügen Sie den Token in das Feld "Eindeutiger Token" ein. Klicken Sie anschließend auf Speichern. Zu diesem Zeitpunkt lautet die Konfiguration
abgeschlossen. Um Ihre Konfiguration zu überprüfen, klicken Sie einfach auf den Namen Amazon S3 im Bereich Log Management



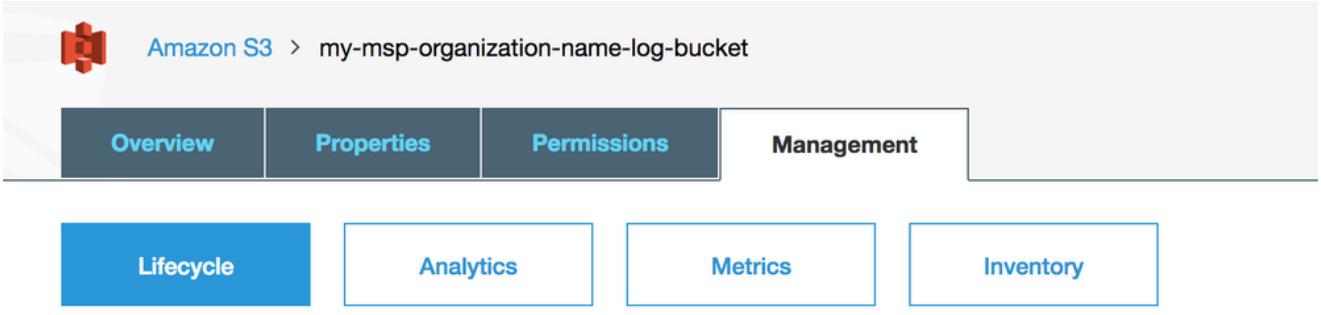
115012848126

Verwalten des Protokoll-Lebenszyklus

Wenn Sie S3 verwenden, können Sie den Lebenszyklus der Daten innerhalb des Buckets so verwalten, dass der Zeitraum, für den Sie die Protokolle aufbewahren möchten, verlängert wird. Je nachdem, aus welchem Grund Sie die externe Protokollverwaltung verwenden, kann die Dauer sehr kurz oder sehr lang sein. So können Sie beispielsweise die Protokolle nach 24 Stunden einfach aus dem S3-Bucket herunterladen und offline speichern oder die Protokolle unbegrenzt in der Cloud speichern. Standardmäßig speichert Amazon die Daten unbegrenzt in einem Bucket, aber unbegrenzter Speicher erhöht die Kosten für die Wartung des Buckets. Weitere Informationen zum S3-Lebenszyklus finden Sie hier.

So konfigurieren Sie den Lebenszyklus Ihres Buckets:

1. Wählen Sie Verwaltung aus, und klicken Sie auf Lebenszyklus



115012848246

2. Klicken Sie auf Regel hinzufügen, und wenden Sie die Regel auf die gesamte Gruppe (oder einen Unterordner, wenn Sie sie entsprechend konfiguriert haben) an.
3. Wählen Sie eine Aktion für Objekte, wie Löschen oder Archivieren, dann wählen Sie den Zeitraum und ob Sie Glacier-Speicher verwenden möchten, um Ihre Amazon-Kosten zu reduzieren. (Bei Glacier handelt es sich um einen Offline-Speicher, der zwar langsamer

zugänglich, aber preisgünstiger ist.)

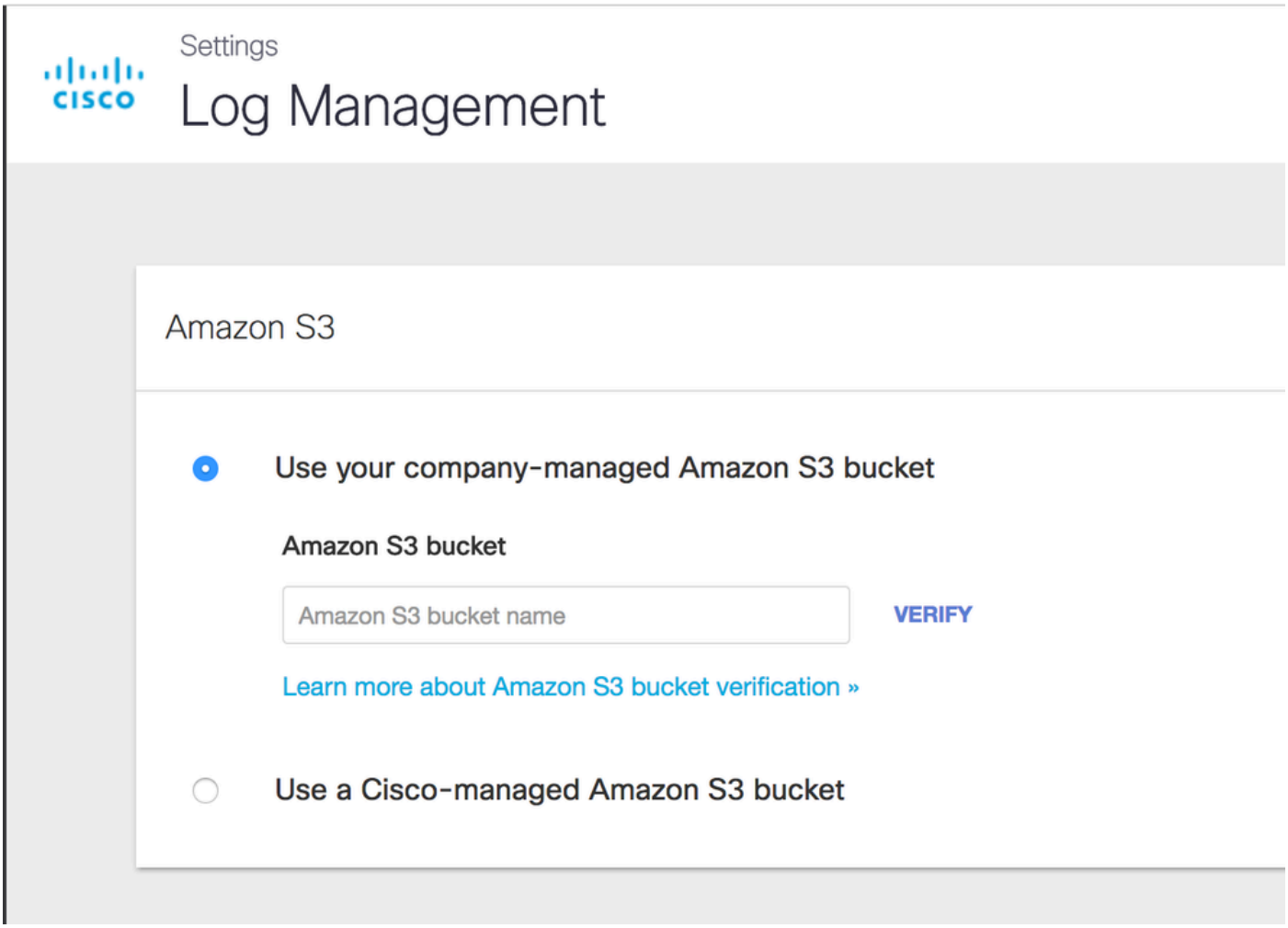
4. Wenn Sie Protokolle lieber mit einer anderen Methode verwalten möchten (z. B. mit Ihrer internen Backup-Lösung), können Sie die Protokolle einfach von S3 herunterladen und auf eine andere Weise aufbewahren. Legen Sie dann Ihre Aufbewahrungszeit auf einige Tage fest.

Konfigurieren eines von Cisco verwalteten S3-Buckets

Navigieren Sie in Ihrem Umbrella Dashboard zu Einstellungen > Protokollverwaltung.

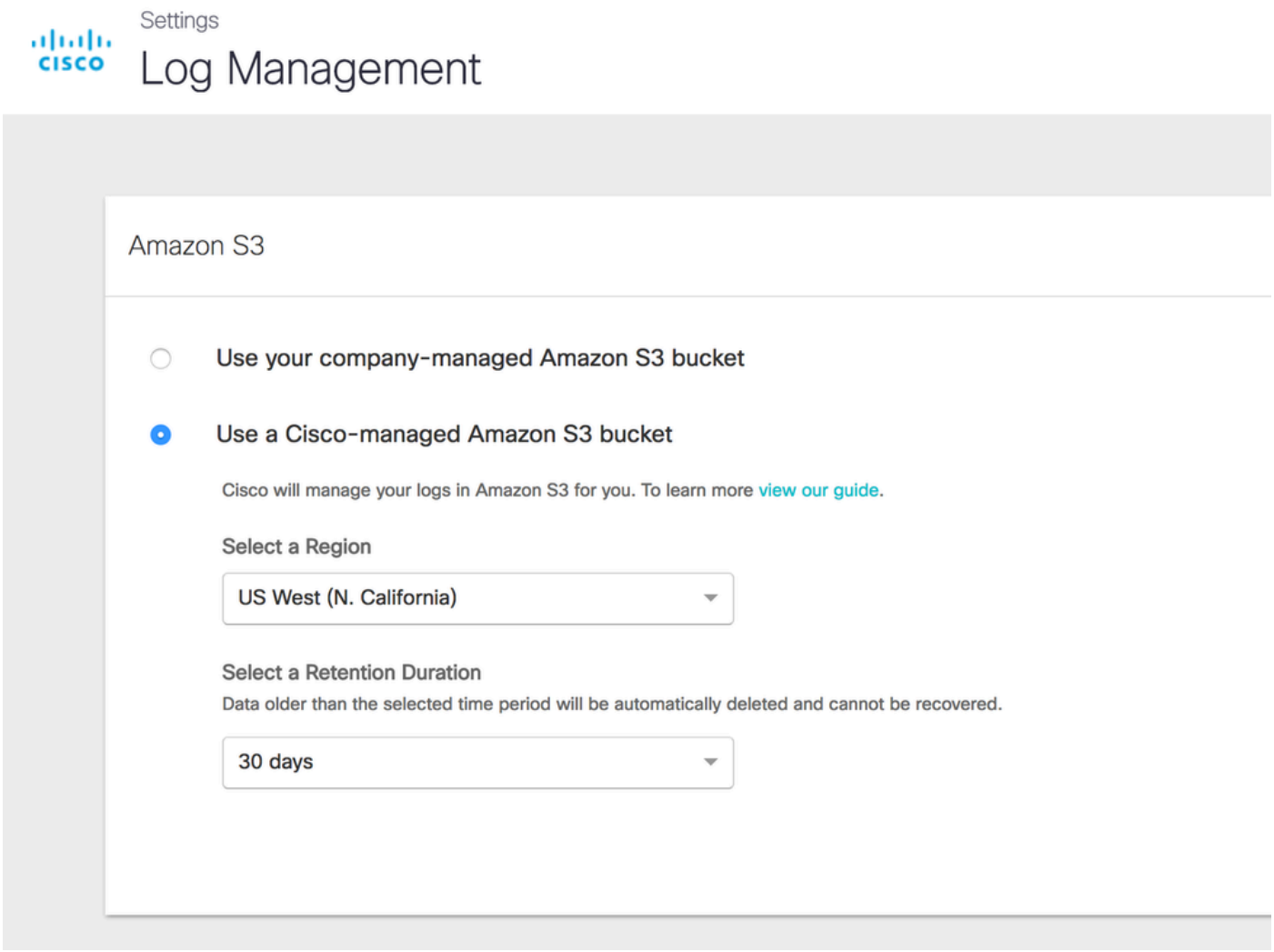
Es gibt zwei Optionen:

- Verwenden Sie Ihre firmenverwaltete Amazon S3 Bucket
- Verwendung einer von Cisco verwalteten Amazon S3-Bucket



25231151138964

Wählen Sie "Use a Cisco managed Amazon S3 bucket" (Von Cisco verwaltete Amazon S3-Bucket verwenden), und Sie erhalten zwei neue Optionen: "Wählen Sie eine Region" und "Wählen Sie eine Aufbewahrungsdauer".



25231151158036

Wählen Sie eine Region

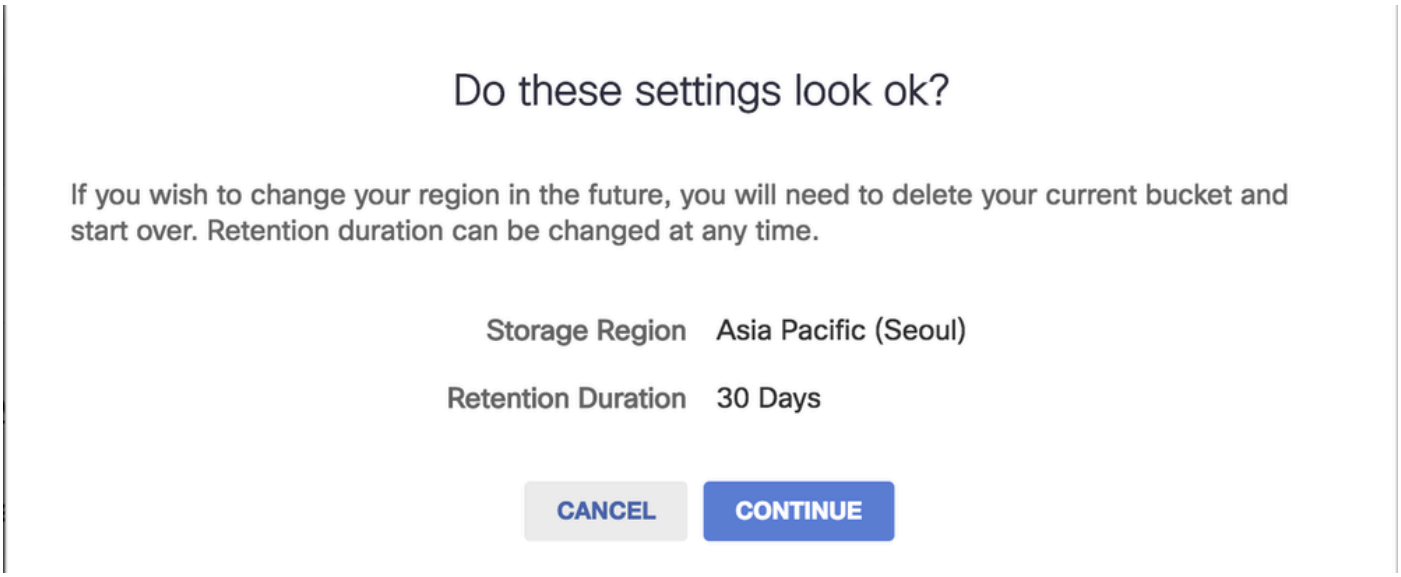
Regionale Endgeräte sind wichtig, um die Latenz beim Herunterladen von Protokollen auf Ihre Server zu minimieren. Die aufgelisteten Regionen entsprechen denen von Amazon S3, aber nicht alle Regionen sind verfügbar. China ist beispielsweise nicht aufgeführt.

Wählen Sie aus dem Dropdown-Menü die Region aus, die Ihnen am nächsten liegt. Wenn Sie Ihre Region in Zukunft ändern möchten, müssen Sie Ihre aktuellen Einstellungen löschen und von vorne anfangen.

Aufbewahrungsdauer auswählen

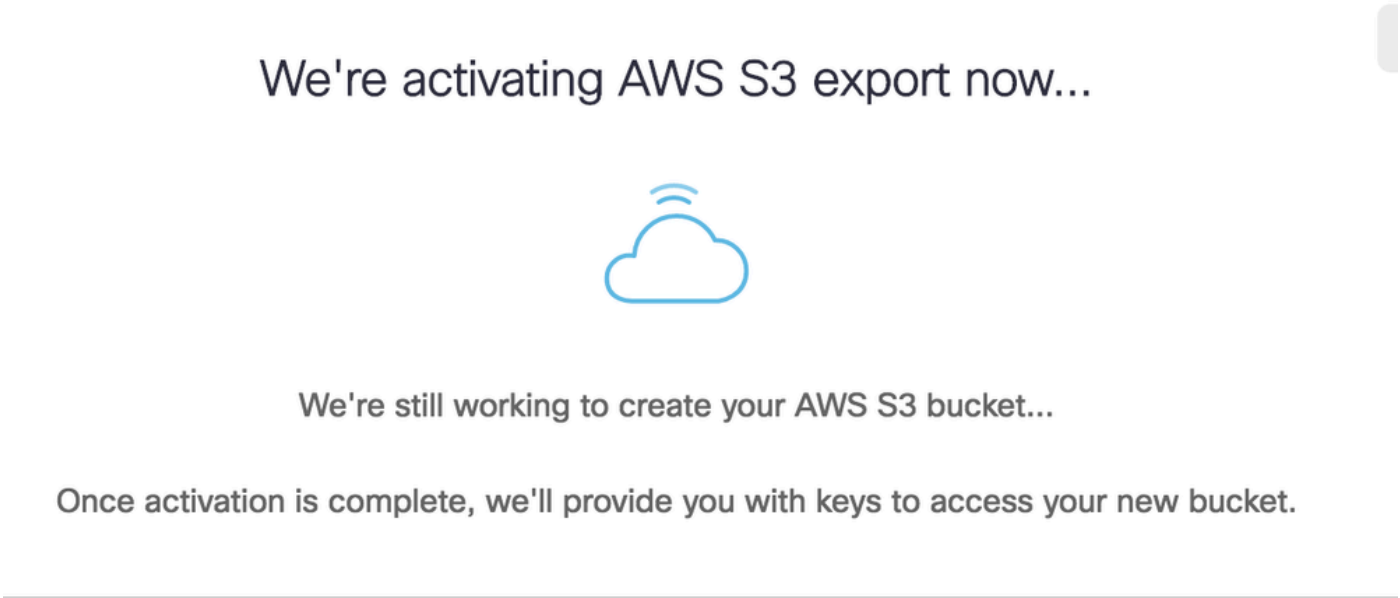
Die Retentionsdauer beträgt einfach 7, 14 oder 30 Tage. Nach dem gewählten Zeitraum werden alle Daten gelöscht und können nicht wiederhergestellt werden. Wir empfehlen Ihnen einen kürzeren Zeitraum, wenn Ihr Einnahmezyklus regelmäßig ist. Die Verweildauer kann zu einem späteren Zeitpunkt geändert werden.

Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf Weiter, und Sie werden aufgefordert, Ihre Region und Dauer zu bestätigen.



25231181211796

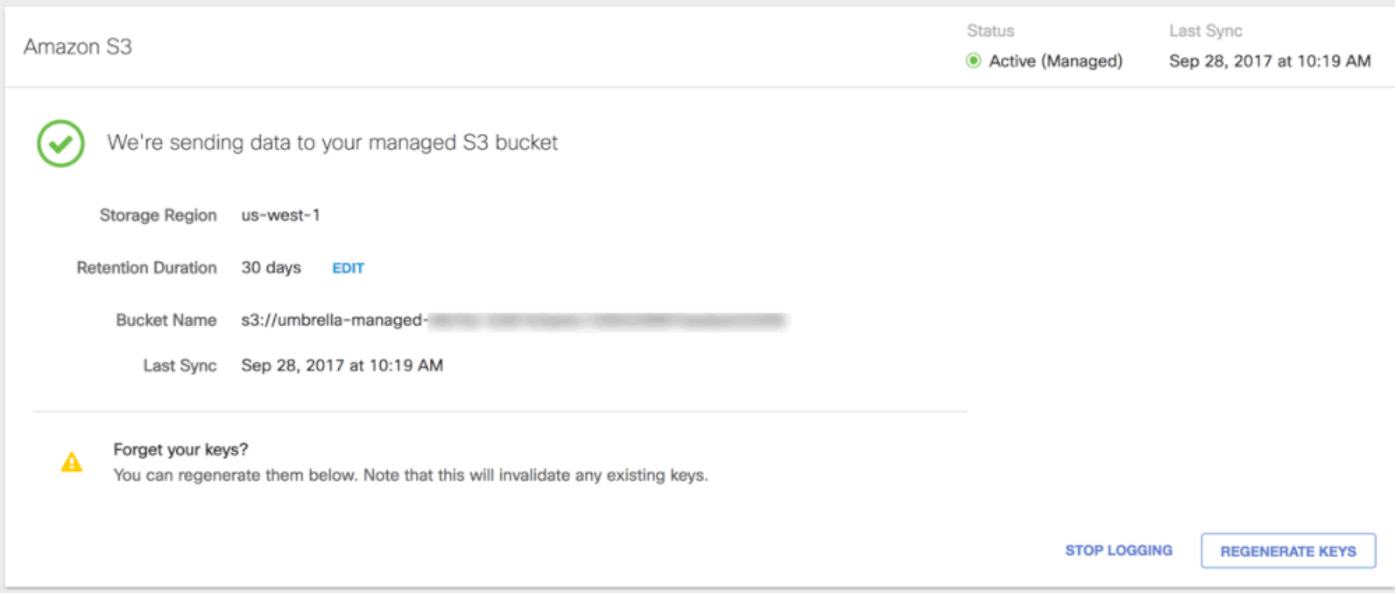
Sobald Sie dem Fortfahren zustimmen, erhalten Sie eine Aktivierungsbenachrichtigung.



25231181218708

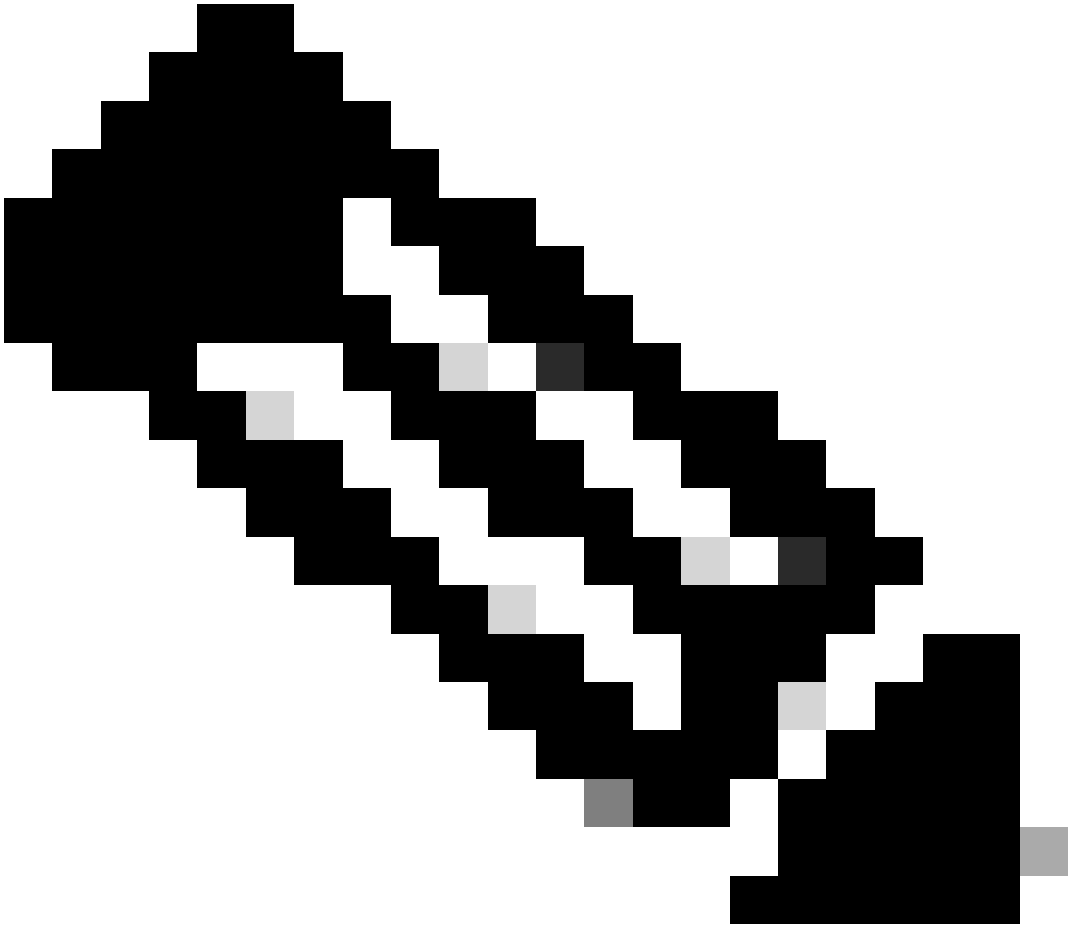
Sie erhalten dann einen Zugriffsschlüssel und einen geheimen Schlüssel. Sie müssen akzeptieren (klicken Sie auf "Got it!"), weil dies das einzige Mal, dass Sie einen der Schlüssel zu sehen. Der Zugriff und geheime Schlüssel sind erforderlich, um Ihren Bucket zugreifen und Ihre Protokolle herunterladen.

Zuletzt sehen Sie den Übersichtsbildschirm mit der Konfiguration und vor allem Ihrem Bucketnamen.



25231181228180

Sie können die An- und Abmeldung zu einem beliebigen Zeitpunkt aktivieren bzw. deaktivieren.



Anmerkung: Cisco löscht weiterhin Protokolle basierend auf der gewählten Aufbewahrungsdauer, auch wenn die Protokollierung deaktiviert wurde.

Optionen nach der Konfiguration

Fehler beim Protokoll-Upload

Falls keine Protokolle von Cisco Umbrella auf Ihren S3-Bucket hochgeladen werden können, gibt es eine Kulanzfrist von vier Stunden, in der der Service alle 20 Minuten wiederholt wird. Nach vier Stunden wird ein Fall mit unserem Support-Team eröffnet, das eine Untersuchung der Problemursache einleitet und Sie proaktiv kontaktiert, um Sie über das Problem zu informieren.

Hochgeladene Protokolle und das hochgeladene Format überprüfen

Protokolle werden in zehnminütigen Intervallen von der Umbrella-Protokollwarteschlange in die S3-Buckets hochgeladen. Nach Abschluss der Konfiguration wird das erste Protokoll innerhalb von zwei Stunden in Ihren S3-Bucket geladen, obwohl der Vorgang in der Regel sofort oder nahezu unmittelbar abläuft. Das Hochladen erfordert jedoch neu generierte Protokolldaten. Wenn Sie dies also in einer Testumgebung versuchen, stellen Sie sicher, dass die Netzwerkdaten in der Aktivitätssuche protokolliert werden.

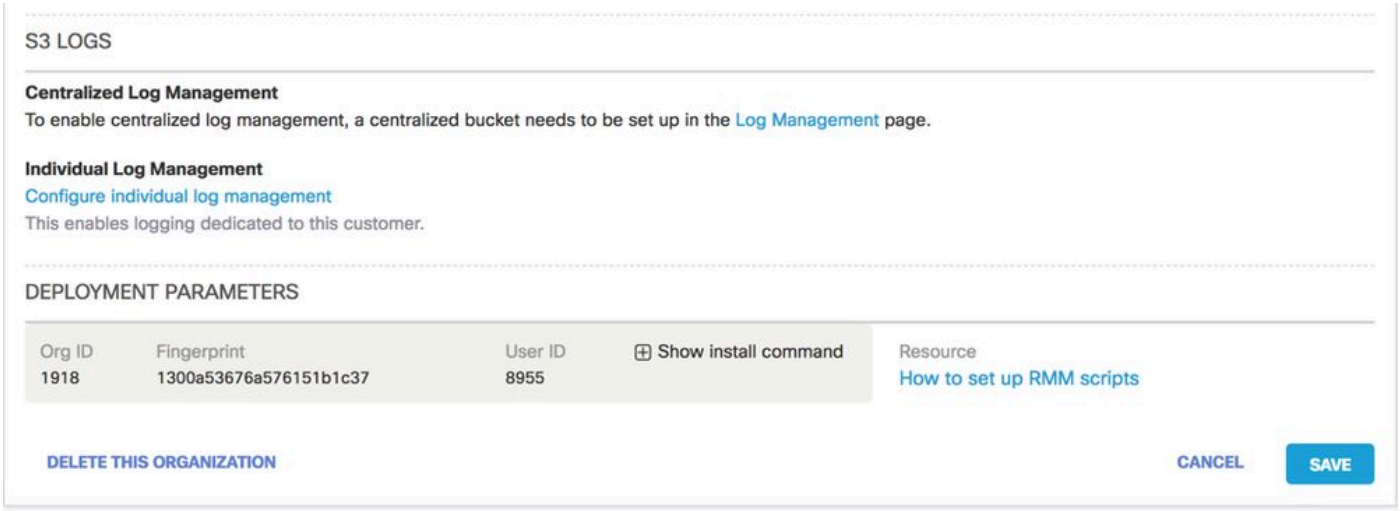
Um zu überprüfen, ob alles funktioniert, wird die letzte Synchronisierungszeit in den Umbrella Dashboard Updates und Protokollen in Ihrer S3-Bucket angezeigt.

Jeder Kunde bzw. jede Organisation ist in Ihrem Eimer mit seiner Organisations-ID versehen. Die Ordnerstruktur sieht daher folgendermaßen aus:

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

<bucket-name> ist Ihr Bucket-Name, <orgID> ist Ihre Organisation, es ist Ihre ID, und <subfolder> sind je nach Art der darin enthaltenen Protokolle entweder dnslogs, proxylogs oder iplogs.

Für MSP- und MSSP-Kunden stimmt die orgID mit der in den Kundeneinstellungen unter den einzelnen Kundendetails im Abschnitt mit den Bereitstellungsparametern überein. Mehrere Kunden können die orgID erfassen, indem sie sich bei jeder einzelnen Unterorganisation anmelden und die orgID in der Browser-URL notieren: (https://dashboard.umbrella.com/o/######/).



360002271623

Derzeit ist die Protokollformatversion für MSP-, MSSP- und Multi-Org-Kunden Version 1.1. Die Protokolle werden im GZIP-Format angezeigt und in S3-Buckets im entsprechenden Unterordner mit dem folgenden Namensformat hochgeladen:

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

<Unterordner> ist entweder dnslogs, proxylogs oder iplogs, abhängig von den Protokolltypen innerhalb. <xxxx> ist eine zufällige Zeichenfolge mit vier alphanumerischen Zeichen, die das Überschreiben doppelter Dateinamen verhindert.

Beispiele:

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

Wenn Sie innerhalb von 10 Minuten keine Protokolle in Ihrem Bucket sehen, wenden Sie sich an den Support, um die bisher unternommenen Schritte zu beschreiben.

Sobald die Protokolle angezeigt werden, empfehlen wir, die Daten zu überprüfen, indem Sie die Inhalte der ersten Log-Uploads entzippen, die empfangen werden, um sicherzustellen, dass die Daten in einem Texteditor (oder sogar Microsoft Excel, häufig die Standarddatei für CSV-Dateien) angezeigt werden können. Weitere Informationen zu den einzelnen Feldern im Protokoll finden Sie hier.

Wenn ein Log-Upload von Cisco Umbrella auf Ihre S3-Bucket fehlschlägt, gibt es eine Kulanzfrist von vier Stunden, in der der Service alle 20 Minuten wiederholt wird. Nach vier Stunden wird ein Ticket in unserem Support-Team geöffnet, das eine Untersuchung der Problemursache einleitet und Sie proaktiv kontaktiert, um Sie über das Problem zu informieren.

Aktivieren der Protokollierung auf Kundenbasis

Sofort einsatzbereit, sofern nicht anders angegeben, ist diese Funktion für alle Kunden aktiviert. Die Funktion kann für einzelne Kunden deaktiviert werden. Dies ist hilfreich, wenn Sie für Kunden, die über die Funktion verfügen, unterschiedliche Servicelevel festlegen. Dies erfolgt unter jedem Kunden über die Einstellungen in der Konsole. Der Screenshot im vorherigen Abschnitt zeigt den Umschalter, um die Funktion zu deaktivieren.

Es ist auch möglich, IAM-Benutzer in Amazon zu erstellen und diese IAM-Benutzer einzelnen orgit is-Unterordnern des Buckets zuzuweisen. Auf diese Weise können Sie einem Endbenutzer den Zugriff auf seine Protokolle gestatten, jedoch nur auf seine Protokolle.

Protokolle herunterladen, Format und Splunk-/QRadar-Integration verstehen

Um die Logs für die Aufbewahrung oder Nutzung herunterzuladen, gibt es einige Ansätze, die DNS-Logs von S3 herunterzuladen.

Möglicherweise haben Sie auch einige Fragen zum Protokollformat und dessen geringfügigen Unterschied zu den Protokollen, die im Umbrella Dashboard angezeigt werden. Weitere Informationen zum exportierten Protokollformat finden Sie in diesem Artikel.

Eine der wichtigsten Einsatzmöglichkeiten für den Export von DNS-Protokollen ist die Integration mit den SIEM-Tools. Obwohl die Konfiguration eines SIEM beim Umgang mit Protokollen wie diesem oft auf die persönlichen Präferenzen eines Administrators zurückzuführen ist, haben wir einige Anleitungen für die gängigsten SIEMs.

Weitere Informationen zum Einrichten des Splunk-Plug-ins für Amazon AWS S3 und Umbrella finden Sie hier.

Informationen zur Konfiguration von IBM QRadar zum Abrufen von Protokollen von Amazon S3 und zum Verarbeiten dieser Protokolle finden Sie hier.

Wie groß sind die S3-Protokolle?

Die Größe der S3-Protokolle hängt von der Anzahl der Ereignisse ab, die auftreten, und ist vom Volumen des DNS-Datenverkehrs abhängig.

Das Protokollformat für die S3-Protokollierung finden Sie hier.

Der Beispieleintrag ist 220 Byte groß, aber die Größe jeder Protokollzeile variiert je nach Anzahl der Einträge (Länge des Domänennamens, Anzahl der Kategorien usw.). Wenn jede Protokollzeile 220 Byte umfasst, beträgt eine Million Anfragen 220 MB.

So erhalten Sie eine Schätzung der Anzahl von DNS-Abfragen pro Tag:

1. Navigieren Sie im Umbrella Dashboard zu Reporting > Activity Search (Berichte > Aktivitätssuche).
2. Führen Sie unter Filter einen Bericht der letzten 24 Stunden aus, und klicken Sie dann auf das Symbol CSV exportieren.
3. Öffnen der heruntergeladenen CSV-Datei Die Anzahl der Zeilen (minus einer für den Header) ist die Anzahl der DNS-Abfragen pro Tag. Multiplizieren Sie das mit 220 Bytes, um die Schätzung für einen Tag zu erhalten.

Was die Kosten angeht, so ist es zwar variabel, aber wir stellen fest, dass selbst unsere größten Kunden nur ein paar Dollar pro Monat für den Service ausgeben. Ein Preis ist an die Speicherzeit und ein anderer an den Datendownload aus S3 in Ihre Umgebung gebunden. Weitere Informationen erhalten Sie bei Amazon.

Wie bei allen unseren Funktionen, ist weit gerne wissen, was Sie denken, vor allem über SIEM-Integrationen oder alle zusätzlichen Fragen, die in dieser Dokumentation behandelt werden. Wenn Sie Feedback haben, lassen Sie es uns bitte wissen!

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.