Comprendre la gestion centralisée des fichiers journaux avec le service S3 d'Amazon pour les clients MSP, MSSP et multi-organisations

Table des matières

Introduction

Ce document décrit la gestion centralisée des journaux Umbrella avec le service S3 d'Amazon pour les clients MSP, MSSP et multi-organisations.

Aperçu

Les consoles MSP, MSSP et Multi-org permettent de stocker hors ligne les journaux DNS, URL et IP de vos clients dans le stockage cloud. Le stockage est dans Amazon S3 et une fois les journaux téléchargés, ils peuvent être téléchargés et conservés pour des raisons de conformité ou d'analyse de sécurité.

Cette documentation vous aide à comprendre cette fonctionnalité, à la configurer dans votre tableau de bord Umbrella et votre console Amazon S3, et à exécuter plusieurs options de configuration, y compris la durée pendant laquelle vous souhaitez que les journaux soient

conservés dans S3.

Umbrella pour MSP, MSSP et Multi-Org ont tous la possibilité de télécharger les journaux d'activité du trafic à partir des organisations enfants de la console et de stocker ces journaux dans le cloud. Le service AWS S3 (Simple Storage Service) d'Amazon archive les journaux et est parfois appelé « stockage hors ligne » ou « rétention des journaux ».

L'archivage des journaux peut être utile pour plusieurs raisons, selon vos besoins. Pour certaines personnes, les journaux exportés et archivés peuvent être importés dans des outils d'analyse des données ou de sécurité, tels que les SIEM. Pour d'autres, une archive des journaux d'activité peut être utile pour l'analyse des données en cas d'incident de sécurité ou pour les enregistrements de ressources humaines.

AWS S3 stocke les journaux dans une archive compressée (gzip) au format CSV. Comme les journaux sont téléchargés toutes les dix minutes, il y a un délai minimal de dix minutes entre le trafic réseau provenant de votre réseau, enregistré par Umbrella, puis mis à disposition pour téléchargement à partir de S3.

Le numéro orgID de la console

Chaque organisation client télécharge ses journaux individuellement, en utilisant le numéro orgID de la console pour mapper chaque client à un dossier. La fonctionnalité peut également être activée ou désactivée pour chaque client/organisation.

Deux types de gestion des journaux Umbrella

La gestion des journaux est effectuée en téléchargeant les journaux dans ce qui est appelé un isbucketit est (essentiellement un dossier dans AWSit est l'environnement S3). Il existe deux façons d'héberger un compartiment pour vos journaux Umbrella :

- Administré, géré et payé par vous, l'administrateur de la société.
- Administré, géré et payé par Cisco Umbrella.

La gestion de votre compartiment S3 par Cisco présente des avantages et des inconvénients.

Les avantages de la gestion de votre bucket par Cisco :

- Extrêmement facile à installer. Cela ne prend que quelques minutes et par la suite, il est extrêmement facile à gérer.
- La gestion des compartiments Cisco est incluse dans votre coût de licence avec Umbrella, rendant ainsi le service gratuit. Bien qu'il soit peu coûteux d'avoir son propre compartiment, les frais généraux de gestion d'une autre facture peuvent être prohibitifs.

Les avantages de la gestion d'une instance S3 vous-même :

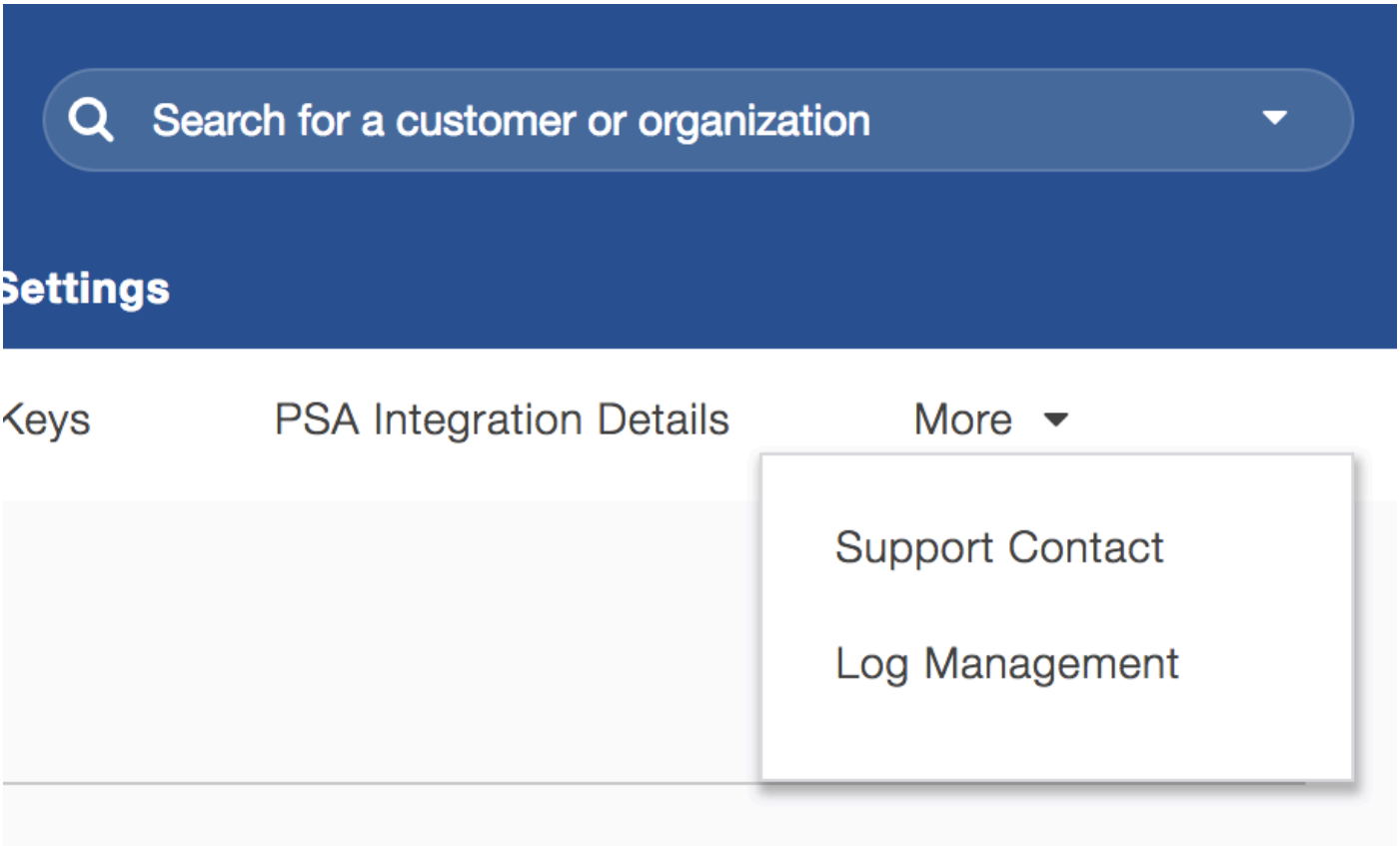
- Il n'y a pas de limite sur la durée pendant laquelle les données peuvent être stockées hors connexion. Cisco limite le stockage hors ligne à 30 jours au maximum.
- Vous pouvez ajouter n'importe quoi à votre bucket, y compris les fichiers journaux d'Umbrella, de sorte que le bucket peut être utilisé par d'autres applications.

- Vous pouvez obtenir une assistance directement auprès d'Amazon pour une assistance à la configuration avancée, telle que l'automatisation ou l'aide avec la ligne de commande.

Pour la plupart des clients, le coût d'entretien d'un seau est très peu coûteux, mais peut s'avérer être difficile.

Pour commencer

La fonction Log Management est disponible dans la Console sous Settings > Log Management (vous pouvez cliquer sur la flèche de la liste déroulante).



115012963103

Configuration d'un groupement S3 autogéré

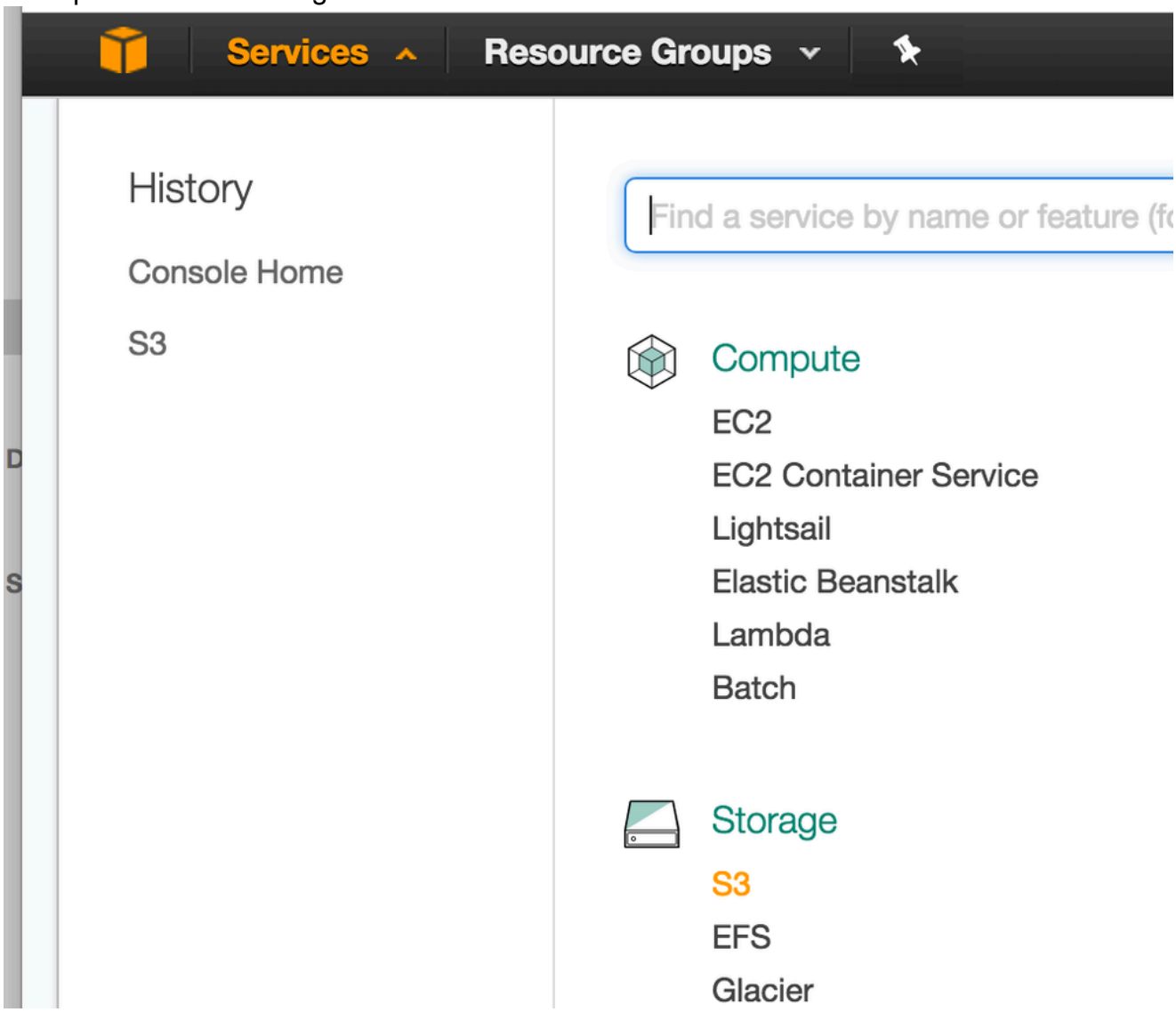
Conditions préalables

Pour archiver les journaux, vous devez répondre aux exigences suivantes :

- Accès administratif complet à la console Cisco Umbrella MSP, MSSP ou Multi-org.
- Une connexion au service Amazon AWS (https://aws.amazon.com/console/). Si vous avez un compte, Amazon vous offre l'inscription gratuite à S3. Cependant, ils ont besoin d'une carte de crédit au cas où votre utilisation dépasserait l'utilisation du forfait gratuit.
- Un compartiment configuré dans Amazon S3 pour le stockage des journaux. Reportez-vous à la section suivante pour obtenir des instructions sur la configuration et la configuration du compartiment Amazon S3.

Configuration de votre compartiment Amazon S3

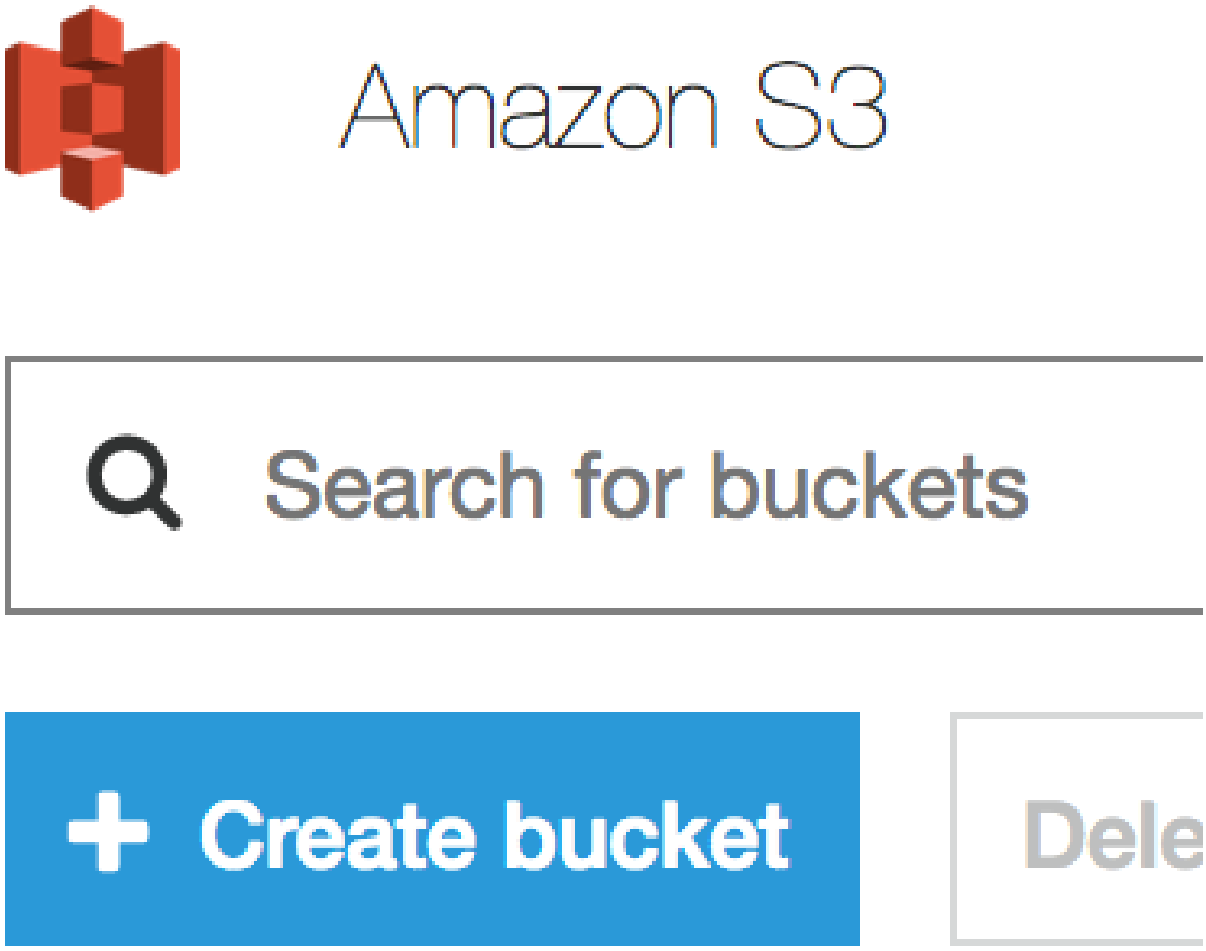
1. Commencez par vous connecter à la console AWS, et en sélectionnant "S3" dans la liste des options sous Stockage.



115012842106

2. Vous voyez un écran d'introduction vous accueillant dans le système de stockage simple Amazon

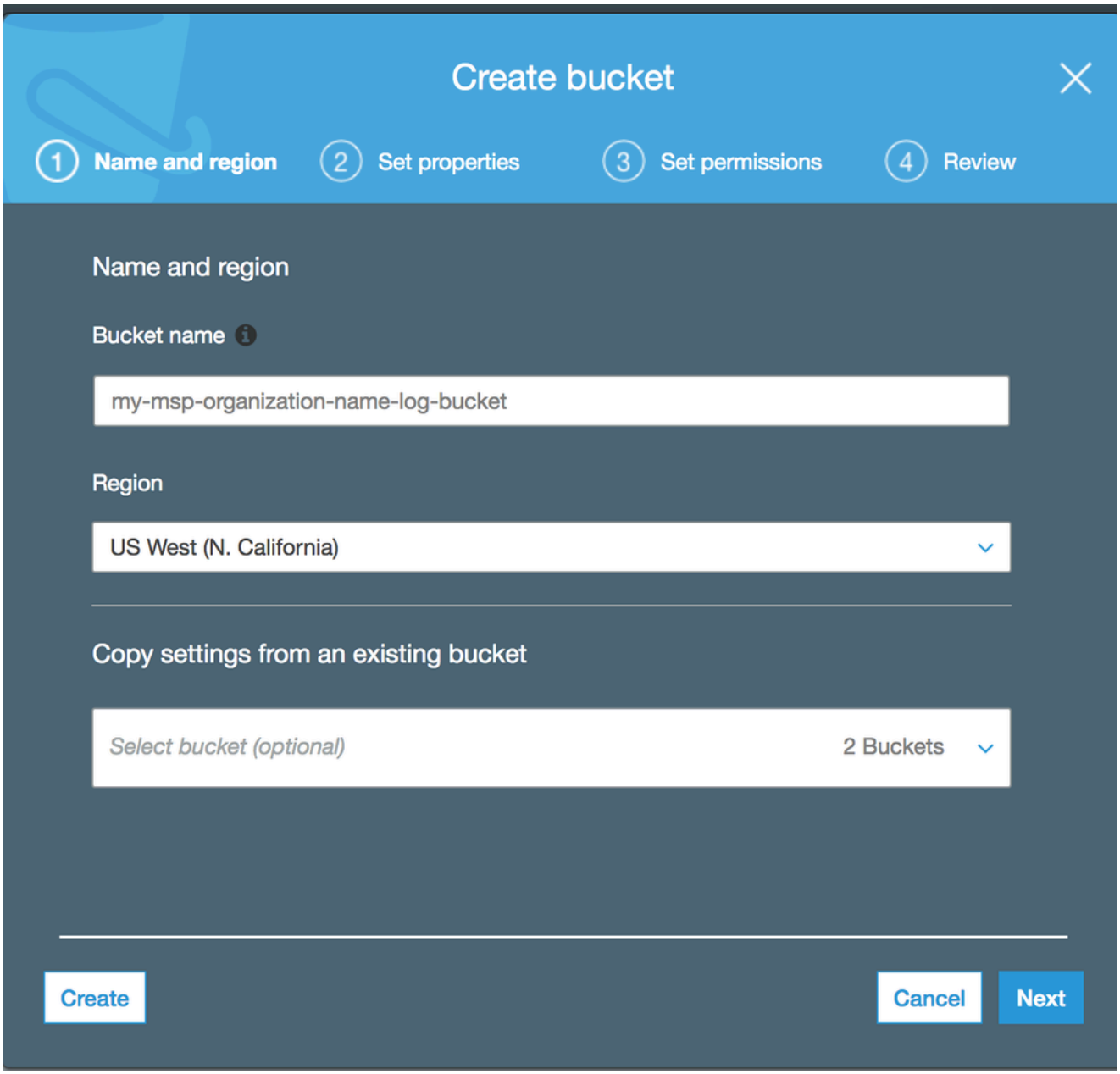
3. Ensuite, si vous n'avez pas encore de compartiment, vous voulez en créer un. Cliquer Créer un compartiment



115012842326

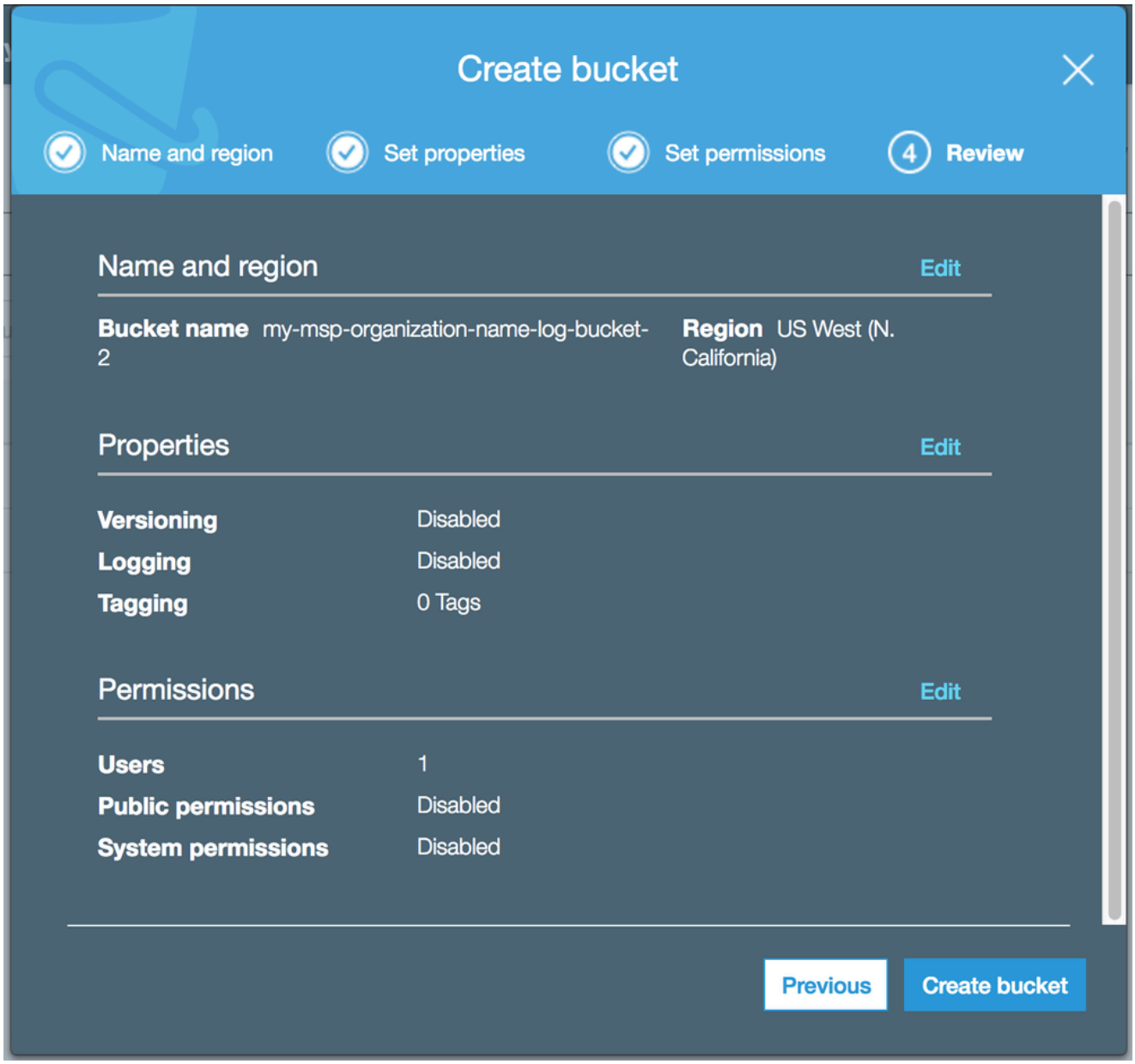
.

4. Commencez par saisir un nom de groupement
   Le nom du seau doit être universellement unique, pas seulement pour votre AWS ou votre Umbrella, mais pour tous les AWS d'Amazon. L'utilisation d'un élément personnel, tel que "my-organization-name-log-bucket" peut vous aider à contourner l'exigence d'un nom de bucket universellement unique. Le nom du compartiment doit uniquement utiliser des lettres minuscules et ne peut pas contenir d'espaces ou de points, et doit être conforme aux conventions d'attribution de noms DNS. Pour plus d'informations sur les restrictions de nom, lisez ici. Pour plus d'informations sur la création du compartiment, y compris l'attribution de noms, lisez ici.



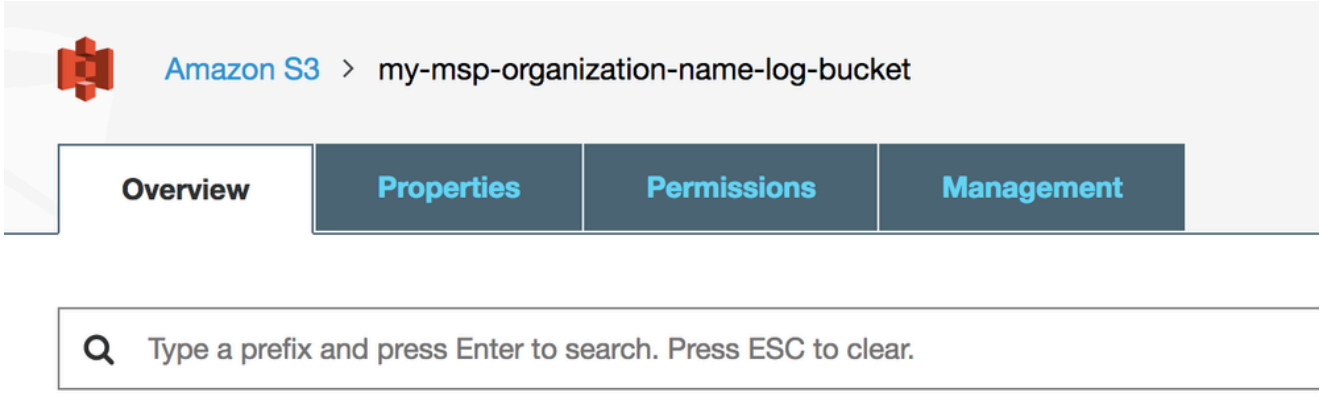
115013010503

5. Sélectionnez la région qui convient le mieux à votre emplacement et cliquez sur Créer. Ne copiez pas les paramètres d'un autre compartiment
6. Dans l'étape "Définir les propriétés", cliquez simplement sur Suivant. Vous pourrez les régler ultérieurement
7. Dans l'étape "Définir les autorisations", cliquez simplement sur Suivant. Nous allons revoir les autorisations ultérieurement pour configurer le compartiment pour le téléchargement
8. Finalisez le processus de révision et cliquez sur Créer un compartiment



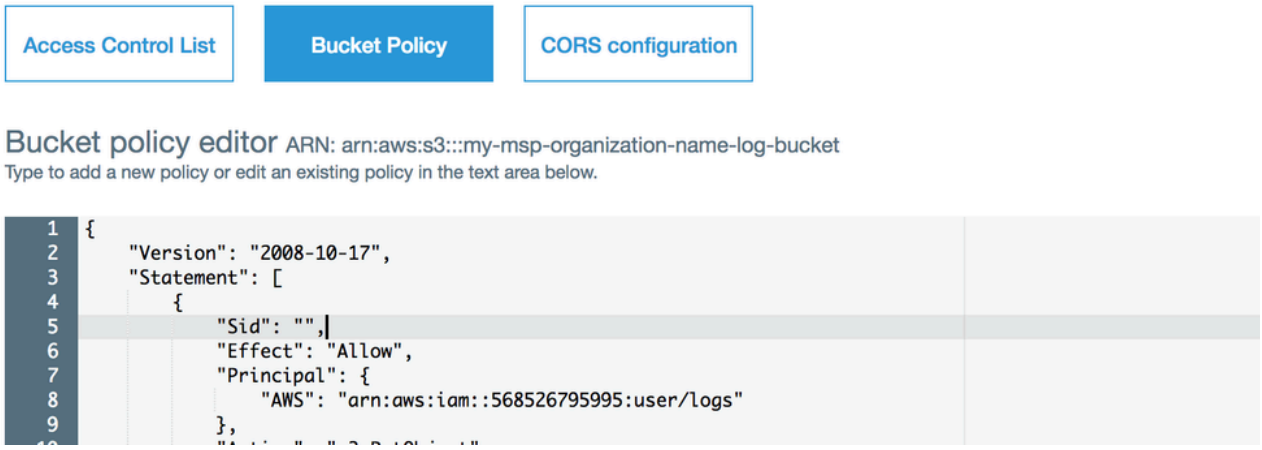
115012842686

9. Ensuite, vous devez configurer le compartiment pour accepter les téléchargements à partir du service Umbrella. Dans S3, il s'agit d'une politique de groupement. Cliquez sur le nom de votre nouveau compartiment configuré, puis sélectionnez l'onglet Autorisations en haut de l'interface



115012842906

10. Sélectionnez Stratégie de groupement, puis vous êtes invité à coller dans le groupement



115012843006

11. Copiez et collez la chaîne JSON ci-dessous, qui contient la stratégie de bucket, dans un éditeur de texte ou collez-la simplement dans la fenêtre. Remplacez le nom exact de votre compartiment par le nom de compartiment spécifié ci-dessous. Si vous ne le faites pas, un message d'erreur apparaît

{
"Version" : "17/10/2008",
"Énoncé" : [
{
"Sid" : "",
"Effet" : "Autoriser",
"Principal" : {
"AWS" : "arn:aws:iam::568526795995:user/logs"
},
"Action" : "s3 : PutObject",
"Ressource" : "arn:aws:s3:::nom_compartiment/*"
},
{
"Sid" : "",
"Effet" : "Refuser",
"Principal" : {
"AWS" : "arn:aws:iam::568526795995:user/logs"
},
"Action" : "s3 : GetObject",
"Ressource" : "arn:aws:s3:::nom_compartiment/*"
},

{
"Sid" : "",
"Effet" : "Autoriser",
"Principal" :

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

,
"Action" : "s3 : GetBucketLocation",
"Ressource" : "arn:aws:s3:::nom_compartiment"
},

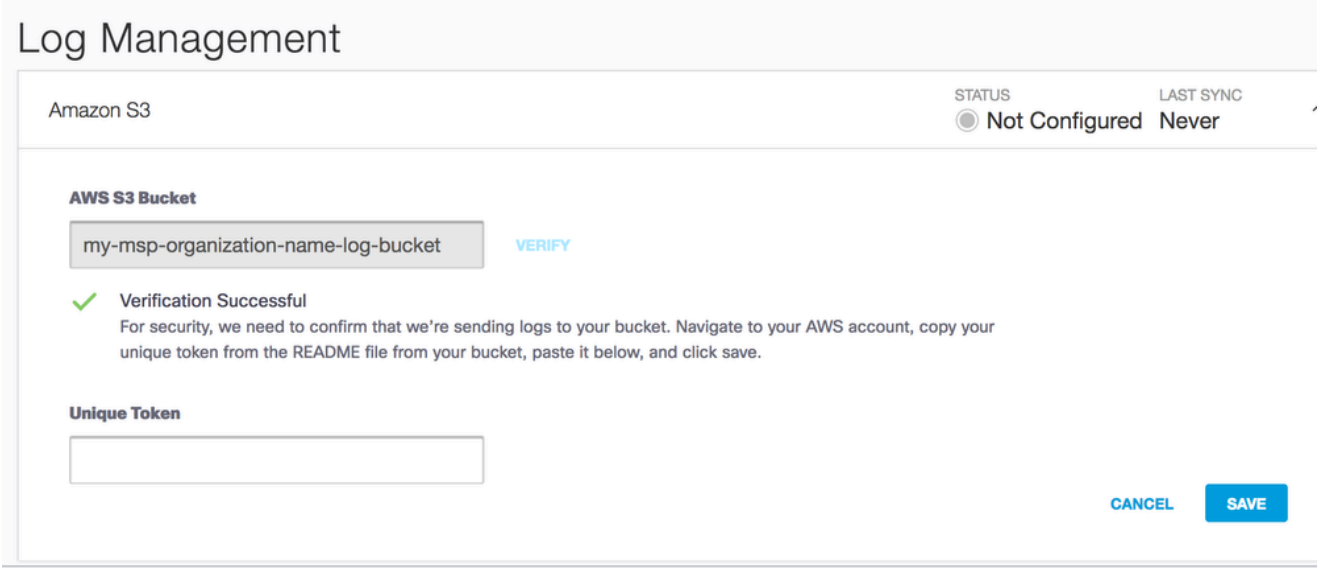
{
"Sid" : "",
"Effet" : "Autoriser",
"Principal" : {
"AWS" : "arn:aws:iam::568526795995:user/logs"
},
"Action" : "s3 : ListBucket",
"Ressource" : "arn:aws:s3:::nom_compartiment"
}
]
}

12. Cliquez sur Enregistrer pour confirmer cette modification

Vérification de votre compartiment Amazon S3

Étape 1 :

1. Revenez à votre console Umbrella et accédez à Paramètres > Gestion des journaux
2. Cliquez sur « Amazon S3 » pour agrandir la fenêtre
3. Dans le champ Nom du compartiment, tapez ou collez le nom de compartiment exact que vous avez créé dans S3 et cliquez sur Vérifier
   Vous recevez un message de confirmation dans votre tableau de bord indiquant que le compartiment a été correctement vérifié.



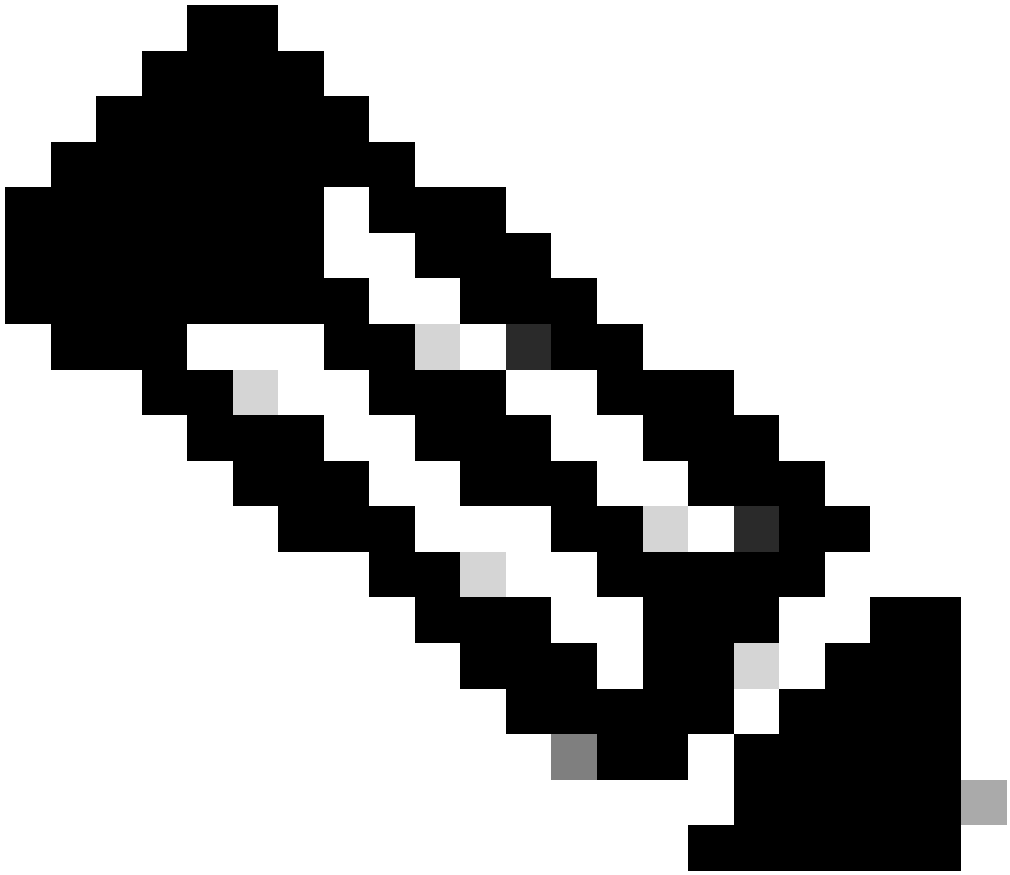
115012847146

Si vous recevez un message d'erreur indiquant que votre compartiment n'a pas pu être vérifié, vérifiez à nouveau la syntaxe du nom du compartiment et passez en revue la configuration. Si les problèmes persistent, veuillez ouvrir un dossier auprès de notre service d'assistance

Étape 2 :

Par mesure de précaution secondaire, afin de vous assurer que le compartiment correct a été spécifié, Umbrella vous demande d'entrer un jeton d'activation unique. Le jeton d'activation peut être obtenu en revisitant votre compartiment S3. Dans le cadre du processus de vérification, un fichier nommé README_FROM_UMBRELLA.txt a été téléchargé depuis Umbrella vers votre compartiment Amazon S3 et s'y affiche.

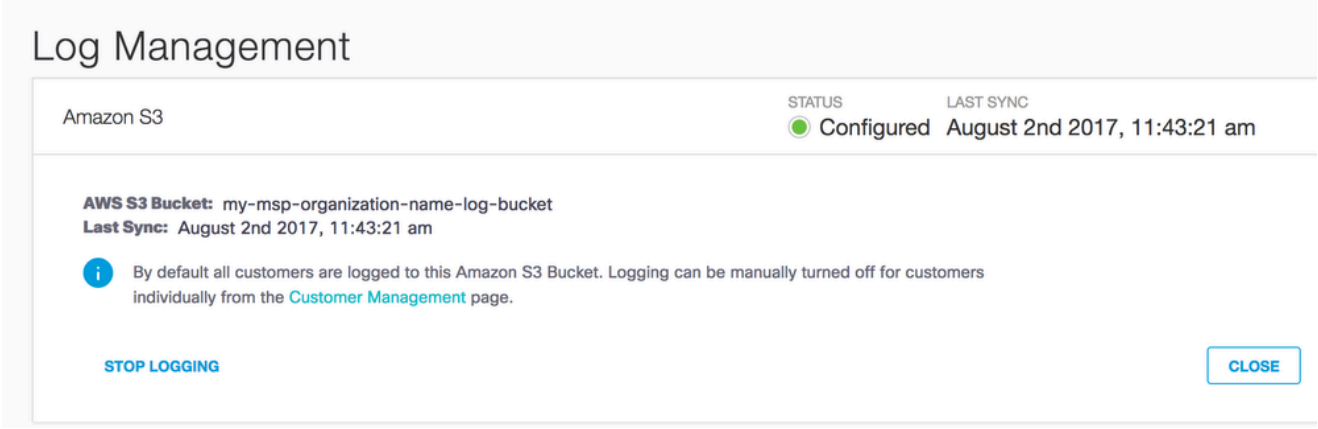
1. Téléchargez le fichier Readme en double-cliquant dessus, puis ouvrez-le dans un éditeur de texte. Dans le fichier, il y a un jeton unique qui lie votre seau S3 à votre tableau de bord Umbrella



Remarque : Vous devrez peut-être actualiser votre bucket S3 dans le navigateur afin de voir le fichier README après son téléchargement.

2. Revenez au tableau de bord Umbrella et collez le jeton dans le champ intitulé "Jeton

unique", puis cliquez sur Enregistrer. À ce stade, la configuration est terminé. Pour vérifier votre configuration, cliquez simplement sur le nom Amazon S3 dans la section Log Management



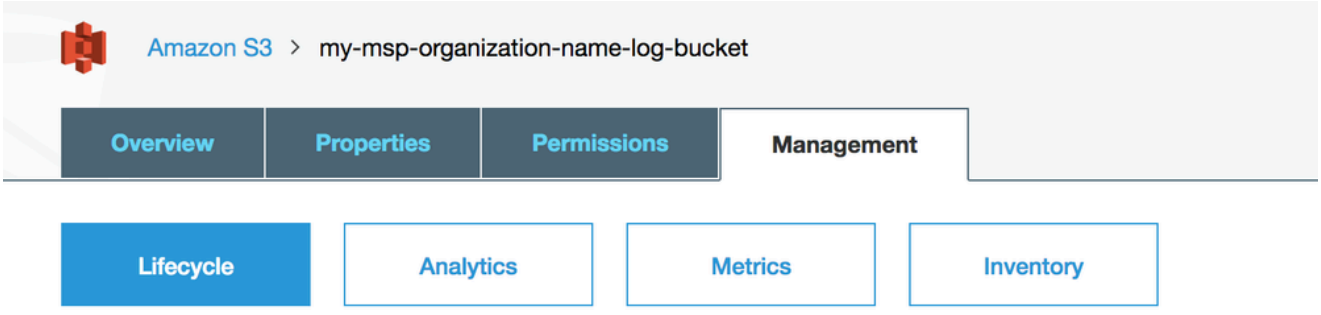
115012848126

Gestion du cycle de vie des journaux

Lorsque vous utilisez S3, vous pouvez gérer le cycle de vie des données dans le compartiment pour prolonger la durée pendant laquelle vous souhaitez conserver les journaux. Selon la raison pour laquelle vous utilisez la gestion de journal externe, la durée peut être très courte ou très longue. Par exemple, vous pouvez simplement télécharger les journaux à partir du compartiment S3 après 24 heures et les stocker hors ligne, ou les conserver indéfiniment dans le cloud. Par défaut, Amazon stocke les données dans un compartiment indéfiniment, mais le stockage illimité augmente le coût de maintenance du compartiment. Pour plus d'informations sur les cycles de vie de S3, lisez ici.

Pour configurer le cycle de vie de votre compartiment :

1. Sélectionnez Management, puis cliquez sur Cycle De Vie



115012848246

2. Cliquez sur Add a Rule, puis sur Apply the Rule to the complete bucket (ou sur un sous-dossier si vous l'avez configuré comme tel).
3. Sélectionnez une action sur les objets, telle que Supprimer ou Archiver, puis sélectionnez la période et si vous souhaitez utiliser le stockage Glacier pour aider à réduire vos coûts Amazon. (Glacier est il iscoldit est stockage hors ligne, qui, bien que plus lent à accéder, est moins cher.)

4. Si vous préférez gérer les journaux avec une autre méthode (comme votre solution de

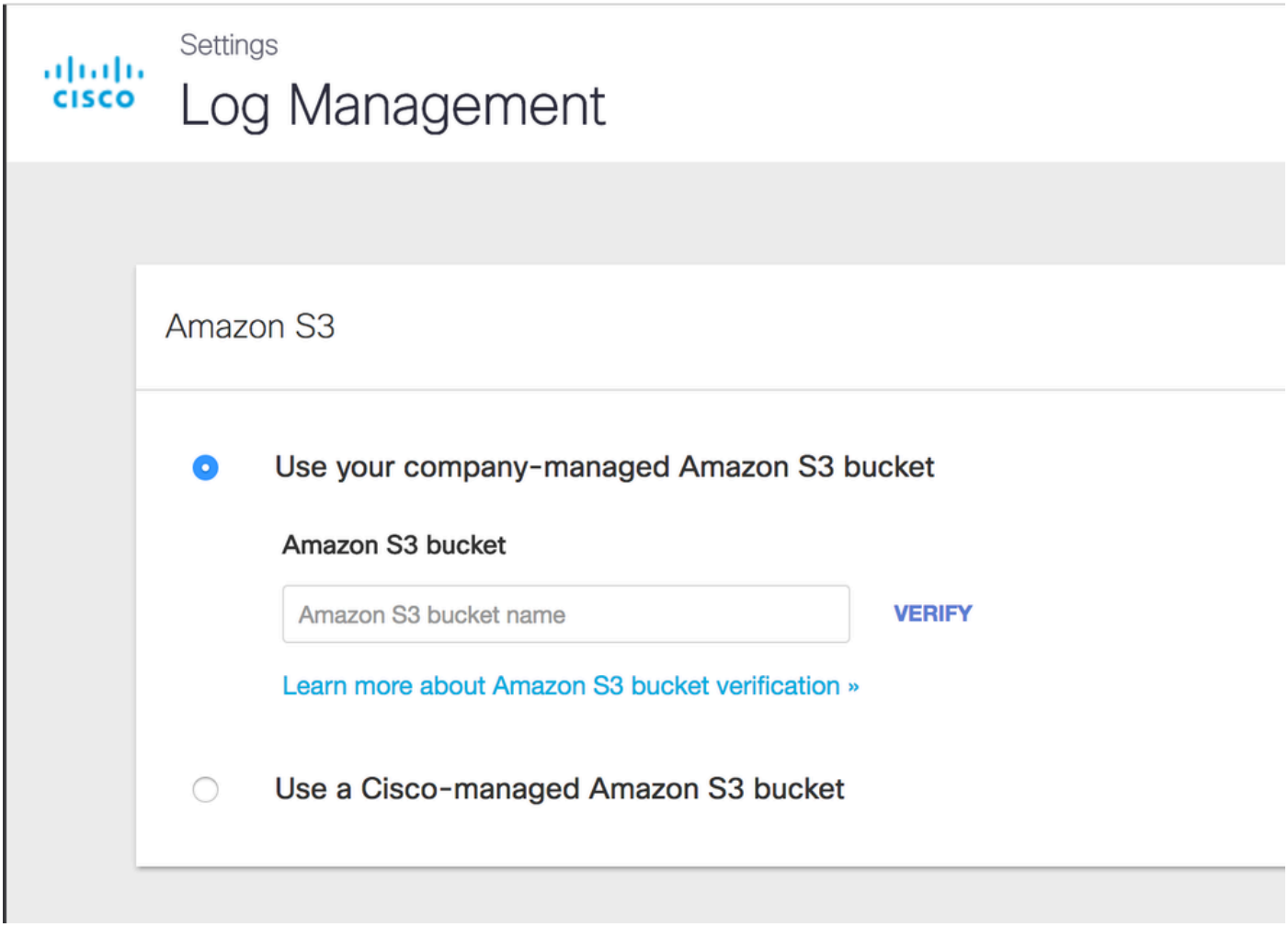
sauvegarde interne), vous pouvez simplement télécharger les journaux à partir de S3 et les conserver d'une autre manière, puis définir votre temps de rétention sur quelques jours.

Configuration d'un groupement S3 géré par Cisco

Accédez à Paramètres > Gestion des journaux dans votre tableau de bord Umbrella.

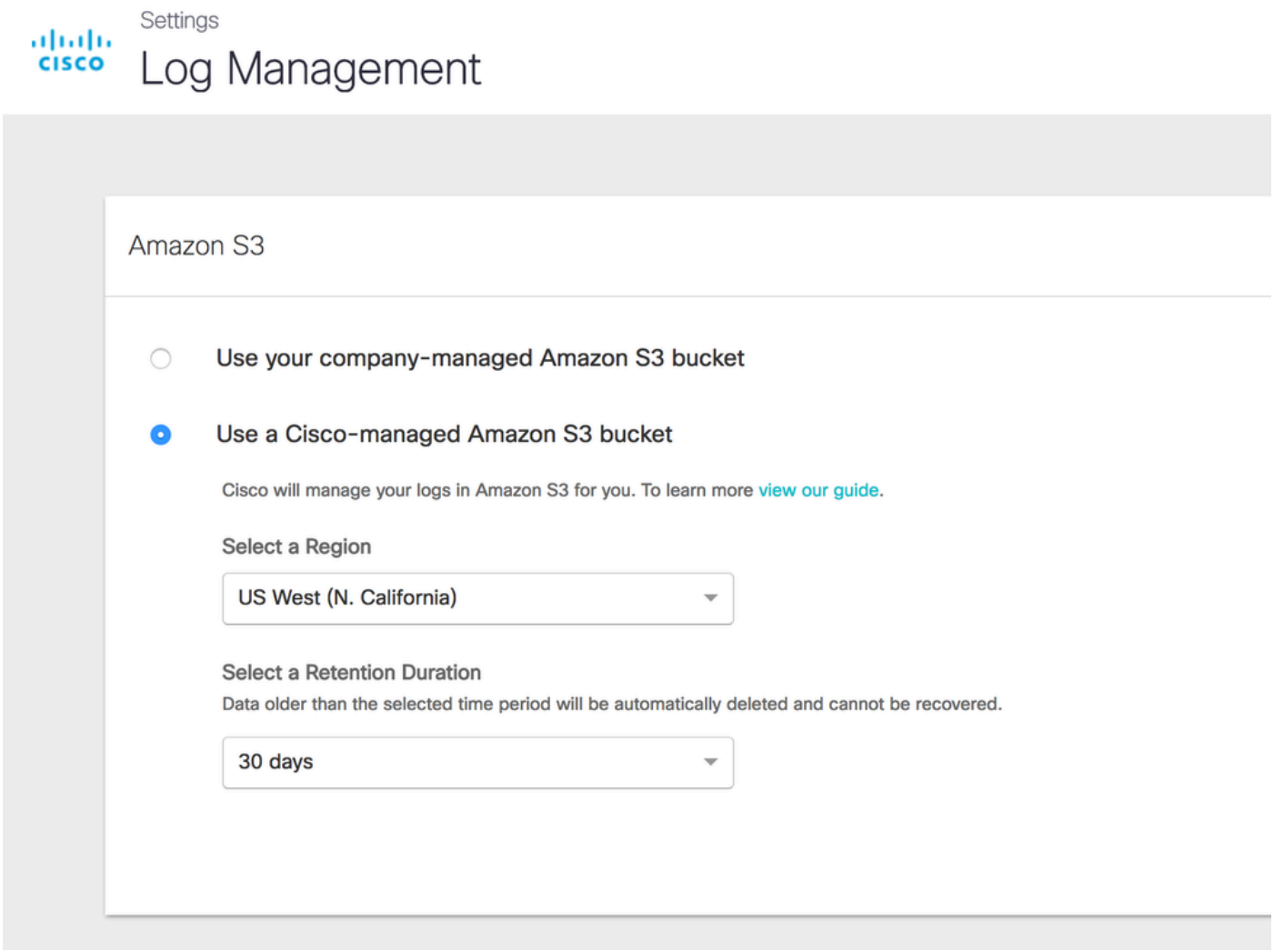
Il existe deux options :

- Utilisez le compartiment Amazon S3 géré par votre entreprise
- Utiliser un compartiment Amazon S3 géré par Cisco



25231151138964

Sélectionnez « Utiliser un compartiment Amazon S3 géré par Cisco » et vous disposez de deux nouvelles options : "Sélectionner une région" et "Sélectionner une durée de conservation".



25231151158036

Sélectionner une région

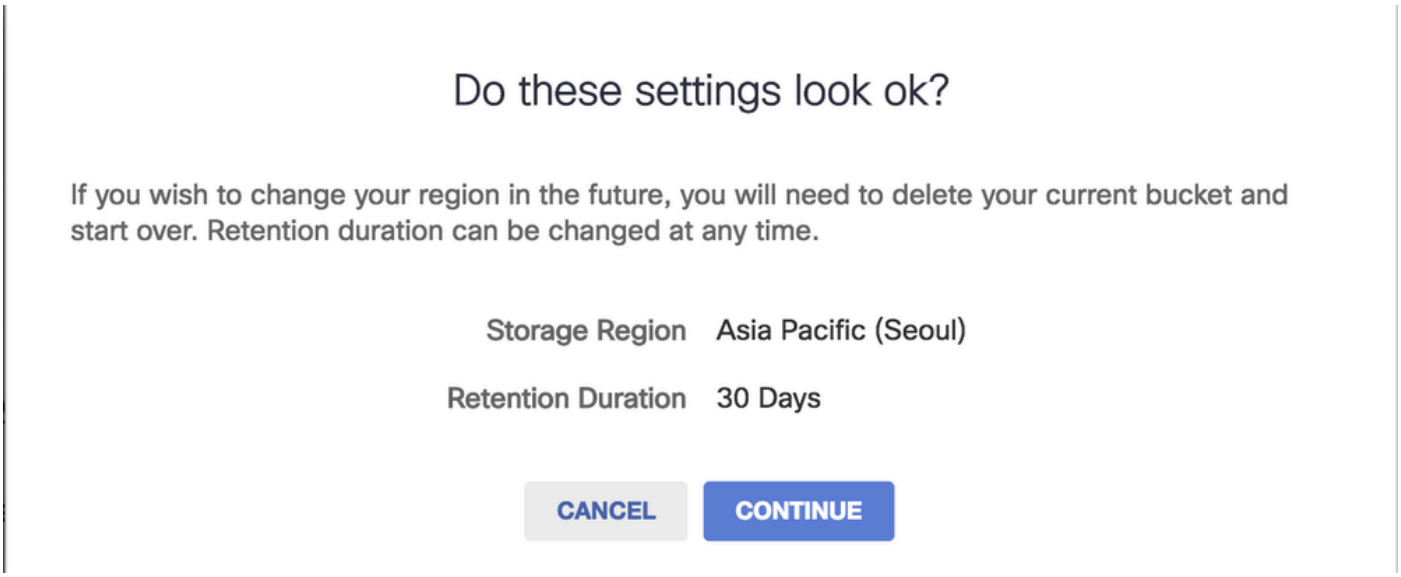
Les terminaux régionaux sont importants pour réduire la latence lors du téléchargement des journaux sur vos serveurs. Les régions répertoriées correspondent à celles disponibles dans Amazon S3, mais toutes les régions ne sont pas disponibles. Par exemple, la Chine n'est pas répertoriée.

Sélectionnez la région la plus proche de vous dans la liste déroulante. Si vous souhaitez modifier votre région à l'avenir, vous devez supprimer vos paramètres actuels et recommencer.

Sélectionner une durée de rétention

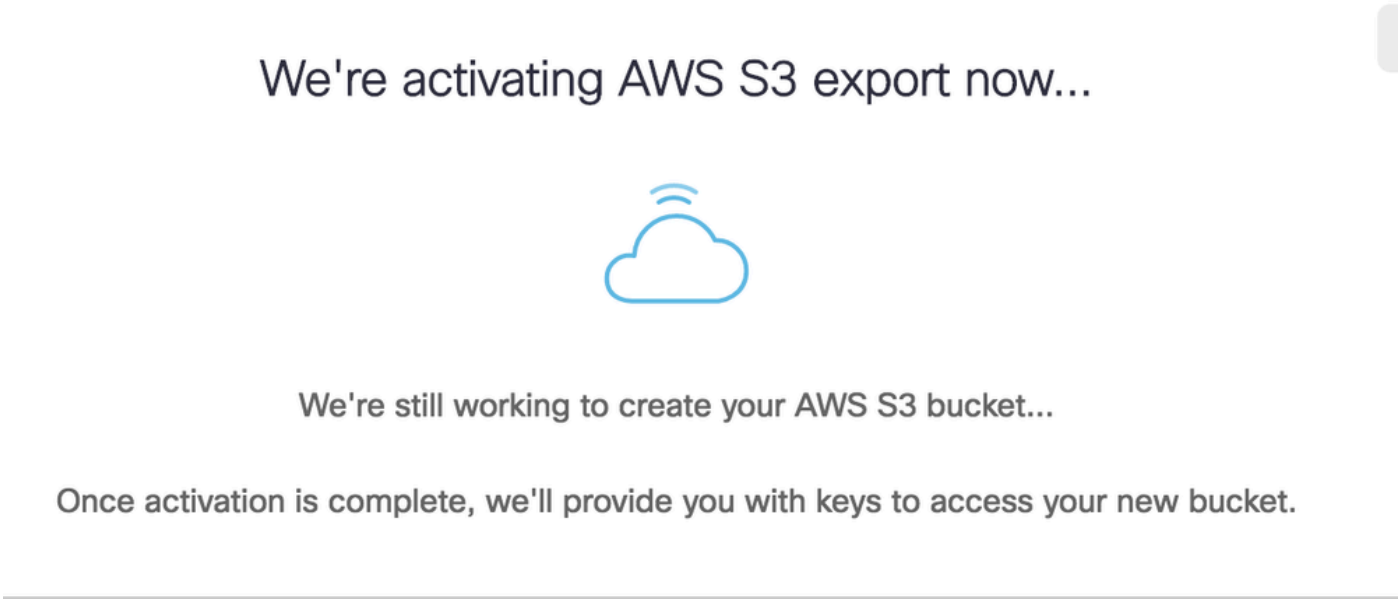
La durée de conservation est simplement de 7, 14 ou 30 jours. Après la période sélectionnée, toutes les données sont purgées et ne peuvent pas être récupérées quoi qu'il arrive. Nous recommandons une période plus courte si votre cycle d'ingestion est régulier. La durée de conservation peut être modifiée ultérieurement.

Après avoir effectué vos sélections, cliquez sur Next et vous êtes invité à confirmer votre région et votre durée



25231181211796

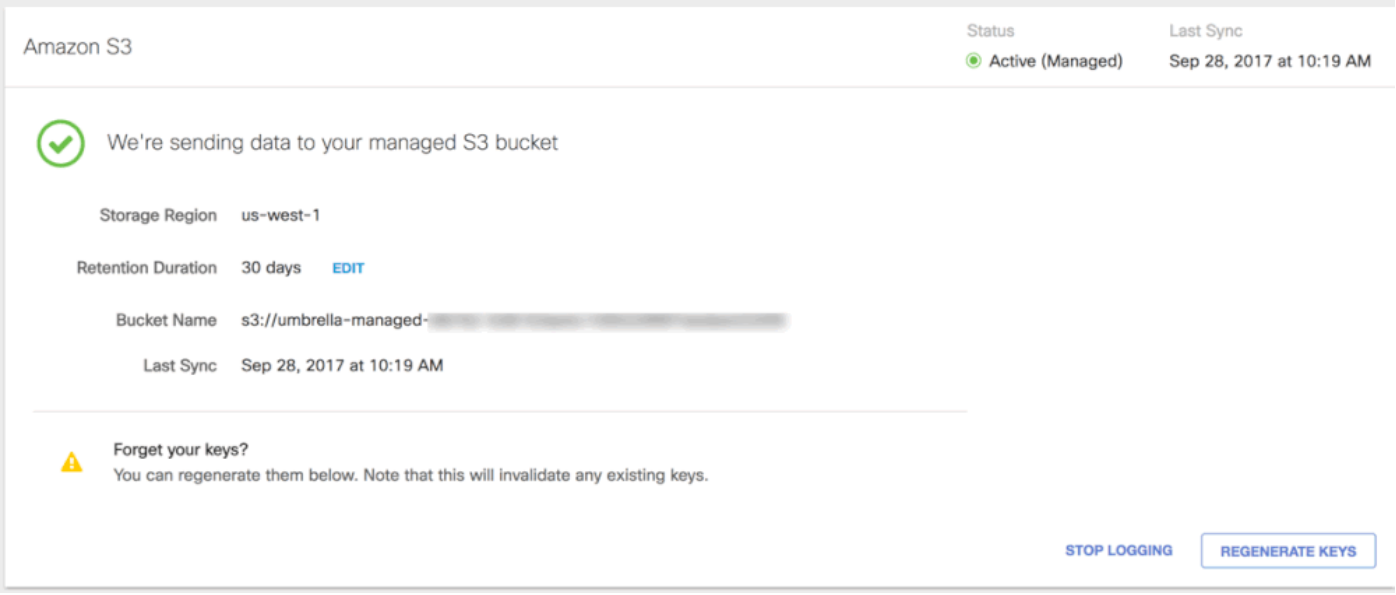
Une fois que vous avez accepté de continuer, vous recevez une notification d'activation.



25231181218708

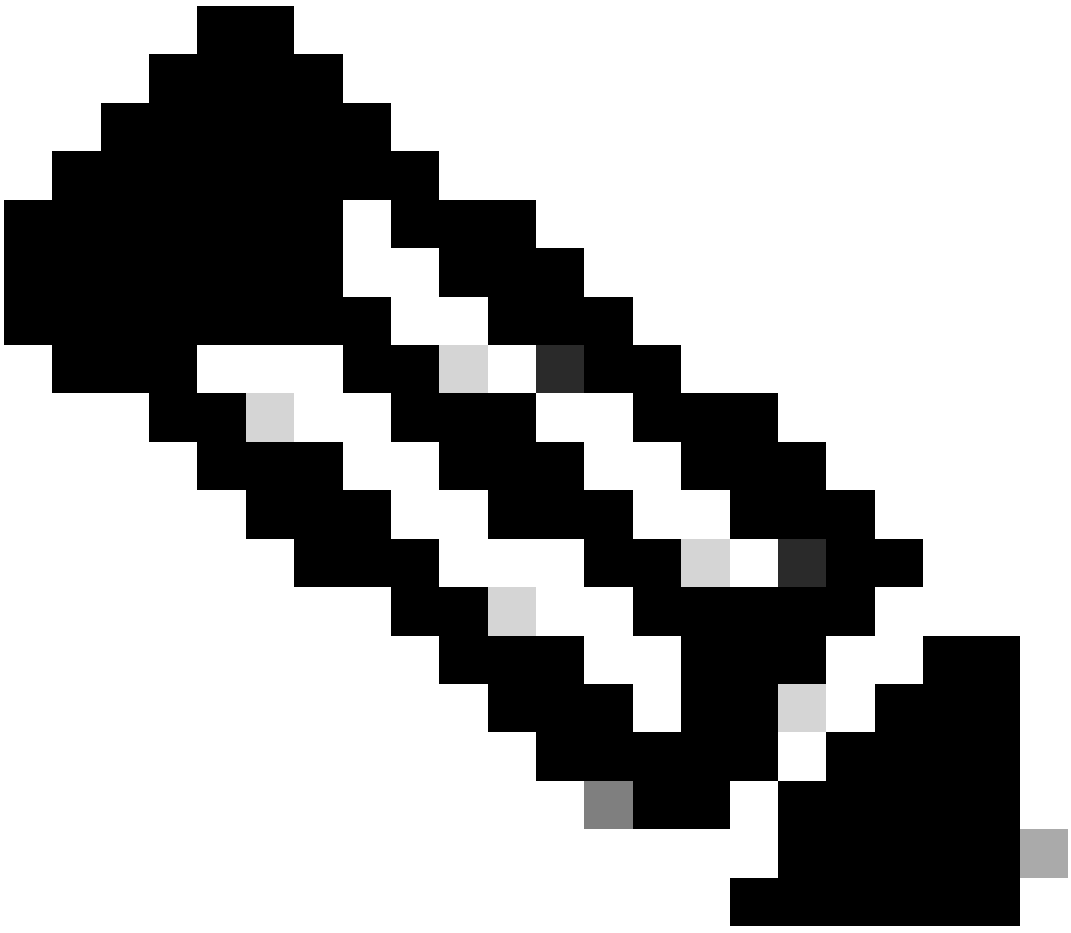
Vous recevez alors une clé d'accès et sa clé secrète. Vous devez accepter (cliquez sur « Obtenu ! ») car c'est la seule fois que vous voyez l'une ou l'autre des clés. Les clés d'accès et secrètes sont nécessaires pour accéder à votre bucket et télécharger vos journaux.

Enfin, l'écran récapitulatif affiche la configuration et, plus important encore, le nom de votre compartiment.



25231181228180

Vous pouvez activer ou désactiver la connexion à votre convenance.



Remarque : Cisco continue de purger les journaux en fonction de la durée de conservation sélectionnée, même si la journalisation a été désactivée.

Options de post-configuration

Échecs de chargement du journal

En cas d'échec du téléchargement des journaux de Cisco Umbrella vers votre compartiment S3, un délai de grâce de quatre heures s'écoule pendant lequel le service effectue une nouvelle tentative toutes les 20 minutes. Après quatre heures, un dossier est ouvert auprès de notre équipe d'assistance, qui commence une enquête sur la cause du problème et vous contacte de manière proactive pour vous informer du problème.

Vérification des journaux et du format téléchargés

Les journaux sont téléchargés à intervalles de dix minutes de la file d'attente des journaux Umbrella vers les compartiments S3. Une fois la configuration terminée, le premier journal est téléchargé dans votre compartiment S3 dans les deux heures, bien que le processus soit généralement immédiat ou presque immédiat. Cependant, le téléchargement de n'importe quel élément nécessite l'existence de données de journal nouvellement générées. Par conséquent, si vous essayez ceci dans un environnement de test, assurez-vous que les données réseau sont consignées dans la recherche d'activité.

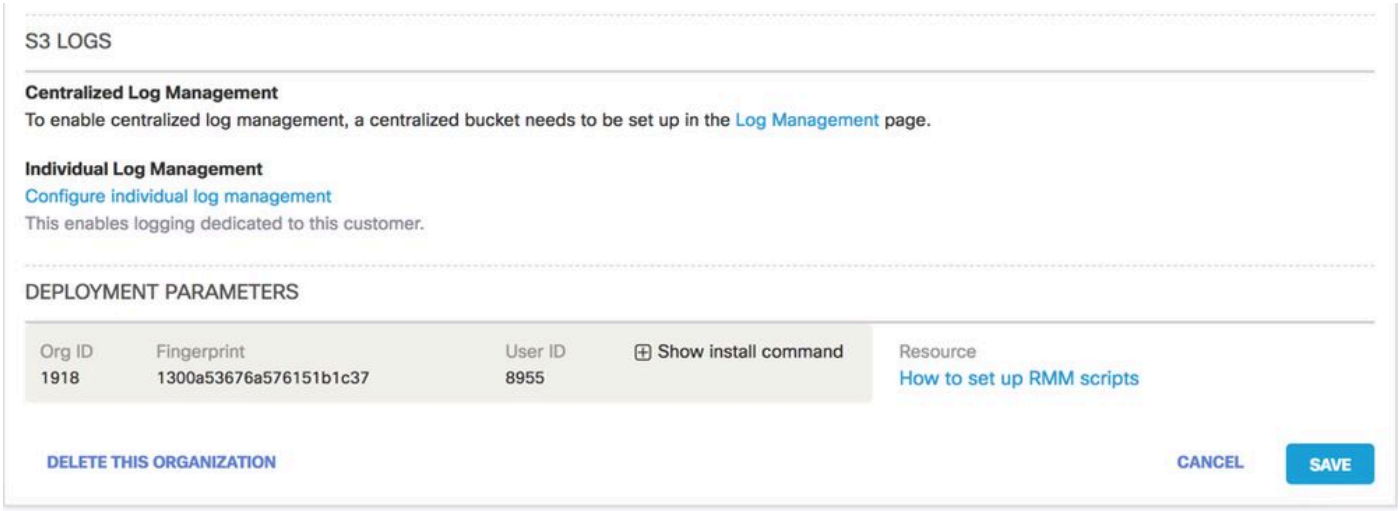
Pour vérifier si tout fonctionne, l'heure de la dernière synchronisation dans les mises à jour et les journaux du tableau de bord Umbrella commencent à apparaître dans votre compartiment S3.

Dans votre compartiment, chaque client ou organisation est étiqueté avec son ID d'organisation, de sorte que la structure de dossiers est :

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

<bucket-name> est le nom de votre bucket, <orgID> est l'ID de votre organisation et <subfolder> sont des dnslogs, des proxylogs ou des iplogs, selon les types de journaux qu'ils contiennent.

Pour les clients MSP et MSSP, l'orgID correspond à celui de la section Paramètres du client sous chaque détail client dans la section Paramètres de déploiement. Les clients multi-organisations peuvent collecter l'orgID en se connectant à chaque sous-organisation et en notant l'orgID dans l'url du navigateur : (https://dashboard.umbrella.com/o/#####/).



360002271623

Actuellement, la version du format de journal pour les clients MSP, MSSP et Multi-org est la version 1.1. Les journaux apparaissent dans un format GZIP et sont téléchargés dans les compartiments S3 dans le sous-dossier approprié avec ce format d'attribution de noms :

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

<sous-dossier> est dnslogs, proxylogs ou iplogs, selon les types de journaux qu'il contient. <xxxx> est une chaîne aléatoire de quatre caractères alphanumériques, qui empêche l'écrasement des noms de fichiers en double.

Exemple :

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

Si vous ne voyez pas de journaux dans votre bucket dans les 10 minutes, veuillez contacter le support décrivant les étapes que vous avez prises jusqu'à présent.

Une fois que les journaux apparaissent, nous vous recommandons de vérifier les données en décompressant le contenu des premiers chargements de journaux reçus pour vous assurer que les données sont visibles dans un éditeur de texte (ou même Microsoft Excel, souvent la valeur par défaut pour .CSV). Pour plus d'informations sur la représentation de chaque champ dans le journal, cliquez ici.

En cas d'échec d'un chargement de journal de Cisco Umbrella vers votre compartiment S3, le service effectue une nouvelle tentative toutes les 20 minutes pendant un délai de grâce de quatre heures. Après quatre heures, un dossier s'ouvre au sein de notre équipe d'assistance, qui commence une enquête sur la cause du problème et vous contacte de manière proactive pour vous informer du problème.

Activer la connexion par client.

Cette fonctionnalité est activée dès la livraison pour tous les clients, sauf indication contraire. La fonctionnalité peut être désactivée pour les clients individuels, ce qui est utile si vous avez différents niveaux de service pour les clients qui ont la fonctionnalité. Il se trouve sous chaque client et ses paramètres dans la console. La capture d'écran de la section précédente montre la bascule permettant de la désactiver.

Il est également possible de créer des utilisateurs IAM dans Amazon et d'affecter ces utilisateurs IAM à des sous-dossiers orgit is individuels du bucket. Ainsi, vous pouvez autoriser un utilisateur final à accéder à ses journaux, mais uniquement à ses journaux.

Téléchargement des journaux, Présentation du format et de l'intégration Splunk / QRadar

Afin de télécharger les journaux pour la rétention ou la consommation, il y a quelques approches pour télécharger les journaux DNS à partir de S3. Weit Vista a créé un article décrivant quelques approches à ce problème ici.

Vous pouvez également vous poser quelques questions sur le format du journal et sur sa différence par rapport aux journaux affichés dans le tableau de bord Umbrella. Pour plus d'informations sur le format de journal exporté, lisez cet article.

Enfin, l'une des principales utilisations de l'exportation des journaux DNS est l'intégration aux outils SIEM. Bien que la configuration d'un SIEM lors de l'utilisation de journaux comme celui-ci puisse souvent revenir à un administrateur, il s'agit de préférences personnelles, nous avons quelques conseils pour les SIEM les plus populaires.

Pour plus d'informations sur la configuration du plug-in Splunk pour Amazon AWS S3 et Umbrella, cliquez ici.

Pour plus d'informations sur la configuration d'IBM QRadar pour extraire les journaux d'Amazon S3 et les digérer, lisez ici.

Quelle est la taille des journaux S3 ?

La taille de vos journaux S3 dépend du nombre d'événements qui se produisent, qui dépend du volume de votre trafic DNS.

Vous pouvez trouver le format de journal pour la journalisation de S3 ici.

L'entrée d'exemple est de 220 octets, mais la taille de chaque ligne de journal varie en fonction d'un certain nombre d'éléments (longueur du nom de domaine, nombre de catégories, etc.). En supposant que chaque ligne de journal comporte 220 octets, un million de requêtes feraient 220 Mo.

Pour obtenir une estimation du nombre de requêtes DNS vues chaque jour :

1. Dans le tableau de bord Umbrella, accédez à Reporting > Activity Search.
2. Sous Filters, exécutez un rapport pour les dernières 24 heures, puis cliquez sur l'icône Export CSV.
3. Ouvrez le fichier .csv téléchargé. Le nombre de lignes (moins un pour l'en-tête) est le nombre de requêtes DNS par jour ; multipliez cette valeur par 220 octets pour obtenir l'estimation pour une journée.

En termes de coût, bien qu'il soit variable, nous constatons que même nos clients les plus volumineux dépensent seulement quelques dollars par mois pour le service. Un coût est lié au temps de stockage et un autre au téléchargement de données de S3 dans votre environnement. Consultez Amazon pour plus de détails.

Comme pour toutes nos fonctionnalités, nous sommes ravis de savoir ce que vous en pensez, en particulier en ce qui concerne les intégrations SIEM ou toute autre question supplémentaire traitée dans cette documentation. Si vous avez des commentaires, n'hésitez pas à nous les faire savoir !

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.