通过Amazon S3服务了解面向MSP、MSSP和多组织客户的集中式伞状日志管理

目录

简介

本文档介绍使用Amazon S3服务为MSP、MSSP和多组织客户进行集中式Umbrella日志管理。

概述

MSP、MSSP和多组织控制台能够在云存储中存储您的离线客户的DNS、URL和IP日志。存储位于Amazon S3中，并且日志上传后，可以出于合规性原因或安全分析而下载并保留它们。

此文档可帮助您了解此功能，在Umbrella控制面板和Amazon S3控制台中对其进行设置，并运行多个配置选项，包括您希望在S3中保留日志的持续时间。

Umbrella for MSP、MSSP和Multi-Org都能够从控制台的子组织上传流量活动日志并将这些日志存储在云中。Amazon的AWS S3(Simple Storage Service)是一项用于归档日志的服务，有时也称为it isoffline storage it is or it islog retention。它是

存档日志可能有用，原因有多种，具体取决于您的需要。对于某些人，可以将导出和存档的日志导入到数据分析或安全调查工具（如SIEM）中。对于其他人来说，活动日志的存档对于安全事件下的数据调查分析或人力资源记录非常有用。

AWS S3以CSV格式将日志存储在压缩(gzip)存档中。由于日志每十分钟上传一次，因此来自您的网络的网络流量之间至少存在十分钟的延迟，这些流量由Umbrella记录，然后可从S3下载。

控制台中的orgID号

每个客户组织都使用控制台中的orgID号单独上载其日志，以将每个客户映射到文件夹。也可以按每个客户/每个组织启用或禁用此功能。

两种类型的Umbrella日志管理

日志管理通过将日志上传到称为it isbucketit is（基本上是AWSit is S3环境中的文件夹）来执行。 有两种方法可为Umbrella日志托管存储桶：

- 由您（公司管理人）管理、管理和付费。
- 由Cisco Umbrella管理、管理和支付。

让思科管理您的S3存储桶有优缺点。

思科管理您的存储桶的优点：

- 非常易于设置。只需几分钟，之后便极易管理。
- Umbrella的许可证成本中包含Cisco bucket-management，有效地使服务免费。尽管拥有自己的桶会增加成本，但管理另一张账单的间接成本可能过高。

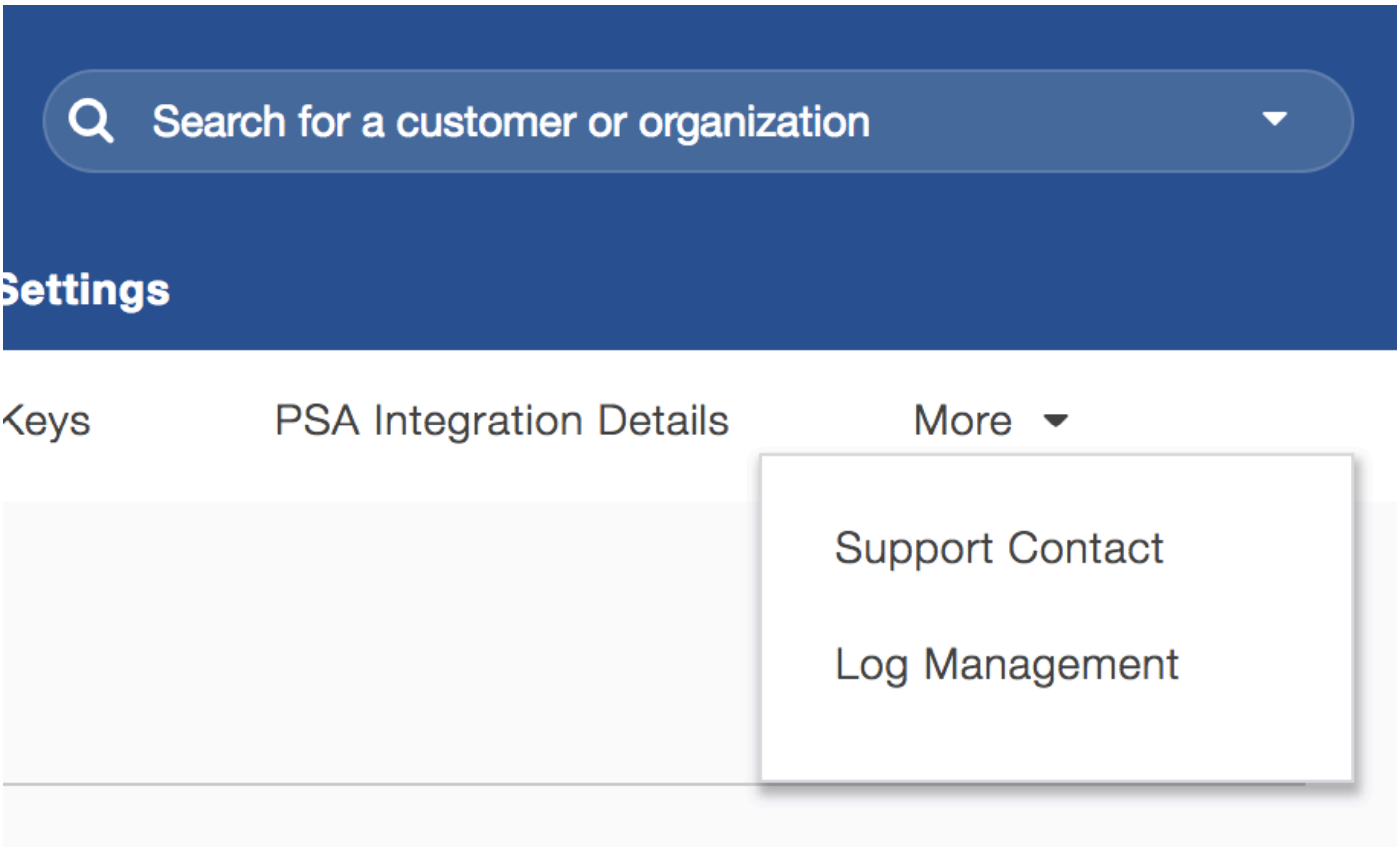
自己管理S3实例的优点：

- 脱机存储数据的时间没有限制。思科将离线存储限制为最多30天。
- 您可以将任何内容添加到存储桶，包括Umbrella中的日志文件，这样存储桶也可被其他应用程序使用。
- 您可以直接从Amazon获得高级配置支持，例如自动化或命令行帮助。

对于大多数客户来说，维护存储桶的成本非常低廉，但事实证明非常麻烦。

入门指南

在Console的Settings > Log Management下可以找到Log Management功能（您可以点击下拉箭头）。



115012963103

配置自我管理的S3存储桶

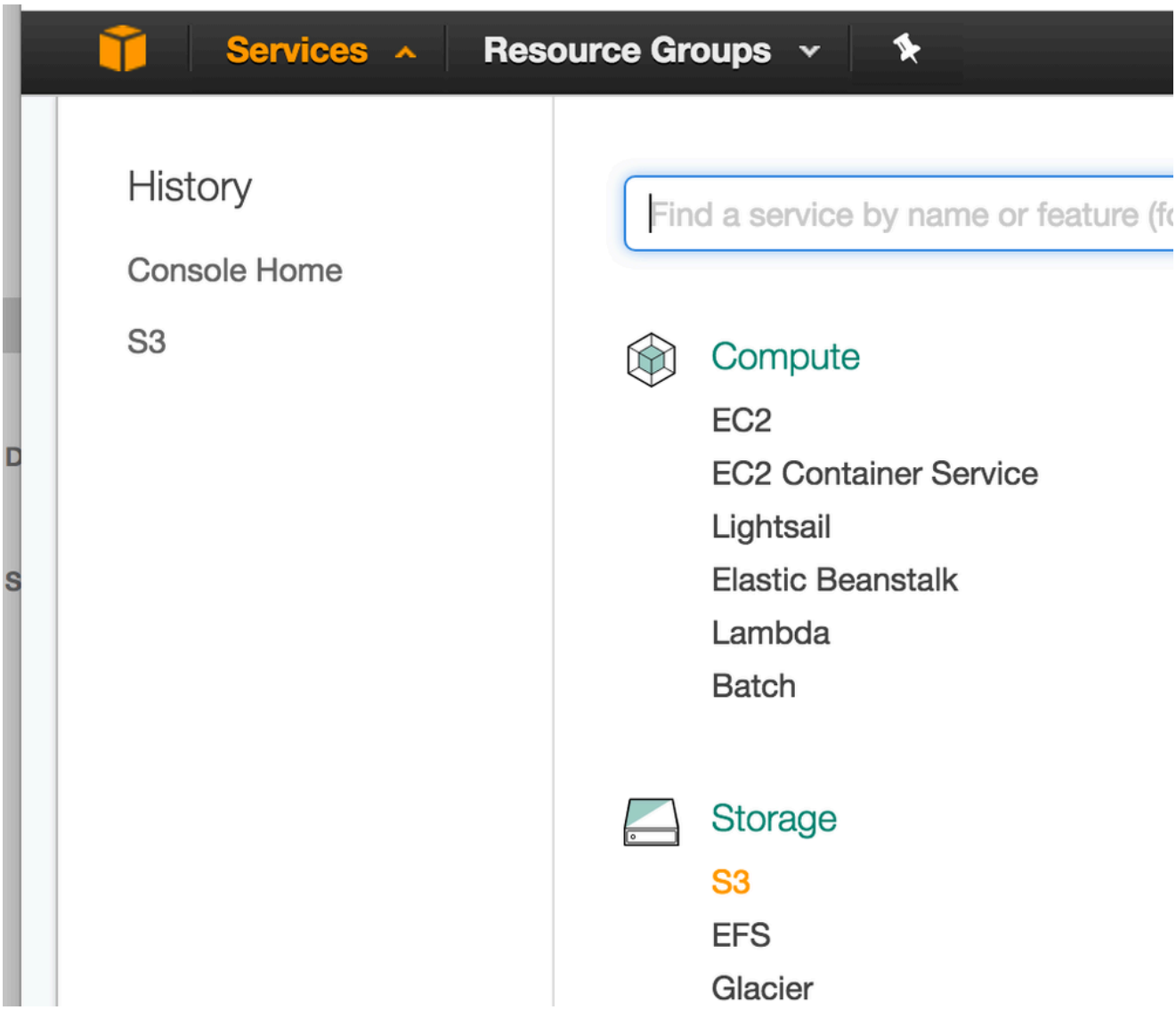
先决条件

要归档日志，必须满足以下要求：

- 对Cisco Umbrella MSP、MSSP或多组织控制台的完全管理访问权限。
- 登录Amazon AWS服务(https://aws.amazon.com/console/)。如果您拥有帐户，Amazon会为S3提供免费注册。但是，如果您的使用超过免费计划使用，则需要使用信用卡。
- 在Amazon S3中为日志存储配置的数据桶。有关配置和设置Amazon S3存储段的说明，请参阅下一节。

设置Amazon S3存储桶

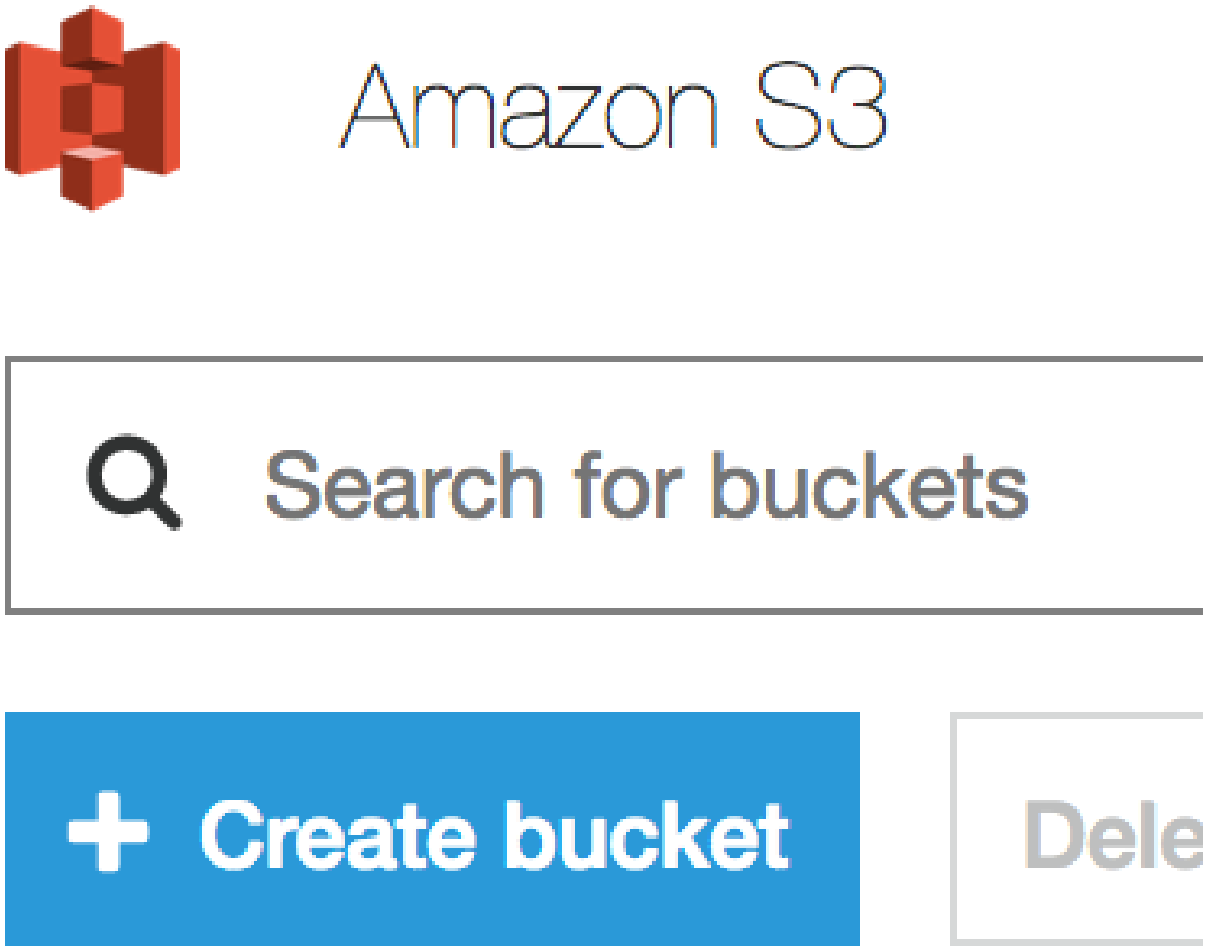
1. 首先登录AWS控制台，然后从Storage下的选项列表中选择“S3”。



115012842106

2. 您会看到欢迎您加入Amazon Simple Storage System的简介屏幕

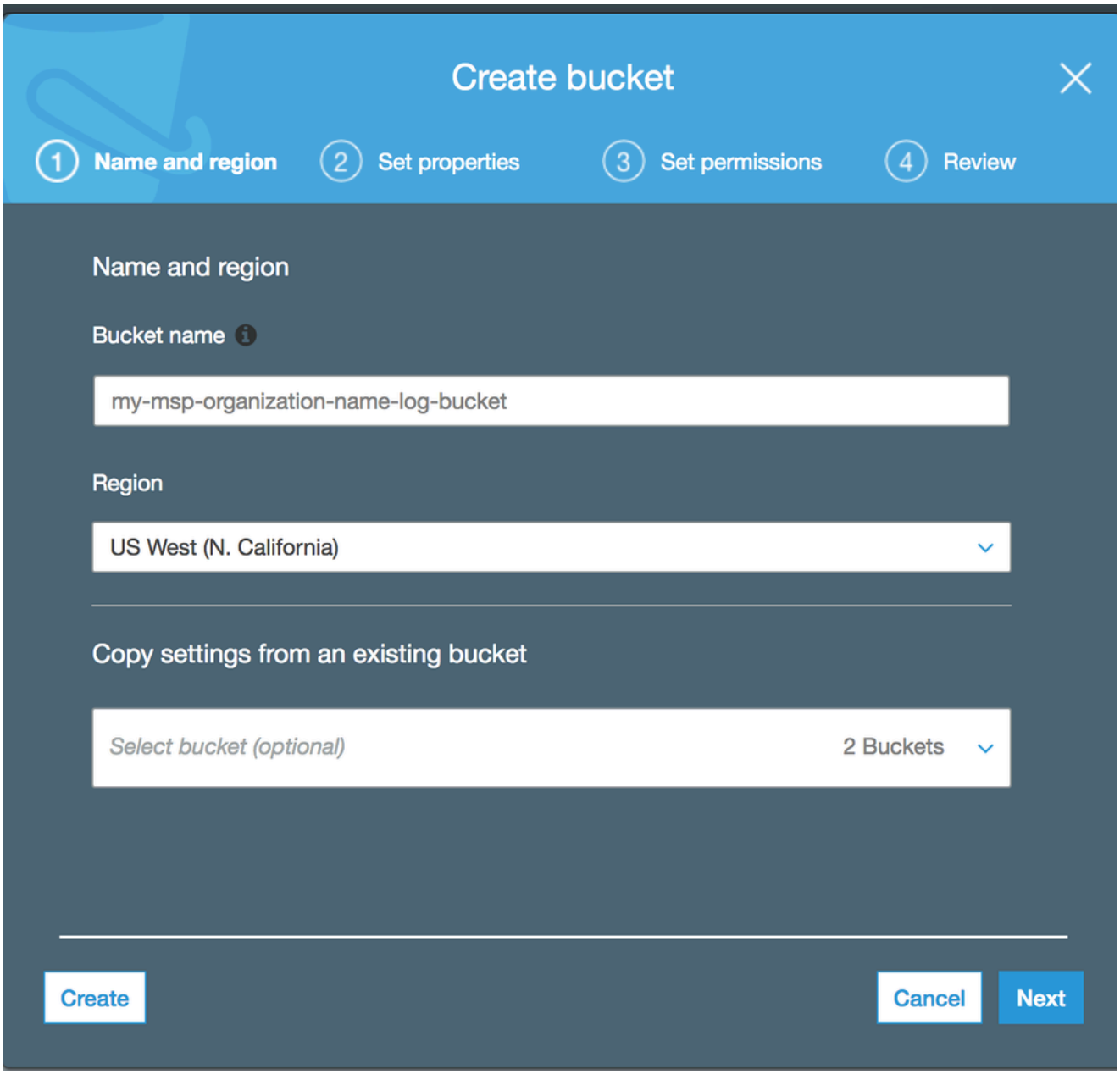
3. 接下来，如果您还没有存储桶，则希望创建一个存储桶。点击 创建存储桶



115012842326

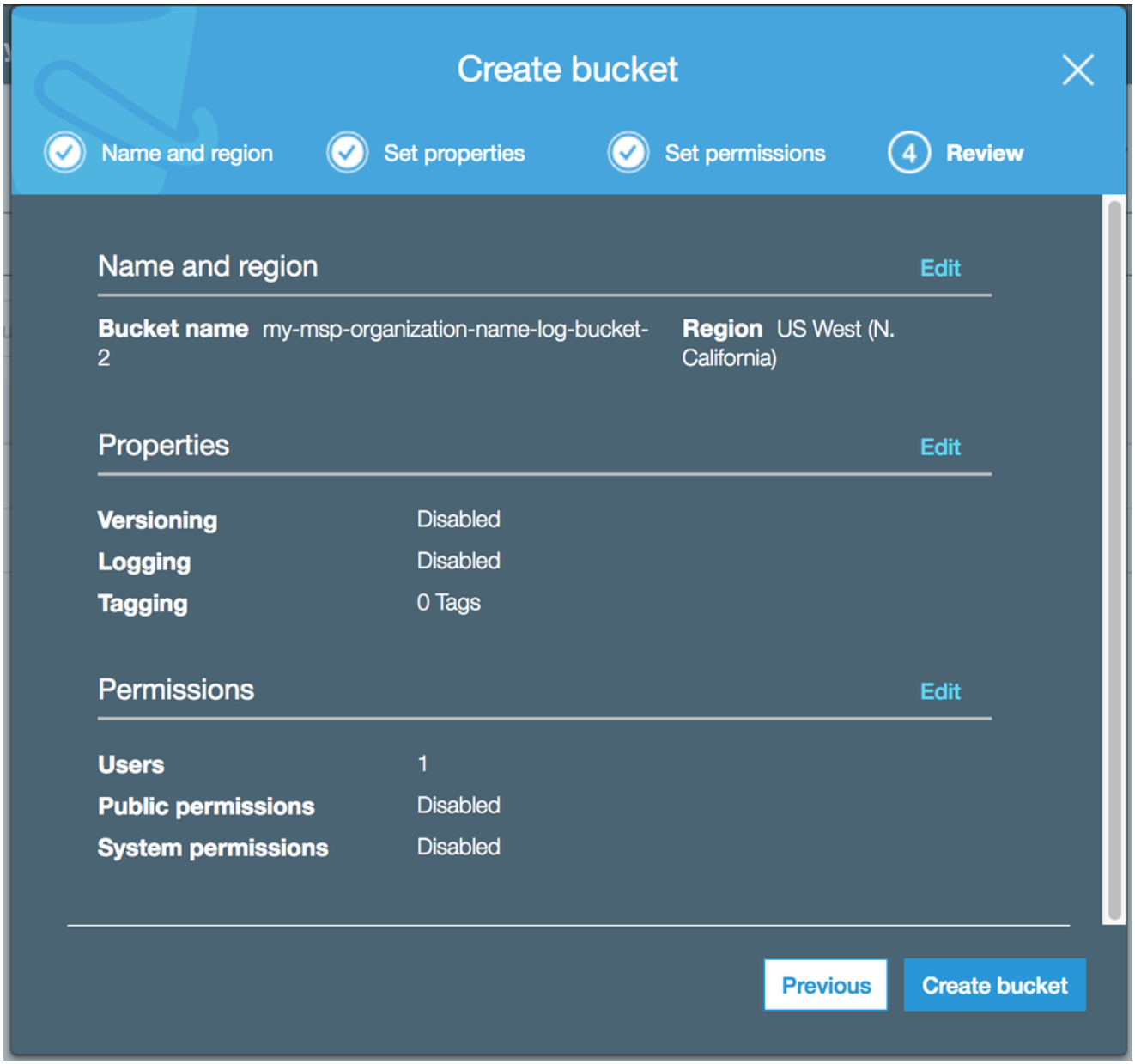
.

4. 首先输入时段名称
   存储桶名称必须是普遍唯一的，不仅对您的AWS或Umbrella是如此，对所有Amazon AWS也是如此。使用个人信息(如“my-organization-name-log-bucket”)可以帮助您绕过通用唯一存储桶名称的要求。桶名称只能使用小写字母，不能包含空格或句点，并且必须符合DNS命名约定。有关名称限制的详细信息，请阅读此。有关桶创建的详细信息，包括命名，请阅读此处。



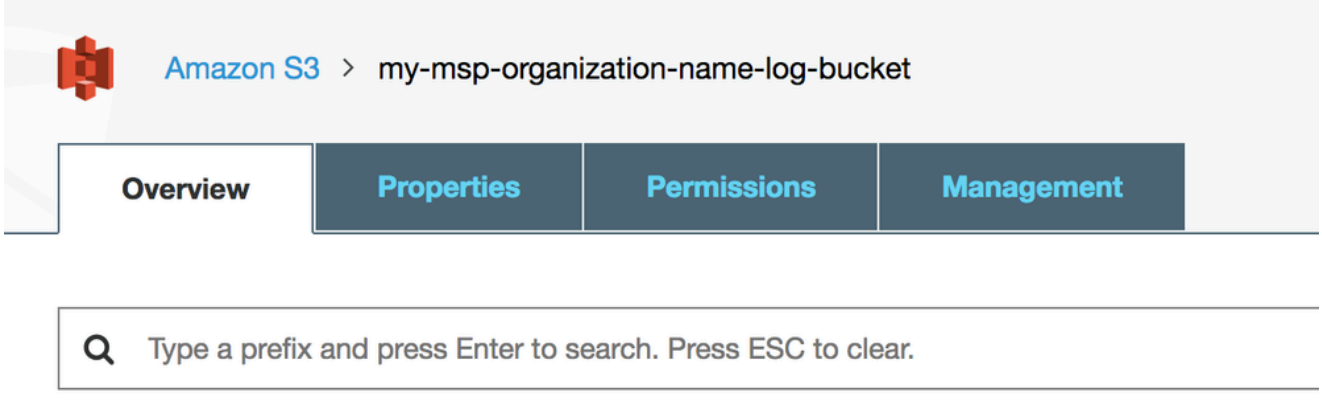
115013010503

5. 选择最适合您所在位置的区域，然后单击Create。请勿从另一个存储桶复制设置
6. 在“设置属性”步骤中，单击下一步。这些可在以后调整
7. 在“设置权限”步骤中，只需单击下一步。我们稍后将重新访问权限，以设置存储段以供上传
8. 完成审核流程，然后单击 创建存储桶



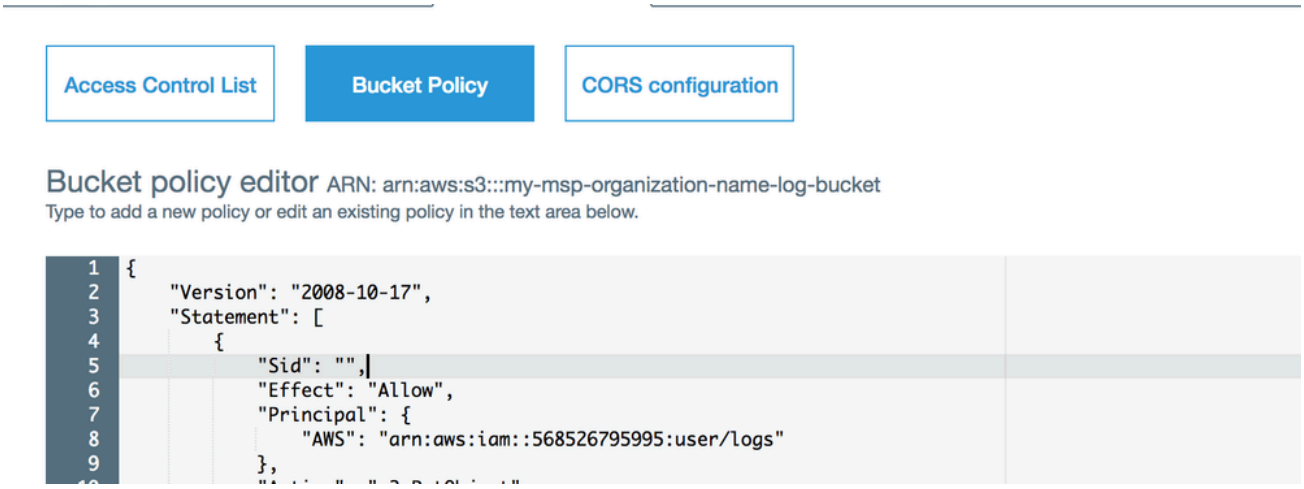
115012842686

9. 接下来，您需要配置存储桶以接受来自Umbrella服务的上传。在S3中，这称为桶策略。单击新配置存储桶的名称，然后选择界面顶部的Permissions选项卡



115012842906

10. 选择Bucket Policy，然后系统将提示您粘贴到桶中



115012843006

11. 将下面包含桶策略的JSON字符串复制并粘贴到文本编辑器中，或者直接将其粘贴到窗口中。在下面指定bucketname的位置替换确切的bucketname。如果未能执行此操作，则会出现错误消息

{
"版本":"2008-10-17",
"声明":[
{
"Sid":"",
"效果":"允许",
"主体":{
“AWS”："arn:aws:iam::568526795995:user/logs"
},
"操作":"s3:PutObject",
"资源":"arn:aws:s3:::bucketname/*"
},
{
"Sid":"",
"效果":"拒绝",
"主体":{
“AWS”："arn:aws:iam::568526795995:user/logs"
},
"操作":"s3:GetObject",
"资源":"arn:aws:s3:::bucketname/*"
},

{
"Sid":"",
"效果":"允许",
"主体":

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

,
"操作":"s3:GetBucketLocation",
"资源":"arn:aws:s3:::bucketname"
},

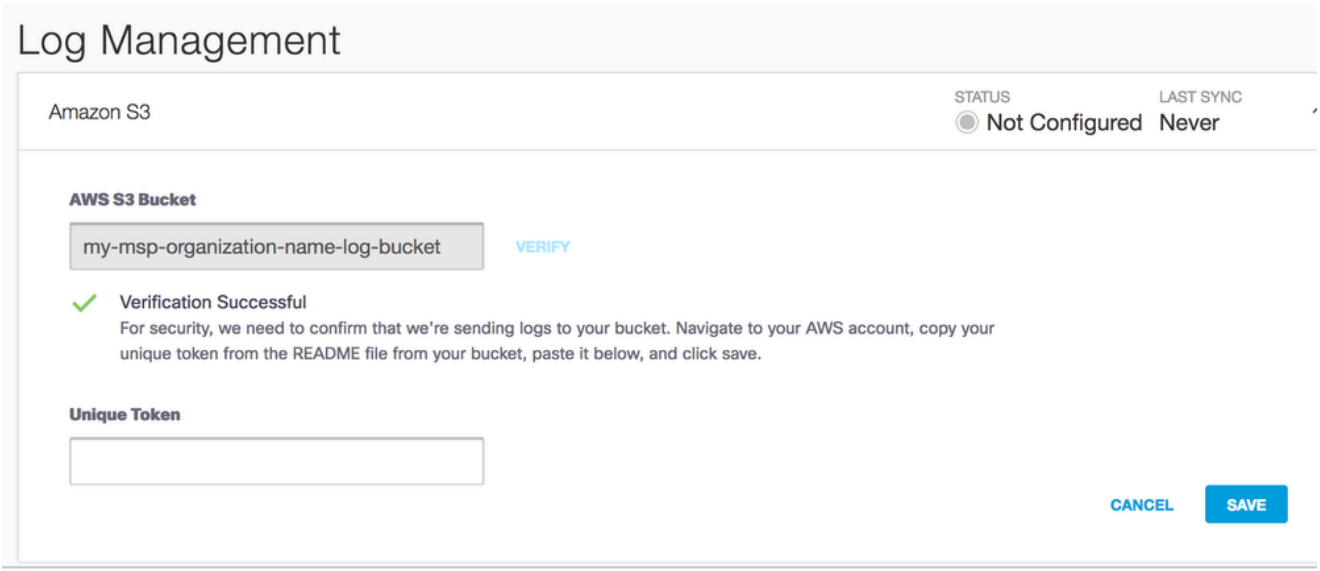
{
"Sid":"",
"效果":"允许",
"主体":{
“AWS”："arn:aws:iam::568526795995:user/logs"
},
"操作":"s3:ListBucket",
"资源":"arn:aws:s3:::bucketname"
}
]
}

12.单击Save确认此更改

验证您的Amazon S3存储桶

步骤 1：

1. 返回到Umbrella控制台并导航到设置>日志管理
2. 点击“Amazon S3”展开窗口
3. 在Bucket Name字段中，键入或粘贴您在S3中创建的确切桶名称，然后点击Verify
   您会在控制面板中收到一条确认消息，指示已成功验证存储桶。



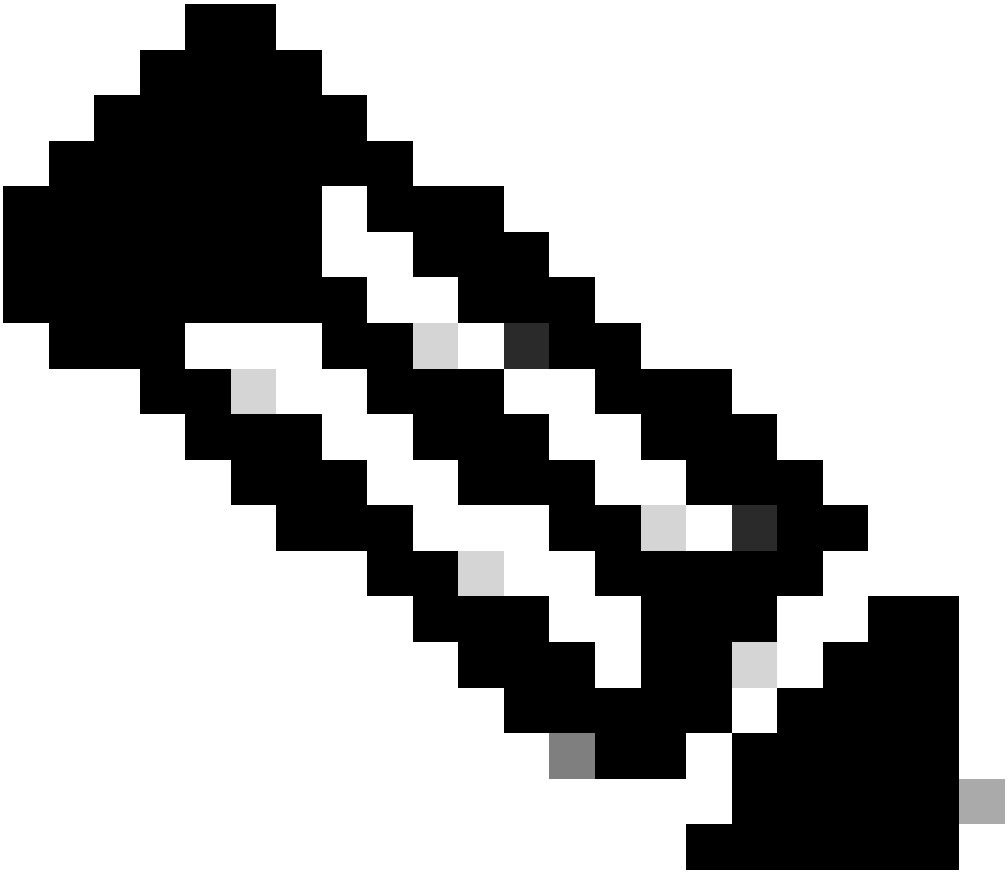
115012847146

如果您收到指示无法验证存储桶的错误，请重新检查存储桶名称的语法并检查配置。如果问题仍然存在，请向我们的支持部门反映问题

步骤 2：

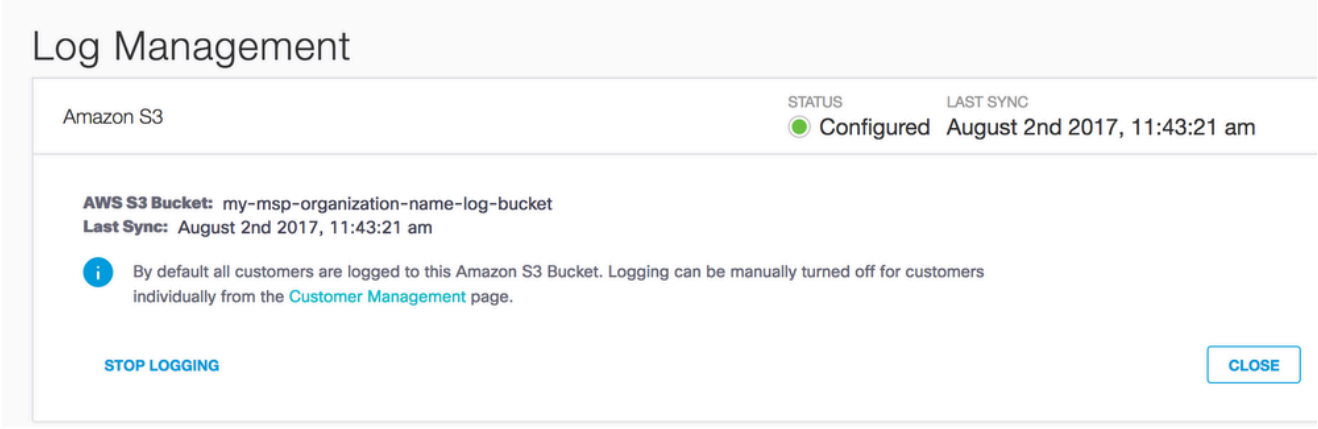
为确保指定了正确的存储桶，Umbrella会要求您输入唯一的激活令牌。可以通过重新访问您的S3存储桶来获取激活令牌。作为验证过程的一部分，一个名为README_FROM_UMBRELLA.txt的文件已从Umbrella上传到您的Amazon S3存储桶并显示。

1. 双击自述文件，然后在文本编辑器中将其打开，从而下载自述文件。在文件中，有一个唯一的令牌将您的S3存储桶绑定到Umbrella控制面板



注意：上传文件后，您可能需要在浏览器中刷新S3存储桶，才能查看README文件。

2. 返回到Umbrella控制面板并将令牌粘贴到标记为“Unique token”的字段中，然后单击Save。此时，配置为
完成。要查看您的配置，只需点击Log Management部分中的Amazon S3名称



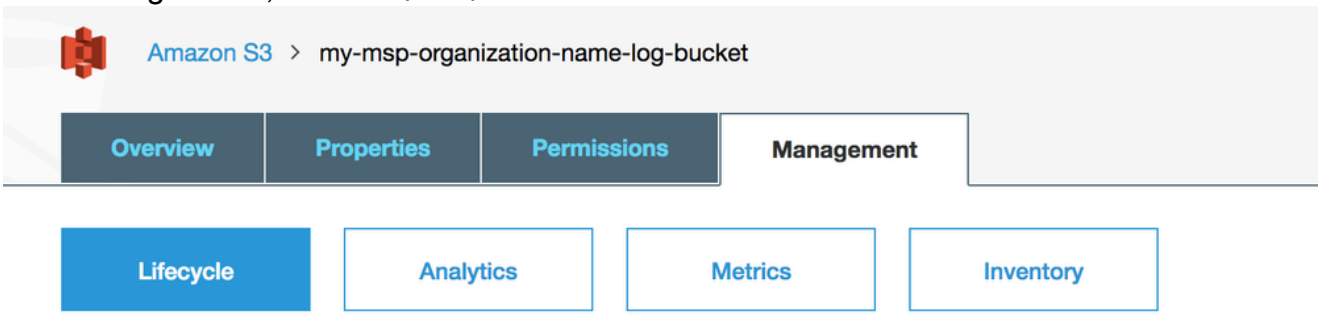
115012848126

管理日志生命周期

使用S3时，您可以管理存储桶中数据的生命周期，从而延长保留日志的时间。根据您使用外部日志管理的原因，持续时间可能很短或很长。例如，您只需在24小时后从S3存储桶下载日志，然后将其脱机存储，或者将日志无限期保留在云中。默认情况下，Amazon将数据无限期存储在存储桶中，但是无限存储确实会提高存储桶维护的成本。有关S3生命周期的详细信息，请阅读此处。

要配置存储桶的生命周期，请执行以下操作：

1. 选择Management，然后单击 生命周期



115012848246

2. 单击Add a Rule，然后单击Apply the Rule to the whole bucket（或子文件夹，如果已进行相应配置）。
3. 选择对对象执行的操作（例如Delete或Archive），然后选择时间段以及是否希望使用Glacier存储来帮助降低Amazon成本。（Glacier是iscoldit是离线存储，虽然访问速度较慢，但成本较低。）

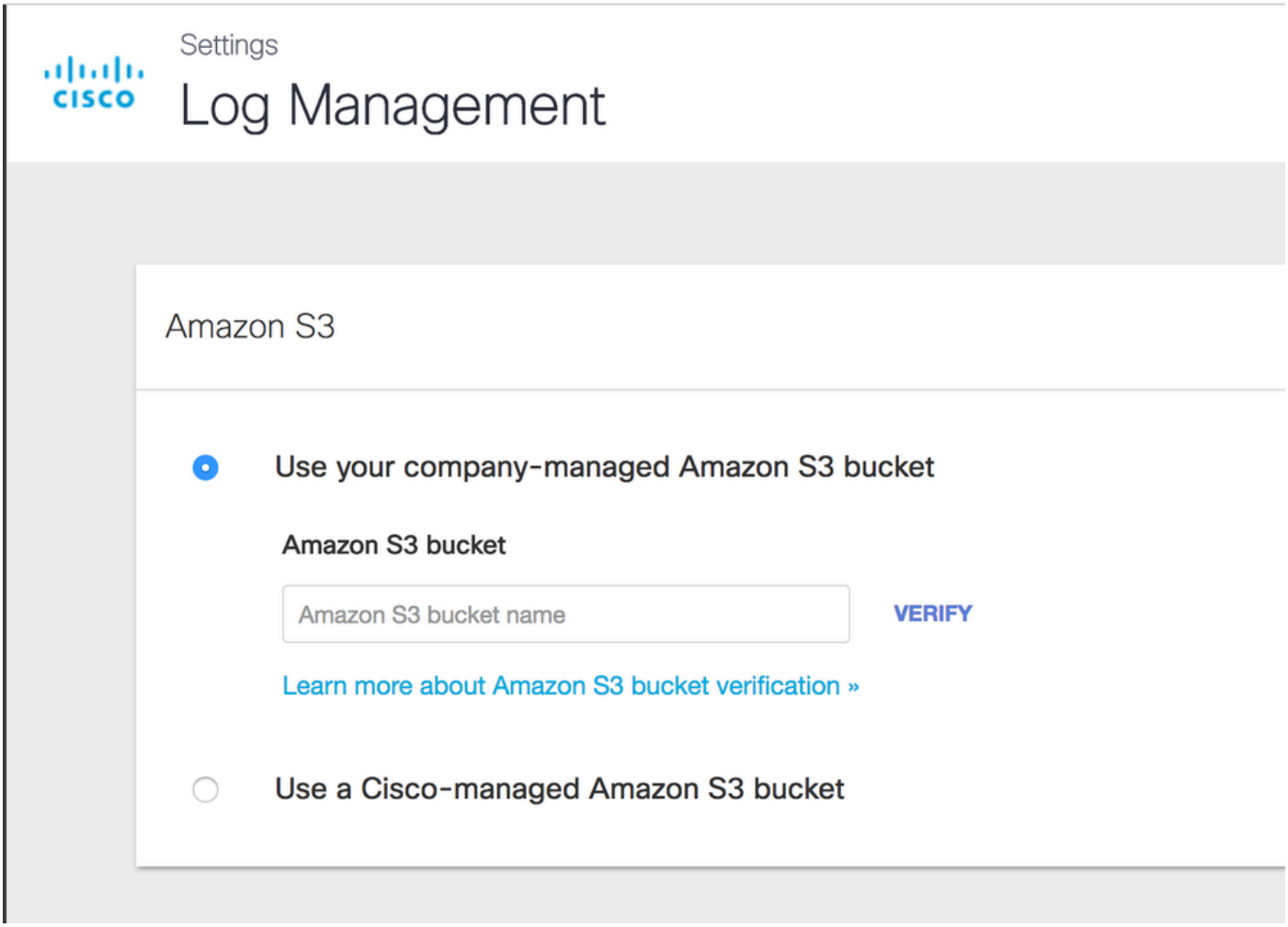
4. 如果您喜欢使用其他方法（如内部备份解决方案）管理日志，只需从S3下载日志并以其他方式保留它们，然后将保留时间设置为几天。

配置思科管理的S3存储桶

在Umbrella控制面板中导航到设置>日志管理。

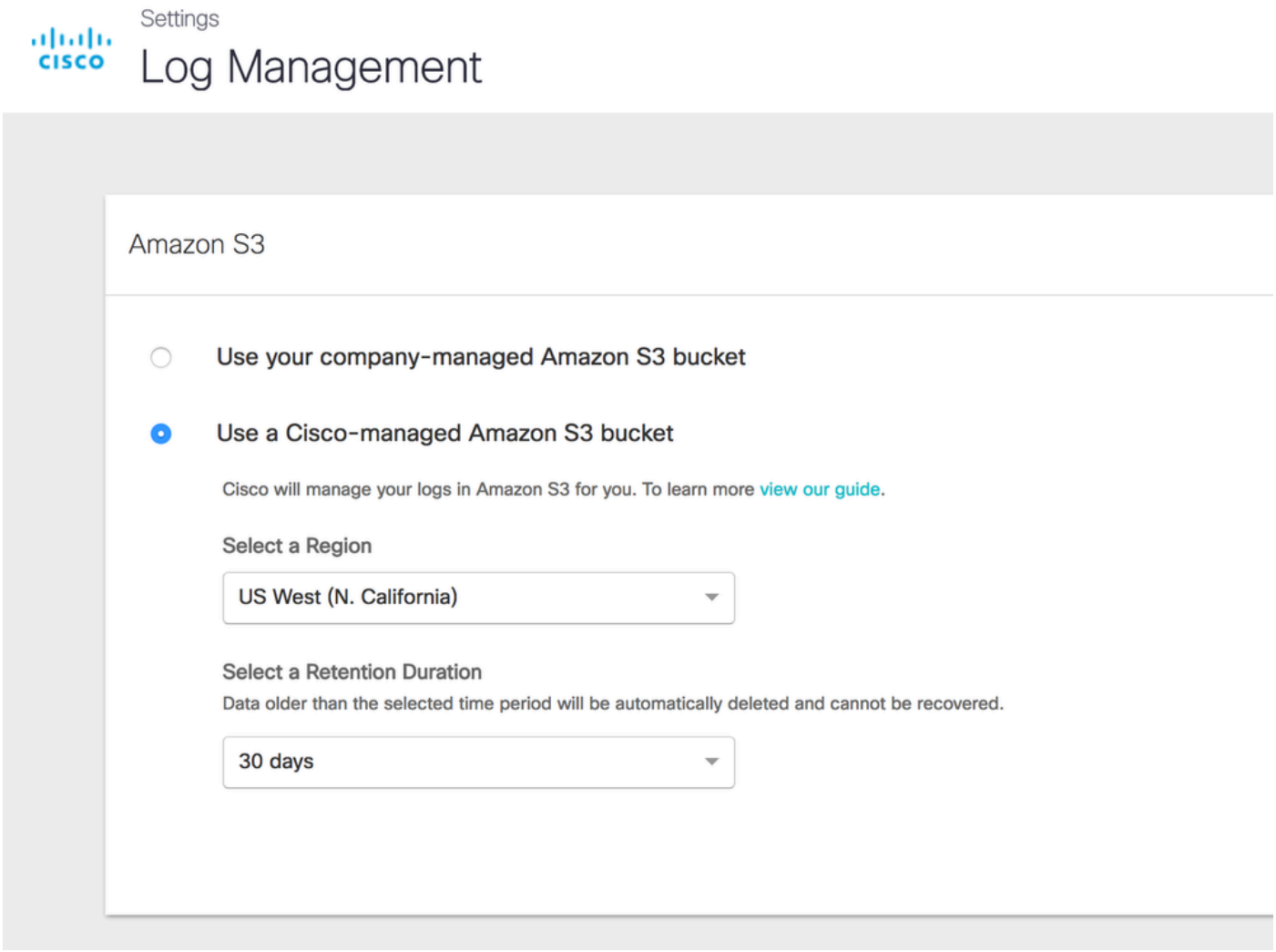
有以下两种选项：

- 使用您公司管理的Amazon S3存储桶
- 使用思科托管的Amazon S3存储桶



25231151138964

选择“使用思科托管的Amazon S3存储桶”，您将获得两个新选项：“选择地区”和“选择保留期限”。



252311511158036

选择区域

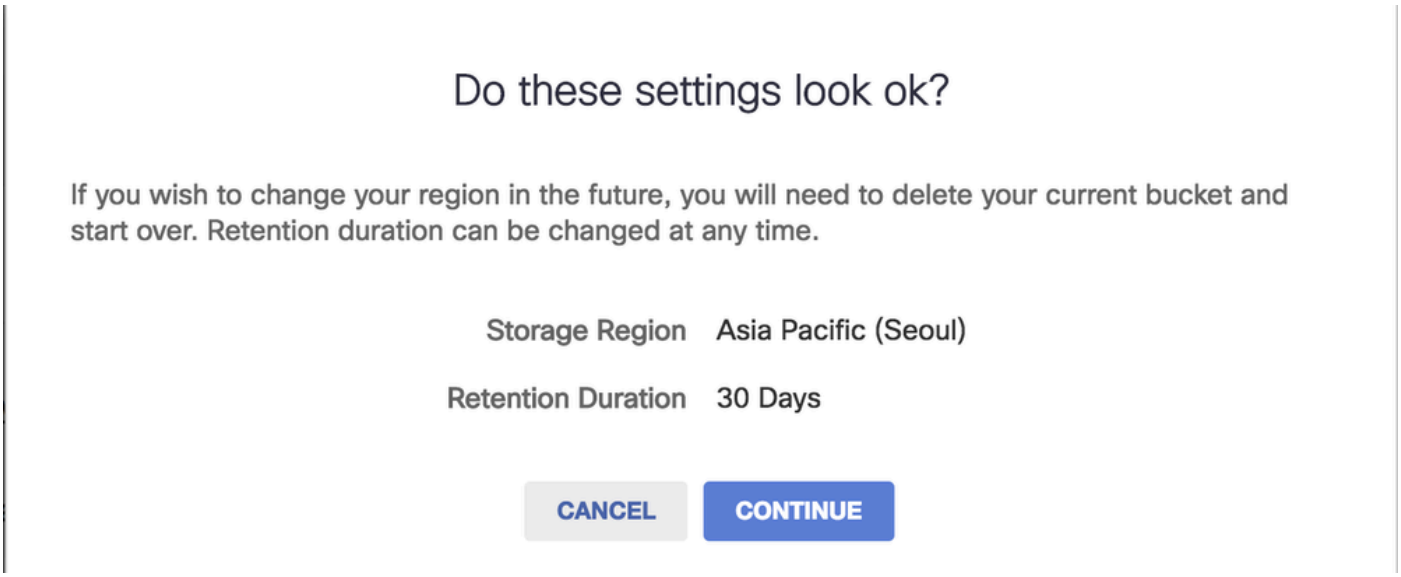
在将日志下载到您的服务器时，区域终端对于最大限度地减少延迟非常重要。列出的区域与Amazon S3中可用的区域匹配，但并非所有区域都可用。例如，中国未列出。

从下拉列表中选择离您最近的区域。如果您希望将来更改您的区域，您需要删除当前设置并重新开始。

选择保留持续时间

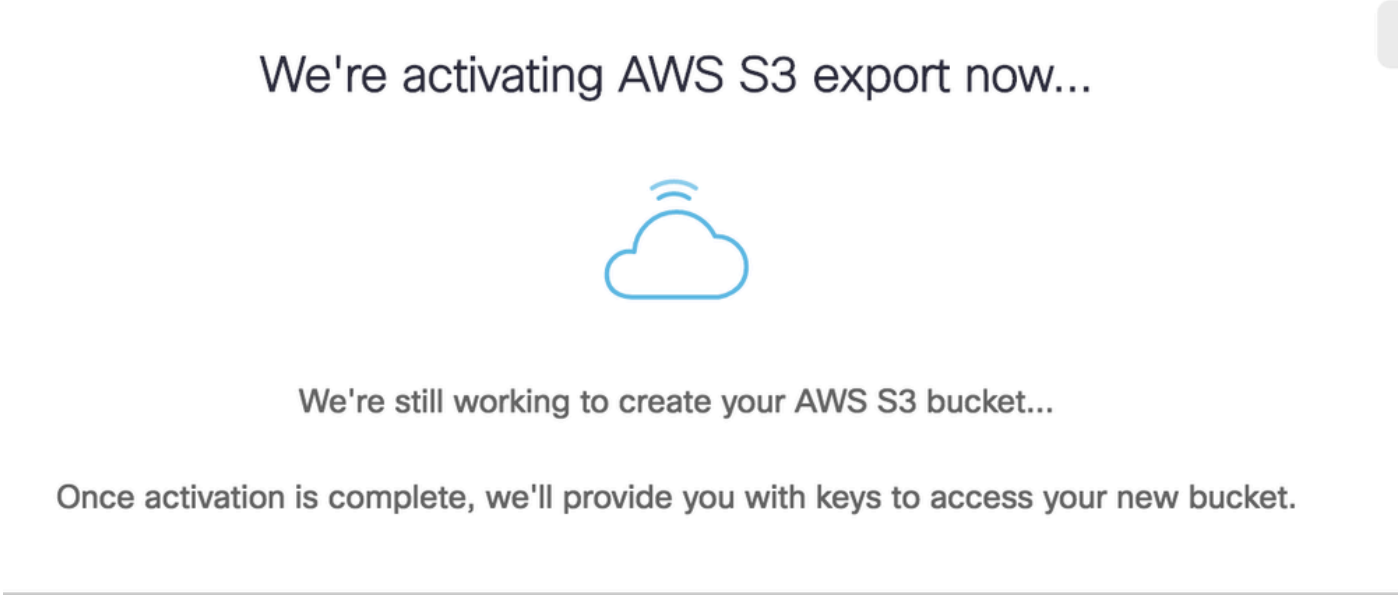
保留期仅为7、14或30天。在选定时间段后，所有数据都会被清除，无论什么数据都无法检索。如果你的摄取周期是正常的，我们建议缩短你的摄取周期。保留持续时间可以在以后更改。

做出选择后，单击Next，系统将提示您确认区域和持续时间



25231181211796

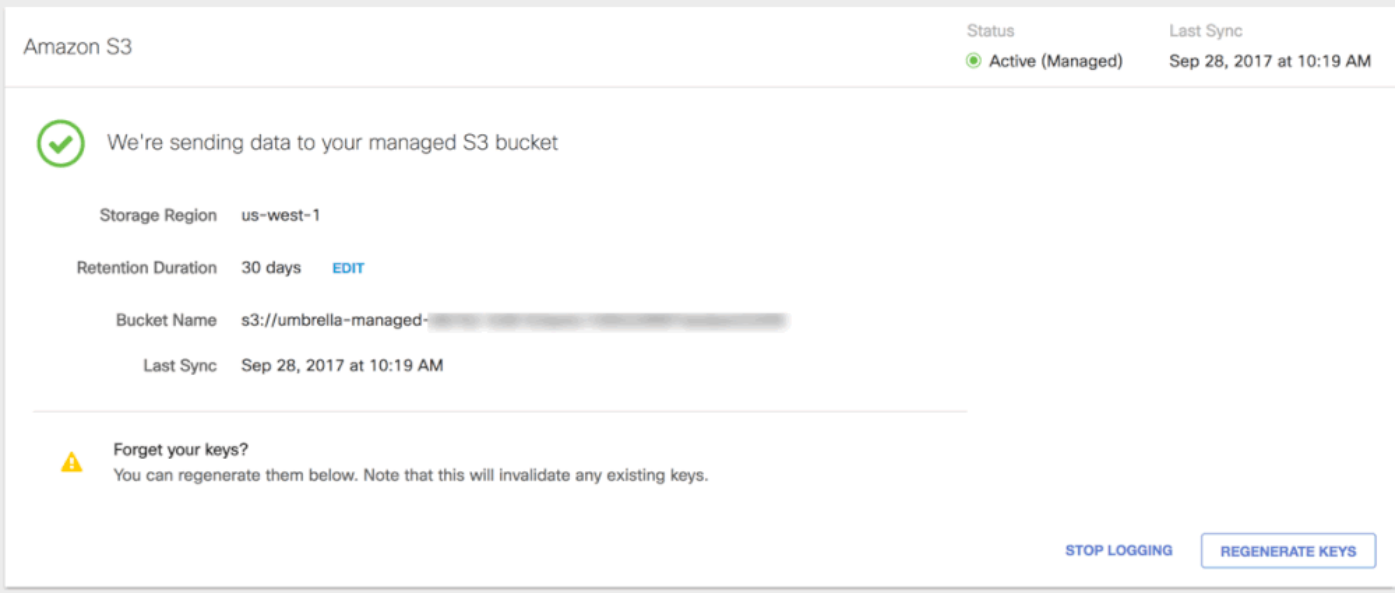
一旦您同意继续，您将收到激活通知。



25231181218708

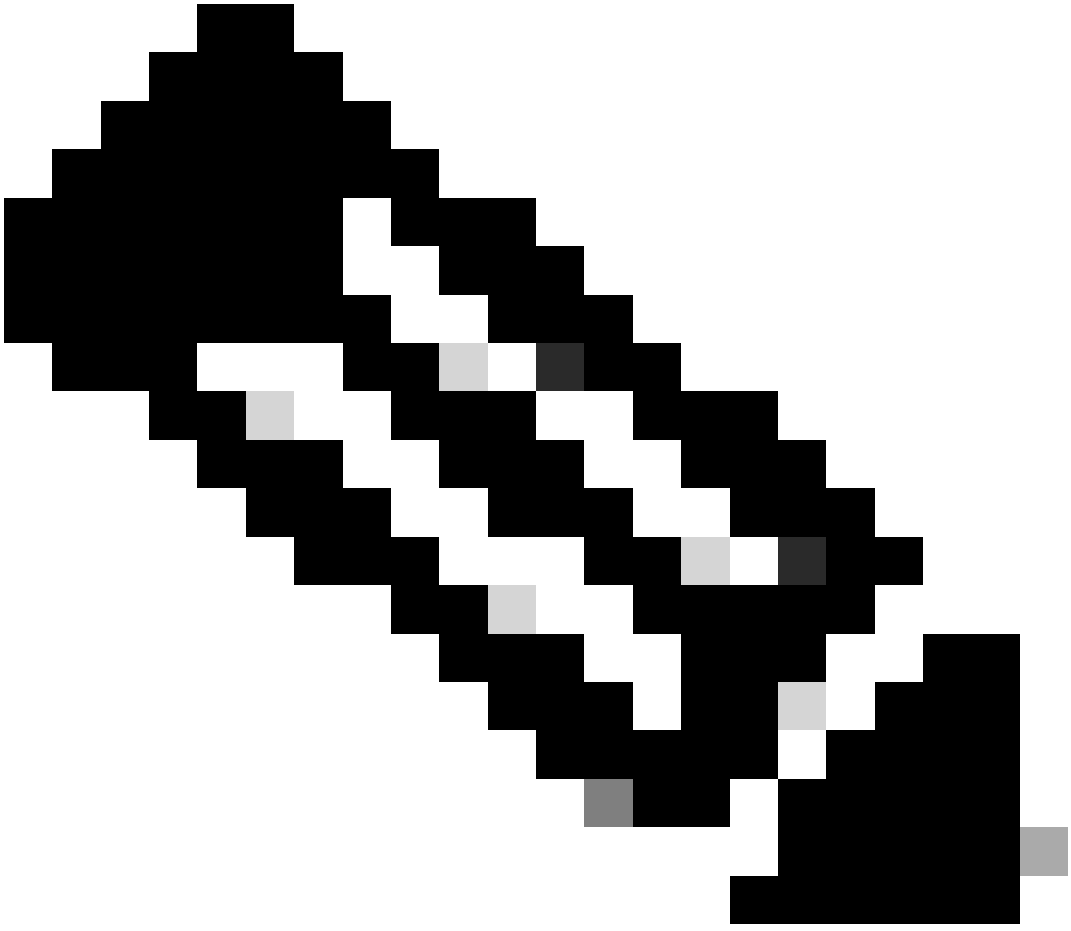
然后，您会收到访问密钥和密钥。您必须接受（单击“获得！”），因为这是您唯一能够看到其中一个密钥的时间。要访问存储桶并下载日志，需要访问密钥和密钥。

最后，您将看到显示配置的摘要屏幕，最重要的是，您的存储桶名称。



25231181228180

您可以在方便时打开或关闭登录。



注意：即使日志记录已关闭，思科仍会根据选定的保留持续时间继续清除日志。

配置后选项

日志上传失败

如果未能将日志从Cisco Umbrella上传到S3存储桶，服务将有4小时的宽限期，期间每20分钟重试一次。四个小时后，我们的支持团队将打开一个案例，他们会开始调查问题的原因，并主动联系您，以便让您知道问题。

检查上传的日志和格式

日志从Umbrella日志队列以10分钟的时间间隔上传到S3存储桶。完成配置后，第一个日志将在两小时内上传到S3存储桶，尽管此过程通常是立即或接近立即的。但是，上传任何内容都需要存在新生成的日志数据，因此，如果您在测试环境中尝试此操作，请确保网络数据正在活动搜索中记录。

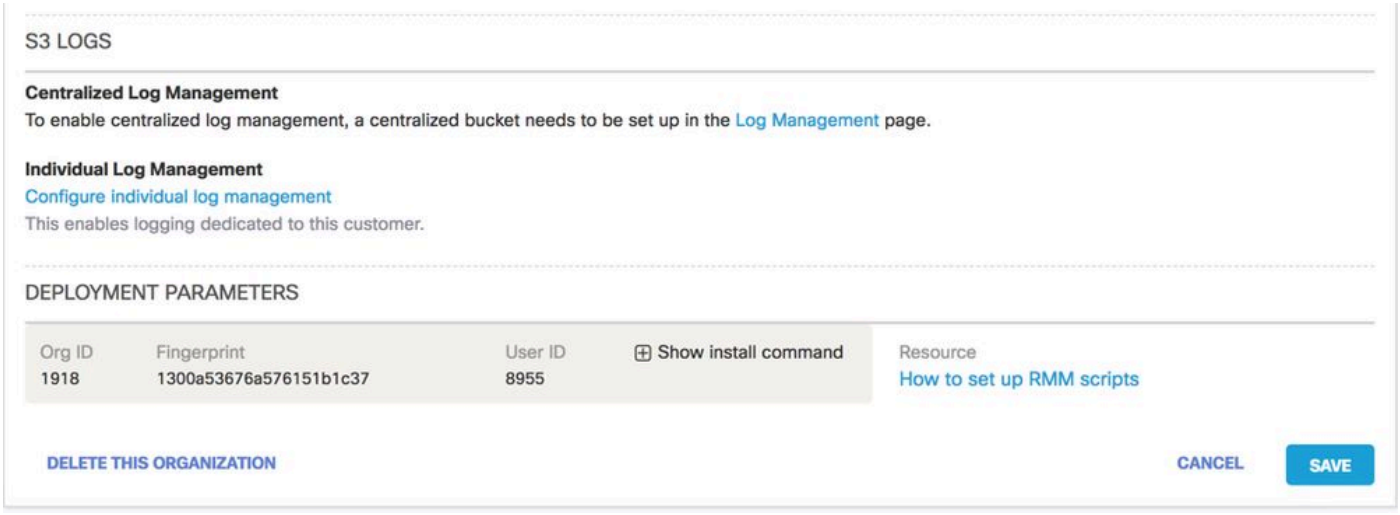
为了验证是否一切正常，Umbrella控制面板中的“上次同步”时间更新和日志开始显示在S3存储桶中。

在时段内，每个客户或组织都标有组织ID，因此文件夹结构为：

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

<bucket-name>是您的存储桶名称，<orgID>是您的组织，它是ID，<subfolder>是dnslogs、proxylogs或iplogs，具体取决于中的日志类型。

对于MSP和MSSP客户，orgID与“部署参数”部分中每个客户详细信息下的“客户设置”中的orgID匹配。多组织客户可以通过登录每个子组织并在浏览器url中注明orgID来收集orgID:(https://dashboard.umbrella.com/o/#####/)。



目前，MSP、MSSP和多组织客户的日志格式版本是1.1版。日志以GZIP格式显示，并以以下命名格式上传到相应子文件夹中的S3存储段：

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

<subfolder>是dnslogs、proxylogs或iplogs，具体取决于中的日志类型。<xxxx>是由四个字母数字字符组成的随机字符串，可防止覆盖重复的文件名。

例如：

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

如果您在10分钟内看不到存储桶中的日志，请与支持部门联系，概述您到目前为止所采取的步骤。

一旦日志确实出现，我们建议通过解压收到的前几个日志上传的内容来查看数据，以确保数据可以在文本编辑器（甚至Microsoft Excel，通常是.CSV的默认格式）中查看。 有关日志中每个字段代表的信息，请阅读此处。

如果从Cisco Umbrella到S3存储桶的日志上传失败，服务将有4小时的宽限期，在此期限内，服务每20分钟重试一次。四个小时后，我们的支持团队内将打开一个案例，该团队将开始调查问题的原因，并主动联系您，以便您了解问题。

启用基于每个客户的登录

除非另有说明，否则此功能将开箱即用，适用于所有客户。您可以为单个客户关闭此功能，如果您为拥有此功能的客户提供了不同的服务级别，此功能会非常有用。这是控制台中每个自定义设置下的设置。上一节中的屏幕截图显示了关闭此功能的切换按钮。

也可以在Amazon中创建IAM用户，并将这些IAM用户分配到各个组织，即存储桶的子文件夹。这样，您可以允许最终用户访问其日志，但只能访问日志。

下载日志、了解格式和Splunk/QRadar集成

为了下载用于保留或使用的日志，有几种方法可以从S3下载DNS日志。Weit Isve撰写了一篇文章，概述了解决此问题的几种方法。

您还可能有一些关于日志格式的问题，以及它与Umbrella控制面板中显示的日志有何细微区别。有关导出的日志格式的详细信息，请阅读本文档。

最后，导出DNS日志的一个主要用途是与SIEM工具集成。尽管处理此类日志时SIEM的配置通常可以归结为管理员个人偏好，但我们仍对最常用的SIEM提供一些指导。

有关为Amazon AWS S3和Umbrella设置Splunk插件的更多信息，请阅读此处。

有关配置IBM QRadar以从Amazon S3提取日志并对其进行摘要的信息，请阅读此处。

S3日志有多大？

S3日志的大小取决于发生的事件数，具体取决于DNS流量的大小。

您可以在此处找到S3日志记录的日志格式。

示例条目为220个字节，但每个日志行的大小取决于项目数（域名长度、类别数等）。 假设每个日志行为220字节，则一百万个请求将为220 MB。

要估计每天可见的DNS查询数量，请执行以下操作：

1. 在Umbrella控制面板中，导航到报告>活动搜索。
2. 在Filters下，运行过去24小时的报告，然后单击Export CSV图标。
3. 打开下载的.csv文件。行数（报头减一）是每天的DNS查询数；将该值乘以220字节，即可得到一天的估计值。

在成本方面，尽管成本是可变的，但我们发现，即使我们流量最大的客户每月也只花几美元用于这项服务。 一个成本与存储时间有关，另一个成本与从S3下载到您的环境的数据有关。有关详情，请与Amazon联系。

与我们的任何功能一样，Weit非常想知道您的想法，尤其是关于SIEM集成或本文档中涉及的任何其他问题。如果您有任何反馈，请告诉我们！

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。