从AWS S3中的Umbrella Log Management下载日志

目录

简介

本文档介绍如何从AWS S3中的Umbrella Log Management下载日志。

概述

一旦您设置并测试Amazon S3中的日志管理功能运行正常，您可能希望开始自动下载日志并将其存储在您的网络基础设施中，以保留或使用（或两者）。

为此，我们概述了使用http://s3tools.org中的s3工具的方法。s3tools对Linux或OS/X使用s3cmd命令行实用程序。对于Windows用户，还有其他工具可以实现类似的功能：

- 对于命令行工具，您可以在此处下载小型命令行可执行文件。
- 如果您更喜欢图形界面，请查看S3 Browser(https://s3browser.com/)，不过由于图形界面无法编写脚本来自动化流程，因此我们并没有介绍如何使用图形界面。本文提供设置这两个命令行工具的步骤。如果需要，可以使用阶段1中的信息配置s3浏览器应用程序。

首先下载要使用的操作系统的工具。目前，我们只介绍适用于OS/X和Linux的s3cmd，不过访问存储桶和下载数据的步骤对于Windows而言实际上是一样的。

从s3tools获取安装程序。

安装程序不需要您安装该程序即可运行命令行，因此只需解压已下载的程序包。

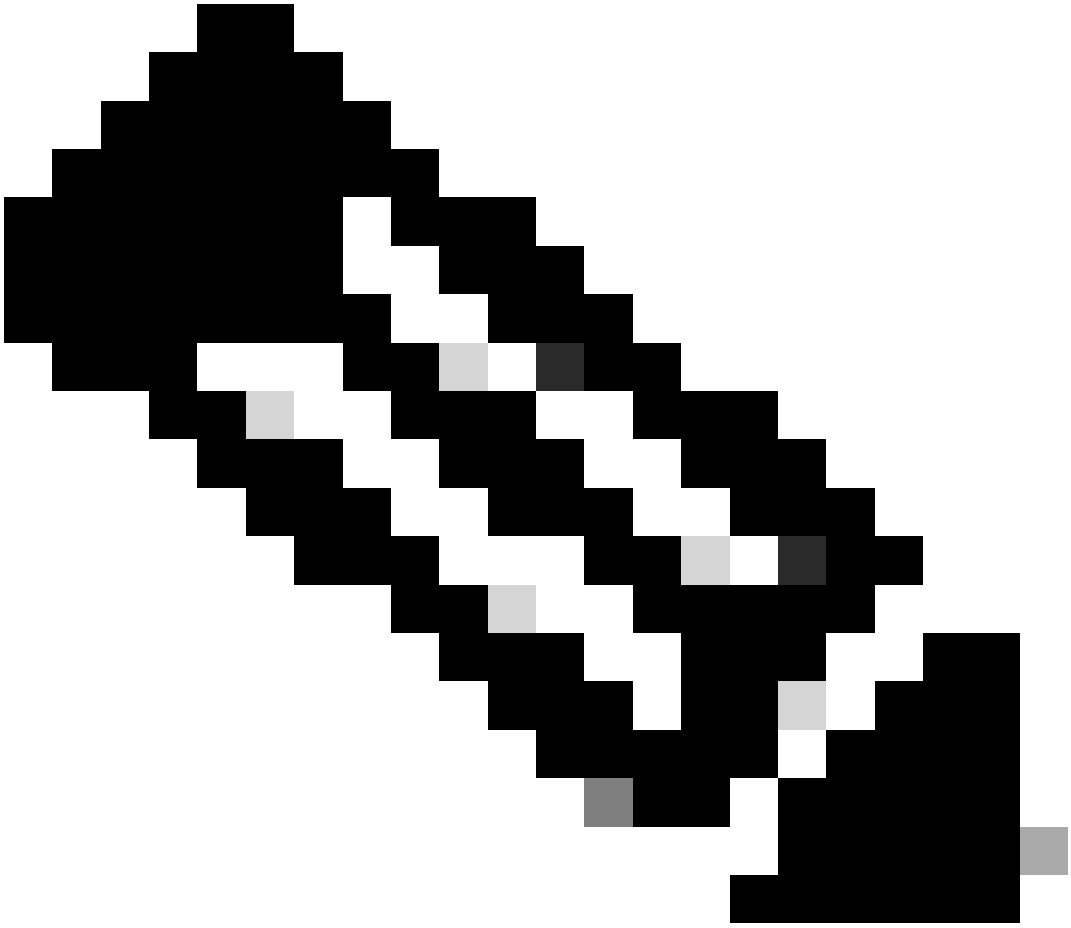
第 1 阶段：在AWS中配置安全凭证

第 1 步

1. 向Amazon Web Services帐户添加访问密钥，以便远程访问您的本地工具，并能够在S3中上传、下载和修改文件。登录AWS，然后点击右上角的帐户名称。在下拉列表中，选择Security Credentials。
2. 提示会指示您使用Amazon最佳实践并创建AWS Identity and Access Management(IAM)用户。实质上，IAM用户会确保s3cmd用于访问存储桶的帐户不是整个S3配置的主帐户（例如，您的帐户）。通过为访问您帐户的用户创建单个IAM用户，您可以为每个IAM用户提供一组唯一的安全凭据。您也可以向每个IAM用户授予不同的权限。如有必要，您可以随时更改或撤消IAM用户的权限。
   有关IAM用户和AWS最佳实践的更多信息，请阅读此处。

第 2 步

1. 单击IAM用户入门以创建有权访问S3存储桶的IAM用户。导航到可以创建IAM用户的屏幕。
2. 单击Create New Users并填写字段。
3. 创建用户帐户后，您只有一次机会获取两个包含Amazon用户安全凭证的关键信息。我们强烈建议您使用右下方的按钮下载这些文件，以对其进行备份。在设置中的此阶段之后，它们将不可用。请确保您记下访问密钥ID和秘密访问密钥，因为在后面的步骤中我们需要它们。



注意：用户帐户不能包含空格。

第 3 步

1. 接下来，您要为IAM用户添加策略，以便他们能够访问您的S3存储桶。点击您刚刚创建的用户，然后向下滚动浏览用户的属性，直到您看到Attach Policy（附加策略）按钮。
2. 单击Attach Policy，然后在策略类型过滤器中输入“s3”。这应显示两个结果“AmazonS3FullAccess”和“AmazonS3ReadOnlyAccess”。
3. 选择AmazonS3FullAccess，然后单击Attach Policy。

第 2 阶段:配置工具从存储桶下载DNS日志

MacOS和Linux的s3cmd

1. 转到已在上一阶段提取了s3cmd的路径，并从终端键入：

```
./s3cmd --configure
```

这应该会提示您提供安全凭证：

在方括号中输入Enter键的新值或接受默认值。

有关所有选项的详细说明，请参阅用户手册。

访问密钥和密钥是您的Amazon S3标识符。留空以使用env变量。

访问密钥[您的访问密钥]:

密钥[您的密钥]:

2.接下来，您将被问到一系列有关如何配置对存储桶的访问的问题。在这种情况下，我们不设置加密密码(GPG)，也不使用HTTPS或代理服务器。如果您的网络或首选项不同，请填写必填字段：

默认区域[US]:

加密密码用于在传输到S3时防止未经授权的人读取您的文件

加密密码：

GPG计划的路径[无]:

使用安全HTTPS协议时，与Amazon S3服务器的所有通信都受到保护，不会受到第三方窃听。此方法是

比普通HTTP慢，并且只能通过Python 2.7或更新版本进行代理

使用HTTPS协议[否]:

在某些网络中，所有Internet访问都必须通过HTTP代理。

如果无法直接连接到S3，请尝试在此处进行设置

HTTP代理服务器名称：

输入任何网络特定设置或任何加密后，您有机会查看：

新设置：

访问键:您的密钥

密钥:您的密钥

默认区域：美国

加密密码：

GPG计划的路径：无

使用HTTPS协议：错误

HTTP代理服务器名称：

HTTP代理服务器端口：0

最后，您需要进行测试，如果成功，请保存设置：

使用提供的凭证测试访问？[Y/n] y

请稍候，正在尝试列出所有存储桶……

成功。您的访问密钥和密钥工作正常��

正在验证加密是否有效……

未配置.算了。

保存设置?[是/否]

Windows命令行可执行文件(s3.exe)

下载工具(https://s3.codeplex.com/releases/view/47595)后，将.exe复制到首选的工作文件夹中，然后在命令提示符下键入以下内容，替换访问密钥和密钥：

<#root>

```
s3 auth [


        ]
```

有关身份验证语法的详细信息，请阅读此处。

第 3 阶段:测试从存储桶下载文件

步骤 1：测试下载

s3cmd，适用于OS/X和Linux

从终端运行此命令，其中“my-organization-name-log-bucket”是已在Umbrella仪表板的日志管理部分中配置的存储桶的名称。在本示例中，此操作从包含s3cmd可执行文件的文件夹运行，文件被传送到相同的路径，但可以更改这些路径：

<#root>

```
./s3cmd sync s3://my-organization-name-log-bucket ./
```

如果存储桶中的文件与磁盘上目标路径中的文件存在差异，则同步应下载缺失或更新的文件。检索到的第一个文件应该是通常上传的自述文件：

./s3cmd sync s3://my-organization-name-log-bucket ./

s3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [第1页，共1页]

1800个100%在0s 15.00 kB/s完成

完成。1.0秒内下载了1800个字节，1800.00 B/s

还会下载存在的所有日志文件。如果要设置cron作业以定期计划此功能，则由您自己决定，但是您现在应该能够将存储桶中的任何新日志文件或已更改的日志文件自动下载到本地路径中以长期保留。

Windows命令行可执行文件(s3.exe)

在命令提示符下，运行此命令，其中“my-organization-name-log-bucket”是已在Umbrella控制面板的“日志管理”部分中配置的存储桶的名称。在本示例中，存储桶中的所有文件（使用星号通配符定义）将下载到\dnslogbackups\文件夹中。

<#root>

```
s3 get my-organization-name-log-bucket/* c:\dnslogbackups\
```

有关此命令语法的详细信息，请阅读此处。

步骤 2：自动下载

测试语法并按预期工作后，将说明复制到脚本设置cron作业(OS X / Linux)或计划任务(Windows)中，或使用您可能有用的任何其他任务自动化工具。下载文件以释放S3实例中的空间后，还可以使用这些工具从存储桶中删除文件。我们建议您查看所用工具的文档，了解哪些内容最适合您的数据保留策略。

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）。