

3 認證用戶

R用戶需要本地系統帳戶，而不管使用哪種RStudio身份驗證方法。您應手動設置本地系統帳戶，然後將驗證用戶映射到這些帳戶。您也可以使用PAM會話將您的用戶主目錄掛載到服務器。

注意：並非所有RStudio產品都需要本地系統帳戶。Shiny Server和RStudio Connect服務於最終用戶，而不是R開發人員，所以這些產品可以在沒有本地系統帳戶的情況下配置。

3.1 PAM認證

*RStudio Server Professional Edition*通過Linux標準PAM（可插入認證模塊）API對用戶進行認證。PAM通常默認配置為針對系統用戶數據庫（`/etc/passwd`）進行身份驗證，但也可以將其配置為針對各種其他系統（包括ActiveDirectory和LDAP）進行身份驗證。

本節介紹安裝後默認用於身份驗證的PAM配置。請注意，PAM可用於身份驗證以及為用戶會話（PAM會話）定制環境。本節僅介紹身份驗證，請參閱[用戶資源和限制]部分以獲取有關RStudio Server如何配置為使用PAM會話的詳細信息。

3.1.1 PAM基礎

PAM配置文件位於 `/etc/pam.d` 目錄中。每個應用程序都可以擁有自己的配置文件，並且還有一個默認的配置文件，用於沒有配置文件的應用程序（根據所運行的Linux版本，默認配置文件的處理方式不同）。

要了解有關PAM的更多信息以及可用的許多選項和模塊，請參閱以下內容：

- http://en.wikipedia.org/wiki/Pluggable_authentication_module
- http://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-pam.html
- <http://tldp.org/HOWTO/User-Authentication-HOWTO/x115.html>
- <http://linux.die.net/man/8/pam>

3.1.2默認PAM配置

Debian / Ubuntu

在Debian和Ubuntu系統上，RStudio Server不提供RStudio特定的PAM配置文件。因此，RStudio服務器使用該 `/etc/pam.d/other` 配置文件，該配置文件默認從一組通用配置文件繼承：

`/etc/pam.d/other`

```
@include common-auth
@include common-account
@include common-password
@include common-session
```

如果 `/etc/pam.d/other` 配置文件反映了您希望RStudio Server使用的認證系統和策略，則不需要進一步的配置。如果要為RStudio創建自定義PAM配置文件，您可以創建一個名為的文件 `/etc/pam.d/rstudio` 並指定適當的設置。

RedHat / CentOS / SUSE

在RedHat上，沒有自己的PAM配置文件的CentOS和SUSE系統應用程序默認被拒絕訪問。因此，為了確保RStudio在安裝後運行並可用，默認的PAM配置文件安裝

在 `/etc/pam.d/rstudio`。此配置文件配置為要求用戶標識大於500，並根據本地系統帳戶對用戶進行身份驗證：

`/etc/pam.d/rstudio`

```
auth      requisite      pam_succeed_if.so uid >= 500 quiet
auth      required       pam_unix.so nodelay
account   required       pam_unix.so
```

此默認的PAM配置文件可能不會反映您想要用於RStudio Server的身份驗證行為。在這種情況下，可能需要一些定制。如果您已經設置了另一個 `/etc/pam.d/login` 具有所需行為的PAM配置文件（例如），那麼簡單地將該配置文件複製到RStudio上就足夠了。例如：

```
$ sudo cp /etc/pam.d/login /etc/pam.d/rstudio
```

3.1.3診斷PAM認證問題

如果您無法登錄到RStudio服務器，則PAM配置可能存在潛在的問題。診斷PAM配置問題的最佳方法是使用該 `pamtester` 實用程序（與RStudio Server捆綁在一起）。通過使用 `pamtester` 您可以在隔離的環境中測試身份驗證，以及查看更詳細的診斷信息。

該 `pamtester` 實用程序位於 `/usr/lib/rstudio-server/bin/pamtester`。要調用它，您需要傳遞幾個參數來指示要測試的PAM配置文件，要測試的用戶以及是否需要詳細輸出。例如：

```
sudo /usr/lib/rstudio-server/bin/pamtester --verbose rstudio <username> authentic
```

您可以在 `pamtester` 這裡找到更詳細的使用文檔：<http://linux.die.net/man/1/pamtester>。

3.1.4管理PAM登錄生存期

使用PAM身份驗證登錄時，用戶可以選擇在瀏覽器會話中保持登錄狀態。默認情況下，當選擇逗留登錄選項時，用戶將保持登錄狀態30天。您可以使用該 `auth-stay-signed-in-days` 設置修改此行為。例如：

```
/etc/rstudio/rserver.conf
```

```
auth-stay-signed-in-days=7
```

您可以完全防止使用該 `auth-stay-signed-in` 設置顯示此選項。例如：

```
/etc/rstudio/rserver.conf
```

```
auth-stay-signed-in=0
```

設置這個選項 `0` 將導致用戶在每次開始一個新的瀏覽器會話時被提示登錄（即只要瀏覽器進程始終保持運行狀態，登錄只會是有效的）。

3.2限制對特定用戶的訪問

3.2.1最小用戶ID

默認情況下，RStudio Server只允許普通用戶（而不是系統用戶）成功進行身份驗證。最小用戶ID是通過讀取文件中的 `UID_MIN` 值來確定的 `/etc/login.defs`。如果文件不存在或 `UID_MIN` 沒有在其中定義，則使用默認值1000。

通過指定 `auth-minimum-user-id` 選項來更改最小用戶ID。例如：

```
/etc/rstudio/rserver.conf
```

```
auth-minimum-user-id=100
```

請注意，您的PAM配置也可能對user-id應用約束（請參閱上面的默認PAM配置部分中的示例）。在這種情況下，您應確保 `auth-minimum-user-id` 與PAM配置中指定的值一致。

3.2.2分組限制

您可以指定只允許某些組的用戶訪問RStudio服務器。要做到這一點你使用的 `auth-required-user-group` 設置。例如：

```
/etc/rstudio/rserver.conf
```

```
auth-required-user-group=rstudio-users
```

您可以像上面的例子那樣指定一個組，或者用逗號分隔的組列表。例如：

```
/etc/rstudio/rserver.conf
```

```
auth-required-user-group=analysts,admins,rstudio-users
```

請注意，此更改在服務器重新啟動之前不會生效。

3.2.2.1創建和管理組成員

要創建一個新組，請使用以下 `groupadd` 命令：

```
$ sudo groupadd <groupname>
```

要將用戶添加到現有組，請使用以下 `usermod` 命令：

```
$ sudo usermod -a -G <groupname> <username>
```

請注意，包含該 `-a` 標誌是至關重要的，因為這表示應將該組添加到用戶，而不是完全替換用戶的組列表。

3.3 Google帳戶

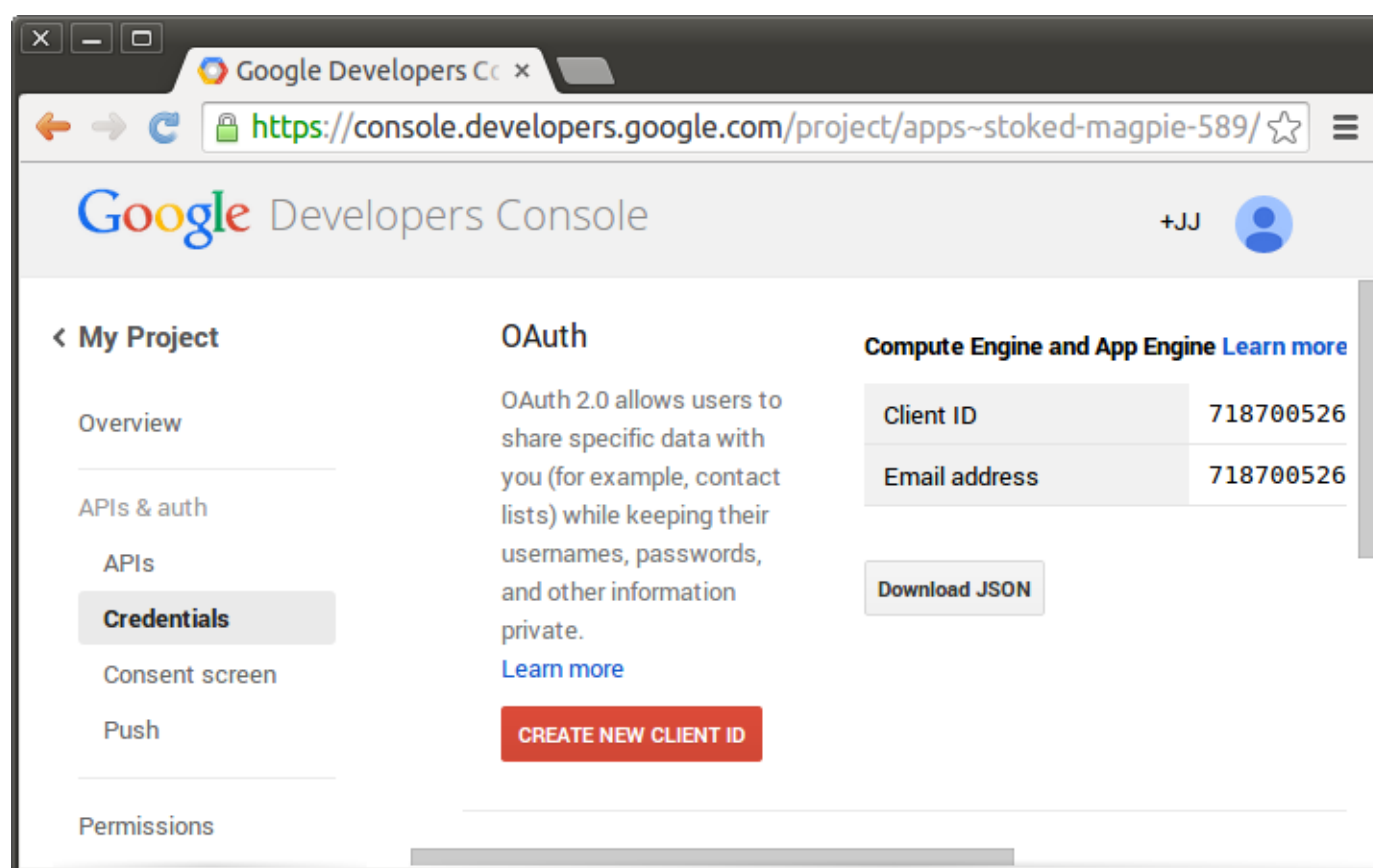
RStudio服務器可以配置為通過Google帳戶對用戶進行身份驗證。這使用戶可以使用其現有的Gmail或Google Apps憑據進行登錄，並在用戶已經登錄到Google帳戶後自動向RStudio Server進行身份驗證。

3.3.1向Google註冊

為了在RStudio Server上使用Google帳戶，您需要在Google上註冊您的服務器以進行OAuth 2.0身份驗證。通過創建在您的服務器的新“項目”做到這一點 [谷歌開發者控制台](#)：

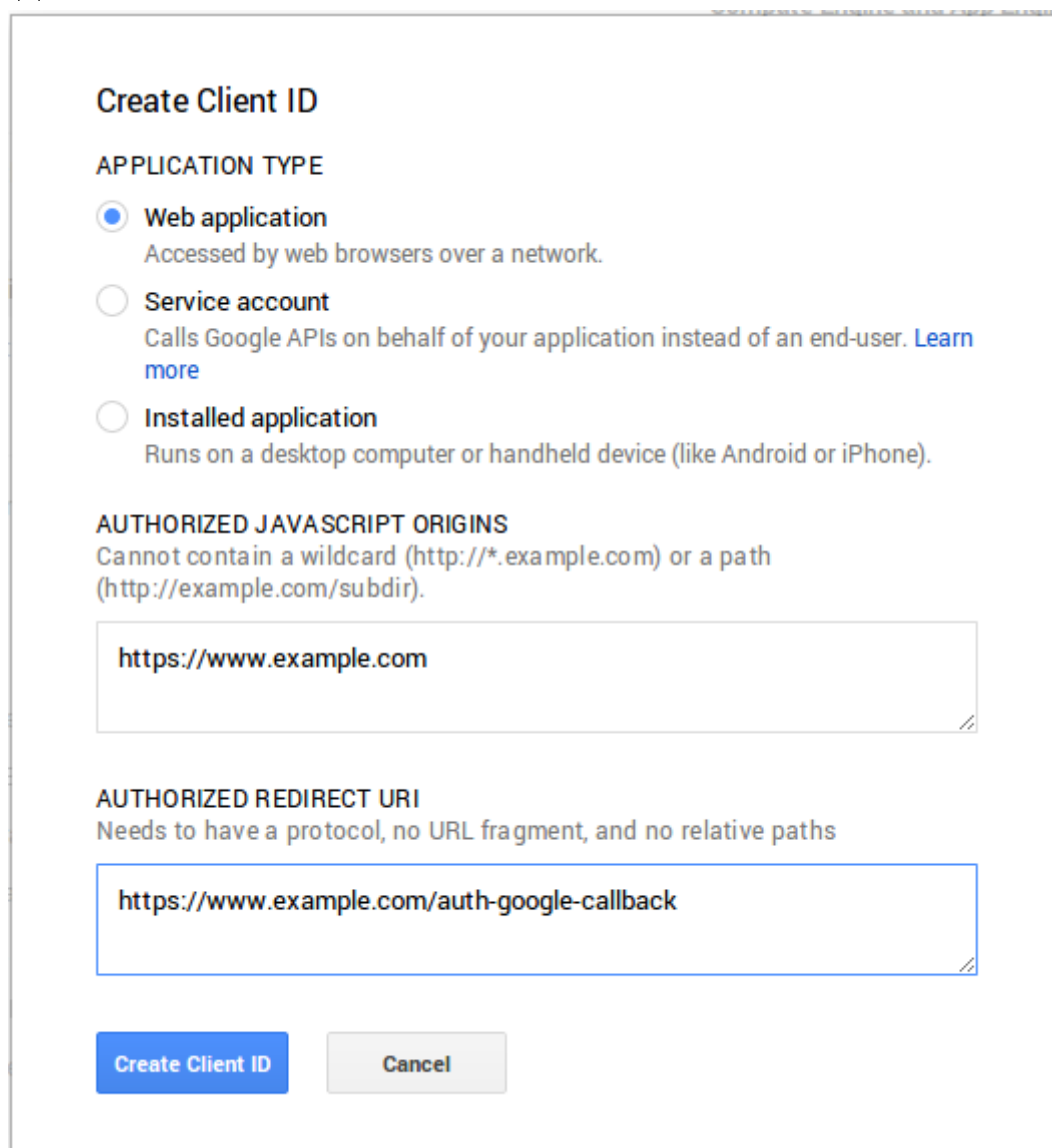
<https://console.developers.google.com/>

一旦你創建了一個項目，你去憑據的區域API和權威性，並選擇創建新客戶端ID：



創建客戶端ID

隨後會出現一個用於創建新客戶端ID的對話框：



Create Client ID

APPLICATION TYPE

☒ **Web application**
Accessed by web browsers over a network.

☐ **Service account**
Calls Google APIs on behalf of your application instead of an end-user. [Learn more](#)

☐ **Installed application**
Runs on a desktop computer or handheld device (like Android or iPhone).

AUTHORIZED JAVASCRIPT ORIGINS
Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).

https://www.example.com

AUTHORIZED REDIRECT URI
Needs to have a protocol, no URL fragment, and no relative paths

https://www.example.com/auth-google-callback

Create Client ID **Cancel**

創建客戶端ID

您應該選擇“Web應用程序”作為應用程序類型，並提供與您正在部署的服務器相對應的兩個 URL。上面的屏幕截圖 `https://www.example.com` 用作主機，您應該在您的配置中替換您自己的域和端口（如果不使用標準的80或443）。

這將導致您需要提供的兩個值作為RStudio服務器配置的一部分：`client-id` 並且 `client-secret`（完成對話框後，它們將顯示在*Google Developer Console*中）。

3.3.2啟用Google帳戶

要啟用Google帳戶驗證，請將該 `auth-google-accounts` 選項添加到RStudio服務器配置文件中：

/etc/rstudio/rserver.conf

```
auth-google-accounts=1
```

此外，還需要添加一個配置文件（`/etc/rstudio/google-client-secret`）包含 `client-id` 和 `client-secret` 你註冊你的網站與谷歌的時候收到。例如，配置文件可能如下所示：

在 `/etc/rstudio` / 谷歌的客戶端秘密

```
client-id=111111111111-xxxxxxxxxxxxxxxxxxxxx.apps.googleusercontent.com
client-secret=BhCC6rK7Sj2ZtPH0ord7l01w
```

該 `/etc/rstudio/google-client-secret` 文件應具有用戶讀/寫文件的權限（即0600），以保護其內容不受其他用戶的影響。你可以確保如下：

```
$ sudo chmod 0600 /etc/rstudio/google-client-secret
```

請注意，以上 `client-id`，`client-secret` 而不是您將使用的實際值。相反，在註冊您的站點進行OAuth身份驗證時，您應該替換從Google獲得的值。

使用Google帳戶啟用身份驗證後，您將無法同時使用PAM和Google帳戶身份驗證。

3.3.3翻譯成本地帳戶

3.3.3.1創建匹配帳戶

一旦用戶通過Google帳戶進行身份驗證，就需要將他們的Google帳戶身份映射到本地系統帳戶。默認和最直接的方法是創建一個本地帳戶，其用戶名與他們的Google電子郵件地址相同。

如果您選擇創建與Google電子郵件地址相匹配的本地帳戶，請務必在帳戶名稱中僅使用小寫字符，因為Google電子郵件地址在將其與本地帳戶名稱匹配之前會轉換為小寫字母。

創建與Google電子郵件地址相匹配的本地帳戶的一個問題是，它們通常包含在Linux用戶名（例如@或。）內默認無效的字符。在Debian / Ubuntu系統上，可以強制系統使用這些字符創建一個用戶。以下是使用用戶名通常包含無效字符創建用戶的示例：

```
$ sudo adduser --force-badname <username>
```

請注意，該 `--force-badname` 選項僅在Debian / Ubuntu系統上可用，在RedHat / CentOS或SLES系統上不可用。

如果您創建的用戶只能通過RStudio訪問服務器，則可能還需要禁用其以普通交互式用戶身份登錄的能力，並指定他們沒有密碼。例如：

```
$ sudo adduser --force-badname --disabled-login --disabled-password <username>
```

3.3.3.2 使用帳戶映射文件

或者，您可以創建與Google電子郵件地址不匹配的本地帳戶，然後通過 `/etc/rstudio/google-accounts` 配置文件指定Google帳戶到本地帳戶的映射。例如：

在 `/etc/rstudio/` 谷歌帳戶

```
john.smith@gmail.com=jsmith  
sally.jones@gmail.com=sjones
```

請注意，對 `google-accounts` 配置文件的更改立即生效，不需要重新啟動服務器。

3.3.4 代理注意事項

如果您在代理服務器後面運行RStudio，則需要配置代理以在 `x-Forwarded-Host` 標頭中設置其主機名，以便RStudio可以通知Google Web服務重定向回正確的位置。例如，如果您的代理服務器設置為在<http://testdomain.com/rstudio/>上提供RStudio請求，則需要確保代理服務器設置 `x-Forwarded-Host` 標頭 `http://testdomain.com/rstudio/`。否則，RStudio將嘗試將其重定向回其內部地址。

或者，如果您在代理之後運行，但 `x-Forwarded-Host` 由於某種原因無法設置正確的標頭，則可以使用 `auth-google-accounts-redirect-base-uri` RStudio Server配置文件中的選項來實現相同的目的：

`/etc/rstudio/rserver.conf`

```
auth-google-accounts-redirect-base-uri=http://testdomain.com/rstudio/
```

3.4 自定義登錄頁面

您可以通過在頁面中包含自定義HTML來自定義RStudio服務器登錄頁面的內容和外觀。這是通過以下任一方式來完

1. 提供 `/etc/rstudio/login.html` 包含額外HTML 的文件以包含在登錄頁面中; 要么

2. `auth-login-page-html` 在 `rserver.conf` 配置文件中指定指向登錄HTML文件的備用位置的選項。例如，以下內容指定位於的文件 `/opt/config/rstudio-login.html` 應包含在登錄頁面中：

```
/etc/rstudio/rserver.conf
```

```
auth-login-page-html=/opt/config/rstudio-login.html
```

指定的HTML文件的內容將包含在標準登錄標題和登錄用戶名/密碼表單之後。如果您想要修改標題的外觀和/或在用戶名/密碼表單上添加內容，您可以在`login.html`文件中使用CSS和JavaScript來在頁面加載後修改頁面。

3.5代理驗證

您可以使用代理身份驗證將RStudio服務器配置為參與現有的基於Web的單一登錄身份驗證方案。在此配置中，所有到RStudio服務器的通信都由代理服務器處理，代理服務器也處理用戶認證。

在這個配置中，代理服務器將一個特殊的HTTP頭添加到RStudio服務器的請求中，讓它知道哪個已認證的用戶正在發出請求。RStudio Server信任這個頭部，啟動並指定流量到指定用戶擁有的R會話。

指定的用戶必須在服務器上有一個本地系統帳戶。您應手動設置本地系統帳戶，然後將驗證用戶映射到這些帳戶。

3.5.1啟用代理身份驗證

要啟用代理身份驗證，您需要同時指定 `auth-proxy` 和 `auth-proxy-sign-in-url` 設置（登錄URL是用戶應該重定向到登錄的頁面的絕對URL）。例如：

```
/etc/rstudio/rserver.conf
```

```
auth-proxy=1
```

```
auth-proxy-sign-in-url=http://example.com/sign-in
```

請注意，在重新啟動服務器之前，對配置的更改不會生效。

3.5.2 實施代理

3.5.2.1 登錄URL

登錄URL應該託管一個用戶指定其憑據的頁面（這可能是例如現有的基於Web的認證系統的主頁面）。在收集和授權證書之後，登錄URL應該重定向回到託管RStudio服務器的URL。

在以下情況下，RStudio將重定向到登錄URL：

1. 每當服務器接收到缺少用戶名頭的HTTP請求時，和
2. 當用戶單擊RStudio IDE用戶界面中的“註銷”按鈕時。

您應該確保在設置代理服務器時，為登錄URL指定的流量不會被轉發到RStudio Server（否則它將以無限重定向循環結束）。

3.5.2.2 轉髮用戶名

當為RStudio服務器代理預先認證的流量時，您需要包含一個特殊的HTTP頭（默認情況下 `x-RStudio-Username`），每個請求都指明請求與哪個用戶相關聯。例如：

```
X-RStudio-Username: jsmith
```

也可以指定係統用戶名和顯示用戶名（在系統帳戶是動態配置的情況下，不表示實際的用戶身份）。例如：

```
X-RStudio-Username: rsuser24/jsmith
```

請注意，強烈建議您不要使用默認 `x-RStudio-Username` 標題名稱。其原因在下面緊接著的安全考慮部分中描述。

3.5.2.3 重新編寫用戶名

您可能正在使用的代理系統以與系統上的用戶不匹配的格式發送用戶名，但可以很容易地將其轉換為（例如，在用戶名之前具有標準的前綴）的用戶名。如果是這種情況，您可以指定 `auth-proxy-user-header-rewrite` 選項來為入站報頭提供重寫規則。例如，以下規則會從用戶名標頭中去掉前綴“UID-”：

```
auth-proxy-user-header-rewrite=^UID-([a-z]+)$ $1
```

重寫規則的格式是正則表達式，後跟空格，然後是替換字符串。替換字符串可以參考拍攝使用正則表達式的一部分 `$1`，`$2` 等等。

3.5.3安全考慮

3.5.3.1保持標題名稱的秘密

使用默認標題名稱 `X-RStudio-Username` 會產生一個安全問題：在代理後面運行的代碼（即R會話中的代碼）可能會將請求返回給模擬其他用戶的服務器（只需在請求中插入標頭）。

為了防止這個問題，你可以指定一個自定義的頭文件名，這個頭文件對最終用戶保密。這是通過創建一個 `/etc/rstudio/secure-proxy-user-header` 包含頭部名稱的特殊配置文件（），然後設置它的文件權限來完成的，以使其不能被普通用戶讀取。例如：

```
sudo sh -c "echo 'X-Secret-User-Header' > /etc/rstudio/secure-proxy-user-header"
sudo chmod 0600 /etc/rstudio/secure-proxy-user-header
```

3.5.3.2防止遠程使用標題

在實現代理時，請記住RStudio Server始終信任用戶名頭以驗證用戶。因此，從安全的角度來看，來自代理的所有請求都具有由代理明確設置的頭部（與允許遠程客戶機指定頭部相反）。

3.5.4使用訪問日誌進行故障排除

如果您想要查看RStudio Server正在接收哪些請求以及它們是否包含預期的用戶名信息，則可以使用以下 `server-access-log` 設置臨時啟用服務器訪問日誌：

`/etc/rstudio/rserver.conf`

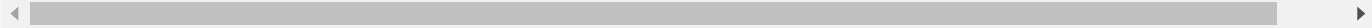
```
server-access-log=1
```

重新啟動RStudio Server後，以下文件將包含對服務器發出的每個HTTP請求的記錄及其HTTP響應代碼：

```
/var/log/rstudio-server/rserver-http-access.log
```

日誌文件將包含如下所示的條目：

```
127.0.0.1 - - [29/Jun/2015:06:30:41 -0400] "GET /s/f01ddf8222bea98a/ HTTP/1.1"
200 91 "http://localhost:8787/s/f01ddf8222bea98a/" "Mozilla/5.0 (X11; Linux x86_64;
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.125 Safari/537.36" "jsmith"
```



請注意，日誌文件條目中的最後一項是 "jsmith" 。這是RStudio Server從代理服務器傳遞的頭中讀取的用戶名。如果顯示為空白（ "-" ），那麼代理服務器不會轉發標頭或在轉發時使用正確的標頭名稱。

重要提示：一旦你完成了故障排除，重要的是你 `server-access-log=1` 從 `/etc/rstudio/rserver.conf` 文件中刪除選項（因為這個日誌文件沒有被旋轉，如果你不刪除這個選項，它最終會消耗大量的磁盤空間）。