Posted in: API (/spaces/127/sandpiper/forums/5044/api)

Sync Credentials (api-key)

Doug Winsby (https://autocare.communifire.com/people/dougwinsby)
5/12/2020

One challenge we have with the sync process is how to authorize it. Both primary and secondary servers have a `users` table to authorize and grant access to their API. Admin users "login" (with a username and password) to manage subscriptions, slices, tags, grains and activity logs.

A sync, however, is different. A sync originates from a secondary server and must be authorized by each primary server it accesses. But how does this authorization work? There is no actual person to enter login credentials for each primary server to authorize a sync.

The answer is to provide a primary API endpoint that creates and returns an "api-key" that is then stored on the secondary server. This key is an encrypted version of the username and password using a very strong AES256 (symmetric key cipher) encryption.

Unlike standard password hash authentication where the secret key is used only for encryption, a symmetric key cipher uses the same secret key for both encryption and decryption. This works for us because only the primary server needs to perform encryption/decryption of the api-key.

So the steps are:

1. The secondary authenticates to a primary server with their normal company-admin credentials.

```
POST /login
{ "username": "companyadmin", "password":"companyadmin" }
```

The primary responds with a JWT authentication token.

```
{
 "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjIjoiMjAwMDAwMDAtMDAwMC0wMDAwLT
AwMDAtMDAwMDAwMDAwIiwiZSI6Im1pY2tleUBnbWFpbC5jb20iLCJleHAiOjE1ODkxNjk3MTMsImlk
IjozLCJyIjoxMjAsInUiOiJjb21wYW55YWRtaW4ifQ.plQu3BhZF9YGJfrdcNtj8fAVo7rOSwRGq3cf0gR
YP-U",
 "expires": "2020-05-10T23:01:53-05:00",
 "refresh_token": "d970dc61f2f78e65db93419a635a1629c9c4057e"
}
```

2. The secondary asks for an api-key on the primary server (using the login JWT bearer token in the request header):

```
POST /apikey
```

The primary determines the user's company (stored as a claim in the JWT) and responds with it's own server ID (actually a company_id) and creates a new "sync user" for that company. This sync user is assigned a random username and password.

```
{
 "username": "sync_c702c466-104a-4d70-b1b2-c18cc9748a41",
 "password":"$2a$10$qeu/oi0g7Rkyo7QeQ9i74.E9AJF6o/Ft4k0GV5LZ6UOApNkIkBSdS"
}
```

As an added security measure, every time a new api-key is generated, a new username and password is created and the existing sync user record is updated. Also, there is only one sync user assigned per company.

Finally, that username and password json is encrypted (AES256) into an api-key and returned in the response:

```
{
 "primary_id": "10000000-0000-0000-0000-000000000000",
 "sync_api_key": "eaac666eeb167e8da790f07cb348fb9e759e9086cef07116caefb39e75a696bf
c6f890e57e936cb7da064171ec27ca3f9787df94f061df3bf74dcd6a47b5ce52ccafbc97480d5608f1
14f0bd6fff850c13dda997015021f176447d5aba52c50cc9136398e31ac17e45e4e85abc8c513f0ed5
eb6e3ad2afc59642e3ef3c"
}
```

3. The secondary would then save this api-key in the primary's company record (identified by the primary_id returned).

4. The secondary `/sync` endpoint is used to initiate a sync operation (with the primary server's company_id):

```
POST /sync/10000000-0000-0000-0000-000000000000
```

5. During a sync operation, the secondary does not login through the normal `/login` API. Instead, it sends a `/synclogin` request and passes the api-key (instead of a plain-text username and password).

6. The primary receives the `/synclogin` request, extracts the username and password from the api-key and authenticates normally (returning a JWT token for subsequent API sync calls).

Update: We were able to handle both plain-text logins and api-key logins using the same `/login` API endpoint (by including both options in the request JSON).

api-key (/spaces/127/sandpiper/searchresults?keyword=%22api-key%22&searchtags=1)
sync_authentication (/spaces/127/sandpiper/searchresults?keyword=%22sync_authentication%22&searchtags=1)
sync_initiation (/spaces/127/sandpiper/searchresults?keyword=%22sync_initiation%22&searchtags=1)

1 Like

Reply (/forums/post?tid=5962&ReplyPostID=5963&SpaceID=127)