Arvados - Bug #18491

Address jwt-go's security advisory

11/29/2021 04:17 PM - Lucas Di Pentima

Status:	Resolved	**Start date:**	11/30/2021
Priority:	Normal	**Due date:**	
Assigned To:	Lucas Di Pentima	**% Done:**	100%
Category:	API	**Estimated time:**	0.00 hour
Target version:	2021-12-08 sprint		

Description

One of controller's dependencies requires an upgrade because of security issues.

https://github.com/advisories/GHSA-w73w-5m7g-f7qc

The project seems to have been taken over by a new maintainer team at: https://github.com/golang-jwt/jwt

Subtasks:

Task # 18493: Review 18491-jwt-go-upgrade	**Resolved**

Associated revisions

Revision e163d0f1 - 11/30/2021 03:59 PM - Lucas Di Pentima

Merge branch '18491-jwt-go-upgrade' into main. Closes #18491.

Arvados-DCO-1.1-Signed-off-by: Lucas Di Pentima <lucas.dipentima@curii.com>

Revision 00b010f9 - 12/06/2021 05:22 PM - Lucas Di Pentima

Merge branch '18491-jwt-go-upgrade' into main. Closes #18491.

Arvados-DCO-1.1-Signed-off-by: Lucas Di Pentima <lucas.dipentima@curii.com>

Revision 5c7b5f03 - 12/06/2021 06:45 PM - Peter Amstutz

github.com/Azure/go-autorest/autorest/azure/auth go-jwt security fix

refs #18491

Arvados-DCO-1.1-Signed-off-by: Peter Amstutz <peter.amstutz@curii.com>

History

#1 - 11/29/2021 07:09 PM - Lucas Di Pentima

By using go mod graph I was able to see which dependency asked for this module:

```
lucas@buster:~/arvados$ go mod graph | grep jwt
github.com/Azure/go-autorest/autorest/adal@v0.9.0 github.com/dgrijalva/jwt-go@v3.2.0+incompatible
github.com/Azure/go-autorest/autorest/adal@v0.9.2 github.com/dgrijalva/jwt-go@v3.2.0+incompatible
lucas@buster:~/arvados$ go mod graph | grep adal@
[...]
github.com/Azure/go-autorest/autorest@v0.11.0 github.com/Azure/go-autorest/autorest/adal@v0.9.0
[...]
github.com/Azure/go-autorest/autorest/azure/cli@v0.4.0 github.com/Azure/go-autorest/autorest/adal@v0.9.0
github.com/Azure/go-autorest/autorest/azure/auth@v0.5.1 github.com/Azure/go-autorest/autorest/adal@v0.9.2
github.com/Azure/go-autorest/autorest@v0.11.3 github.com/Azure/go-autorest/autorest/adal@v0.9.0
lucas@buster:~/arvados$ go mod graph | grep azure/cli
[...]
github.com/Azure/go-autorest/autorest/azure/auth@v0.5.1 github.com/Azure/go-autorest/autorest/azure/cli@v0.4.0
lucas@buster:~/arvados$ go mod graph | grep azure/auth
git.arvados.org/arvados.git github.com/Azure/go-autorest/autorest/azure/auth@v0.5.1
[...]
```

It seems that github.com/Azure/go-autorest/autorest/azure/auth@v0.5.1 is the root of this requirement chain, I'll attempting an upgrade on it.

#2 - 11/29/2021 07:24 PM - Lucas Di Pentima

Updates at d69ebd24d - branch 18491-jwt-go-upgrade

Test run: developer-run-tests: #2818 icon?job=developer-run-tests&build=2818

- Upgrades github.com/Azure/go-autorest/autorest/azure/auth to v.0.5.9 and all its dependencies.
- Removes unused modules (including github.com/dgrijalva/jwt-go) by running: go mod tidy

#3 - 11/29/2021 08:20 PM - Lucas Di Pentima

I'm getting the following test failure and I'm not sure why:

```
16:32:26 ----------------------------------------------------------------------
16:32:26 FAIL: container_gateway_test.go:189: ContainerGatewaySuite.TestConnect
16:32:26
16:32:26 connecting to localhost:37559
16:32:26 container_gateway_test.go:213:
16:32:26     c.Check(buf[:4], check.DeepEquals, []byte{0, 0, 1, 0xfc})
16:32:26 ... obtained []uint8 = []byte{0x0, 0x0, 0x2, 0xc}
16:32:26 ... expected []uint8 = []byte{0x0, 0x0, 0x1, 0xfc}
```

#4 - 11/30/2021 03:14 PM - Tom Clegg

IIRC when I wrote that test I didn't know what the bytes meant, they just seemed to be equal each time. Now that I bother to look at RFC4253 it seems they're just the length of a data packet, so not worth testing. I think we can just delete that check. The previous line already checks that we can read 4 bytes after sending our banner, which seems good enough for this test's purposes.

#5 - 11/30/2021 03:40 PM - Lucas Di Pentima

Thanks for the explanation!

I've updated the test at bc3637c90
Test run: developer-run-tests: #2822 icon?job=developer-run-tests&build=2822

#6 - 11/30/2021 03:54 PM - Tom Clegg

LGTM, thanks!

#7 - 11/30/2021 04:43 PM - Lucas Di Pentima

- Status changed from In Progress to Resolved

Applied in changeset arvados-private:commit:arvados|e163d0f19b52b4c15adb3d97f49bcacdbaf8dc89.

#8 - 12/06/2021 05:54 PM - Lucas Di Pentima

To re-do this on the 2.3-dev branch, run the following:

```
$ go get -u github.com/Azure/go-autorest/autorest/azure/auth
$ go mod tidy
```

then, fix a test by removing the check from line 213 at file lib/controller/localdb/container_gateway_test.go