Arvados - Story #15348
[pam] PAM module in Go
06/11/2019 02:48 PM - Tom Clegg

<table>
<thead>
<tr>
<th>Status:</th>
<th>Resolved</th>
<th>Start date:</th>
<th>06/23/2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assigned To:</td>
<td>Tom Clegg</td>
<td>% Done:</td>
<td>100%</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Target version:</td>
<td>2020-07-15</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

Functionally equivalent to [source:sdk/pam](source:sdk/pam) but reliable, and packaged as a binary (no dependency on python-pam, python, etc).

The glue for interfacing with PAM, building a shared library, etc. can be taken from MIT-licensed [https://github.com/uber/pam-ussh](https://github.com/uber/pam-ussh)

**Authentication:**

- Get desired username from PAM
- Call PAM to prompt for token (in python this was token = pamh.conversation(pamh.Message(pamh.PAM_PROMPT_ECHO_OFF, prompt)).resp)
- Use given token to look up current user
- Use given token to look up virtual_machine matching configured hostname
- Use given token to look up permission link with matching VM uuid, user uuid, can_login, and properties[username]
- Log request & outcome
- Return true/false

**Subtasks:**

Task # 16550: Review 15348-pam-module

**Related issues:**

- Related to Arvados - Story #14964: Port arvados-pam to Python 3  - Rejected
- Related to Arvados - Bug #6649: [Documentation] webshell installation  - Resolved 07/16/2015
- Related to Arvados - Bug #16100: [keep-web] Avoid sniffing for content type w...  - Resolved 02/14/2020
- Related to Arvados - Bug #16920: [libpam-arvados-go] the deployed pam config ...  - Resolved

**Associated revisions**

Revision 4fa1cccc - 07/06/2020 06:18 PM - Tom Clegg

Merge branch '15348-pam-module'

refs #15348

Arvados-DCO-1.1-Signed-off-by: Tom Clegg <tom@tomclegg.ca>

Revision 99df0022 - 09/09/2020 05:50 PM - Ward Vandewege

The new libpam-arvados-go package should conflict with the old libpam-arvados package.

refs #15348

Arvados-DCO-1.1-Signed-off-by: Ward Vandewege <ward@curii.com>

Revision 3ebf3b70 - 09/10/2020 08:18 PM - Ward Vandewege

Bugfix: make sure that any fpm_args defined in fpm-info.sh get introduced at the correct position in the fpm argument list. This only affects non-Python packages (we already did the right thing for Python packages).

refs #15348

Arvados-DCO-1.1-Signed-off-by: Ward Vandewege <ward@curii.com>

Revision 5cefb12b - 09/29/2020 09:53 PM - Ward Vandewege
libpam-arvados-go: do not put a file with comments in /usr/share/pam-configs, the `pam-auth-update` command does not take kindly to that. Put that file in the package documentation directory instead.

refs #15348

Arvados-DCO-1.1-Signed-off-by: Ward Vandewege <ward@curii.com>

History

#1 - 06/11/2019 02:48 PM - Tom Clegg
- Related to Story #14964: Port arvados-pam to Python 3 added

#2 - 06/12/2019 02:41 PM - Tom Morris
- Target version set to Arvados Future Sprints
- Story points set to 3.0

#3 - 06/17/2020 04:30 PM - Tom Clegg
- Target version changed from Arvados Future Sprints to 2020-07-01 Sprint
- Assigned To set to Tom Clegg

#4 - 06/19/2020 03:02 PM - Tom Clegg
- Status changed from New to In Progress

#5 - 06/23/2020 01:45 PM - Tom Clegg

Manual testing

```
~/arvados $ WORKSPACE=`pwd` ./build/run-build-packages-one-target.sh --target debian10 --only-build libpam-arvados-experimental --build-version `git describe --tags`
~/arvados $ docker run --rm -it -v ~/arvados/packages/debian10:/pkg:ro debian:10 bash
root@6106d894ce52:/# apt update && apt install rsyslog ca-certificates && /etc/init.d/rsyslog start
root@6106d894ce52:/# dpkg -i /pkg/libpam-arvados-experimental_2.0.0-551-gb694b711c_amd64.deb
root@6106d894ce52:/# perl -pi~ -e 's{pam_unix.so nullok_secure}{/usr/lib/pam_arvados.so 9tee4.arvadosapi.com tom.shell debug}' /etc/pam.d/common-auth
root@6106d894ce52:/# adduser tom
root@6106d894ce52:/# login
6106d894ce52 login: tom
Password: {asdfasdfasdfasdf}
DEBU[0001] username="tom" arvados_api_host="9tee4.arvadosapi.com" hostname="tom.shell" insecure=false
ERR[0001] authentication failed error="request failed: https://9tee4.arvadosapi.com/arvados/v1/virtual_machines?cluster_id=&count=&filters=%5B%5B%22hostname%22%2C%22%3D%22%2C%22%2C%22tom.shell%22%5D%5D&limit=2&offset=0: 401 Unauthorized: Not logged in (req-1j6dbhbi5vbih1xol40md)"
Login incorrect
6106d894ce52 login: tom
Password: {valid token}
DEBU[0012] username="tom" arvados_api_host="9tee4.arvadosapi.com" hostname="tom.shell" insecure=false
DEBU[0012] permission granted based on link with UUID 9tee4-6b521-70navy5our34x9
Last login: Tue Jan 23 13:58:02 UTC 2020 on pts/0
Linux 6106d894ce52 4.9.0-12-amd64 #1 SMP Debian 4.9.210-1 (2020-01-20) x86_64 ...
tom@6106d894ce52:/$ whoami

tom
```

Questions

- Should we list ca-certificates as a recommended/dependency pkg? Without it, even valid certs fail verification -- but the "insecure" option means verification isn't strictly necessary.
- Should the package also drop an example/template file in /usr/share/pam-configs/arvados like its python-based predecessor? This is how docker_test.go enables the module, but it doesn't work out of the box IRL because the operator needs to specify their real API host. (If there was a default/conventional API host name like "api", we could use that, but we don't have that rn.)
- Should we make the "vm name" config arg optional, and call gethostname() if it isn't provided?

15348-pam-module @ b694b711c69dfd46b6732a6d6c67e37951dab39 -- https://ci.arvados.org/view/Developer/job/developer-run-tests/1927/

#6 - 06/23/2020 02:22 PM - Tom Clegg
- File libpam-arvados-experimental_2.0.0-551-gb694b711c_amd64.deb added
Manual testing

```bash
WORKSPACE=`pwd` bash -x ./build/run-build-packages-one-target.sh --target debian10 --only-build lib/pam --build-version `git describe --tags`
```
read -rd '\000' helpmessage
++ basename ./build/run-build-packages-one-target.sh
++ basename ./build/run-build-packages-one-target.sh
+ set -e
+ [ -n /home/nico/jobs/curii/arvados ]
+ [ -d /home/nico/jobs/curii/arvados ]
++ getopt --name ./build/run-build-packages-one-target.sh --longoptions help,debug,test-packages,target:,command:,only-test:,force-test,only-build,force-build,build-version: -- '' --target debian10 --only-build lib/pam --build-version 2.0.0-553-ge37223349 + PARSEDOPTS='' --target ''\'\'debian10''\'\'' --only-build ''\'\'lib/pam''\'\'' --build-version ''\'\''2.0.0-553-ge37223349```
```
+ '[' 0 -ne 0 '']'
+ TARGET=debian10
+ FORCE_BUILD=0 + COMMAND=
+ DEBUG=
+ eval set -- ' --target ''\'\'debian10''\'\'' --only-build ''\'\'lib/pam''\'\'' --build-version ''\'\''2.0.0-553-ge37223349''\'\'' --
+ '[' 7 -gt 0 '']'
+ case "$1" in
+ TARGET=debian10
+ shift
+ shift
+ '[' 5 -gt 0 '']'
+ case "$1" in
+ ONLY_BUILD=lib/pam
+ shift
+ shift
+ '[' 3 -gt 0 '']'
+ case "$1" in
+ [ -z 2.0.0-553-ge37223349 ])
+ [ 2.0.0-553-ge37223349 =~ (.*)-(.* )]
+ ARVADOS_BUILDING_VERSION=2.0.0-553
+ ARVADOS_BUILDING_ITERATION=ge37223349
+ shift
+ shift
+ '[' 1 -gt 0 '']'
+ case "$1" in
+ '[' 0 -gt 0 '']'
+ shift
+ shift
+ '[' -n 2.0.0-553 ]]
++ echo 'build version='''2.0.0-553''', package iteration='''ge37223349''''
build version='''2.0.0-553'', package iteration='''ge37223349'''
++ '[' -n '' '']'
+ IMAGE=arvados/build:debian10
+ ['[ '' != '' ]]
++ readlink -e ./build/run-build-packages-one-target.sh
++ dirname /home/nico/jobs/curii/arvados/build/run-build-packages-one-target.sh
+ JENKINS_DIR=/home/nico/jobs/curii/arvados/build
+ ['[ -n '' ]]
++ pushd /home/nico/jobs/curii/arvados/build/package-build-dockerfiles
+ echo 'build version='''2.0.0-553''', package iteration='''ge37223349'''
+ echo debian10/generated
wget -c-q0 common-generated/gol.13.4.linux-amd64.tar.gz https://dl.google.com/go/gol.13.4.linux-amd64.tar.gz
wget -c-q0 common-generated/node-v6.11.2-linux-x64.tar.xz https://nodejs.org/dist/v6.11.2/node-v6.11.2-linux-x64.tar.xz
wget -c-q0 common-generated/mpapis.asc https://rpm.io/mpapis.asc
wget -c-q0 common-generated/pkuczynski.asc https://rpm.io/pkuczynski.asc
test -d debian10/generated || mkdir debian10/generated
cp -rlt debian10/generated common-generated/* + echo debian10
```
```
+ cd debian10
+ docker build --tag=arvados/build:debian10 .

Sending build context to Docker daemon 129.3MB

Step 1/15 : FROM debian:buster
 ---> 1b686a959dbf
Step 2/15 : MAINTAINER Ward Vandewege <vvandewege@veritasgenetics.com>
 ---> Using cache
 ---> b7f49096ee66
Step 3/15 : ENV DEBIAN_FRONTEND noninteractive
 ---> Using cache
 ---> 8b3083e2c043e
Step 4/15 : RUN /usr/bin/apt-get update && /usr/bin/apt-get install -q -y python2.7-dev python3 python-setuptools python3-setuptools dev E

Step 5/15 : RUN /usr/bin/pip install 'virtualenv<20'
 ---> Using cache
 ---> 84a15a95a74a
Step 6/15 : ADD generated/mpapis.asc /tmp/
 ---> Using cache
 ---> ef75c80a4b11
Step 7/15 : ADD generated/pkuczynski.asc /tmp/
 ---> Using cache
 ---> 4ff108d4e7f4
 ---> Using cache
 ---> 05087b319b2
Step 9/15 : ADD generated/go1.13.4.linux-amd64.tar.gz /usr/local/
 ---> Using cache
 ---> 19e8c1347c2
Step 10/15 : ADD generated/node-v6.11.2-linux-x64.tar.xz /usr/local/
 ---> Using cache
 ---> 293a6057d340
Step 11/15 : ADD generated/go1.13.4.linux-amd64.tar.gz
 ---> Using cache
 ---> 254067212682
Step 12/15 : ADD generated/node-v6.11.2-linux-x64.tar.xz
 ---> Using cache
 ---> 06bf7df0704e
Step 13/15 : ADD generated/go1.13.4.linux-amd64.tar.gz
 ---> Using cache
 ---> 769e26445baf
Successfully built 769e26445baf
Successfully tagged arvados/build:debian10

real 0m0.483s
user 0m0.053s
sys 0m0.106s
+ popd
-/jobs/curii/arvados
+ test -z ''
+ packages="arvados-api-server
arvados-client
arvados-docker-cleaner
arvados-git-httpd
arvados-node-manager
arvados-src
arvados-workbench
crunch-dispatch-local
crunch-dispatch-slurm
crunch-run"
crunchstat
keep-balance
keep-block-check
keepproxy
keep-rsync
keepstore
keep-web
libarvados-perl
python-arvados-fuse
python-arvados-python-client
python-arvados-cwl-runner'
+ FINAL_EXITCODE=0
+ package_fails=
+ mkdir -p /home/nico/jobs/curii/arvados/apps/workbench/vendor/cache-debian10
+ mkdir -p /home/nico/jobs/curii/arvados/services/api/vendor/cache-debian10
+ [[ -n '' ]]
+ echo
+ echo 'START: build packages on arvados/build:debian10'
START: build packages on arvados/build:debian10
+ [[ ! -e /home/nico/jobs/curii/arvados/packages/debian10/processed ]]
+ set +e
+ mv -f /home/nico/jobs/curii/arvados/packages/debian10/processed /home/nico/jobs/curii/arvados/packages/debian10/processed/
+ set -e
/usr/local/lib/python2.7/dist-packages/setuptools/dist.py:476: UserWarning: Normalizing '2.0.0-553' to '2.0.0.post553'
normalized_version,
Cloning into 'cwltest'...
Cloning into 'cwltest'...
Cloning into 'cwltest'...
You are in 'detached HEAD' state. You can look around, make experimental changes and commit them, and you can discard any commits you make in this state without impacting any branches by performing another checkout.
Note: checking out '1.0.20190906212748'.
If you want to create a new branch to retain commits you create, you may do so (now or later) by using -b with the checkout command again. Example:

git checkout -b <new-branch-name>

HEAD is now at 98ca3c9 Merge pull request #95 from common-workflow-language/valid_package_data
go: finding cloud.google.com/go v0.38.0

go: finding github.com/arvados/goamz v0.0.0-20190905141525-1bb109f407ef

go: finding github.com/Azure/azure-sdk-go v19.1.0+incompatible

go: finding github.com/alcortesm/tgz v0.0.0-20161002113705-648efa622239

go: finding github.com/alecthomas/template v0.0.0-20190718012654-fb15b899a751

go: finding github.com/alcortesm/tgz v0.0.0-20161220082320-9c5f6e88206d7

go: finding github.com/alcortesm/template v0.0.0-20190718012654-fb15b899a751

go: finding github.com/alcortesm/units v0.0.0-20190717042225-c3de453c63f4

go: finding github.com/anmitsu/go-shlex v0.0.0-20161002113705-648efa622239

go: finding github.com/arvados/cgofuse v1.2.0-arvados1

go: finding github.com/aws/aws-sdk-go v1.25.30

go: finding github.com/beorn7/perks v1.0.1

go: finding github.com/bgrunt/better-regex v0.2.0

go: finding github.com/bradleyheid/podinfo v0.0.0-20170216002349-c249933bc092

go: finding github.com/cembre/xxhash/v2 v2.0.1

go: finding github.com/client9/misspell/v0.3.4

go: finding github.com/coreos/go-oidc v2.1.0+incompatible

go: finding github.com/coreos/go-systemd v0.0.0-20180108085132-cc4f39464dc7

go: finding github.com/davech/gop-spew v1.1.1

go: finding github.com/dgrjialva/jwt-go v3.1.0+incompatible

go: finding github.com/dimchansky/utfbom v1.0.0
I get the successful message but the deb package isn’t there.

```
[nico@jobs/curii/arvados] master ± find -name *deb
[nico@jobs/curii/arvados] master ± cd packages/debian10
[nico@jobs/curii/arvados/packages/debian10] master ± find .
```

I think this was a successful test (even if error="permission denied" was emitted) I don’t have shell access in that machine.

```
root@bdd7de30d774:/# login nico
Password:
DEBU[0002] username="nico" arvados_api_host="su921.arvadosapi.com" hostname="shell" insecure=false
ERRO[0002] authentication failed error="request failed: https://su921.arvadosapi.com/arvados/v1/virtual_machines?cluster_id=&count=&filters=%5B%5B%22hostname%22%2C%22%3D%22%3D%22%2C%22shell%22%22%5D%5D%5D&limit=2&offset=0: 401 Unauthorized: Not logged in (req-8kxe4zmvi1817kk5man)"
Login incorrect
```

#8 - 06/25/2020 03:21 PM - Nico César

I think this was a successful test (even if error="permission denied" was emitted) I don’t have shell access in that machine.

```
root@bdd7de30d774:/# login nico
Password:
DEBU[0002] username="nico" arvados_api_host="su921.arvadosapi.com" hostname="shell" insecure=false
ERRO[0002] authentication failed error="request failed: https://su921.arvadosapi.com/arvados/v1/virtual_machines?cluster_id=&count=&filters=%5B%5B%22hostname%22%2C%22%3D%22%3D%22%2C%22shell%22%22%5D%5D%5D&limit=2&offset=0: 401 Unauthorized: Not logged in (req-8kxe4zmvi1817kk5man)"
Login incorrect
```

#9 - 06/25/2020 04:05 PM - Ward Vandewege

- Related to Bug #6649: [Documentation] webshell installation added

#10 - 06/25/2020 04:39 PM - Nico César

I’ve been trying out different things and here are the results:

If the user has not been enabled with the "Setup Account" dialog in the cluster, there will be a somehow confusing error: no results for hostname "shell". I think this is because the virtual machine will look like a 404 to that token.

```
root@bdd7de30d774:/# login nico
Password:
DEBU[0002] username="nico" arvados_api_host="su921.arvadosapi.com" hostname="shell" insecure=false
ERRO[0002] authentication failed error="no results for hostname \"shell\"
```

After asking Javier to enable the account, the expected behaviour happened (with wrong token and with correct token below):

```
root@bdd7de30d774:/# login nico
Password:
DEBU[0002] username="nico" arvados_api_host="su921.arvadosapi.com" hostname="shell" insecure=false
ERRO[0003] authentication failed error="request failed: https://su921.arvadosapi.com/arvados/v1/virtual_machines?cluster_id=&count=&filters=%5B%5B%22hostname%22%2C%22%3D%22%3D%22%2C%22shell%22%22%5D%5D%5D&limit=2&offset=0: 401 Unauthorized: Not logged in (req-c46udilgizfl146us3cn)"
```
Login incorrect
bdd7de30d774 login:

root@bdd7de30d774:/# login nico
Password:
DEBU[0002] username="nico" arvados_api_host="pirca.arvadosapi.com" hostname="shell" insecure=false
DEBU[0002] permission granted based on link with UUID pirca-o0j2j-jsltqiqcm88kgvj
Linux bdd7de30d774 5.6.0-2-amd64 #1 SMP Debian 5.6.14-1 (2020-05-23) x86_64
The programs included with the Debian GNU/Linux system are free software;
#11 - 06/26/2020 08:29 PM - Tom Clegg
Updated error message.

- return fmt.Errorf("no results for hostname %q", hostname)
+ // It's possible there is no VM entry for the
+ // configured hostname, but typically this just means
+ // the user does not have permission to see (let alone
+ // log in to) this VM.
+ return errors.New("permission denied")

15348-pam-module @ ce3903121eb9645e99f6f6846de421b9af1bb23f -- https://ci.arvados.org/view/Developer/job/developer-run-tests/1934/

#12 - 06/29/2020 03:58 PM - Nico César
My personal opinion to this questions

Should we list ca-certificates as a recommended/dependency pkg? Without it, even valid certs fail verification -- but the "insecure" option means verification isn't strictly necessary.

I say yes to this, we have to look all the distros we supporta and see if the ca-certificates (or equivalent) works as we expect.

Should the package also drop an example/template file in /usr/share/pam-configs/arvados like its python-based predecessor? This is how docker_test.go enables the module, but it doesn't work out of the box IRL because the operator needs to specify their real API host. (If there was a default/conventional API host name like "api", we could use that, but we don't have that rn.)

Yes. drop the file and also have a message when you install the package that has the words "YOU NEED TO CONFIGURE THIS" large, friendly letters.

Should we make the "vm name" config arg optional, and call gethostname() if it isn’t provided?

My take here: make it optional. Most of the gethostname() results could be pretty random, not every sysadmin takes the time to make it right, specially with cloud instances (and sometimes the cloud agent will sabotage you when rebooting the machine, I'm talking to you Azure).

#13 - 06/29/2020 03:59 PM - Nico César
commit ce3903121eb9645e99f6f6846de421b9af1bb23f LGTM

#14 - 06/29/2020 04:03 PM - Ward Vandewege
Tom Clegg wrote:

Questions

● Should we list ca-certificates as a recommended/dependency pkg? Without it, even valid certs fail verification -- but the "insecure" option means verification isn't strictly necessary.

I'm leaning towards making ca-certificates a dependency. It's pretty annoying to debug pam problems; removing a pitfall seems smart.

● Should the package also drop an example/template file in /usr/share/pam-configs/arvados like its python-based predecessor? This is how docker_test.go enables the module, but it doesn't work out of the box IRL because the operator needs to specify their real API host. (If there was a default/conventional API host name like "api", we could use that, but we don't have that rn.)

Probably unnecessary if we document things well. Do what Nico said above, please.

● Should we make the "vm name" config arg optional, and call gethostname() if it isn’t provided?
That’s a nice to have from my perspective, I wouldn’t block on it or spend much time on it.

#15 - 07/01/2020 03:32 PM - Peter Amstutz
- Target version changed from 2020-07-01 Sprint to 2020-07-15

#16 - 07/01/2020 03:38 PM - Tom Clegg
- Target version changed from 2020-07-15 to To Be Groomed

#17 - 07/02/2020 03:28 PM - Tom Clegg
15348-pam-module @ 183f8c6f6eb5d3dabf36a1a4af1122607f55617 -- https://ci.arvados.org/view/Developer/job/developer-run-tests/1940/  
- rename pkg to libpam-arvados-go  
- webshell install docs say to use libpam-arvados-go instead of the python one  
- package includes /usr/share/doc/libpam-arvados-go/README with usage summary and a link to webshell doc page  
- package includes an example/template file in /usr/share/pam-configs that pam-auth-update can use  
- hostname is optional; if omitted (or "-" which is needed as a placeholder if you’re using insecure/debug options) the current hostname is used instead  
- package lists ca-certificates as a dependency  
  (edit: see note below)

#18 - 07/02/2020 09:03 PM - Tom Clegg
Found & fixed the packaging bug so the dependency works now.

This also means the next version of keep-web will actually have the fix we thought we added in #16100 (cf. http://apt.arvados.org/pool/buster/main/k/keep-web/keep-web_2.0.3-1_amd64.deb which does not actually list any dependencies).

15348-pam-module @ d5b5f3d7c9a218c26cb40c5e1d79136b2d75749 -- https://ci.arvados.org/view/Developer/job/developer-run-tests/1941/  
- File libpam-arvados-go_2.0.0-599-gd5b5f3d7c_amd64.deb added

#20 - 07/06/2020 03:29 PM - Tom Clegg
- Target version changed from To Be Groomed to 2020-07-15

#21 - 07/06/2020 03:49 PM - Ward Vandewege
- Related to Bug #16100: [keep-web] Avoid sniffing for content type when file extension matches a MIME type added

#22 - 07/06/2020 03:56 PM - Ward Vandewege
15348-pam-module @ d5b5f3d7c9a218c26cb40c5e1d79136b2d75749 LGTM. We will need to cherry pick this commit and do an errata for the #16100 bugfix in the release notes for the next point release, if we do another one on the 2.0 series.

#23 - 07/06/2020 06:18 PM - Ward Vandewege
- Release set to 34

Added to release 2.0.4 because we should include d5b5f3d7c9a218c26cb40c5e1d79136b2d75749 to fix the package dependency bug that affected #16100

#24 - 07/06/2020 07:08 PM - Tom Clegg
- Status changed from In Progress to Resolved

#25 - 08/04/2020 08:28 PM - Ward Vandewege
- Release changed from 34 to 25

#26 - 09/29/2020 09:57 PM - Ward Vandewege
- Related to Bug #16920: [libpam-arvados-go] the deployed pam config breaks /usr/sbin/pam-auth-update added

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>libpam-arvados-experimental_2.0.0-551-gb694b711c_amd64.deb</td>
<td>6.33 MB</td>
<td>06/23/2020</td>
</tr>
<tr>
<td>libpam-arvados-go_2.0.0-599-gd5b5f3d7c_amd64.deb</td>
<td>6.33 MB</td>
<td>07/02/2020</td>
</tr>
</tbody>
</table>

05/07/2021