Adopting enterprise domain clients to Silverblue

FreeIPA view

Alexander Bokovoy

Sr. Principal Software Engineer // Red Hat

A tale of a tree

Let’s register an ostree system

To the FreeIPA domain!

We have a Fedora Silverblue system that should be enrolled into a FreeIPA domain

- Installed using official Fedora Silverblue image
- … then rebased to a custom image that has all required packages
- We want to register it automatically
    - But do it manually first time

First attempt

```
root@fedora:~# ipa-client-install --domain example.test
This program will set up IPA client.
Version 4.12.1

Discovery was successful!
Do you want to configure chrony with NTP server or pool address? [no]: no
Client hostname: silverblue.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: id.example.test
BaseDN: dc=example,dc=test

Continue to configure the system with these values? [no]: yes
[Errno 2] No such file or directory: '/var/lib/ipa-client/sysrestore/sysrestore.state'
The ipa-client-install command failed. See /var/log/ipaclient-install.log for more information
```

A directory is not present

But it is in the package!

- /var has special handling in ostree
- /var was created by the original Silverblue installation without freeipa-client and dependent packages
- FreeIPA needs to move to use tmpfiles.d to create own directories in /var

Fixing the directories for FreeIPA, we get next

```
Continue to configure the system with these values? [no]: yes
Synchronizing time
Configuration of chrony was changed by installer.
Attempting to sync time with chronyc.
Process chronyc waitsync failed to sync time!
Unable to sync time with chrony server, assuming the time is in sync. Please check that 123 UDP port is opened
, and any time server is on network.
Please make sure the following ports are opened in the firewall settings:
     TCP: 80, 88, 389
     UDP: 88 (at least one of TCP/UDP ports 88 has to be open)
Also note that following ports are necessary for ipa-client working properly after enrollment:
     TCP: 464
     UDP: 464, 123 (if NTP enabled)
Installation failed. Rolling back changes.
Failed to start certmonger: CalledProcessError(Command ['/bin/systemctl', 'start', 'certmonger.service'] retur
ned non-zero exit status 1: 'Job for certmonger.service failed because the control process exited with error c
ode.\nSee "systemctl status certmonger.service" and "journalctl -xeu certmonger.service" for details.\n')
CalledProcessError(Command ['/bin/systemctl', 'start', 'certmonger.service'] returned non-zero exit status 1:
'Job for certmonger.service failed because the control process exited with error code.\nSee "systemctl status
certmonger.service" and "journalctl -xeu certmonger.service" for details.\n')
```

Certmonger has the same problem

```
Aug 07 22:53:49 silverblue.example.test systemd[1]: Starting certmonger.service - Certificate monitoring and P
KI enrollment...
Aug 07 22:53:49 silverblue.example.test certmonger[4524]: 2024-08-07 22:53:49 [4524] Changing to root director
y.
Aug 07 22:53:49 silverblue.example.test certmonger[4524]: 2024-08-07 22:53:49 [4524] Obtaining system lock.
Aug 07 22:53:49 silverblue.example.test certmonger[4524]: Error opening lockfile "/var/lib/certmonger/lock": N
o such file or directory
Aug 07 22:53:49 silverblue.example.test systemd[1]: certmonger.service: Main process exited, code=exited, stat
us=1/FAILURE
Aug 07 22:53:49 silverblue.example.test systemd[1]: certmonger.service: Failed with result 'exit-code'.
Aug 07 22:53:49 silverblue.example.test systemd[1]: Failed to start certmonger.service - Certificate monitorin
g and PKI enrollment.
```

- Same here: /var/lib/certmonger would need to be created if missing via tmpfiles.d

Now we are successful

```
...
Enrolled in IPA realm EXAMPLE.TEST
Created /etc/ipa/default.conf
Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring example.test as NIS domain.
Configured /etc/krb5.conf for IPA realm EXAMPLE.TEST
Client configuration complete.
The ipa-client-install command was successful
```

```
# sssctl domain-status example.test
Online status: Online

Active servers:
IPA: id.example.test

Discovered IPA servers:
- id.example.test
- id.example.test
```

Grafting the tree

Adjust FreeIPA to ostree realities

(not so) easy fruits

- tmpfiles.d
- Configuration generators vs reuse of pre-defined layers
- Automated domain join
- Security
- Flatpaks and toolboxes

tmpfiles.d

Easy fruits

- FreeIPA client
  - Fixing /var/lib/ipa-client/sysrestore and /var/lib/certmonger is enough
- FreeIPA server
  - A lot more work

Configuration generators

Traditional way

- FreeIPA client installer
  - Discovers deployment configuration (domain, Kerberos realm, CA chain trust, etc.)
  - Creates SSSD and Kerberos configuration
  - Changes system setup for PAM and nsswitch.conf via authselect
  - Enables various systemd services

Reuse of pre-defined layers

Alternative approach

- Custom image is anyway needed
  - Add required packages to enable enrollment/services
  - IPA deployment configuration can be distributed as an image layer (FROM … AS … statement in Containerfile)
    - Content of the layer can be verified for integrity at runtime
    - New tooling would be needed to generate content layer data out of existing IPA deployment
- IPA client installer could detect the ostree-based environment and adjust itself automatically

Better domain join experience

ostree image is accessible

To attackers

- “They all look the same”
- Secrets and credentials
- Integrity checks
- Automation and validation

Boxes, boxes, boxes

factory-provisioned

- “They all look the same”
- Secrets and credentials
- Integrity checks
- Automation and validation

Side-load

credentials

- Ignition et al.
- systemd-creds (https://systemd.io/CREDENTIALS/) and pass-in from the hypervisors or container managers
- TPM or PKCS#11 tokens

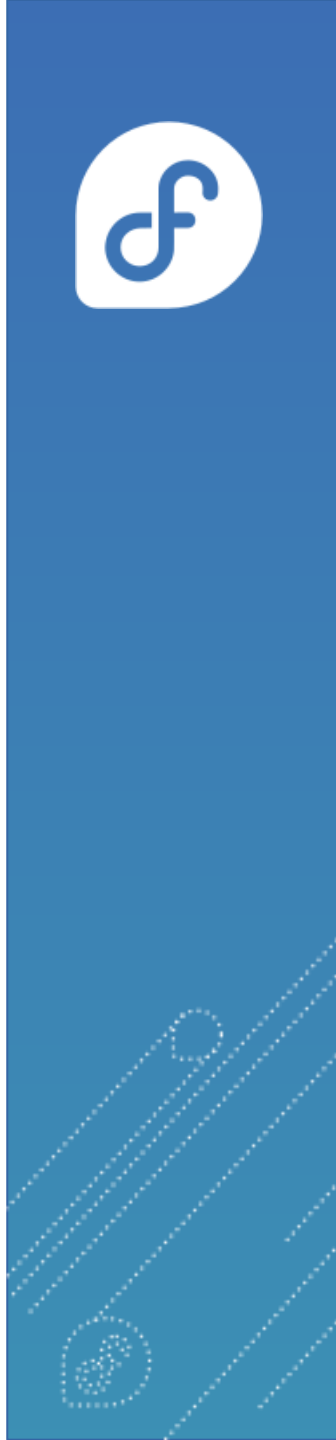
But how to use them to enroll into FreeIPA?

Certificate-based enrollment

Bug #2075452

Alexandre Maumené 2022-04-14 09:19:17 UTC Description

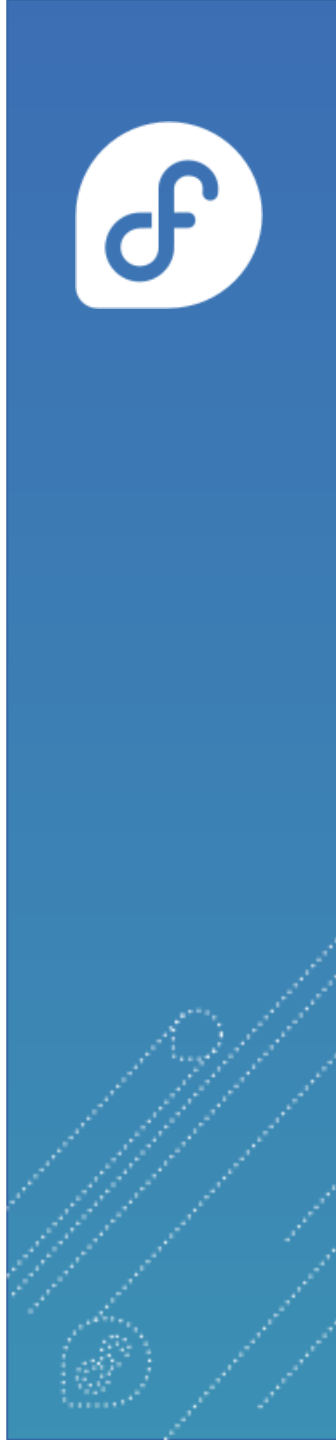
```
Description of problem:

We would like to deploy 5G Distributed Unit (basically x86 servers strapped on
pole, next to a 5G antenna) in a ZTP (Zero Touch Provisioning) manner. The DU
servers will be provisioned in factory and then send directly on site. Since we
want to achieve ZTP we cannot register our servers with ipa-client using a One
Time Password. Those servers will be installed outdoor (and not in DC) so there
won't be possibility for an operator to connect to it prior its installation.

But from factory, the servers will each be provisioned with its own certificate
We would like to know if it would be possible to use such certificate to
register the server with IDM.

Thanks in advance.
```



Kerberos PKINIT

using certificates to authenticate to IPA server during install

- Credentials for enrollment
  - Can be certificate and key files or PKCS#11 (smartcard/HSM/TPM) tokens, even remotely forwarded with p11-kit proxy
- Behind the scenes
  - Take care! Fraser Tweedale's PKINIT talk at FOSDEM 2023: https://archive.fosdem.org/2023/schedule/event/security_kerberos_pkinit/
- Extensions



Podengo project

https://github.com/podengo-project

- Domain and identity services for console.redhat.com
  - Currently deployed in staging
- ipa-hcc
  - IPA server extensions
  - Client integration

Client side integration

Rather, subscription manager integration

- Register with RHSM/Insights
- Self-register host to IPA
- Use RHSM-provisioned certificate to enroll to IPA

```
# rhc connect
...

# curl \
    --cacert /root/kdc-ca-bundle.pem \
    --cert /etc/pki/consumer/cert.pem \
    --key /etc/pki/consumer/key.pem \
    https://ipaserver.hmsidm.test/hcc
...

# ipa-client-install \
  --pkinit-identity=FILE:/etc/pki/consumer/cert.pem,/etc/pki/consumer/key.pem \
  --pkinit-anchor=FILE:/root/kdc-ca-bundle.pem \
  --server ipaserver.hmsidm.test --domain hmsidm.test -U -N
...
```

Flatpaks and toolboxes

Roots, roots everywhere!

System-wide security settings

- Enterprise requirements and government regulations
  - FIPS 140-3 enforcement
- crypto-policy
  - System-wide cryptographical libraries' defaults
  - Configuration assumes presence of certain libraries and plugins
- Kerberos configuration
  - Plugins, libraries, configurations, and tools

Thank you!