Upgrading to HTCondor 9.0

Why is this upgrade different?

- HTCondor now ships with a secure configuration.
- This configuration does not use host-based security.
- Many existing HTCondor configurations depend on host-based security.
- This talk will be about dealing with the implications of this change.

New Default Configuration

- The meta-knob `use security:recommended_v9_0` lets us update the default configuration without touching your configuration files.
  - `condor_config_val use security:recommended_v9_0`
- Authentication, encryption, and integrity required
  - except for READ, which is optional
- Authorizations for “condor”, “condor_pool”, and “root”
  - except for WRITE, which authorizes all authenticated users
  - and READ, which authorizes everyone

Written Instructions

- Instructions for upgrading from 8.8 are in the manual.
- The instructions for upgrading from 8.9 are very similar, but have two additional points dealing with changes made during the development IDTOKENs.
- You should also review the significant changes listed in the manual for other potential issues.

Four Upgrade Paths

Consider putting jobs on hold before upgrading.

- Retain (strong security)
- Reinstall
- Reconfigure
- Revert (to weaker security)

Retain Strong Security

- Benefits
  - Easy to do.
  - Your pool remains secure.
  - Certain to maintain existing non-security configuration.
- Drawbacks
  - Doesn’t apply to everyone.
  - If your strong security method is GSI, you’re just delaying the inevitable, and it may be easier to switch to IDTOKENS by reinstalling.

Retain Strong Security (Directions)

1. Install the new HTCondor binaries in your usual way.
   - For RPMs or debs, use the new repository locations.
2. Disable the newly-installed configuration.
   - Empty out `/etc/condor/config.d/00-htcondor-9.0.config`
   - Will be reinstalled if missing, so don't delete it!
3. Update any obsolete configuration.
   - Set (if necessary) `ALLOW_DAEMON` (based on `ALLOW_WRITE`)
   - Replace (if necessary) `HOSTALLOW`, `HOSTDENY`

Reinstall

- Benefits
  - Your pool becomes more secure.
  - You don’t have to create or distribute signing keys or tokens.
  - Start with a clean, well-known, and well-supported configuration.
- Drawbacks
  - Must learn new *get_htcondor* tool.
  - Must re-customize the configuration (potentially tricky).

Reinstall (Overview)

1. Back up your existing configuration.
2. Save your existing configuration changes:

```
condor_config_val -summary > saved_configuration
```

3. Back up the spool directory (on the schedd):

```
cp -a `condor_config_val SPOOL` path/to/backup/spool
```

4. Uninstall HTCondor and remove existing configuration.
5. Reinstall using *get_htcondor*.
6. Restore your previous non-security custom configuration.

get_htcondor

› On the web, for new Linux installations only.

```
$ curl -fsSL https://get.htcondor.org | /bin/bash -s --
# Installing mini HTCondor for Ubuntu focal

# Adding our repository
apt-get update
apt-get install -y gnupg
curl -fsSL https://research.cs.wisc.edu/htcondor/repo/keys/HTCondor-current-Key | apt-key add -
echo "deb [arch=amd64] https://research.cs.wisc.edu/htcondor/repo/ubuntu/current focal main" \
    > /etc/apt/sources.list.d/htcondor.list
echo "deb-src https://research.cs.wisc.edu/htcondor/repo/ubuntu/current focal main" \
    >> /etc/apt/sources.list.d/htcondor.list

…
```

get_htcondor

- stand-alone installation:
  - **curl -fsSL https://get.htcondor.org | sudo /bin/bash -s -- --no-dry-run**
- multi-machine installation:
  - curl -fsSL https://get.htcondor.org | GET_HTCONDOR_PASSWORD="$htcondor_password" sudo /bin/bash -s -- --no-dry-run --central-manager $central_manager_name
  - curl -fsSL https://get.htcondor.org | GET_HTCONDOR_PASSWORD="$htcondor_password" sudo /bin/bash -s -- --no-dry-run --submit $central_manager_name
  - curl -fsSL https://get.htcondor.org | GET_HTCONDOR_PASSWORD="htcondor_password" sudo /bin/bash -s -- --no-dry-run --execute $central_manager_name

get_htcondor (Security)

- Very similar, but not identical to `recommended_v9_0`.
  - Explicitly limits authentication methods to FS and IDTOKENS.
  - Adds ANONYMOUS for READ only, instead of relaxing authorization, encryption, or integrity.
  - Is more specific about authorized identities (because it creates all of them); does not include “condor_pool”.

Recustomizing Configuration

- Read `/etc/condor/config.d/01-<role>.config`
- Begin with the `saved_configuration` file from step 2.
  - Each stanza in this file came from a different file on disk, which you may wish to re-create.
  - Check the originals for meta-knobs.
  - You probably had comments in each of those original files that this file does not; it may be worth fishing them out of the back-up.
  - Remove security-specific configuration.
    - Probably anything with `SEC` in it.
    - Probably anything with `ALLOW` or `DENY` in it.

Reconfigure

- Benefits
  - Your pool becomes more secure.
  - You don’t have to re-install.
  - Highly likely to maintain existing non-security configuration.
- Drawbacks
  - Potentially tricky to get right.

Reconfigure (Directions 1)

1. Install the new HTCondor binaries in your usual way.
   - For RPMs or debs, use the new repository locations.
2. Remove all other security settings.
3. Set up IDTOKENs:
   1. Create signing key
   2. Create IDTOKEN
   3. Repeat on each machine in the pool (with the same password)
      or
      securely copy resulting files to each machine in the pool
4. Update any obsolete configuration.

Reconfigure (Directions 2)

Create signing key (as root):

```
condor_store_cred -c add
```

(file is `condor_config_val SEC_PASSWORD_FILE`)

Create IDTOKEN (as root):

```
umask 0077; condor_token_create –identity \
  condor@mypool > /etc/condor/tokens.d/condor@mypool
```

Revert to Lower Security

- Benefits
  - Easy to do.
  - Certain to maintain existing non-security configuration.
- Drawbacks
  - Your pool remains less secure.
  - You will be maintaining a non-standard configuration.

Revert to Lower Security (Directions)

1. Install the new HTCondor binaries in your usual way.
   - For RPMs or debs, use the new repository locations.
2. Adjust the newly-installed configuration file
   1. Read `/etc/condor/config.d/00-htcondor-9.0.config`
      - Will be reinstalled if missing, so don't delete it!
   2. Comment out `use security:recommended_v9_0`
   3. Uncomment `use security:host_based`
3. Update any obsolete configuration.
   - Set (if necessary) `ALLOW_DAEMON` (based on `ALLOW_WRITE`)
   - Replace (if necessary) `HOSTALLOW`, `HOSTDENY`

Demonstration

- Go through the re-install method on Debian 10.

New Configuration for Old Clients

- For example, old Python bindings in a virtualenv.
- Old clients don't understand the new default configuration.
- Two choices:
  - Comment out, paste in results of

    ```
    condor_config_val use security:recommended_v9_0
    ```

  - Make conditional on HTCondor version:

    ```
    if version > 9.0.0
        use security:recommended_v9_0
    endif
    ```

Questions?

htcondor-admin@cs.wisc.edu

IDTOKEN Extensions

- Issue an IDTOKEN for each user
  - Use `condor_token_create -identity`
- Issue an IDTOKEN to a remote pool (flock in)
  - Create a token, add its identity to `FLOCK_FROM`.
- Use an IDTOKEN for a remote pool (flock out)
  - Copy token to `/etc/condor/tokens.d`.
  - Add its central manager to `FLOCK_TO`.