NAME

pro – Manage Ubuntu Pro services from Canonical

SYNOPSIS

pro <command> [<args>]
ua <command> [<args>]
ubuntu-advantage <command> [<args>]

DESCRIPTION

Ubuntu Pro is a collection of services offered by Canonical to Ubuntu users. The Ubuntu Pro command line tool is used to attach a system to an Ubuntu Pro contract to then enable and disable services from Canonical. The available commands and services are described in more detail below.

COMMANDS

attach [--no-auto-enable] [--attach-config=/path/to/file.yaml] <token>

Connect an Ubuntu Pro support contract to this machine.

The *token* parameter can be obtained from https://auth.contracts.canonical.com/.

The *--attach-config* option can be used to provide a file with the token and optionally, a list of services to enable after attaching. The *token* parameter should not be used if this option is provided. An attach config file looks like the following:

```
token: YOUR_TOKEN_HERE  # required
enable_services:        # optional list of service names to auto-enable
  - esm-infra
  - esm-apps
  - cis
```

The optional *--no-auto-enable* flag will disable the automatic enablement of recommended entitlements which usually happens immediately after a successful attach.

The exit code can be:

0: on successful attach
1: in case of any error while trying to attach
2: if the machine is already attached

collect-logs [-o <file>| --output <file>]

Create a tarball with all relevant logs and debug data.

The *--output* parameter defines the path to the tarball. If not provided, the file is saved as **ua_logs.tar.gz** in the current directory.

detach Remove the Ubuntu Pro support contract from this machine. This also disables all enabled services that can be.

disable [cc-eal|cis|esm|fips|fips-updates|livepatch|ros|ros-updates]

Disable this machine's access to an Ubuntu Pro service.

enable [cc-eal|cis|esm|fips|fips-updates|livepatch|ros|ros-updates]
Activate and configure this machine's access to an Ubuntu Pro service.

fix <security_issue>
Fix a CVE or USN on the system by upgrading the appropriate package(s).

<security_issue> can be any of the following formats: CVE-yyyy-nnnn, CVE-yyyy-nnnnnnn, or USN-nnnn-dd.

The exit code can be 0, 1, or 2.
0: the fix was successfully applied
1: the fix cannot be applied
2: the fix was applied but requires a reboot before it takes effect

refresh Refresh contract and service details from Canonical.

security-status
Show security updates for packages in the system, including all available ESM related content.

status [--format=tabular|json|yaml] [--simulate-with-token TOKEN] [--all]
Report current status of Ubuntu Pro services on system.

This shows whether this machine is attached to an Ubuntu Pro support contract. When attached, the report includes the specific support contract details including contract name, expiry dates, and the status of each service on this system.

The attached status output has four columns:

SERVICE: name of the service

ENTITLED: whether the contract to which this machine is attached entitles use of this service. Possible values are: *yes* or *no*

STATUS: whether the service is enabled on this machine. Possible values are: *enabled*, *disabled*, *n/a* (if your contract entitles you to the service, but it isn't available for this machine) or — (if you aren't entitled to this service)

DESCRIPTION: a brief description of the service

The unattached status output instead has three columns. **SERVICE** and **DESCRIPTION** are the same as above, and there is the addition of:

AVAILABLE: whether this service would be available if this machine were attached. The possible values are *yes* or *no*.

If --simulate-with-token is used, then the output has five columns. **SERVICE**, **AVAILABLE**, **ENTITLED** and **DESCRIPTION** are the same as mentioned above, and **AUTO_ENABLED** shows whether the service is set to be enabled when that token is attached.

If the --all flag is set, beta and unavailable services are also listed in the output.

version
Show version of the Ubuntu Pro package.

PRO UPGRADE DAEMON

Ubuntu Pro client sets up a daemon on supported platforms (currently GCP only) to detect if an Ubuntu Pro license is purchased for the machine. If an Ubuntu Pro license is detected, then the machine is automatically attached. If you are uninterested in Ubuntu Pro services, you can safely stop and disable the daemon using systemctl:

sudo systemctl stop ubuntu-advantage.service sudo systemctl disable ubuntu-advantage.service

TIMER JOBS

Ubuntu Pro client sets up a systemd timer to run jobs that need to be executed recurrently. The timer itself ticks every 5 minutes on average, and decides which jobs need to be executed based on their intervals.

Jobs are executed by the timer script if the script has not yet run successfully, or their interval since last successful run is already exceeded. There is a random delay applied to the timer, to desynchronize job execution time on machines spinned at the same time, avoiding multiple synchronized calls to the same service.

Current jobs being checked and executed are:

update_messaging
Makes sure that the MOTD and APT messages match the available/enabled services on the system, showing information about available packages or security updates.

CONFIGURATION

By default, Ubuntu Pro client configuration options are read from **/etc/ubuntu-advantage/uaclient.conf.**

The following configuration options are available:

contract_url
The Ubuntu Pro contract server URL

security_url
The Ubuntu Pro security server URL

data_dir
Where Ubuntu Pro client stores its data files

log_level
The logging level used when writing to **log_file**

log_file The log file for the Ubuntu Pro client cli

timer_log_file
The log file for the Ubuntu Pro timer and timer jobs

daemon_log_file
The log file for the Ubuntu Pro daemon

The following options must be nested under the "ua_config" key:

http_proxy
If set, pro will use the specified http proxy when making any http requests

https_proxy
If set, pro will use the specified https proxy when making any https requests

apt_http_proxy
[DEPRECATED] If set, pro will configure apt to use the specified http proxy by writing a apt config file to /etc/apt/apt.conf.d/90ubuntu-advantage-aptproxy. (Please use **global_apt_http_proxy**)

apt_https_proxy
[DEPRECATED] If set, pro will configure apt to use the specified https proxy by writing a apt config file to /etc/apt/apt.conf.d/90ubuntu-advantage-aptproxy. (Please use **global_apt_https_proxy**)

global_apt_http_proxy
If set, pro will configure apt to use the specified http proxy by writing a apt config file to /etc/apt/apt.conf.d/90ubuntu-advantage-aptproxy. Set this if you prefer a global proxy for all resources, not just the ones from *esm.ubuntu.com*

global_apt_https_proxy
If set, pro will configure apt to use the specified https proxy by writing a apt config file to /etc/apt/apt.conf.d/90ubuntu-advantage-aptproxy. Set this if you prefer a global proxy for all resources, not just the ones from *esm.ubuntu.com*

ua_apt_http_proxy
If set, pro will configure apt to use the specified http proxy by writing a apt config file to /etc/apt/apt.conf.d/90ubuntu-advantage-aptproxy. This proxy is limited to accessing resources from *esm.ubuntu.com*

ua_apt_https_proxy
If set, pro will configure apt to use the specified https proxy by writing a apt config file to /etc/apt/apt.conf.d/90ubuntu-advantage-aptproxy. This proxy is limited to accessing resources from *esm.ubuntu.com*

<job_name>_timer
Sets the timer running interval for a specific job. Those intervals are checked every time the systemd timer runs.

If needed, authentication to the proxy server can be performed by setting username and password in the URL itself, as in:

```
http_proxy: http://<username>:<password>@<fqdn>:<port>
```

Additionally, some configuration options can be overridden in the environment by setting an environment variable prefaced by **UA_<option_name>**. Both uppercase and lowercase environment variables are allowed. The configuration options that support this are: data_dir, log_file, timer_log_file, daemon_log_file, log_level, and security_url.

For example, the following overrides the log_level found in uaclient.conf:

```
UA_LOG_LEVEL=info pro attach
```

SERVICES

Common Criteria EAL2 Provisioning (cc-eal)
Enables and install the Common Criteria artifacts.

The artifacts include a configure script, a tarball with additional packages, and post install scripts. The artifacts will be installed in /usr/lib/common-criteria directory and the README and configuration guide are available in /usr/share/doc/ubuntu-commoncriteria directory.

CIS Audit (cis)
Enables and installs the CIS Audit artifacts.

Expanded Security Maintenance (esm)
Expanded Security Maintenance ensures the ongoing security and integrity of systems running Ubuntu Long Term Support (LTS) releases through Ubuntu Pro for Infrastructure.

See https://ubuntu.com/esm for more information.

FIPS 140-2 certified modules (fips)
Install, configure, and enable FIPS 140-2 certified modules.

After successfully enabling FIPS, the system MUST be rebooted. Failing to reboot will result in the system not running the updated FIPS kernel.

Disabling FIPS is not currently supported.

FIPS 140-2 certified modules with updates (fips-updates)
Install, configure, and enable FIPS 140-2 certified modules with updates. Enabling FIPS with updates will take the system out of FIPS compliance as the updated modules are not FIPS certified.

After successfully enabling FIPS with updates, the system MUST be rebooted. Failing to reboot will result in the system not running the updated FIPS kernel.

Disabling FIPS with updates is not currently supported.

Livepatch Service (livepatch)
Automatically apply critical kernel patches without rebooting. Reduces downtime, keeping your Ubuntu LTS systems secure and compliant.

See https://ubuntu.com/livepatch for more information.

ROS ESM Security Updates (ros)
Robot Operating System Expanded Security Maintenance - Only Security Updates provides security fixes for ROS packages to ensure the ongoing integrity of ROS based applications.

See https://ubuntu.com/robotics/ros-esm for more information.

ROS ESM All Updates (ros-updates)
Robot Operating System Expanded Security Maintenance - All Updates provides additional bug fixes in addition to security fixes for ROS packages to ensure the ongoing integrity of ROS based applications.

See https://ubuntu.com/robotics/ros-esm for more information.

REPORTING BUGS

Please report bugs either by running ‘ubuntu-bug ubuntu-advantage-tools‘ or login to Launchpad and navigate to https://bugs.launchpad.net/ubuntu/+source/ubuntu-advantage-tools/+filebug

COPYRIGHT