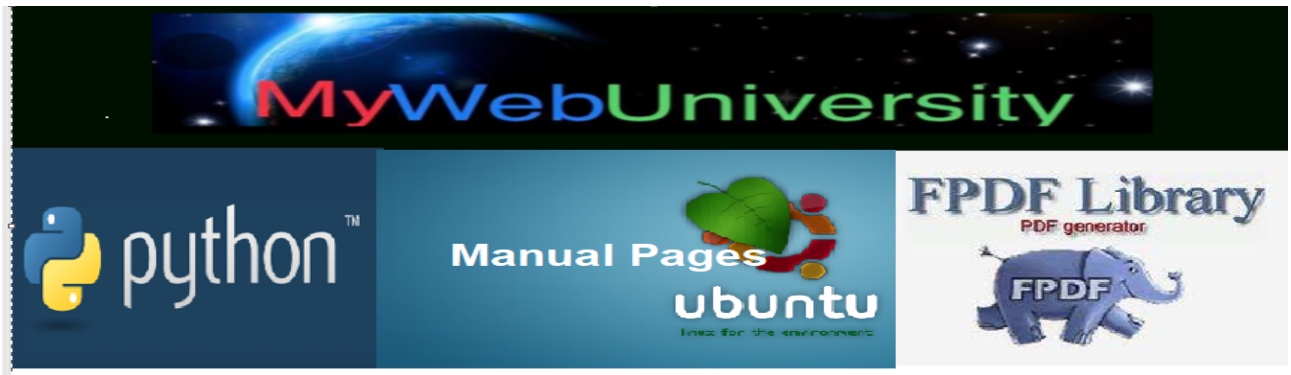

Full credit is given to the above companies including the OS that this PDF file was generated!

Linux Ubuntu 26.04 Manual Pages on command 'pro.1'

$ man pro.1

UBUNTU-PRO(1) Ubuntu Pro UBUNTU-PRO(1)

NAME

pro - Manage Ubuntu Pro services from Canonical

SYNOPSIS

pro [-h] [--debug] [--version] <command> ...

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.

OPTIONS

-h, --help

Show help for pro or for the specified pro command.

--debug

Redirect all the debugging logs to the console.

--version

Show the Pro Client version and exit.

COMMANDS

api [-h] [--show-progress] [--args [OPTIONS ...]] [--data DATA] endpoint

Calls the Client API endpoints.

For a list of all of the supported endpoints and their structure, please refer to the

Pro Client API reference guide:

https://canonical-ubuntu-pro-client.readthedocs-hosted.com/en/latest/references/api/

attach [-h] [--no-auto-enable] [--attach-config ATTACH_CONFIG] [--format {cli,json}] [token]

Attach this machine to an Ubuntu Pro subscription with a token obtained from: https://ubuntu.com/pro/dashboard

When running this command without a token, it will generate a short code and prompt you to attach the machine to your Ubuntu Pro account using a web browser.

The "attach-config" option can be used to provide a file with the token and option? ally, a list of services to enable after attaching. To know more, visit: https://canonical-ubuntu-pro-client.readthedocs-hosted.com/en/latest/howtogu? ides/how_to_attach_with_config_file/

The exit code will be:

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

auto-attach [-h]

Automatically attach on an Ubuntu Pro cloud instance.

collect-logs [-h] [-o OUTPUT]

Collect logs and relevant system information into a tarball. This information can be later used for triaging/debugging issues.

cve [-h] cve

Show all available information about a given CVE.

cves [-h] [--unfixable] [--fixable]

List the CVE vulnerabilities that affects the system.

config [-h] {show,set,unset} ...

Manage Ubuntu Pro Client configuration on this machine.

show [-h] [key]

Show customizable configuration settings.

set [-h] key_value_pair

Set and apply Ubuntu Pro configuration settings.

unset [-h] key

Unset an Ubuntu Pro configuration setting, restoring the default value.

detach [-h] [--assume-yes] [--format {cli,json}]

Detach this machine from an Ubuntu Pro subscription.

disable [-h] [--assume-yes] [--format {cli,json}] [--purge] service [service ...]

Disable one or more Ubuntu Pro services.

enable [-h] [--access-only] [--assume-yes] [--auto] [--beta] [--format {cli,json}] [--vari?
ant VARIANT] [service ...]

Activate and configure this machine's access to one or more Ubuntu Pro services.

fix [-h] [--dry-run] [--no-related] security_issue

Inspect and resolve Common Vulnerabilities and Exposures (CVEs) and Ubuntu Security Notices (USNs) on this machine.

The exit code will be:

* 0: the fix was successfully applied or the system is not affected
* 1: the fix cannot be applied
* 2: the fix was applied but requires a reboot before it takes effect

help [-h] [--format {tabular,json,yaml}] [--all] [service]

Provide detailed information about Ubuntu Pro services.

refresh [-h] [{contract,config,messages}]

Refresh three distinct Ubuntu Pro related artifacts in the system:

* contract: Update contract details from the server.
* config: Reload the config file.
* messages: Update APT and MOTD messages related to Pro.

You can individually target any of the three specific actions, by passing the target name to the command. If no target is specified, all targets are refreshed.

security-status [-h] [--format {json,yaml,text}] [--thirdparty | --unavailable | --esm-infra
| --esm-apps]

Show security updates for packages in the system, including all available Expanded Security Maintenance (ESM) related content.

Shows counts of how many packages are supported for security updates in the system.

If the format is set to JSON or YAML it shows a summary of the installed packages based on the origin:

- main/restricted/universe/multiverse: Packages from the Ubuntu archive.
- esm-infra/esm-apps: Packages from the ESM archive.
- third-party: Packages installed from non-Ubuntu sources.
- unknown: Packages which don't have an installation source (like local deb packages or packages for which the source was removed).

The output contains basic information about Ubuntu Pro. For a complete status on

Ubuntu Pro services, run 'pro status'.

status [-h] [--wait] [--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 con? tract 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, AVAIL? ABLE, 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 out? put.

system [-h] {reboot-required} ...

Output system-related information about Pro services.

reboot-required [-h]

Report the current reboot-required status for the machine.

This command will output one of the three following states for the machine regarding reboot:

* no: The machine doesn't require a reboot.
* yes: The machine requires a reboot.
* yes-kernel-livepatches-applied: There are only kernel-related

packages that require a reboot, but Livepatch has already provided patches for the current running kernel. The machine still needs a reboot, but you can assess if the reboot can be performed in the nearest maintenance window.

SERVICES

Anbox Cloud (anbox-cloud)

Anbox Cloud lets you stream mobile apps securely, at any scale, to any device, let? ting you focus on your apps. Run Android in system containers on public or private clouds with ultra low streaming latency. When the anbox-cloud service is enabled, by default, the Appliance variant is enabled. Enabling this service allows orchestration to provision a PPA with the Anbox Cloud resources. This step also configures the An? box Management Service (AMS) with the necessary image server credentials.

To learn more about Anbox Cloud, see https://anbox-cloud.io

Common Criteria EAL2 Provisioning (cc-eal)

Common Criteria is an Information Technology Security Evaluation standard (ISO/IEC IS 15408) for computer security certification. Ubuntu 16.04 has been evaluated to assur? ance level EAL2 through CSEC. The evaluation was performed on Intel x86_64, IBM Power8 and IBM Z hardware platforms.

CIS Audit (cis)/Ubuntu Security Guide (usg)

Ubuntu Security Guide is a tool for hardening and auditing, allowing for environment-specific customizations. It enables compliance with profiles such as DISA-STIG and the CIS benchmarks.

Find out more at https://ubuntu.com/security/certifications/docs/usg

Expanded Security Maintenance for Infrastructure (esm-infra)

Expanded Security Maintenance for Infrastructure provides access to a private PPA which includes available high and critical CVE fixes for Ubuntu LTS packages in the Ubuntu Main repository between the end of the standard Ubuntu LTS security mainte? nance and its end of life. It is enabled by default with Ubuntu Pro.

You can find out more about the service at https://ubuntu.com/security/esm

Expanded Security Maintenance for Applications (esm-apps)

Expanded Security Maintenance for Applications is enabled by default on entitled workloads. It provides access to a private PPA which includes available high and critical CVE fixes for Ubuntu LTS packages in the Ubuntu Main and Ubuntu Universe

repositories from the Ubuntu LTS release date until its end of life.

You can find out more about the esm service at https://ubuntu.com/security/esm

FIPS 140-2 certified modules (fips)

Installs FIPS 140 crypto packages for FedRAMP, FISMA and compliance use cases. Note that "fips" does not provide security patching. For FIPS certified modules with secu? rity patches please see "fips-updates". If you are unsure, choose "fips-updates" for maximum security.

Find out more at https://ubuntu.com/security/fips

FIPS 140-2 certified modules with updates (fips-updates)

fips-updates installs FIPS 140 crypto packages including all security patches for those modules that have been provided since their certification date.

You can find out more at https://ubuntu.com/security/fips

Landscape (landscape)

Landscape Client can be installed on this machine and enrolled in Canonical's Land? scape SaaS: https://landscape.canonical.com or a self-hosted Landscape: https://ubuntu.com/landscape/install

Landscape allows you to manage many machines as easily as one, with an intuitive dashboard and API interface for automation, hardening, auditing, and more.

Find out more about Landscape at https://ubuntu.com/landscape

Livepatch Service (livepatch)

Livepatch provides selected high and critical kernel CVE fixes and other non-security bug fixes as kernel livepatches. Livepatches are applied without rebooting a machine which drastically limits the need for unscheduled system reboots. Due to the nature of fips compliance, livepatches cannot be enabled on fips-enabled systems.

You can find out more about Ubuntu Kernel Livepatch service at https://ubuntu.com/se? curity/livepatch

ROS ESM Security Updates (ros)

ros provides access to a private PPA which includes security-related updates for available high and critical CVE fixes for Robot Operating System (ROS) packages. For access to ROS ESM and security updates, both esm-infra and esm-apps services will also be enabled. To get additional non-security updates, enable ros-updates.

You can find out more about the ROS ESM service at https://ubuntu.com/robotics/ros- esm

ROS ESM All Updates (ros-updates)

ros-updates provides access to a private PPA that includes non-security-related up?
dates for Robot Operating System (ROS) packages. For full access to ROS ESM, security
and non-security updates, the esm-infra, esm-apps, and ros services will also be en?
abled.

You can find out more about the ROS ESM service at https://ubuntu.com/robotics/ros-
esm

CONFIGURATION SETTINGS

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 con?
fig 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 con?
fig 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 con?
fig 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 con?
fig 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 con?
fig 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 con?
fig 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.

apt_news

If set to false, the Pro client will no longer display apt news messages on the out?
put of apt upgrade.

apt_news_url

Sets the url where the Pro client will consume apt news information from.

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

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

PRO UPGRADE DAEMON

Ubuntu Pro client sets up a daemon on supported platforms (currently on Azure and GCP) 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 exe?
cuted 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, avoid?
ing 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.

metering

If attached, this job will ping the Canonical servers telling which services are en?

abled on the machine.

REPORTING BUGS

Please report bugs either by running `ubuntu-bug ubuntu-advantage-tools` or login to Launch?

pad and navigate to https://bugs.launchpad.net/ubuntu/+source/ubuntu-advantage-tools/+file?

bug

COPYRIGHT