Comply with CIS or DISA STIG on Ubuntu 20.04 with Ubuntu Security Guide

1. Overview

What is the Ubuntu Security Guide?

Security Technical Implementation Guides like the CIS benchmark <https://ubuntu.com/security/cis> or DISA-STIG <https://ubuntu.com/security/disa-stig> have hundreds of configuration recommendations, so hardening and auditing a Linux system manually can be very tedious. Ubuntu Security Guide (USG) is a new tool available with Ubuntu 20.04 LTS that greatly improves the usability of hardening and auditing, and allows for environment-specific customizations. The following sections provide more information on hardening and auditing with usg.

In this tutorial, we will learn how to audit with the CIS benchmark or DISA-STIG on Ubuntu 20.04 LTS machines, while using an Ubuntu Advantage <https://ubuntu.com/support> or Ubuntu Pro subscription.

Understanding the UA client

The Ubuntu Advantage (UA) client is a tool designed to automate access to UA services like Extended Security Maintenance (ESM), USG, FIPS, and more.

What you'll learn:

- How to check which version of the UA client is installed on your machine and how to update it if necessary
- How to attach the UA client to your Ubuntu Advantage account using your UA token
- How to enable the USG on your Ubuntu machine

- How to perform an audit for CIS or DISA-STIG

What you'll need:

- An active Ubuntu Advantage for Infrastructure <http://ubuntu.com/advantage> or Ubuntu Pro subscription.
- An Ubuntu machine running a fresh install* of Ubuntu server or desktop 20.04 LTS
- Please note that if you use the tool to harden an existing Ubuntu image, the hardening process may take long.

---

2. Installing the UA client

In this step, we will install the latest version of the UA client to ensure that it contains support for USG. Use the following commands:

```
$ sudo apt update
$ sudo apt install ubuntu-advantage-tools
```

---

3. Retrieving your UA token from the Ubuntu Advantage dashboard and attaching it to the UA client

If you are enabling USG on an Ubuntu Pro instance, you can skip this step and go straight to step 4! For non-Pro images, your UA token is used to connect the UA client you have installed on your machines to your Ubuntu Advantage for Infrastructure subscription.

Let's first check whether we have already attached our UA token to the UA client by running :

```
$ sudo ua status
```

```
SERVICE          AVAILABLE      DESCRIPTION
esm-infra        yes            UA Infra: Extended Security Maintenance (ESM)
fips             yes            NIST-certified FIPS modules
fips-updates     yes            Uncertified security updates to FIPS modules
livepatch        yes            Canonical Livepatch service
This machine is not attached to a UA subscription.
See [https://ubuntu.com/advantage](https://ubuntu.com/advantage)
```

We can see that this is not yet attached to a UA subscription. Let's fix that now.

Your UA token can be found on your Ubuntu Advantage dashboard. To access your dashboard, you need an Ubuntu One account <https://login.ubuntu.com/> . If you still need to create one, ensure that you use the email address used to purchase your subscription.

The Ubuntu One account functions as a Single Sign On, so once logged in we can go straight to the Ubuntu Advantage dashboard at ubuntu.com/advantage <http://ubuntu.com/advantage> . Then click on the 'Machines' column in the Your Paid Subscriptions table to reveal your token.

Now we're ready to attach our UA token to the UA client:

```
$ sudo ua attach <your_ua_token>
```

```
Enabling default service esm-infra
Updating package lists
ESM Infra enabled
Enabling default service livepatch
Canonical livepatch enabled.

This machine is now attached to 'your account name'

SERVICE      ENTITLED    STATUS   DESCRIPTION
cis          yes         disabled Center for Internet Security Audit Tools
esm-infra    yes         enabled  UA Infra: Extended Security Maintenance (ESM)
fips         yes         n/a      NIST-certified FIPS modules
fips-updates yes         n/a      Uncertified security updates to FIPS modules
livepatch    yes         enabled  Canonical Livepatch service
```

---

4. Enabling the Ubuntu Security Guide

Now it is time to enable USG. First, we want to run the following command to see the USG service and its status:

```
$ ua status --all
```

We should see an output like this:

```
SERVICE        ENTITLED       STATUS       DESCRIPTION
cc-eal         yes            n/a          Common Criteria EAL2 Provisioning Packages
usg            yes            n/a          Security compliance and audit tools
esm-apps       no             –            UA Apps: Extended Security Maintenance (ESM)
esm-infra      yes            enabled      UA Infra: Extended Security Maintenance (ESM)
fips           yes            n/a          NIST-certified FIPS modules
fips-updates   yes            n/a          Uncertified security updates to FIPS modules
livepatch      yes            enabled      Canonical Livepatch service
Enable services with: ua enable <service>
```

Now we're ready to enable and install USG:

```
$ sudo ua enable usg
$ sudo apt install usg
```

> One moment, checking your subscription first
>
> Updating package lists
>
> USG enabled

---

5. Run the Ubuntu Security Guide

You have successfully enabled USG tool and are ready to use it to audit or harden your Ubuntu machine. To audit use the following command, replacing `<PROFILE>` with `cis_level1_server`, with `cis_level1_workstation` or `disa_stig`, depending on the compliance target.

```
$ sudo usg audit <PROFILE>
```

The output of this command will show the compliance status, and it will also point to an html file containing the audit report. Use a browser to view the file. It will look similarly to the one below.

Screenshot from 2021-12-17 15-46-29

For more complex operations you can proceed with the steps from Ubuntu's Security certifications documentation <https://ubuntu.com/security/certifications/docs/usg> to complete the hardening process.

---

6. Congratulations!

Congratulations, you have successfully used the UA client to audit your Ubuntu image!

Was this tutorial useful?