Remote Systems Management

Go back to Pandora FMS documentation index

Remote system management with Pandora FMS

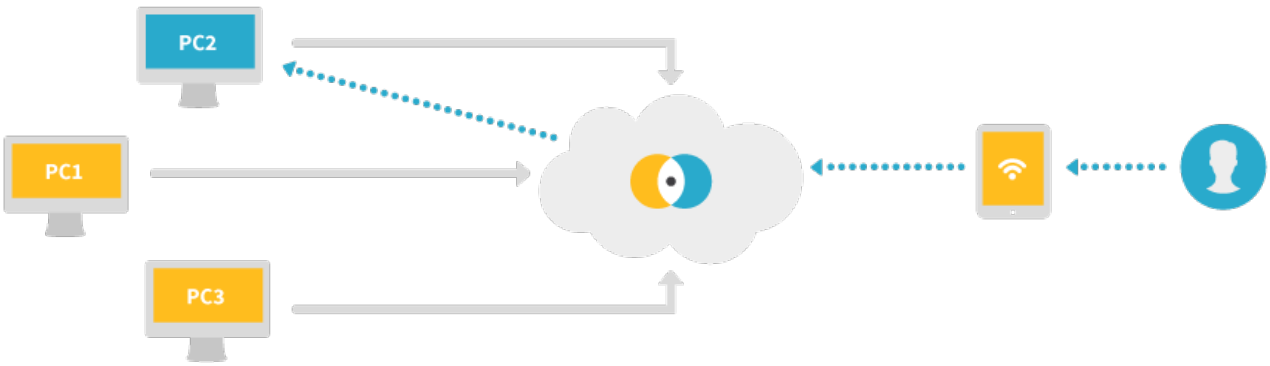
Introduction

Pandora FMS is a monitoring tool, and based on its work ethic, it does not use agents to connect to the equipment, so it uses other methods to allow operators to remotely control the monitored systems. Some systems, such as routers and switches can be managed by Telnet or SSH and in order to access them, you only need to launch the command. To do this, use an *optional* extension based on the Anytermd tool that has not been installed as standard since version 7.0. It is present in the Pandora FMS module library [1)]

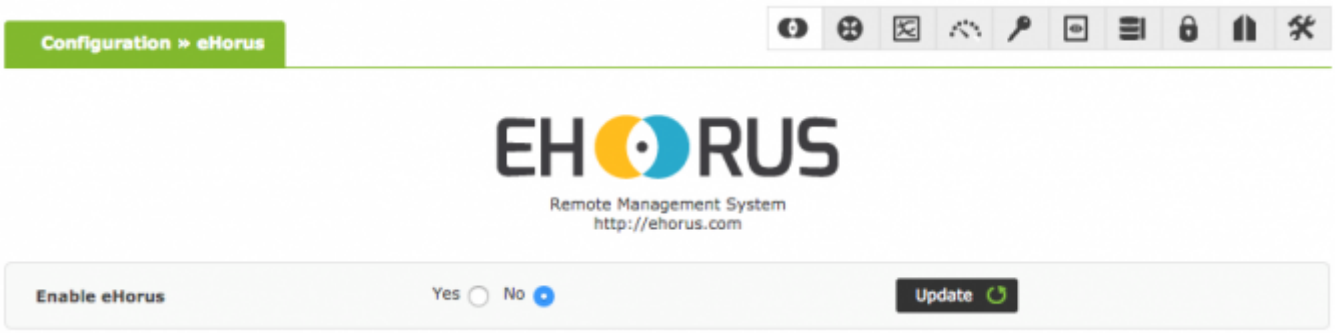
The standard tool in Pandora FMS to have access to remote systems (whether it may be windows, mac or Windows) is eHorus [2)], a remote control tool that since it is WEB, it is totally integrated in Pandora FMS interface.

Using eHorus with Pandora FMS

eHorus is a remote management system that relies on the cloud (SaaS) to connect to the computers, regardless of changes in IP, firewalls or other problems discussed previously.

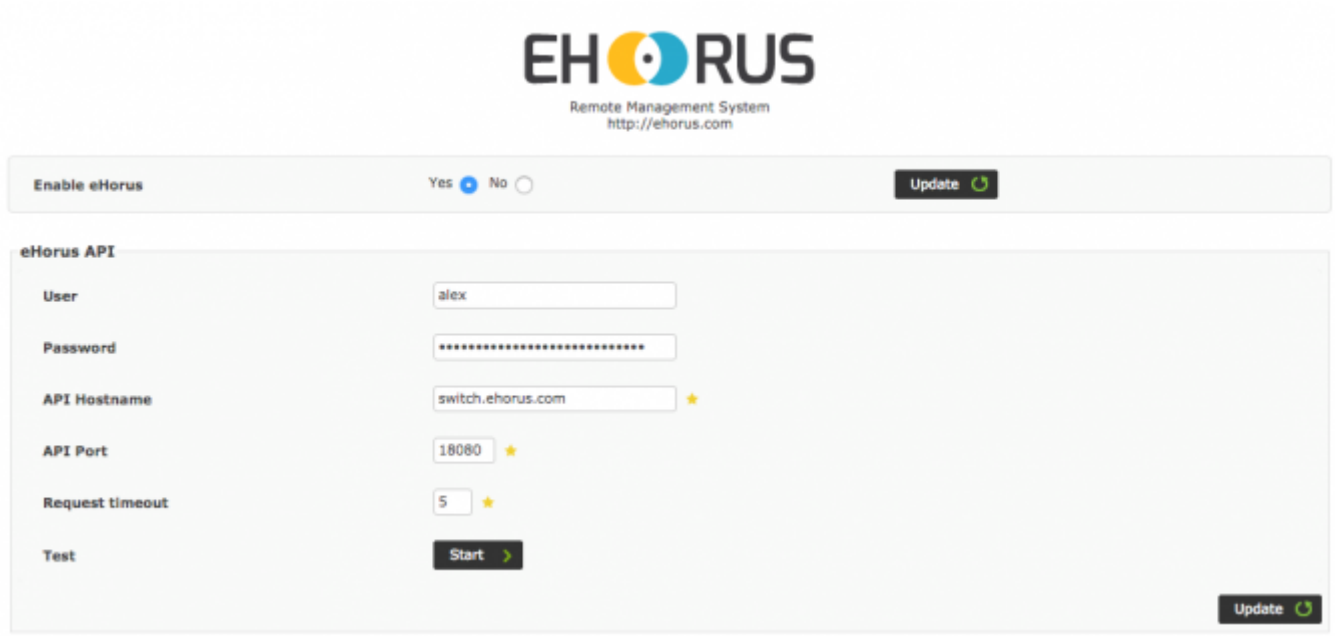


To enable it, activate the integration in its configuration section.



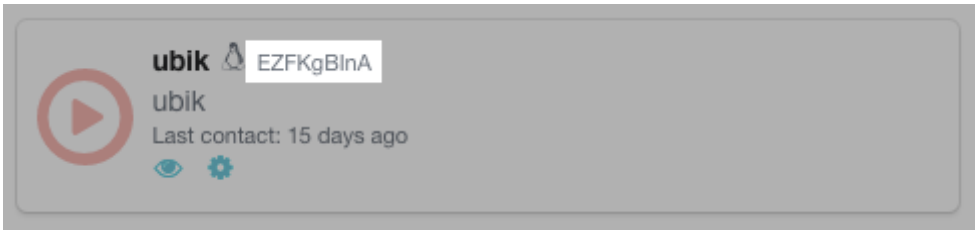
After that, enter a valid login from a service user. This user will be used to authorize the remote connection to the provided agents.

It is possible, although probably not necessary, to use another eHorus provider editing the fields *API Hostname* (*switch.ehorus.com* by default) and *API Port* (*18080* by default).



Remember to check if the connection works properly before saving the changes.

Once the connection is configured, you will be able to check that a new custom field appears in the agent view, called **eHorusID**. This field should contain the eHorus agent ID to be managed. You can find this ID in several places, such as the eHorus agent running on the machine or in the eHorus Portal (see image).



If you are using Pandora FMS 7.0 or higher agents, they already automatically support a parameter to automatically obtain the eHorus ID, through the following configuration token:

```
ehorus_conf <path>
```

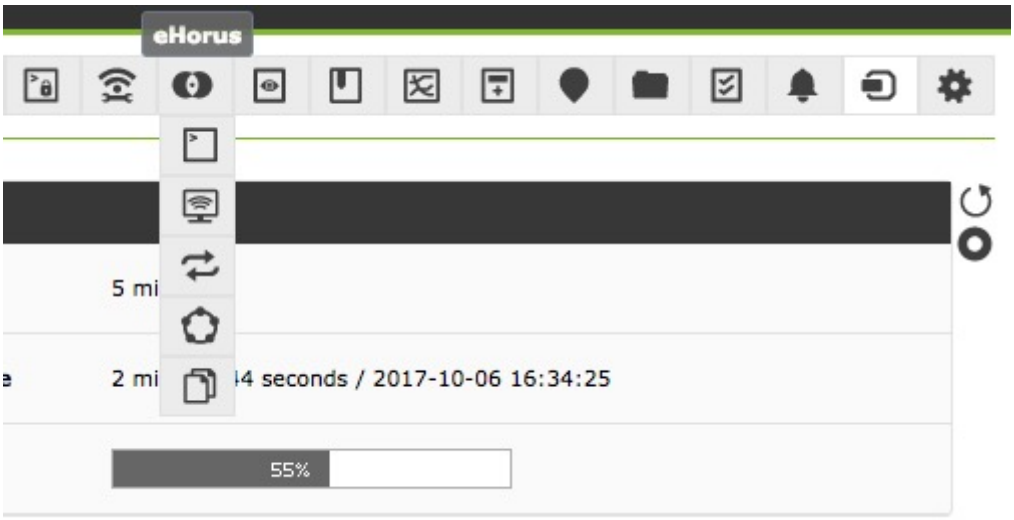
The configuration token supports the absolute path to a valid configuration file of an eHorus agent. The agent will create a custom field called eHorusID that contains the identification key of the eHorus agent.

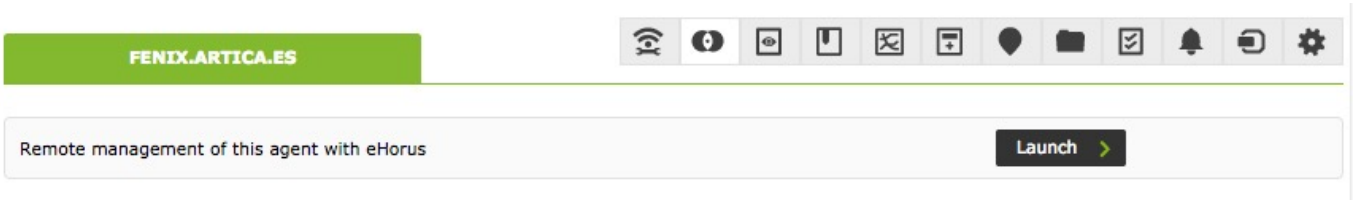
The eHorus agent to be managed must be visible by the configured user in the configuration section of the integration.

When the Pandora FMS agent has defined the ID of the eHorus agent in its customized field, the administrator users or those that have agent management permissions, will see a new tab in the agent menu from which they will be able to use the eHorus client from inside Pandora FMS.

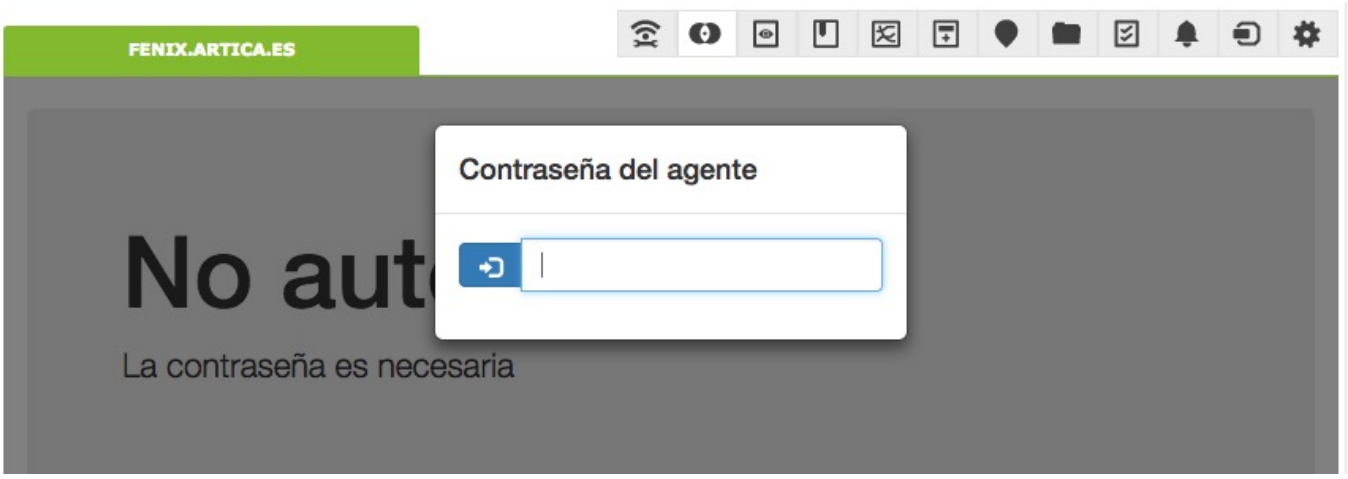
The eHorus id (EKID) is entered in this agent custom field:

Once configured, just click on any of the sections that the remote control extension with eHorus presents of that agent: remote control via Shell, remote desktop, process view, services or copy files.

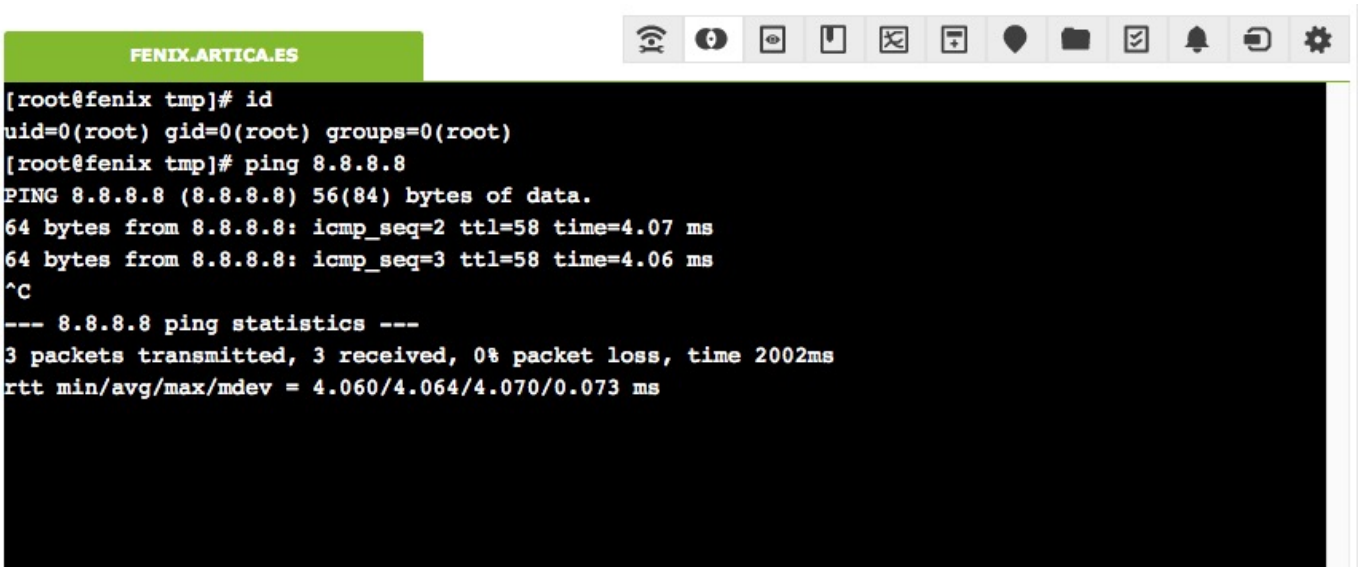




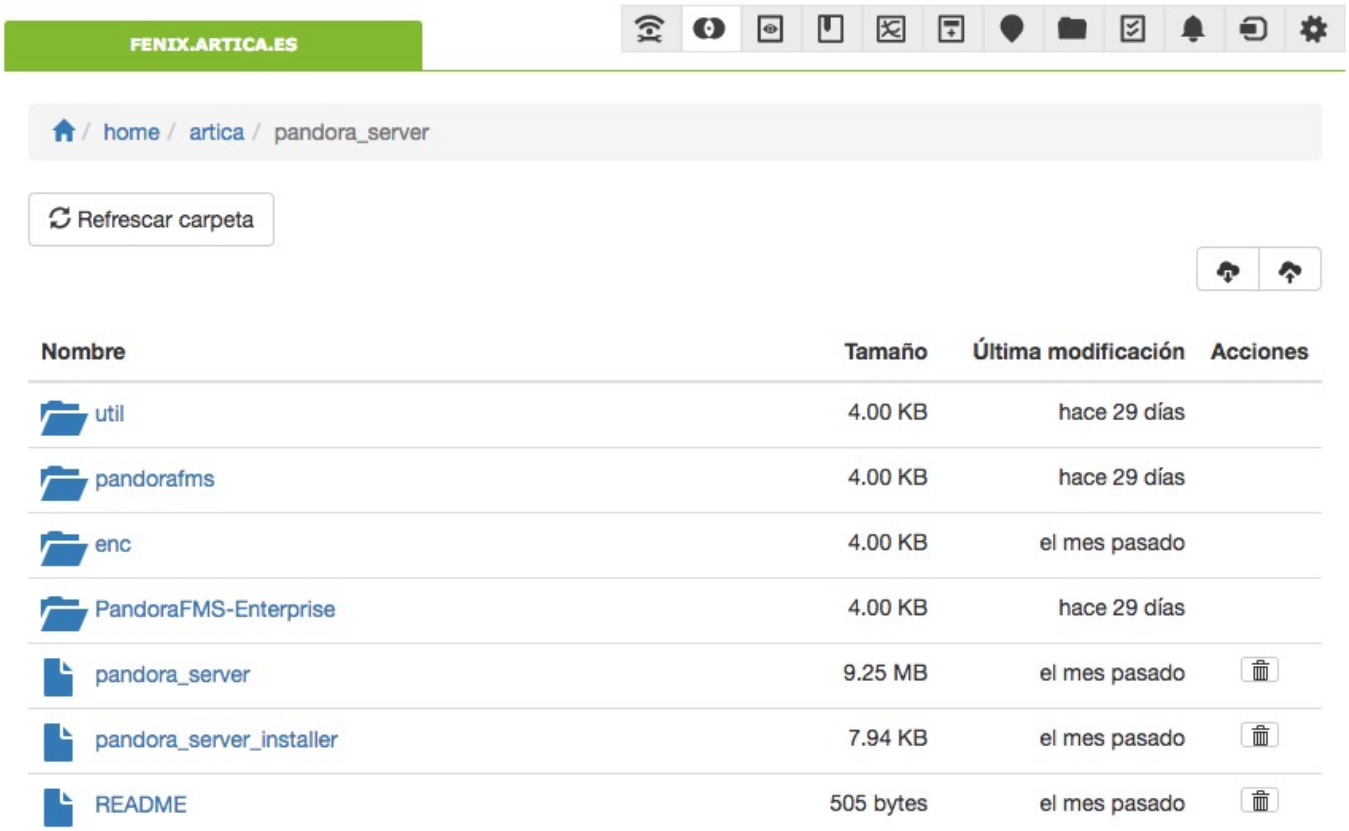
It is always recommended using a local password in the eHorus agent. If configured, we will be prompted interactively:

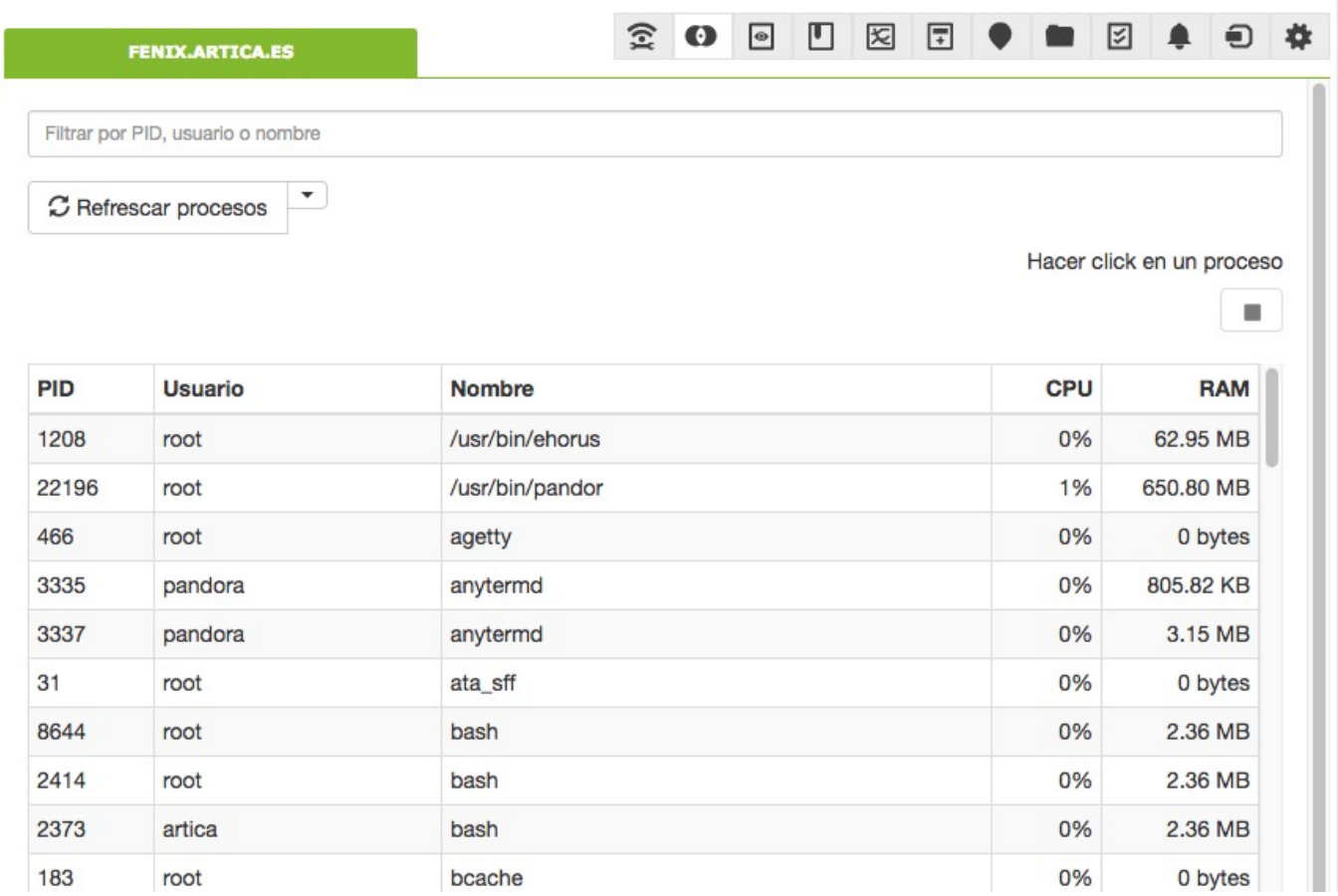


Once authenticated, you may access the interactive command line session (linux, mac and windows) with root permissions:



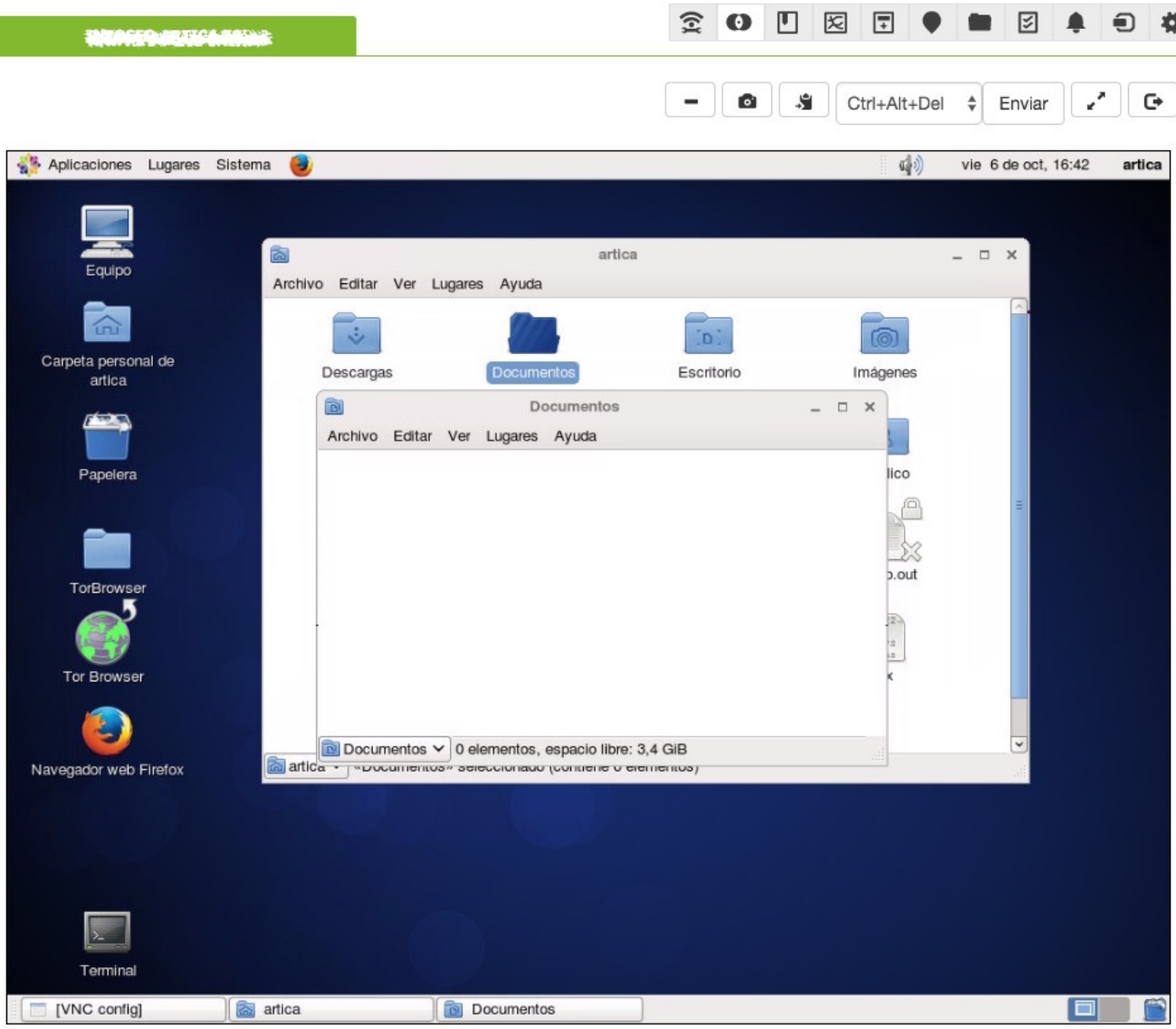
And the same goes for managing remote processes and copying files (both upload and download):





PID	Usuario	Nombre	CPU	RAM
1208	root	/usr/bin/ehorus	0%	62.95 MB
22196	root	/usr/bin/pandor	1%	650.80 MB
466	root	agetty	0%	0 bytes
3335	pandora	anytermd	0%	805.82 KB
3337	pandora	anytermd	0%	3.15 MB
31	root	ata_sff	0%	0 bytes
8644	root	bash	0%	2.36 MB
2414	root	bash	0%	2.36 MB
2373	artica	bash	0%	2.36 MB
183	root	bcache	0%	0 bytes

And of course, the remote desktop (Windows, Linux and Mac):



For more information about eHorus, you can visit their website https://ehorus.com. eHorus is free up to 10 computers. eHorus is developed by the same team that made Pandora FMS possible.

If you are running Pandora FMS on Windows, download the Mozilla CA certificate store in PEM format and add `curl.cainfo&#61;{path}\cacert.pem` to the php.ini file.

For more information about Pandora FMS remote management check the following link.

Go back to Pandora FMS documentation index

1)

https://library.pandorafms.com/index.php?sec=Library&sec2=repository&lng=es&action=view_PUI&i

d_PUI=818
2)

https://ehorus.com