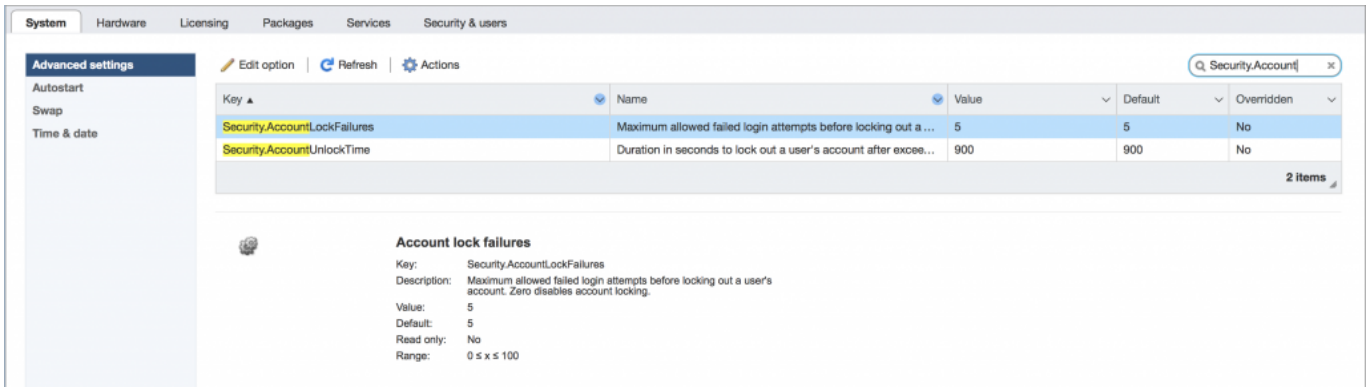
Resetting vSphere 6.x ESXi Account Lockouts via SSH

VMware vSphere has had a good security feature added since vSphere ESXi 6.0 to add a root account lockout for safety. After a number of failed login attempts, the server will trigger a lockout. This is a good safety measure for when you have public facing servers and is even important for internally exposed servers on your corporate network. We can't always assume that it is external bad actors who are the only ones attempting to breach your devices.

VMware vSphere ESXi Root Account Locked – Where to Start

Using the vSphere web client shows us the settings which are used to define the lockout count and duration. The parameters under the Advanced settings are as follows:

```
Security.AccountLockFailures
Security.AccountUnlockTime
```



Are you seeing this dreaded message?

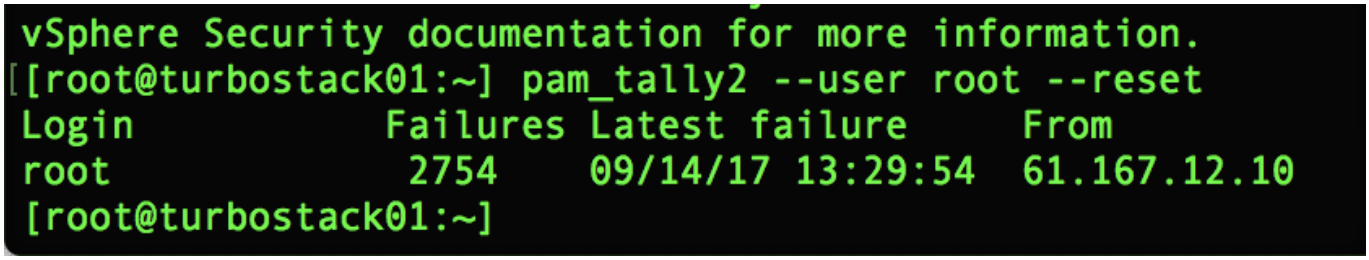
> remote access for esxi local user account 'root' has been locked for 900 seconds

Do not worry, you are in the right place. Now, let's look at what to do if your ESXi root account is locked.

Resetting your ESXi Failed Login Attempts with pam_tally2

There is a rather simple but effective tool to help you do this. It's called `pam_tally2` and is baked in with your ESXi installation. The command line to clear the lockout status and reset the count to zero for an account is shown here with the root account as an example:

```
pam_tally2 --user root --reset
```



In order to gain access to do this, you will need to have SSH access or console access to your server. Console access could be at a physical or virtual console. For SSH access, you need to use SSH keys to make sure that you won't fall victim to the lockouts for administrative users. In fact, this should be a standard practice. Setting up the SSH keys is relatively simple and is nicely documented in the Knowledge Base article **Allowing SSH access to ESXi/ESX hosts with public/private key authentication (1002866)**

https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1002866

Uploading a key can be done with the `vifs` command as shown here:

https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-392ADDE9-FD3B-49A2-BF64-4ACBB60EB149.html

The real question will come as to why you have the interface exposed publicly. This is a deeper question that we have to make sure to ask ourselves at all times. It's generally not recommended as you can imagine. Ensuring you always use complex passwords and 2-factor authentication is another layer which we will explore. Hopefully this quick tip to safely reset your accounts for login is a good first step.