



GABE'S VIRTUAL WORLD

Your P.I. On Virtualization



[HOME](#) [HOT CASES](#) [COLD CASES](#) [TOP CASES](#) [COPYRIGHTS](#) [YOUR P.I.](#) [TWITTER](#) [RSS](#)

About ESXi lockdown mode

30 November, 2009

When you build your virtual infrastructure with only ESXi hosts that you also lock down for security reasons, you might be in for a little surprise when you want to get your VI up and running again after major maintenance or a failure. First thing to do after the virtual infrastructure has been down, is to get vCenter up and running again. In a previous post "[How to quickly recover from disaster](#)" I already explained the idea of running vCenter always on the first host in your cluster. In case of failure you don't have to search where DRS left your vCenter VM, you just connect the VI Client to the first host and start the vCenter VM. Don't forget you need your Active Directory and SQL database before starting vCenter.

With an all ESXi environment and locked down hosts, you cannot use the VI Client to connect and start the necessary VMs, at least that is what many think, but this isn't completely true. The Locked down mode does NOT prevent direct VI Client connections as many think, it does however prevent direct VI Client connections made with the root-user account. The same goes for PowerCLI, vCLI, vMA, or any of the other public APIs. In locked down mode the root user has no direct access. You can however create an extra user on your ESXi install and assign this user administrator rights. Then, after enabling locked down mode, you can still make a direct VI Client connection to your ESXi box and perform some admin tasks like starting VMs.

Another option would be to just get access to the console of the ESXi host using ILO, KVM, DRAC or similar techniques and disable lockdown mode. After disabling lockdown mode, you can then again make root access using the VI Client.

To summarize:

- Lockdown mode for ESXi **does prevent** root access using VI Client, PowerCLI, vMA, API's etc.
- Lockdown mode for ESXi **does NOT prevent** other users accessing the ESXi host using above mentioned tools. Just be sure to first create this user.
- Procedure in an enterprise to create that local user on all ESXi hosts, would be to use (for example) PowerShell to create that admin user and then enable the lockdown mode.

by Gabriele van Zanten

Loading comments...



[blog comments powered by Disqus](#)

« [BUG? VMware View4 and User Access Control using PCoIP Dutch VMUG dec 11th 2009](#) »

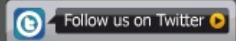
Search my blog

Search

Hot Cases

Memory management and compression in vSphere 4.1
Setting logfile location, swap file, SNMP and vmkcore partition in ESXi
VMware vSphere 4.1 released – What's new?
First vSphere Plugin for WordPress! by Nicholas Weaver
[RUMOR] VMware to buy Novell?
Must have apps for the iPad
Interview with Matt McSpirit – Partner technology advisor at Microsoft UK

Follow Virtualization



Voted #8 blog at
[vSphere-land.com](#)

My Home Lab

CPU: 30,928 MHz
RAM: 20,409 MB
Storage: 8,815 GB

ESX Hosts: 3
Resource Pools: 5
Virtual Machines: 34

VMotions: 73
Power States:
□(11) □(23) □(0)

last update
0 days, 17 hrs and 51 min.

plugin by nickappa