OpenNebula - Bug #5149
Potential security risk in RAW field in templates!

05/10/2017 01:16 PM - kvaps kvaps

Status:	Closed		**Start date:**	05/10/2017
Priority:	High		**Due date:**	
Assignee:	Javi Fontan		**% Done:**	0%
Category:	Core & System		**Estimated time:**	0.00 hour
Target version:	Release 5.4			
Resolution:	fixed		**Pull request:**	
Affected Versions:	OpenNebula 4.0, OpenNebula 4.10, OpenNebula 4.12, OpenNebula 4.14, OpenNebula 4.2, OpenNebula 4.4, OpenN

Description

Be careful if you allow users to create templates byself.

It may be very dangerous even if you disabled this other-tab in sunstone interface, advanced view may be used for todo this.

User can do anything with this field, for example:

Passthrough host filesystem:

```
RAW = [
 DATA = "<devices>
  <filesystem type='mount' accessmode='passthrough'>
   <source dir='/'/>
   <target dir='hostroot'/>
  </filesystem>
 </devices>",
 TYPE = "kvm" ]
```

Then inside vm:

```
mount hostroot /mnt/ -t 9p -o trans=virtio
```

- You can get access to some files on the host accessed from the libvirt user.

- You can get access to /var/lib/one/datastores and can get access to data of vm's that not owned by you.

- You can dump other vm disks and get access to passwords of web-services or databases of other users.

- You can create big file on the host and attach it as vm disk.

- You can create internal network interface and get access to vnc consoles of all vm's and other services in your internal network.

And this is only part of the thoughts to what it can lead...

Associated revisions

Revision 8f11a1d6 - 05/16/2017 09:51 AM - Abel Coronado

F #5149 Removed autorefresh option (#302)

Revision 7edd0675 - 05/16/2017 10:08 AM - Abel Coronado

Bug #5149 Removed autorefresh option in sunstone-config (#303)

Revision e646b2eb - 07/10/2017 01:57 PM - Javi Fontan

B #5149: set RAW as a restricted attribute

Revision 33b7c27d - 07/10/2017 01:59 PM - Javi Fontan

B #5149: add RAW as restricted attribute

History

#1 - 05/11/2017 02:00 PM - kvaps kvaps

- Private changed from Yes to No

Hello,

Ruben is answered me about this issue:
This is may be solved by adding this option into oned.conf:

    VM_RESTRICTED_ATTR = "RAW"

I think we need to include this option by default into oned.conf
So I'm directing this issue for this.

#2 - 05/16/2017 09:28 AM - Ruben S. Montero

- Target version set to Release 5.4

- Resolution deleted (wontfix)

#3 - 05/16/2017 09:37 AM - Abel Coronado

- Assignee set to Abel Coronado

#4 - 05/16/2017 09:43 AM - Abel Coronado

- % Done changed from 0 to 100

#5 - 05/16/2017 09:44 AM - Abel Coronado

- Assignee deleted (Abel Coronado)

- % Done changed from 100 to 0

#6 - 05/25/2017 02:32 PM - Ruben S. Montero

- Assignee set to Javi Fontan

#7 - 07/10/2017 03:23 PM - Javi Fontan

- Status changed from Pending to Closed

- Resolution set to fixed

Added restricted attribute to both 5.2 and master branches.