White Paper
Integration of VMware ESXi hosts into ServerView Operations Manager and RAID Manager using accounts based on least privileges

This document describes the steps required to integrate ESXi hosts into FUJITSU Software ServerView Operations Manager and RAID Manager with a most restricted user account.
Introduction

For the purpose of this description the following software versions have been used:
- ServerView Operations Manager 7.02.02 and the RAID Manager 6.2.6 on a Windows Server 2012 R2;
- ESXi server on 6.0.0.2715440 (350-2).

Please ensure that you are familiar with these FUJITSU Software ServerView Suite manuals:
- ServerView Operations Manager V7.02 – User Guide
- ServerView RAID Manager, June 2015 – User Guide

1. Most restrictive user account for ServerView RAID Manager (Read only)

We are going to use a comparable approach like vCenter server and the “root” account to connect the server to the ServerView RAID Manager. This is accomplished by an “Administrator”. The read only restrictions are implemented by ServerView RAID Manager.

Leverage the built-in capabilities of RAID Manager.
This topic is well documented in the manual ServerView RAID Manager – User Guide, Chapter: Login

1.1. After the installation of ServerView RAID Manager only members of the local user group “Administrators” are allowed to log into RAID Manager. All other users will fail.

1.2. Two local groups are predefined:
raid-adm and raid-usr

Member of the Admin group are validated as “RAID Administrator” with “Write permissions”.

Member of the User group are validated as “RAID Observer” with “Read only permissions”.

1.3. Ensure that the proposed users are listed in the supposed User Group (default: raid-usr).

1.4. Logon to ServerView Raid Manager as an “Administrator” and ensure that you have “Write access”.

Note: The first user automatically has read/write authorization. Every subsequent user only has read authorization, but – provided they have appropriate administration rights – can obtain write authorization. The user who had write authorization up to this point is then informed of this.
1.5. Add the server node.

1.6. Provide the hostname and the credentials and create the connection.

1.7. Check if the node was successfully added.
1.8. Logon with a “RAID Observer” account: “Read only”!
2. **Most restrictive user account for ServerView RAID Manager (Read only) and ESXi Server**

Some projects even the RAID manager “Administrators” have no access to the root password of the ESXi Server. There is a need for a “Read only” account on the ESXi Server.

2.1. Define an ESXi role with the least privileges for the ServerView RAID account: “CIM” and “System Management” is required.

Open **vSphere Client** and select **Home – Roles – Add Role**:

The Add New Role dialog is displayed.

Add the new role Monitor under Name and check • Host – CIM – CIM Interaction
• Host – Configuration – System Management under All Privileges.

Define a meaningful role name, e.g. R-SVRAID.

2.2. Go to **Home – Inventory** and click on the **Users** tab.

2.3. Select **Add** a new user in the context menu of the Users View: The Add New User dialog is displayed.

Create a new local user and use a complex password.
2.4. Click to Permissions tab and select Add Permission in the context menu:
The Assign Permissions dialog is displayed.
Assign the role R-SVRAID to the user U-SVRAID for the ESXi host.

2.5. Login to the ESXi Host (e.g. SSH) and edit the file /etc/group and add the user U-SVRAID to the root group (first line).

2.6. Prevent the account (e.g. U-SVRAID) from logging on.
Edit the file /etc/passwd and replace the default shell for the user (e.g. U-SVRAID from /bin/sh into /sbin/nologin)

2.7. Now you can follow the description in chapter:
Most restrictive user account for ServerView RAID Manager (Read only)
The only difference in the steps will be:
Provide the hostname and the credentials and create the connection.
Instead of the root account, we are using the newly created account U-SVRAID
3. Most restrictive user account for ServerView Operations Manager (Read only)

3.1. Define an ESXi role with the least privileges for the ServerView Monitor account: "CIM" is required.

Open vSphere Client and select Home – Roles – Add Role:
The Add New Role dialog is displayed.

Add the new role Monitor under Name and check
• Host – CIM – CIM Interaction
under All Privileges.

Define a meaningful role name, e.g. R-SVMONITOR

3.2. Go to Home – Inventory and click on the Users tab.

Select Add a new user in the context menu of the Users View: The Add New User dialog is displayed.

Create a new local user and use a complex password.

3.3. Click to Permissions tab and select Add Permission in the context menu:
The Assign Permissions dialog is displayed.

Assign the role R-SVMONITOR to the user U-SVMONITOR for the ESXi host.

3.4. Login to the ESXi Host (e.g. SSH) and edit the file /etc/group and add the user U-SVMONITOR to the root group (first line).

After this your /etc/group file should look like:
```
root:x:0:root, U-SVMONITOR
...
U-SVRAID:x:1000:
```

3.5. Prevent the account (e.g. U-SVMONITOR) from logging on. Edit the file `/etc/passwd` and replace the default shell for the user (e.g. U-SVMONITOR) from `/bin/sh` into `/sbin/nologin`.

After this your `/etc/passwd` file should look like:

```
root:x:0:0:Administrator://:/bin/sh
... 
U-SVMONITOR:x:1000:1000:ESXi User:/sbin/nologin
```

3.6. Logon to ServerView Operations Manager and add the newly created user.

3.7. Add host to the ServerView ServerList and check connectivity.

---

ServerView® Integration – further information

ServerView® Integration packs and best practice information enable the seamless and easy integration of Fujitsu PRIMERGY servers in enterprise management systems. PRIMERGY servers can thus be monitored and managed from a central management console as a single point of control and administration for heterogeneous environments.