

# SFM 2.0 Frequently Asked Questions

## General

### Where is the SFM User Guide?

All SFM user documentation is online and accessed by clicking on the Help link at the top of the SFM web page.

### Are there any URLs that can be accessed without user giving a password?

Yes, SFM does not allow scripts to be accessed only built-in (i.e. response directly from xprtld) these are read-only URLs.

### Does SFM 2.0 need anything installed on the Managed Host (MH) to work with Storage Foundation (SF) 5.x?

Yes. Every version of SF that SFM manages requires the same *VRTSsfmh* package to be installed. This package will be bundled in the next version of SF and it is not part of the SF 5.0 installation.

### When adding a new host, why do I get an error saying that the host is already added or already part of a domain?

This may occur if an error occurred while previously adding the host. There is a workaround for SFM 2.0GA, and this issue will be fixed formally in future versions.

To fix on SFM 2.0, login to the central server (CMS) host and perform the following:

```
# /opt/VRTSsfmh/bin/xprtld -l https://localhost:5634/agent/domain/unregister -d  
host=<hostname> -d id=<hostguid>
```

Example of fully formed command:

```
# /opt/VRTSsfmh/bin/xprtld -l https://localhost:5634/agent/domain/unregister -d  
host=myhost.domain.com -d id={00020003-ba39-d718-0000-00008339d718}
```

Note: You can get the exact hostname and hostguid using this command:

```
# /opt/VRTSsfmh/bin/xprtld -l https://localhost:5634/agent/domain/enum | grep  
<hostname>
```

### **Does SFM interfere with SF's functionality?**

No.

### **Does SFM require the Veritas Enterprise Administrator (VEA)?**

Yes and No. It does require VEA on the managed host for SNMP traps and running administration commands like create volume etc. However, it does not require VEA for discovery on UNIX SF 4.x and higher. On Windows and HP-UX 3.5, VEA is required for SFM to operate properly.

### **How frequently is Managed Host (MH) information updated to the SFM central server (CMS) Database?**

The discovery on each MH is broken down into families to focus on a particular functional area that SFM discovers information about.

<b>Family</b>	<b>Frequency (minutes)</b>	<b>Information Discovered</b>
Host	1440	Basic host details concerning the operating system, licenses, packages, and networking. It is assumed that most information relating to this family does not change very frequently.
SF	30*	All aspects of Volume Manager, File Systems, and related storage network information.
VCS	60*	VCS and its related information.
DB	15	Oracle and DB2 Databases and their storage dependencies.
NR	5	Configuration status and external faults.

\*SF and VCS families are also event driven, so discovery is triggered when configuration change events occur. Because of this information should be update into the CMS database in near real time.

With the exception of a small heartbeat communication occurring every 10 minutes, no additional data is sent across to the CMS unless changes to the configuration are detected.

Please refer to the SFM Administrators Guide for more information on SFM MH Discovery.

### **How does SFM display localized (i.e. Japanese or Chinese) File System mount points?**

SFM does support the display of localized mount points. The standard encoding SFM uses is UTF-8. Any other encoding that is used requires that the xprtld daemon on the managed host be run under the locale/encoding that the mount point names were created. English, Japanese, Simplified Chinese, and all UTF-8 locales are generally supported.

### **How much space is required for the SFM central server (CMS) database?**

By default, the SFM installation puts the database in /var on the CMS. It is probably good to change this to be located on its own partition or volume. If possible, it is recommended that this be put on a striped mirror for performance. The recommended size depends on the amount of resources that will be managed. On a larger environment with 1000 hosts, it is good to have around 10 Gigabytes available.

### **How much space is required for a SFM Managed Host (MH)?**

1 Gigabyte should be more than enough no matter how big the host is.

### **Does SFM support other non-Symantec Volume Managers?**

For Linux, HP-UX, AIX, and Solaris SFM only supports the discovery of VxVM related information. For Windows, it does support discovery of both Basic and Dynamic Volumes.

### **Does SFM support other non-Symantec File Systems?**

Yes. SFM does support discovery of vxfs as well as many other platform file systems including ext3, reiserfs, hfs, ufs, jfs, jfs2, and ntfs.

### **Does SFM support other non-Symantec Multipathing Solutions?**

Yes. Besides support for Veritas DMP, SFM also supports discovery of EMC PowerPath and Microsoft MPIO multipathing. However, the DMP Management Add-on only supports Veritas DMP.

## **Networking**

### **What is the protocol used for SFM 2.0?**

SFM uses HTTP based protocol which differs from previous versions. Essentially, it uses Web Services as the underlying message exchange format

### **What are the networking requirements? What firewall ports need to be opened?**

All communication between Managed Hosts and the SFM Central Server (CMS) goes through port tcp/5634. This needs to be opened (bi-directional) if there is a firewall. For the user interface, you need to open port 14161 between the client desktop (where the web browser runs) and the CMS. NO other port is required.

The CMS's hostname needs to be resolvable from the Managed Host. It is recommended that DNS be used for this. If the hostname is not resolvable, you can specify a valid IP address, however this may impact the usability of the product as the IP is what will be displayed for the Host name in the SFM Web Console.

### **What kind of network traffic can be expected if SFM is deployed?**

Managed Hosts send an HTTP request (a.k.a. ping) to the CMS indicating that it is alive every 10 minutes. This request is a very simple request with less than 1 Kilobyte of payload (max). When there is a change detected in the managed host, the managed host sends a HTTP POST to the CMS indicating the change. However, only differences (diffs) are sent. So, in a static (not changing environment) there is no traffic other than the 10 min pings from each managed host. When there is a change, the payload size depends on the amount of change which is never more than a full (initial) discovery of that host. On large systems with 15 thousand LUNs and a couple thousand File Systems and Volumes the full discovery payload can be as large as a few Megabytes.

### **What kind of SNMP support is there in SFM?**

There is limited SNMP trap support in SFM. It does require that VEA be installed and running on the Managed Host (MH) because it is the source of events that are sent to SNMP server. SFM ships with an SNMP MIB as part of the CMS package. You can select the specific events to be forwarded. Please look at the rule manager under "Monitoring" tab.

Please refer to the SFM documentation for more details.

## **Virtualization**

### **Can SFM manage Storage Foundation for Windows (SFW) running in a VMware virtual machine?**

Yes, but there are some caveats.

Since in most cases VMware does not expose the HBA directly to the guests, SFM would not be able to discover the Array Port (of any LUNs) as well as the HBA ports. However, SFM will still give you the Enclosure information for any raw device mapped LUNs. Non-RDM disks are plain old SCSI disks since they are abstracted from the guest.

### **Can you install the SFM Central Server (CMS) on a virtual machine, Solaris Zone, or LDOM?**

Yes, all it requires is an Operating System that is in the list supported by SFM 2.0 CMS. If using VMware, please note that SFM requires a 64 bit Operating System for Linux and Windows. The SFM CMS can also be installed in its own Zone or LDOM.

## **Add-ons**

### **What is an SFM Add-on?**

SFM Add-ons allow the extension of the base functionality included in SFM. Please refer to [http://www.symantec.com/sfm\\_addons/](http://www.symantec.com/sfm_addons/) for more information about specific Add-ons.

### **Do Add-ons install anything on the Managed Host (MH)?**

It depends on the Add-on.

There are Add-ons that install purely on the CMS. However, there are also add-ons like that install pieces on both MH and CMS. The installation of the MH components is done automatically as part of the add-on install. The user does not have to do anything special to the MH for this.

## **Security**

### **What privilege or account do you need on Managed Host?**

For adding a host into a domain, you need to know the root user and password of the managed host. Once a host is added a secure channel is setup between the CMS and the managed host using PKI/PKCS mechanisms. After the host is added to the domain, the password for the root user can be changed and it does not affect the operation of SFM.

### **Does xprtld allow for PAM, Active Directory, or LDAP based authentication?**

This is allowed for xprtld running on the central server (CMS). For the Managed host, SFM allows native OS authentication for end users.

### **What is a Security Group?**

Security Groups provide a simple authorization mechanism to users of SFM. A security group associates the authentication group and the authentication domain with a predefined role. For the Admin role, you can associate Application Groups with the security group to limit the authorized scope of a particular user.

### **What should be specified in the name of a security group?**

This should be the name of the security group that you want to create. Make sure that the name of the name of the authentication group and the name that you specify for the security group are the same. Authentication group can be an OS group, LDAP/Authentication Domain group, or PAM/NIS group.

## **Administer Link**

**Why do I see the Administer link on the Host detail page as RED instead of GREEN even after I add a managed host successfully to the SFM central server (CMS)?**

After the host is added to the central server successfully the discovery process takes a minimum of 5 minutes to update the database with the discovered details of the added host. As there is some time lag between addition of the host and discovery completion, the admin link will show up as RED until the discovery has completed. Please try refreshing the page after 5 minutes, and you should be able to see the admin link as GREEN.

**When I click on the Administer link for objects other than hosts (like Disk Groups, Disks, Volumes, etc), it doesn't take me to the detail page of that object. Rather it takes me to the view which shows all of the objects of that type for that host.**

Look for the object that you clicked the Administer link for in the previous page in the resulting table. Click on its link in the first column, and you will be taken to the desired detail page.

## **Infrastructure**

**Are there any CLIs for SFM?**

SFM on the CMS has a CLI called xinfo. This allows you the options to get information about the state of the SFM infrastructure.

Please refer to the SFM documentation for more details.

**Is xprtld a web server?**

Yes.

It is a modified embedded web server based on the popular open source shttpd that listens on port 5634. It only does authenticated SSL. It also has a built-in role based authorization mechanism. Anything with the url containing "admin" can only be accessed by "root" or a OS account with admin privilege. All scripts within agent directory under

/opt/VRTSsfmh/web/agent can be accessed from other managed host as "root". These scripts are hardened and use Perl with Taint mode turned on.

### **What is fault.pl?**

There are several aspects of the system that SFM monitors as part of VRTSsfmh package that is installed on the Managed Host (MH). However, this is obviously not all encompassing. A user of SFM can choose to add their own discovery and exception detection scripts to augment our offering. Fault.pl allows you to indicate if a host is faulted or at-risk and it will show up in the dashboard. A simple http server monitoring script that runs off of cron can just call fault.pl if it stops running and clear it when it starts running again.

Please refer to the SFM documentation for more details.

### **What is xdist?**

Xdist is an extremely powerful command that allows you to push a script to managed hosts in the SFM domain and execute them. Typical use cases could include provisioning a server, updating a patch on multiple machines, or detecting compliance related anomalies in your environment. This command can only be executed as root on the central server and it will execute commands as root on the target systems. It is quite secure and arbitrary commands cannot be called unless you bypass it using your own scripts. It utilizes a white listing mechanism for authorized commands similar to how sudo operates.

Please refer to the SFM documentation for more details.

### **Can I access the SFM Central Database directly?**

No. That is not supported at this time.