

Install KernSafe Virtual iSCSI SAN into XenServer or ESX/ESXi

Friday, September 15, 2017

KernSafe Technologies, Inc.

www.kernsafe.com

Copyright © KernSafe Technologies 2006-2017. All right reserved.

Table of Contents

Overview	3
Install KernSafe Virtual iSCSI SAN into XenServer.....	4
Download VirtualSAN	4
Unzip and Install.....	5
Configure firewall.....	6
Install KernSafe Virtual iSCSI SAN into ESX / ESXi Host.....	7
Prepare Datastore for VirtualSAN Installation.....	7
Enable SSH	7
Download VritualSAN	7
Configure firewall.....	9
Manage Virtual iSCSI SAN from Windows Desktop	10
Contact.....	13

Overview

The Virtual SAN is native version of KernSafe iSCSI SAN cross-platform which can work in the VMWare vSphere (ESX, ESXi) and Citrix XenServer host machine. It quickly brings the benefits are:

Build Hyper-Converged Infrastructure or high availability visualization server with only two servers (two nodes high availability).

Convert VMWare vSphere and Citrix XenServer into hyper converged servers, allows it can provide both compute and storage service.

The document provides a step-by-step guide for installing KernSafe VirtualSAN into Citrix Xenserver or VMWare ESX / ESXi virtualization host machine.

Install KernSafe Virtual iSCSI SAN into XenServer

Install KernSafe Virtual iSCSI SAN Citrix XenServer means convert a XenServer machine into hyper-converged, one machine can offer both compute and storage services. install KernSafe Virtual iSCSI SAN software into XenServer is very easy.

Download VirtualSAN

Before we install it into XenServer, log on into XenServer via ssh with root account:

```
[root@xenserver1 ~]#
```

A screenshot of a terminal window with a black background. The prompt is [root@xenserver1 ~]# followed by a green cursor bar. The rest of the terminal area is empty.

Type the following command to download KernSafe Virtual iSCSI SAN for XenServer:

wget <http://www.kernsafe.com/download/virtual-native-san.5.50.tar.gz>

```
[root@xenserver1 ~]# wget http://www.kernsafe.com/download/virtual-native-san.5.50.tar.gz
--2017-09-16 20:33:21-- http://www.kernsafe.com/download/virtual-native-san.5.50.tar.gz
Resolving www.kernsafe.com (www.kernsafe.com)... 104.24.29.20, 104.24.28.20, 2400:cb00:2048:1::6818:1c14, ...
Connecting to www.kernsafe.com (www.kernsafe.com)|104.24.29.20|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2451801 (2.3M) [application/x-gzip]
Saving to: 'virtual-native-san.5.50.tar.gz'

100%[=====>] 2,451,801 590KB/s in 4.9s

2017-09-16 20:33:27 (493 KB/s) - 'virtual-native-san.5.50.tar.gz' saved [2451801/2451801]

[root@xenserver1 ~]# █
```

Please note that the file name of the url may be changed, please concern our website to learn the newest versions, the url was named by file name and version.

Unzip and Install

```
tar -zxvf virtual-native-san.5.50.tar.gz
cd VirtualSAN
./install.sh
```

```

[root@xenserver1 ~]# tar -zxvf virtual-native-san.5.50.tar.gz
VirtualSAN/
VirtualSAN/supersand
VirtualSAN/Users.db
VirtualSAN/asyncplugin.so
VirtualSAN/autosnapplugin.so
VirtualSAN/cdppplugin.so
VirtualSAN/failoverplugin.so
VirtualSAN/imageplugin.so
VirtualSAN/logplugin.so
VirtualSAN/memdiskplugin.so
VirtualSAN/mirrorplugin.so
VirtualSAN/partitionplugin.so
VirtualSAN/smtppplugin.so
VirtualSAN/snapshot.so
VirtualSAN/userplugin.so
VirtualSAN/vhdplugin.so
VirtualSAN/vhdxplugin.so
VirtualSAN/ximageplugin.so
VirtualSAN/supersan
VirtualSAN/install.sh
VirtualSAN/storagepool.so
VirtualSAN/uninstall.sh
[root@xenserver1 ~]# cd VirtualSAN/
[root@xenserver1 VirtualSAN]# ./install.sh
Installing supersand...
Copying files...
Setting up service...
Starting service...
Starting supersand (via systemctl): [ OK ]
Finished.
[root@xenserver1 VirtualSAN]# █

```

Configure firewall

If you are running a test machine, you can simply stop XenServer firewall settings by the command:
systemctl stop iptables

Otherwise, you can use the following commands to configure the iptables:

```

iptables -A INPUT -p tcp -m tcp --dport 3260 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 3261 -j ACCEPT

```

Now the KernSafe Virtual iSCSI SAN software was installed into the XenServer, now need to download KernSafe iSCSI SAN management console to manage it from Windows desktop as described by the following chapter.

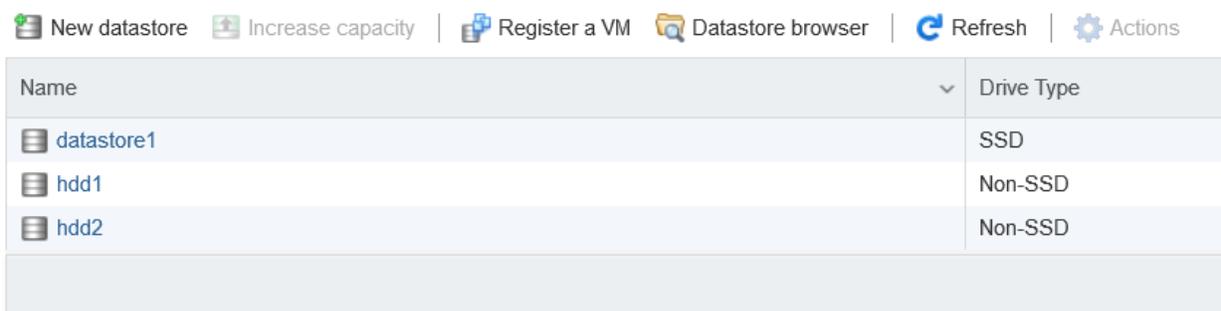
Install KernSafe Virtual iSCSI SAN into ESX / ESXi Host

Install KernSafe Virtual iSCSI SAN into ESX / ESXi means convert a ESX / ESXi machine into hyper-converged, one machine can offer both compute and storage services. install KernSafe Virtual iSCSI SAN software on ESX / ESXi is very easy.

Prepare Datastore for VirtualSAN Installation

KernSafe VirtualSAN need to run in a datastore folder as ESX/ESXi is running in readonly mode. Therefore user need at least one local Datastore to install it, and can use the same datastore or separated datastore to store iSCSI images.

Now we use "datastore1" as an example.



The screenshot shows the VMware vSphere Datastore browser interface. At the top, there are several action buttons: "New datastore", "Increase capacity", "Register a VM", "Datastore browser", "Refresh", and "Actions". Below the buttons is a table with two columns: "Name" and "Drive Type". The table contains three rows of data:

Name	Drive Type
datastore1	SSD
hdd1	Non-SSD
hdd2	Non-SSD

Enable SSH

In VMWare ESX/ESXi web management interface, select host, and click on the Action link in the right content panel.

Select Service->Enable Secure Shell (SSH).

Now it shows ssh was enabled.



Download VirtualSAN

Log on to ESX/ESXi host machine via ssh, enter into the path of datastore1 by:

```
cd /vmfs/volumes/datastore1
```

then enter these commands:

```
wget http://www.kernsafe.com/download/virtualsan.esx.5.50.tar.gz
```

```
tar -zxvf virtualsan.esx.5.50.tar.gz
```

```
[root@esxi:/vmfs/volumes/59521271-21ec59e7-217d-f4ce468806b4] wget http://www.kernsafe.com/download/virtualsan.esx.5.50.tar.gz
Connecting to www.kernsafe.com (104.24.29.20:80)
virtualsan.esx.5.50. 100% |*****| 2392k 0:00:00 ETA
[root@esxi:/vmfs/volumes/59521271-21ec59e7-217d-f4ce468806b4] tar -zxvf virtualsan.esx.5.50.tar.gz
supersan-esx/
supersan-esx/Users.db
supersan-esx/asyncplugin.so
supersan-esx/autosnapplugin.so
supersan-esx/cdppplugin.so
supersan-esx/failoverplugin.so
supersan-esx/imageplugin.so
supersan-esx/logplugin.so
supersan-esx/memdiskplugin.so
supersan-esx/mirrorplugin.so
supersan-esx/partitionplugin.so
supersan-esx/smtpplugin.so
supersan-esx/snapshot.so
supersan-esx/userplugin.so
supersan-esx/vhdplugin.so
supersan-esx/vhdxplugin.so
supersan-esx/ximageplugin.so
supersan-esx/supersan
supersan-esx/storagepool.so
supersan-esx/init_on_esx.sh
supersan-esx/supersand-esx
supersan-esx/libaio.so.1
[root@esxi:/vmfs/volumes/59521271-21ec59e7-217d-f4ce468806b4] █
```

Please note that the file name of the url may be changed, please concern our website to learn the newest versions, the url was named by file name and version.

Enter supersan-esx folder

```
cd supersan-esx
```

and type the command:

```
./init_on_esx.sh /vmfs/volumes/datastore1
```

```
[root@esxi:/vmfs/volumes/59521271-21ec59e7-217d-f4ce468806b4/supersan-esx] ./init_on_esx.sh /vmfs/volumes/
datastore1
Starting KernSafe SuperSAN

done.
Done.
[root@esxi:/vmfs/volumes/59521271-21ec59e7-217d-f4ce468806b4/supersan-esx] █
```

Now the KernSafe Virtual SAN has been initialized in ESX/ESXi host machine.

Please note supersan-esx folder must exist and can't be removed.

Configure firewall

If you are running a test machine, you can simply stop ESX / ESXi firewall settings by the command:

```
esxcli network firewall unload
```

Otherwise, user can use ESX / ESXi management to open the following TCP port or allow access from specified client.:

```
esxcli network firewall ruleset allowedip add
```

TCP ports are: 3260 and 3261.

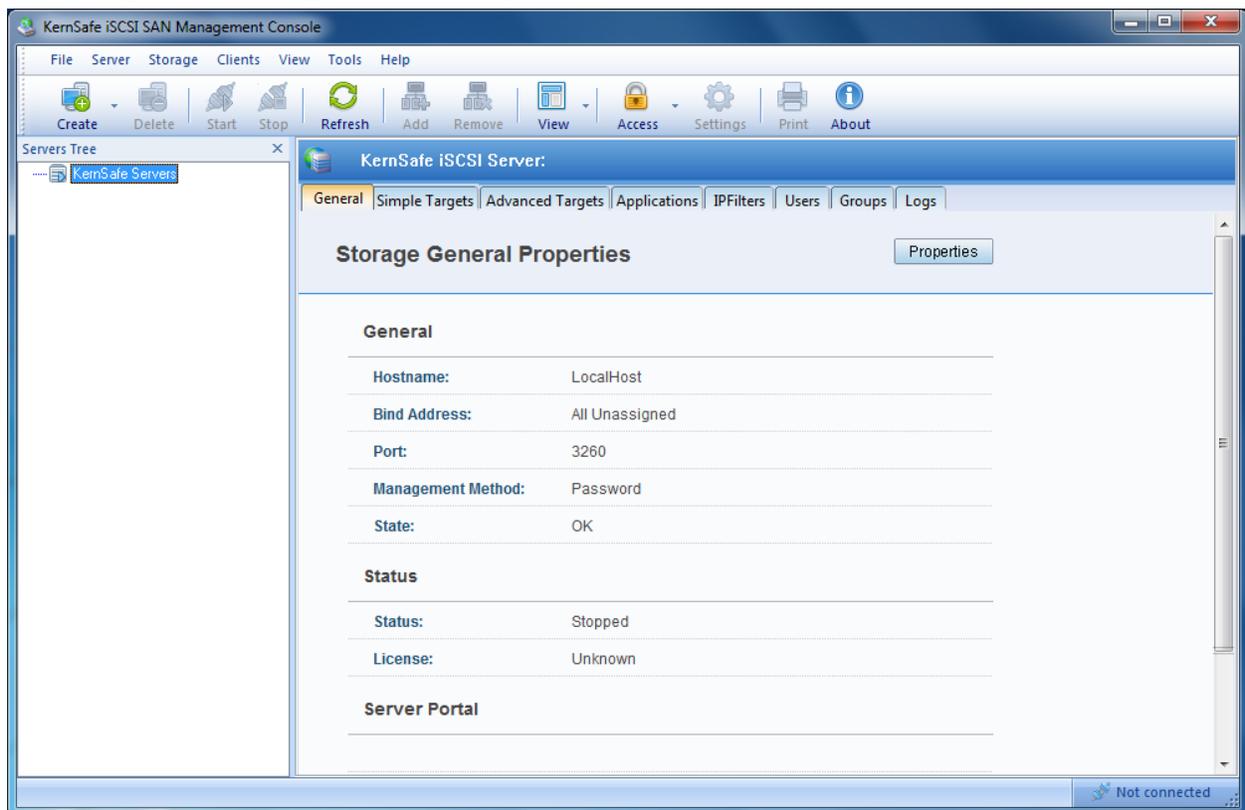
Now the KernSafe iSCSI SAN software was configured on the ESX / ESXi host machine, now need to download KernSafe iSCSI SAN management console to manage it from Windows desktop.

Here you can get the newest version of iSCSI SAN management console:

<http://www.kernsafe.com/download/virtual-iscsi-san.aspx>

Manage Virtual iSCSI SAN from Windows Desktop

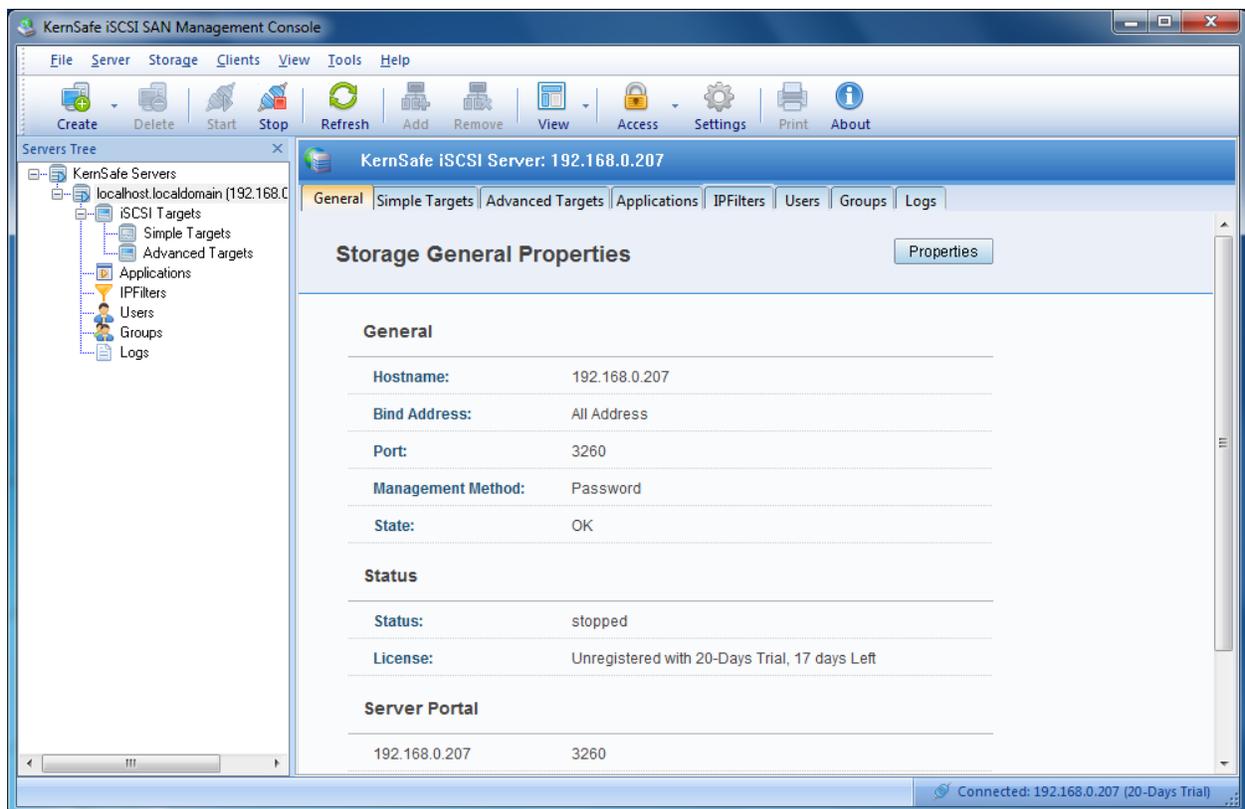
From Windows desktop, unzip the iSCSI SAN management console and execute iSCSI-Mangment.exe or iSCSI-Mangment-x64.exe (x64 bit machine).



Select Server menu and then choose Add Server menu item, now Add Server dialog shows.



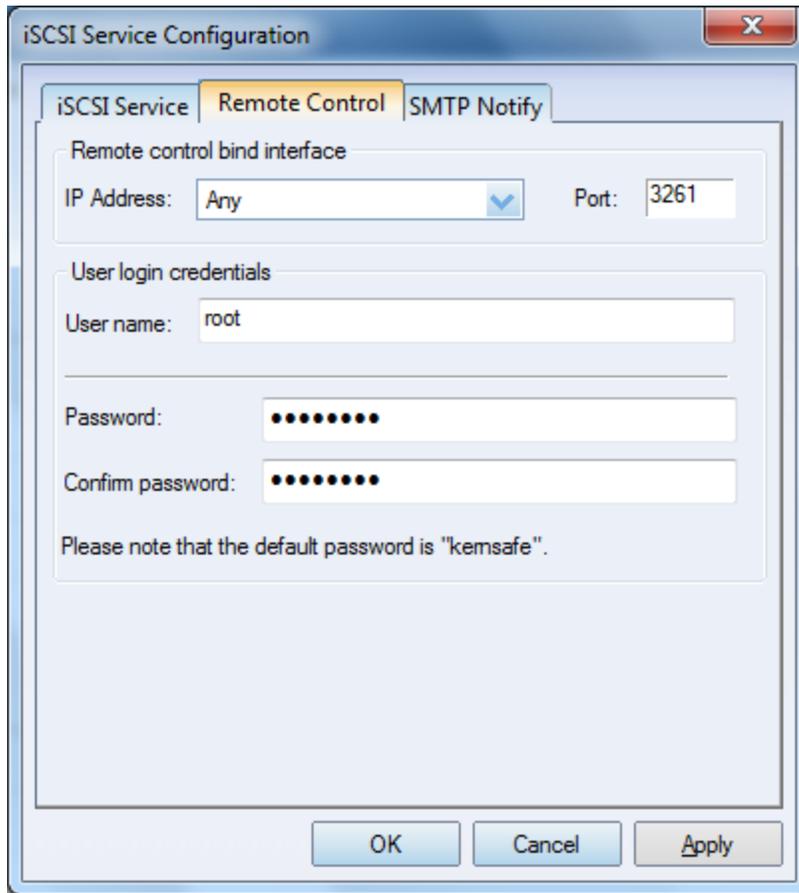
Type the address of the ESX / ESXi machine, click the OK button to add.



If successful, the Linux server will be added to the console for management, for considering security, you should modify remote management credentials.

Click the Settings button, then the iSCSI Settings dialog shows.

Change to Remote Control page.



The image shows a Windows-style dialog box titled "iSCSI Service Configuration". It has three tabs: "iSCSI Service", "Remote Control" (which is selected and highlighted in yellow), and "SMTP Notify". The "Remote Control" tab contains the following fields and controls:

- Remote control bind interface:**
 - IP Address: A dropdown menu currently set to "Any".
 - Port: A text input field containing "3261".
- User login credentials:**
 - User name: A text input field containing "root".
 - Password: A text input field with 10 black dots.
 - Confirm password: A text input field with 10 black dots.
- A note at the bottom of the tab: "Please note that the default password is 'kernsafe'".

At the bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".

Type a new Password and Confirm password, click the OK to save changes.

Now you can fully manage KernSafe iSCSI SAN on ESX / ESXi, for more information of the product using or put it into production, please see user's manual and solution white papers.

Contact

Support: support@kernsafe.com
Sales: sales@kernsafe.com
Home Page: <http://www.kernsafe.com/>
Product Page: <http://www.kernsafe.com/product/free-virtual-native-san.aspx>
Licenses <http://www.kernsafe.com/product/virtual-native-iscsi-san/license-compares.aspx>
Forum: <http://www.kernsafe.com/forum/>

KernSafe Technologies, Inc.

www.kernsafe.com

Copyright © KernSafe Technologies 2006-2017. All right reserved.