Local Storage for Video Archives Using iSCSI

Contents

The objections of this document is to understand the storage requirements for IP Video Surveillance at a branch location. Then, to support the iSCSI server, a branch topology is shown to provide network access to the iSCSI server for configuration and management as well as for the transport of the TCP session between the VMSS network module and the iSCSI server.

An example of how to configure the iSCSI server and format the volume for use and then select the volume for storing archives from the Video Surveillance Management Console (VMSC). There is also sample configurations and **show** commands relevant to the iSCSI file system.

Disk Space Requirements

There are many iSCSI servers in the market which provide data protection by using various RAID levels for data protection. RAID 5 is commonly used due to its low cost of redundancy. For example, a system advertised at 1 Terabyte has four individual disks, each with a raw capacity of 232 Gigabytes per disk, for a total capacity of (232 * 4) 928 Gigabytes of storage. With RAID mode 5, the usable capacity is 676 Gigabytes of usable space. With RADI mode 1 only half the total capacity is available for use. It is important to consider the usable capacity of the iSCSI server, as well as the initial cost of the chassis, the number of disk drives included in the entry level system, as well as the number of empty expansion bays available. Before selecting a system, make sure the usable capacity will meet the storage requirements of the site.

Typically the most cost effective solution on a per-Gigabyte basis is a fully populated chassis. This spreads the cost of the chassis over the maximum number of disks. On the market today, iSCSI storage can be obtained for for less than $2.00 per GB using SATA drives. Systems are available that range in scale from 2 to 96 Terabytes (TBs) of storage. Entry level systems that may support 1, 2, or 4 TB of raw storage may range in price less than $5000 USD, but for systems that support up to 96 TB of storage, the initial, minimal chassis investment may be $8,000 USD or more.

To provide some guidance on the amount of disk space required for a typical branch video surveillance deployment, Table 1 shows the amount of space required for a one-hour archive. Various media types, resolution, frame rate/target bit rates are shown for the Cisco 2500 Series IP camera as well as other cameras.

Table 1   Disk Space Required for One Hour Archive

	Media Type	Resolution	Rate (Frames or Bits Per Second	Reserved Mbytes	Actual Mbytes
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	512	241	243
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	768	347	357
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	1024	475	480
AutoDome - Analog GW	MPEG-4	704 x 480 (4CIF)	1024	477	462
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	2000	953	943
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	4000	1,860	1,800
Axis 223M	MJPEG	1600 x 1200	5	1,840	1,850
Axis 223M	MPEG-4	640 x 480 (VGA)	2000	931	68
Axis 207	MPEG-4	640 x 480 (VGA)	1024	477	405
Axis 207MW	MJPEG	1280 x 720	10	812	5,000

Now that a baseline is provided for an archive of one-hour duration, the next section shows an estimate of the total amount of storage required for multiple cameras based on a typical retention period.
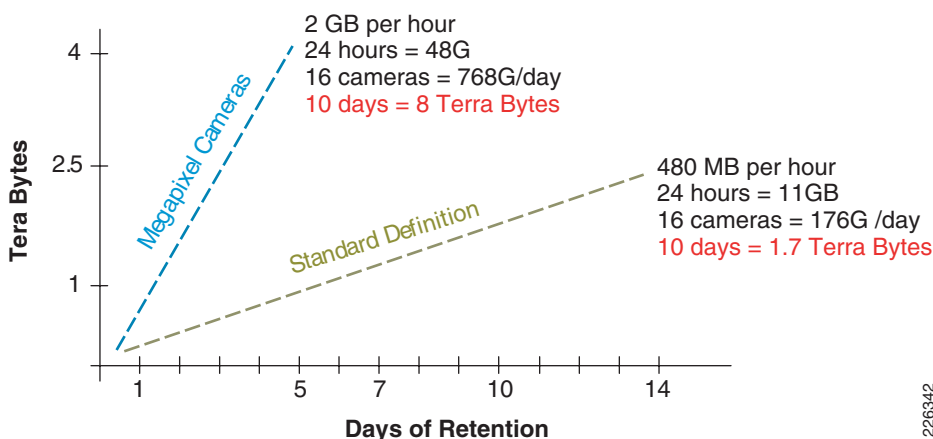
Archive Retention and Storage Requirements

Given the enterprise may deploy standard definition cameras today and consider a megapixel (high) definition cameras in the future, or have a mixture of both, we look at both in this analysis. The Axis 223M is a megapixel camera with a resolution of 1600 x 1200 pixels. At 5 frames per-second, this camera

requires almost 2GB per-hour of archived recording. The Cisco 2500 Series standard definition camera at 720x480 (D1) resolution with a target bit-rate of 1024Kbps requires 480MB of disk space per-hour of archive retained.

Assuming the enterprise has a retention period of 10 days per camera, a 16 camera deployment archiving 24 hours per day requires between 2 and 8TB of storage capacity. The megapixel camera has almost four times the storage requirements as the standard definition camera. This is illustrated in Figure 1.

Figure 1 **Branch Office Video Surveillance Storage Requirements**

Retention periods vary from organization to organization and some cameras may have a longer retention period than others. There may be multiple archives created from a single camera, with the longer retention period having a lower frame rate while a higher frame rate may have a retention of only a few days. Some archives are initiated only on triggered events. Additionally, the amount of storage for stored clips (local BWM/X clip repository) and backup (backup repository) must also be considered. Capacity for future camera installations as well as replacement of standard definition with high definition in the future must also be considered.

VMSS Network Module

This section provides a brief overview of the available hardware configurations of the VMSS network module. There are three models of VMSS network modules. Their characteristics are shown in Table 2.
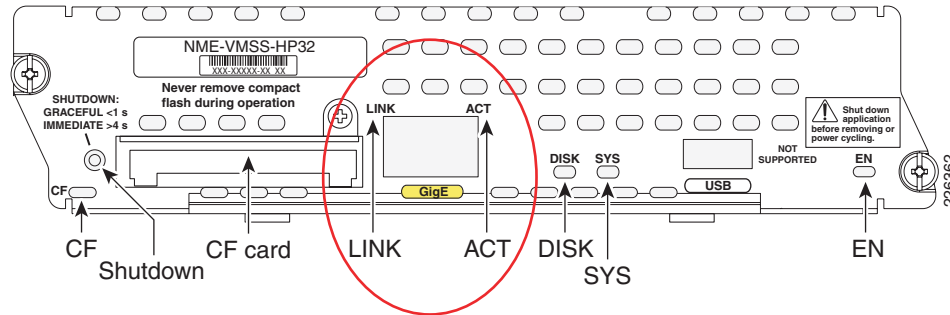
Table 2 **VMSS Models**

Model	Processor	Hard Disk	Memory
NME-VMSS-16	1.0 GHz	120 GB (SATA)	512 MB
NME-VMSS-HP16	1.4 GHz	160 GB (SATA)	2 GB
NME-VMSS-HP32	1.4 GHz	160 GB (SATA)	2 GB

Not all the listed hard disk space is available for archives, because the operating system files are contained on the disk as well. Assume that less than half the actual hard drive is available for local archive use. It is sufficient for initial testing, but should not be considered as an option for fully functional production environment. To meet the video archive storage requirements of the branch location, attaching an Internet SCSI (iSCSI) appliance to the VMSS network module external interface is the preferred solution.

The VMSS faceplate has an external Gigabit Ethernet port for physically connecting to a switch to communicate with the iSCSI server. The location of the port is shown in Figure 2.

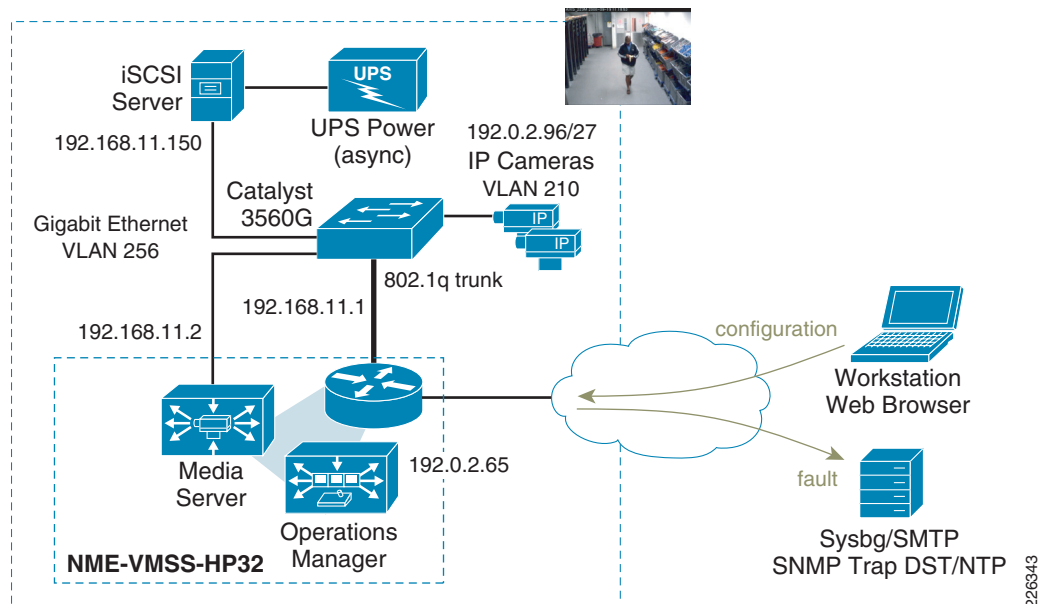*Figure 2   VMSS Faceplate Showing External GigabitEthernet*

In testing three separate Buffalo TeraStation Pro II iSCSI Rackmount units are deployed on Cisco ISR 2851, 3825, and 3845 routers using the NME-VMSS-16, NME-VMSS-16HP and NME-VMSS-32 network modules. This brand of iSCSI server is used because of low initial cost, features, and availability. It is not a product recommendation. This server is available in 1,2, and 4TB configurations. In most customer deployments, servers with substantially higher storage capacity may be required.

Deployment Topology

A typical branch router deployment topology using iSCSI for local storage is shown in Figure 3.

Figure 3   Branch Router Deployment Topology using iSCSI

The LAN switch in this deployment is a Cisco Catalyst 3560G-48TS. This switch supports 48 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports in a 1RU form factor. The Cisco ISR router GigabitEthernet 0/1 interface is an 802.1q trunked interface. There is an isolated VLAN, 256, for the

iSCSI network. The GigabitEthernet port on the face place of the VMSS network module is connected to a non-trunked switch port in VLAN 256. The Buffalo TeraStation Pro II iSCSI Rackmount TS-RI1.0TGL/R5 server is also attached to a non-trunked port on VLAN 256.

This iSCSI server has a facility for SMTP email alerts, NTP, syslog, and has an imbedded web server for configuration and management. To use these management functions and to access the server from the central campus location, the default gateway of the server is configured with the IP address of the branch router Gigabit Ethernet interface, 192.168.11.1. This network is advertised by the dynamic routing protocol (EIGRP) configured on the branch router.

The IP addressing of the router, external interface of the VMSS module and the iSCSI server are shown in Table 3.

Table 3   Devices and their IP Addresses

Device	IP Address
Branch router GigE VLAN 256	192.168.11.1
VMSS External Interface	192.168.11.2
iSCSI Server	192.168.11.150
VMSS-HP32 (VSOM/Media Server)	192.0.2.65

There are two interfaces connected to subnet 192.168.11.0/25 from the branch router; one through the GigabitEthernet interface on the ISR router chassis, the second through the external interface of the VMSS network module.
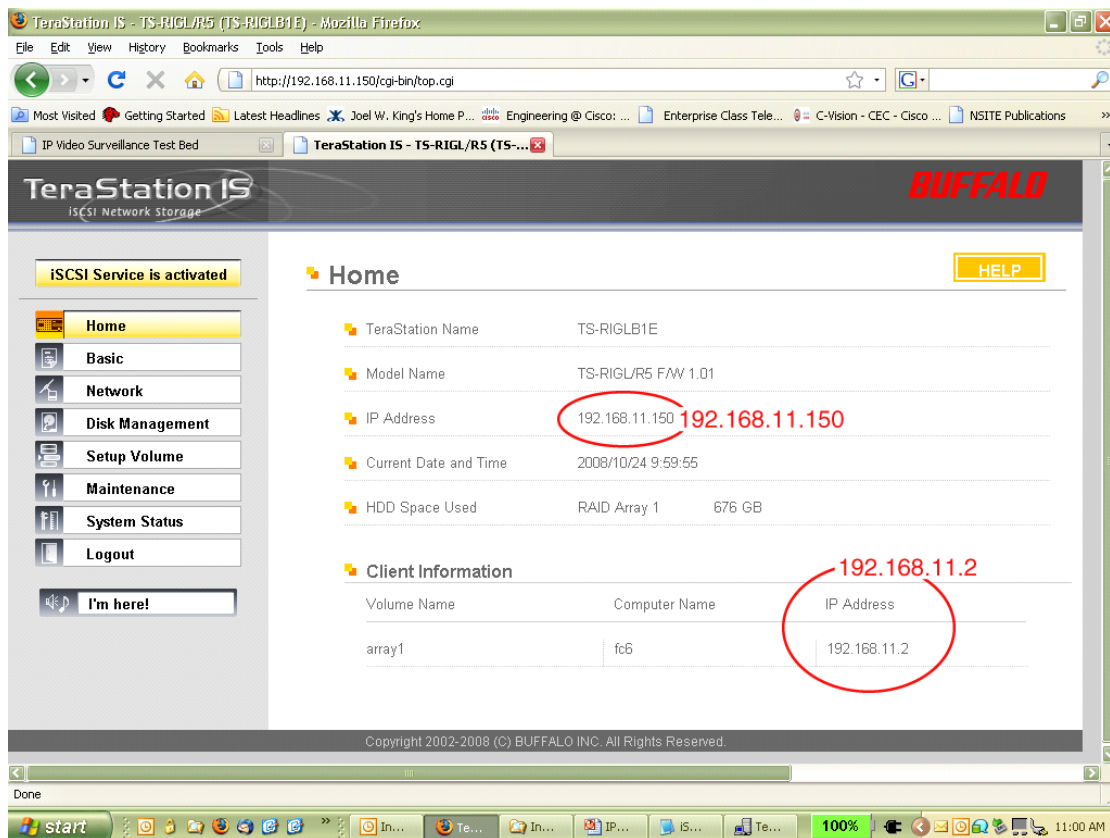
Installation and Configuration of iSCSI Server

This iSCSI server implementation uses DCHP to obtain an initial IP address, or if no DHCP server is accessible on the network, defaults to a documented static IP address. The recommended implementation approach is to configure a DHCP pool on the branch router, connect the iSCSI server to the network and and power up. After waiting a few minutes for the server to boot and obtain an IP address from this pool, use the **show ip dhcp binding** command to determine the IP address allocated to the server. Use a workstation and web browser to connect to the IP address of the server. The server used in testing also displays the IP address on the LCD status panel on the front of the unit.

From the web browser, change the default password, configure the NTP parameters, SNMP server, syslog server address, and any other parameters that may be relevant. Finally, change the IP address of the server to a static IP address and update this information in the corporate DNS services. Because the VMSS network module must be configured with a target IP address or hostname in the configuration, a static IP address is needed.

The following sample iSCSI configuration screen is shown in Figure 4.

Figure 4 *Sample iSCSI configuration screen*

The screen shot in Figure 4 shows the VMSS network module's external address listed as a client connection at IP address 192.168.11.2. The IP address of the server is 192.168.11.150. The default gateway is the ISR router at address 192.168.11.1. Default network access through the router allows the iSCSI server to communicate with the corporate network devices through the ISR router while maintaining a direct, LAN-based connection to the iSCSI client, the VMSS network module.

Sample Branch Router iSCSI Configuration

The following configuration is the relevant portion of the branch router interfaces related to the iSCSI server deployment.

```
!
hostname vpn1-3845-1
!
interface GigabitEthernet0/1
 description Trunk
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.150
 description Outside (WAN) Interface
 encapsulation dot1Q 150
 ip address dhcp
!
```

```
interface GigabitEthernet0/1.250
 description INSIDE VLAN
 encapsulation dot1Q 250
 ip address 10.81.7.1 255.255.255.248
!
interface GigabitEthernet0/1.256
 description iSCSI VLAN
 encapsulation dot1Q 256
```

This is the default gateway IP address for the iSCSI server.

```
 ip address 192.168.11.1 255.255.255.0

!
interface Integrated-Service-Engine3/0
 description NME-VMSS-HP32
 ip address 192.0.2.64 255.255.255.254
 ip flow ingress
```

The VMSS operating system learns the external IP address from this configuration statement

```
 service-module external ip address 192.168.11.2 255.255.255.0
 service-module ip address 192.0.2.65 255.255.255.254
 service-module ip default-gateway 192.0.2.64
 no keepalive
!
router eigrp 64
 network 10.0.0.0
 network 192.0.2.64 0.0.0.63
```

A network statement for the iSCSI subnet is included to advertise this network to the intranet.

```
 network 192.168.11.0
 no auto-summary
 eigrp stub connected
!
end
```

Tip Following the configuration of the external IP address, the network module must be reloaded for the VMSS operating system to learn the configured address; for example, **service-module in2/0 reload**.

Verify IP Addressing on the VMSS Network Module

After completing the configuration of the external IP address and the module reload, use the **service-module** *<interface>* **session** command to access the console of the network module and verify the IP addresses are configured. Issue the **show interfaces** command as shown below.

```
VMSS-SITE140# show interfaces
GigabitEthernet 0 is up, line protocol is up
  Internet address is 192.0.2.65 mask 255.255.255.254 (configured on router)
    9101 packets input, 961197 bytes
    0 input errors, 0 dropped, 0 overrun, 0 frame errors
    9560 packets output, 2449037 bytes
    0 output errors, 0 dropped, 0 overrun, 0 collision errors
    0 output carrier detect errors

GigabitEthernet 1 is up, line protocol is up
  Internet address is 192.168.11.2 mask 255.255.255.0 (configured on router)
    382068 packets input, 31118652 bytes
    0 input errors, 0 dropped, 0 overrun, 0 frame errors
    8074102 packets output, 3415145010 bytes
    0 output errors, 0 dropped, 0 overrun, 0 collision errors
```

```
     0 output carrier detect errors

IDE hd0 is up, line protocol is up
    18699 reads, 2678064128 bytes
    0 read errors
    115791 write, 817836032 bytes
    0 write errors
```

If the GigabitEthernet 0 and 1 interfaces are not configured with an IP address from the router, verify the ISR router interface configuration and reload.

Formatting iSCSI Storage

The iSCSI storage must be formatted by the VMSS network module prior to use. While remaining on the console of the network module, enter configuration mode (**configure terminal**) and define the iSCSI tag (media 1 to 9) and target IP address of the iSCSI appliance. The IP address must be a static IP address defined in the corporate DNS, not the DHCP supplied IP address used in the initial configuration. The iSCSI server used in testing had an option to disable and enable the iSCSI service. Verify that the service is enabled, otherwise these steps will fail. The following examples assume the iSCSI tag is **media1**.

Configure the target IP address of ISCSI server as follows:

```
VMSS-SITE140(config)# storages iscsi media1
VMSS-SITE140(config-iscsi)# target-ip 192.168.11.150
VMSS-SITE140(config-iscsi)#exit
```

Verify/attach External Gig E port of the network module to the LAN switch as follows:

```
VMSS-SITE140(config)# storages iscsi media1
Modifying existing iscsi
VMSS-SITE140(config-iscsi)# state enable
iSCSI volume not formatted or unsupported file system:
VMSS-SITE140(config-iscsi)#exit
```

Format the storage as follows:

```
VMSS-SITE140# format storages iscsi media1
The storage device you are about to format has the following parameters:

Target name: iqn.2004-08.jp.buffalo:TS-RIGLB1E-001D73262B1E:array1 LUN: 0

[output deleted for brevity]

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 21 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
    Done.
To use the storage, please issue "state disable" then "state enable"
 on media1

VMSS-SITE140(config)# storages iscsi media1
Modifying existing iscsi
VMSS-SITE140(config-iscsi)# state disable
VMSS-SITE140(config-iscsi)# state enable
```
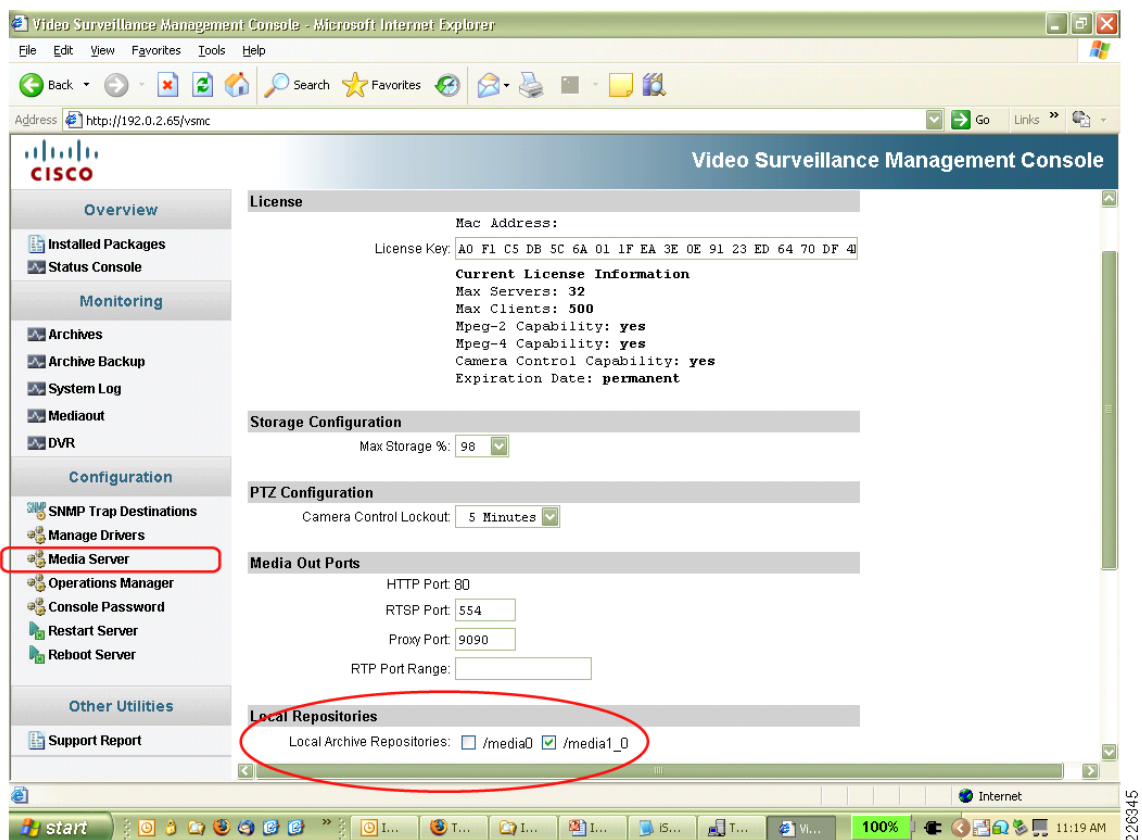
```
Media successfully enabled!
```

At this point the volume is formatted and available for use.

Select iSCSI Volume for Use

Now that the volume is mounted and ready, connect to the Video Surveillance Management Console (http://192.0.2.65/vsmc) and select Media Server and at Local Repositories, deselect the on-board disk at **/media0** and select iSCSI disk **/media1_0** as shown in Figure 5.

Figure 5   Video Surveillance Management Console

Clipping and backup can also be directed to the iSCSI device.

VMSS Network Module Configuration

After formatting is complete, the configuration of the VMSS network module appears as follows.

The **target-ip** line with the volume name and the iSCSI Qualified Name (IQN) is entered automatically, only the **target-ip** address need be manually configured.

```
storages iSCSI media1
 target-ip 192.168.11.150
```

```
   target-ip 192.168.11.150 volumeName iqn.2004-08.jp.buffalo:TS-RIGLB1E-001D7326
2B1E:array1 LUN 0

 end storages-iscsi
end
```

To verify the detailed status of the volume, the **show storages iscsi** command can be entered.

```
VMSS-SITE140# show storages iscsi status  detail
      Fou Log                                                  Portal
 Tag  nd  in  Device   Mounts    LUN FS Types     iSCSI Portal      Reachab
le IO Target Name
====== === === ======== =========== === ======== ===================== =======
== == ==============
media1 yes yes /dev/sdb /media1_0    0   ext3     192.168.11.150:3260,1   Yes
   rw iqn.2004-08.jp.buffalo:TS-RIGLB1E-001D73262B1E:array1
```

Tip The status of 'rw'read-write should be verified. If the status is 'ro', read-only, the volume cannot be written to and archives will fail.

Summary

In practically all branch office video surveillance deployments, an external iSCSI device is needed to provide sufficient disk space for storage of local video archives. The branch topology must be configured to provide network connectivity for fault and configuration management of the iSCSI server. The enterprise network management system must monitor the iSCSI server, router and VMSS network modules to insure the operational health of the surveillance system at the branch location.