

Release Notes for Windows Host Drivers, 3.0.6-Windows

These release notes document information about the current release of Oracle's Xsigo Windows host drivers for Oracle's Xsigo Fabric Director. Additional release notes exist for:

- Oracle's Xsigo Linux host drivers
- Oracle's Xsigo Fabric Director and XgOS
- Oracle's Xsigo Fabric Manager GUI
- Oracle's Xsigo ESX Server 4.1/4.1i host drivers
- Oracle's Xsigo ESXi Server 5.0 host drivers
- Oracle's Xsigo HCA Option ROM and Firmware



Note

If you are upgrading to 3.0.6 host drivers, be aware that the upgrade procedure has changed slightly. For information, see [Upgrading Software for Servers](#) on page 15.

Also, if you are using IP over IB in your Windows host environment, you need to manually install and enable the IP over IB drivers after the 3.0.6 Windows host driver package is installed the first time. See [Considerations for Using IP over IB](#) on page 3.

These release notes contain the following sections:

- [What's New in this Release](#) on page 2.
- [System Requirements](#) on page 2
- [System Limitations and Restrictions](#) on page 14
- [User Guides](#) on page 17
- [Documentation Erratum](#) on page 17
- [Supported Host Drivers](#) on page 17
- [Considerations for Windows Server 2008 and Hyper-V](#) on page 17
- [Known Problems](#) on page 23
- [Fixed Problems](#) on page 26
- [Technical Support Contact Information](#) on page 28

Xsigo Systems
70 West Plumeria Drive
San Jose, CA 95134
USA
<http://www.xsigo.com>
Tel: +1.408.329.5600



Overview

Oracle's Xsigo Fabric Director is a service-oriented platform that interconnects data-center resources based on application demands.

Customers and partners are requested to send comments and report bugs to Xsigo by filing a customer case through the Xsigo Technical Support web portal (<http://support.xsigo.com>). Xsigo is fully committed to responding to all feedback regarding our product and greatly appreciates customer involvement. If you need to contact Xsigo Customer Support, you can facilitate your interaction with Customer Support by first gathering some troubleshooting information. For more information, see [Technical Support Contact Information](#) on page 28.

What's New in this Release

This release contains the following new or changed content:

- The MTU size for Windows hosts is now settable, and interacts with the MTU set through the XgOS to negotiate an optimal MTU for vNICs or HA vNICs on the host. For more information, see [MTU Usage on Host-Side vNIC Devices Has Been Enhanced](#) on page 2.
- The `xg_fwupdate.vbs` script has been deprecated. For more information, see [The `xg_fwupdate.vbs` Utility is No Longer Supported](#) on page 14.
- The procedure for upgrading the host drivers on Windows servers has been modified. For more information, see [Upgrading Software for Servers](#) on page 15.
- Important fixes for customer issues have been added. For more information, see [Fixed Problems](#) on page 26.



Note

In this release, if you are doing a fresh install of host drivers (uninstalling the older host drivers, then installing the new host drivers), you will need to recreate the host-side IP configuration.

System Requirements

The following architectures are tested in this release:

- Microsoft Windows Server 2003 SP2 R2
- Microsoft Windows Server 2008 SP2
- Microsoft Windows Server 2008 R2

MTU Usage on Host-Side vNIC Devices Has Been Enhanced

For Xsigo vNICs and HA vNICs, a new property (MTU) is settable under the vNIC device's network device properties on the Windows host (*Device Manager->Network->vNIC or HA vNIC Device Properties*). There is also an MTU value that is used by the XgOS. The way that the vNIC-device MTU and the XgOS MTU are used is the heart of the behavior change.

Now that this field is settable on the vNIC device as well as in the XgOS, the usage of the vNIC device's MTU can either be used or ignored. In version 3.0.6, this MTU property for vNIC or HA vNIC devices operates as follows:

- By default, the MTU field will be zero on the vNIC device. If this value is not changed, the `IO PortMTU` value (which is derived from the XgOS) will be used.
- If the MTU field is set or changed on the host's vNIC device, and this value is less than or equal to the XgOS's `IO Port MTU` size, then the vNIC device MTU will be used. In all other cases, the vNIC-device MTU value will be ignored and the XgOS `IO Port MTU` will be used instead.



Note

The maximum allowed value for the vNIC device's MTU is 9194, which is the same maximum supported in the XgOS.

Regardless of which MTU is used, the Fabric Director's event log will contain either of the following messages whenever the MTU is being set for the vNIC device:

- If the vNIC-device MTU is used:

```
System Event, Type : Information : "<vnic name> Used RegMTU <registry
configured mtu size>, VNMtu <Xgos IO Port MTU size>"
```

- If the vNIC-device MTU is ignored:

```
System Event, Type : Warning : "<vnic name> Used VNMtu <Xgos IO Port MTU
size>, Ignored RegMTU <registry configured mtu size>"
```

Considerations for Using IP over IB

For this release only, Windows hosts that are using IP over IB need to have the IP over IB software stack manually installed and enabled.

The **setup.exe** program will successfully copy the IP over IB stack onto the Windows server, but you must explicitly install and enable the IP over IB stack for the IP over IB feature to run. Without this user intervention, the IP over IB host feature will not work automatically after an install or upgrade until you perform the required adjustments.



Note

In this release of Windows host drivers, the IP over IB stack is not WHQL signed.

Also, be aware that if you had IP over IB running before installing or upgrading your host drivers, the IP over IB software will be disabled after you install or upgrade 3.0.6 host drivers unless you enable the IP over IB software at install or upgrade time. However, if IP over IB was installed before you upgrade or install the 3.0.6 drivers, and you do not explicitly install the driver with IP over IP enabled ([Enabling IP over IB at Install or Upgrade Time](#) on page 4), you will see a message displayed during installation that indicates the IP over IB drivers are installed, but will not active after the upgrade.

You can manually enable IP over IB by using either of the following methods:

- by enabling IP over IB at the time the host drivers are installed or upgraded. This method is the easiest and quickest. G13
- by enabling IP over IB after the host drivers are already installed or upgraded. This method is helpful if the host is already up and running on the 3.0.6 Windows host drivers and your IP over IB service is disabled. You will need to explicitly enable this service by using either of the following methods.

Enabling IP over IB at Install or Upgrade Time



Note

If you have already loaded the 3.0.6 Windows host drivers and rebooted the host, you can use the procedure in the next section to enable IP over IB using the tools in the Windows OS.

The **setup.exe** tool allows for standard Windows command-line switches. One of the switches that Xsigo has added to the command-line is `/ipoib-enable` which causes the IP over IB stack to activate when it is disabled. To manually enable the IP over IB software on Windows hosts, follow this step:

- Step 1** If you have not already installed or upgrade to the 3.0.6 Windows host drivers, start the Windows command-line. For example, select **Run...** then enter `cmd` in the resulting dialog.
- Step 2** At the Windows host command-line, run **setup.exe /ipoib_enable** to install the Windows 3.0.6 host drivers with IP over IB enabled.

Enabling IP over IB After the Install or Upgrade



Note

If you have not already installed the 3.0.6 Windows host drivers, you can install the Windows host drivers

To manually enable IP over IB through the native Windows OS, perform the following steps in the order shown:

1. After the host drivers are installed the first time, you must specify the file path to the IP over IB stack. See [Manually Specify the File Path to the IP over IB Software](#).
2. After specifying the file path to the IP over IB stack, select the IP over IB device and enable it as trusted software. See [Manually Set the IP over IB Stack as a Trusted Device](#).



Note

If your environment does not use IP over IB, you can skip the following two sections.

3. As an alternative, you can also run **setup.exe /ipoib_enable** after the host drivers are installed, then

Manually Specify the File Path to the IP over IB Software

After you download the 3.0.6 Windows host drivers, unzip them on the host server, and run **setup.exe** to install them, the IP over IB stack is not automatically enabled. As a result, you must manually enable this component of the host driver package. The IP over IB stack is the only component of the host drivers that you must enable manually. You must enable the IP over IB stack only if your Windows host environment uses the IP over IB feature.



Note

The following procedure assumes that you have already downloaded the 3.0.6 Windows host drivers, unzipped them, and run `setup.exe` once to completely install the host drivers once.

After the server has been rebooted at the end of a host driver install, use the following procedure to specify the file path to the IP over IB stack:

- Step 1 On the Windows host, select *Computer Management->Device Manager->Other Devices*.
- Step 2 Select the IPoIB device, right-click, and select *Update Driver Software...* as shown in [Figure 1](#).



Figure 1 Selecting the IP over IB Adapter

When you make this selection, the Update Driver Software — OpenIB IPoIB Adapter dialog is displayed as shown in [Figure 2](#) on page 5.

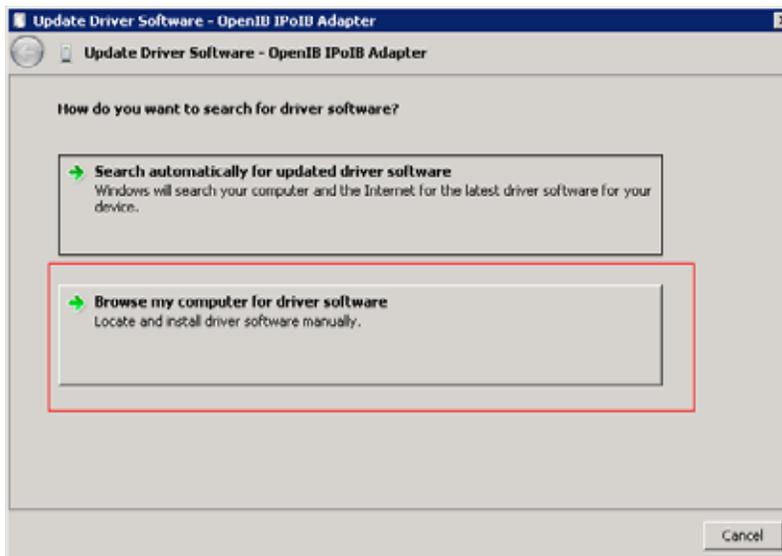


Figure 2 Selecting to Manually Specify the File Path to the IP over Stack

- Step 3 Click *Browse my computer for driver software*. The Update Driver Software — OpenIB IPoIB Adapter dialog is displayed again, as shown in [Figure 3](#).

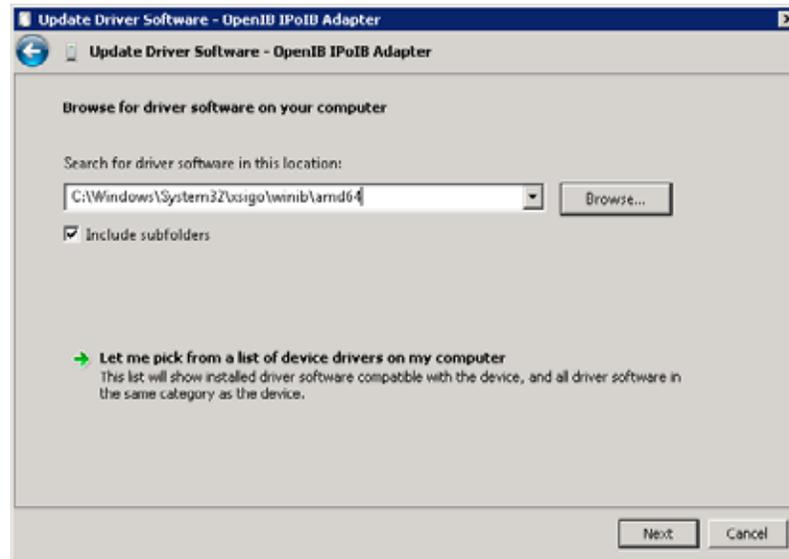


Figure 3 Browsing to the System Location of the IP over IB Stack

- Step 4 Use the *Browse...* button to specify the location of the IP over IB stack. Browse to either of the following system locations based on the type of server:
- For 64-bit servers, browse to `c:\windows\system32\xsigo\winib\amd64` (shown, as an example in [Figure 3](#) on page 6)
 - For 32-bit servers, browse to `c:\windows\system32\xsigo\winib\x86`

- Step 5 Click *Next*, and proceed to the next section.

Manually Set the IP over IB Stack as a Trusted Device

Now that the file path has been specified for the IP over IB software stack, you need to set the IP over IB software as trusted software so that it predictably is installed and usable each time the server is rebooted.

After completing all the steps in the previous section, follow this procedure:

- Step 6 When you clicked Next in the last step, the Windows Security pop up dialog is displayed as shown in [Figure 4](#).

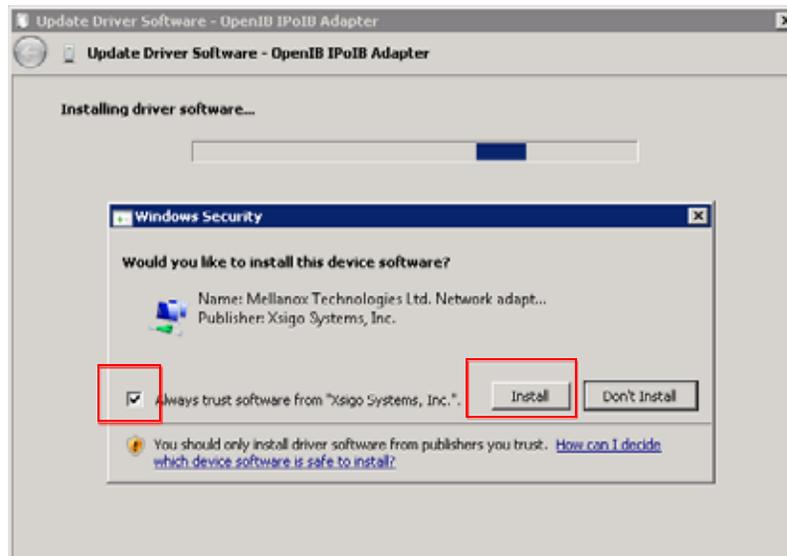


Figure 4 Setting the Trusted Software Option for the IP over IB Stack

- Step 7 On the pop up, click the Always trust software from “Xsigo Systems, Inc.” checkbox. This checkbox must contain a checkmark to allow the IP over IB stack to be loaded every time after this procedure is complete.
- Step 8 When the checkbox is selected, click **Install** to display the Update Driver Software — Mellanox IPoIB Adapter dialog as shown in Figure 5 on page 7.

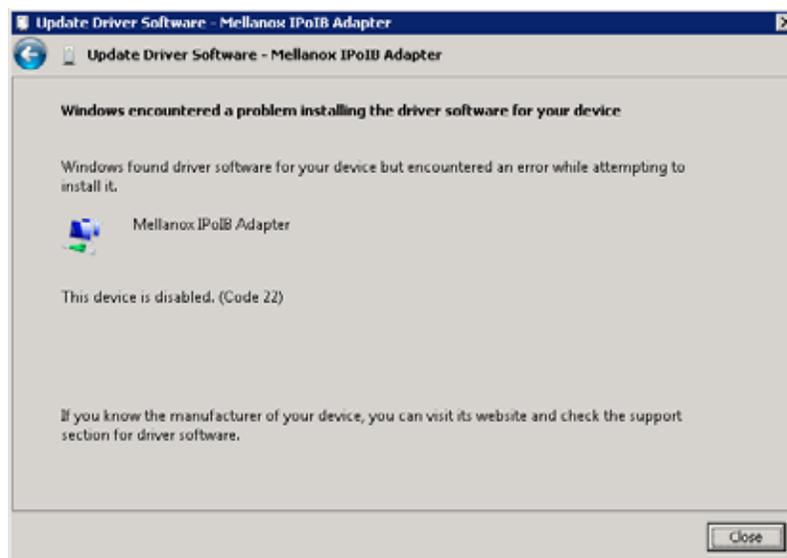


Figure 5 Verifying that the IP over IB Adapter is Present, But Disabled

- Step 9 Verify that the dialog indicates the Mellanox IPoIB Adapter, then click **Close**.

Step 10 On the Windows host, select *Computer Management->Device Manager->Network adapters*.



Figure 6 Enabling the Mellanox IP over IB Adapter

Step 11 Select the Mellanox IPoIB Adapter, right-click, then select **Enable** as shown in [Figure 6](#).

Step 12 Close Computer Management.

At this point, the procedure is complete. You have specified the file path so that the Windows host can use the IP over IB stack, and you have enabled the IP over IB stack as trusted software. The IP over IB feature is now enabled and running on the host, and after any reboots, the IP over IB software will be active and usable without additional user intervention.

Procedure to Set Correct UUIDs on Blades in Blade Servers

Due to a restriction in hardware, some blades within blade servers do not have unique UUIDs. Instead, they inherit the UUID of the blade server's chassis which causes multiple blades to have the same UUID. You can use the following procedure to set unique UUIDs for blades that are hosting Windows hosts.

The following procedure must be performed on each blade that does not have its own unique UUID. To assign a unique UUID to blades hosting Windows servers:

Step 1 Start the `regedit` tool.

Step 2 In the Registry Editor, display the XSIGOIOV service, as shown in [Figure 7](#).

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XSIGOIOV
```

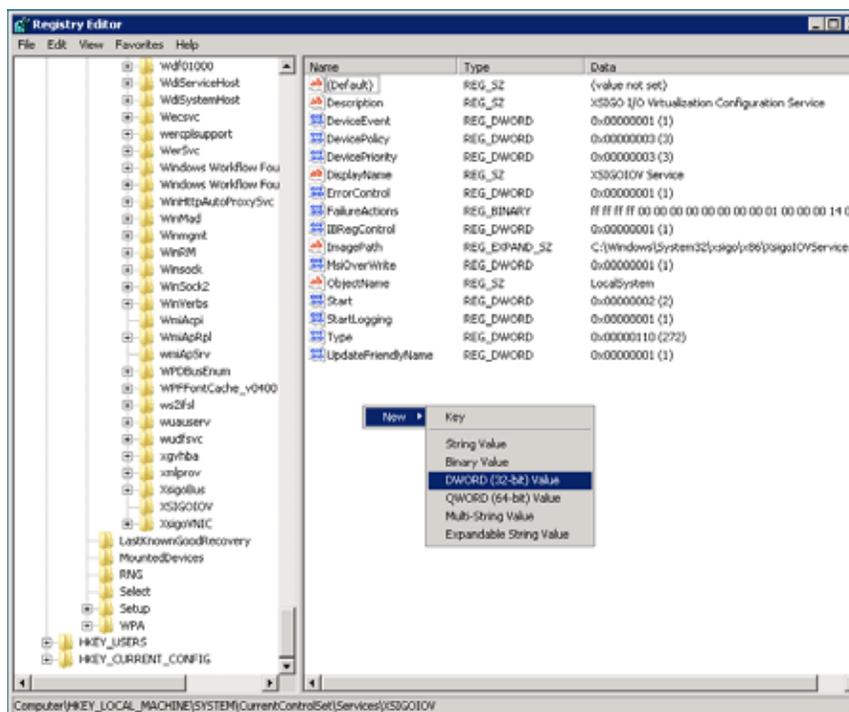


Figure 7 Creating the Registry Key that Allows a Unique UUID for a Blade

- Step 3 Right-click on the XsigoIOV service, then right-click, and select *New->DWORD (32-bit) Value* to add a new entry.
- Step 4 Name the new entry `RegUsePortGUIDasUUID` and make sure that it is named exactly this name.
- Step 5 Right-click the `RegUsePortGUIDasUUID` entry, and select *Modify...* to display the Edit DWORD dialog as shown in Figure 8 on page 9.

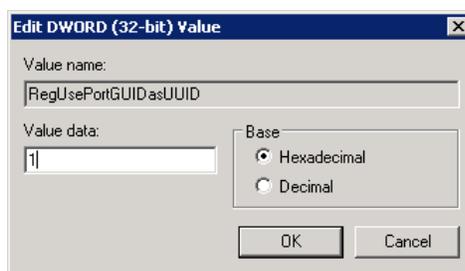


Figure 8 Enabling Unique UUIDs for a Blade through the Edit DWORD Dialog

- Step 6 In the *Value data* field, enter 1 to enable using the Port GUID as the blade's UUID.
- Step 7 Click **OK**, and close all the open dialogs.
- Step 8 Open Server Manager and display the XsigoIOV service (*Server Manager->Configuration->Services*).

Step 9 On the Services page, select the “XsigioIOV Service,” right-click, and select **Restart** as shown in Figure 9.

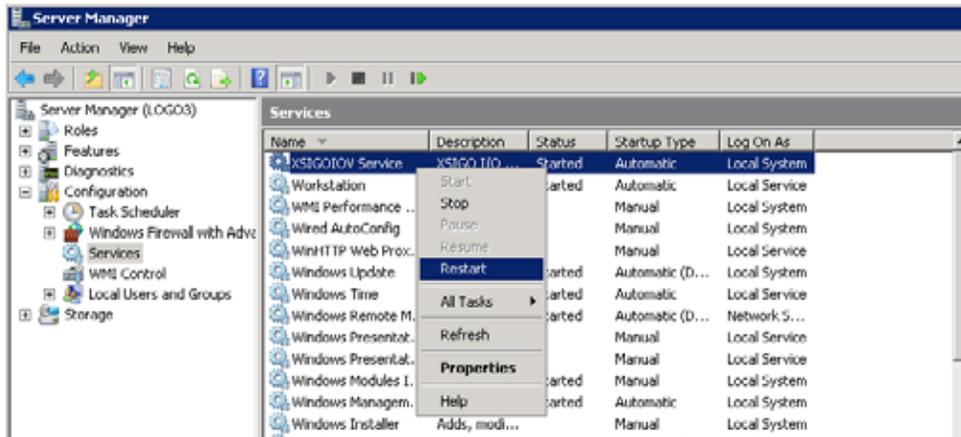


Figure 9 Restarting the XsigioIOV Service from Server Manager

When you select restart, after a short amount of time, the XsigioIOV service is restarted. At this point, the blade hosting the Windows server will receive a correct, and unique, UUID.

Step 10 Repeat this procedure on each blade hosting a Windows server if that blade does not have a unique UUID.

Supported Firmware Version for ConnectX HCAs

Version 3.0.6-Windows supports ConnectX HCAs with the requirement that the Mellanox firmware version is at least 2.7.0 and less than 2.8.0, and the XgBoot Option ROM is either version 2.7.9, or 2.8.6 and later.

For PVS deployments, the Option ROM version must be 2.8.9 or later. Any version of Option ROM earlier than 2.8.9 is not supported in PVS environments.

Supported Firmware Version for InfiniHost HCAs

Version 3.0.6-Windows supports InfiniHost HCAs with the requirement that the firmware version is at least 5.3.0.

Required Versions of Windows Server OS

The minimum host OS version for Window hosts are:

- Microsoft Windows Server 2003 with R2 SP2
- Windows Server 2008 SP2
- Windows Server 2008 R2

If you are not running the minimum version of the host OS, you must upgrade.

Unblock the Windows Host Driver ZIP File Before Unzipping It

The Xsigo Windows host drivers are provided in a ZIP file. When you install or upgrade these host drivers, **do not** install the host drivers directly from the ZIP file by double clicking the host driver package to open it, then running `setup.exe`. Instead unblock the ZIP file before unzipping it. This requirement exists for all the supported Windows server OSes.

To unblock the host drivers .ZIP package before unzipping it, follow this procedure:

- Step 1 Right click the host drivers .ZIP file to display the popup menu, then select Properties as shown in [Figure 10](#).

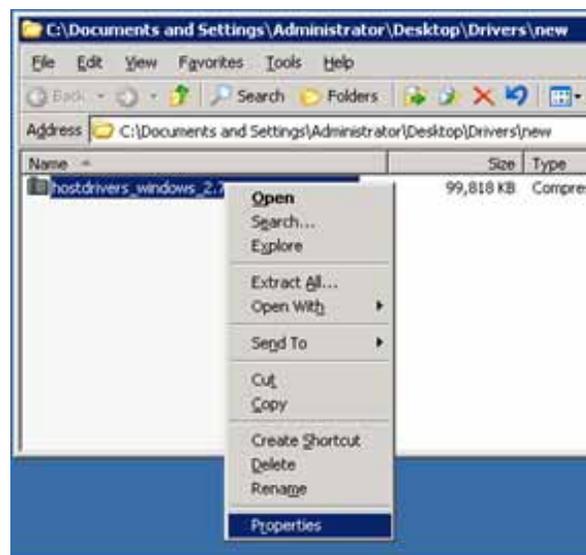


Figure 10 Host Drivers ZIP File Pop-up Dialog

- Step 2 On the Properties dialog, click **Unblock** as shown in [Figure 11](#) on page 12.

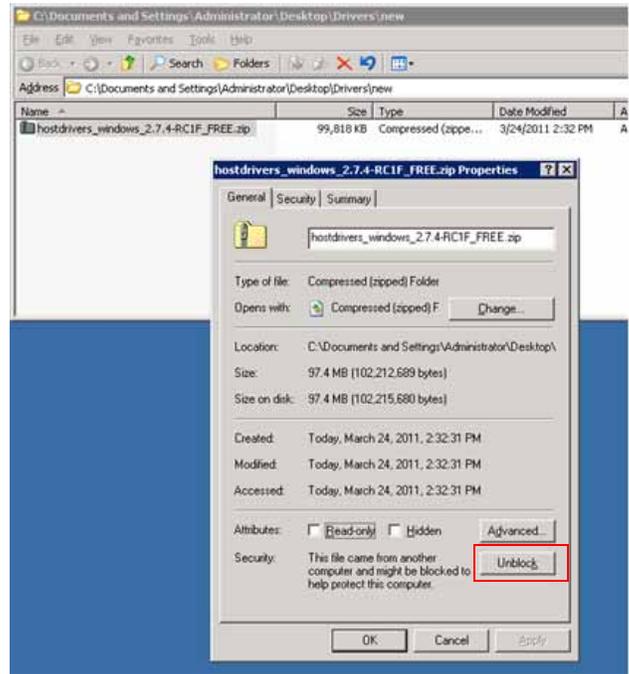


Figure 11 Host Driver ZIP File Properties Dialog

Step 3 Click **OK**. The file is successfully unblocked when the **Unblock** button is greyed out, or not present on the dialog. At this point, the file can be unzipped and will bypass Microsoft Firewall’s security setting.

Do Not Include Mellanox ConnectX HCA Driver in Optional Updates

When checking for Windows Server OS updates, the Mellanox ConnectX Virtual Channel Adapter driver for the HCA is included by default in the Optional Updates dialog as shown in [Figure 12](#).

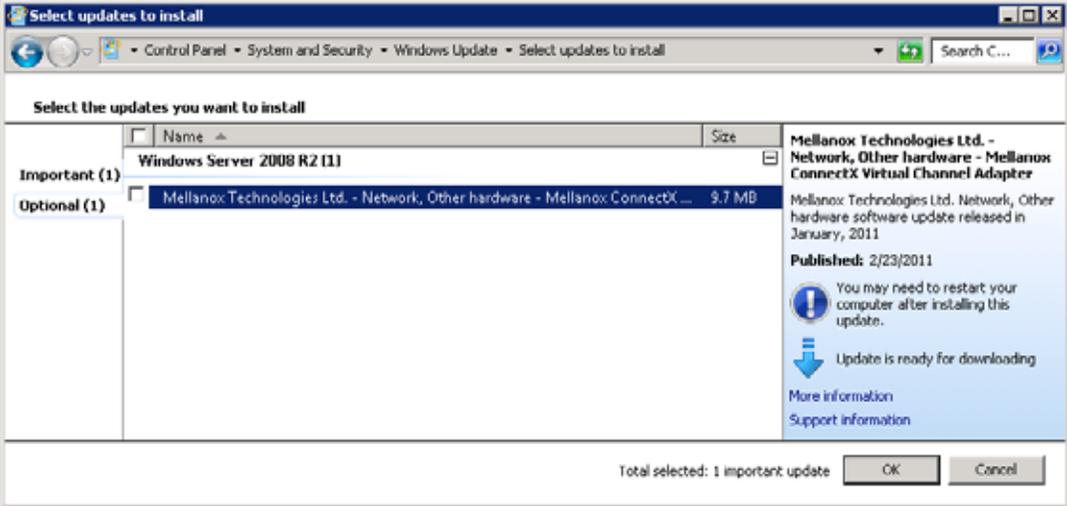


Figure 12 Optional Updates — Mellanox HCA Driver

Do not include the Mellanox ConnectX HCA driver as an Optional Update when checking for Windows server updates. The Mellanox driver is part of the Xsigo host driver package, so it will be installed automatically when the Xsigo host drivers are loaded on the Windows server. If you include the Mellanox HCA driver as a Windows Optional Update, two instances of the Mellanox HCA driver will exist, which causes a conflict that prevents the Xsigo host drivers from functioning correctly.

If IPoIB is Disabled, Do Not Click on the OpenIB IPoIB Adapter Dialog

If you run setup.exe when IPoIB is disabled, the Found New Hardware Wizard will show the OpenIB IPoIB Adapter as an installable option. The *Found New Hardware Wizard* is displayed differently depending on the Windows server's OS, and the way to install the drivers is slightly different between these OSES.

Windows 2003 32- and 64-Bit OS

Figure 13 shows the Found New Hardware dialog in Windows 2003 32- and 64-bit OS.

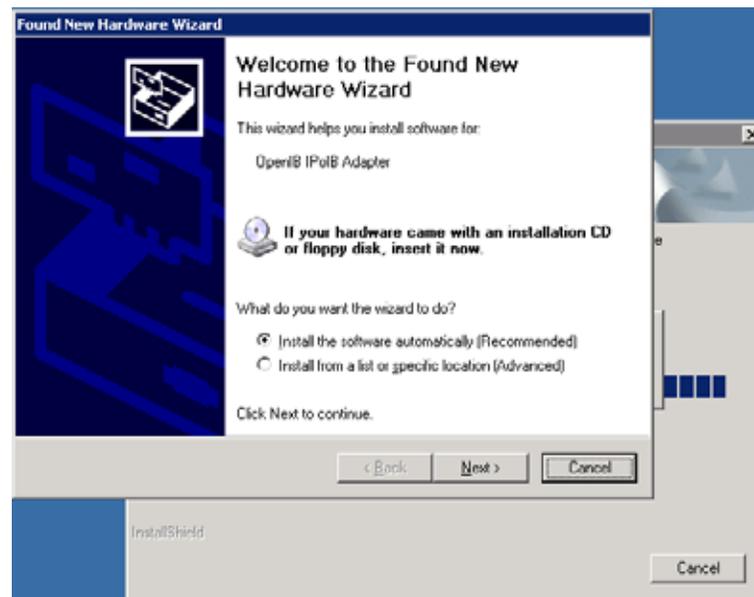


Figure 13 Found New Hardware Wizard — OpenIB IPoIB Adapter Dialog

Do not click *Next* or *Cancel*. Instead, allow the installation to continue in the background. (In fact, you can see the driver installation dialog under the Found New Hardware dialog in this example.) Please be patient. The Found New Hardware dialog will eventually disappear on its own. When prompted to reboot the server, do so.

Windows 2008 32- and 64-Bit OS

Figure 14 on page 14 shows the *Found New Hardware* dialog in Windows 2008 32- and 64-bit OS.



Figure 14 Found New Hardware Dialog — OpenIB IPoIB Adapter Dialog

Do not click any of the options. Instead, allow the installation to continue in the background. (Although not displayed in this example, the host driver installation continues to run in the background.) Please be patient. The Found New Hardware dialog will eventually disappear on its own. When prompted to reboot the server, do so.

System Limitations and Restrictions

This section documents system limitations and restrictions for the host drivers.

The `xg_fwupdate.vbs` Utility is No Longer Supported

In this version of host drivers for Windows, the functionality of the `xg_fwupdate.vbs` script is no longer supported. In this release, if you attempt to run the `xg_fwupdate.vbs` script, no information is displayed. Instead, only version information about the VBS shell utility is displayed—for example:

```
cmd>cscript Xg_FWUpdate.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
```

Because this script is intricately embedded into the Xsigo installer for Windows host drivers, some of the file system structure and binaries are still present after the host drivers are installed. Even though the `FirmwareUpdate` directory is present with the 3.0.6 host drivers, do not use this directory or any of its contents.

Virtual NICs and Virtual HBAs Must be Uniquely Named

With this release of Xsigo Windows host drivers, be aware that each vNIC and vHBA must be uniquely named across Fabric Directors. If the same name is used for multiple vNICs or vHBAs, the first instance of the vNIC or vHBA is installed, but after the first instance is installed, the remaining devices that attempt to install with that name do not install. When you create your vNICs and vHBAs, make sure to assign a unique name to each.



Note

This restriction does not affect HA vNICs. For HA vNICs, the Fabric Directors expect that an HA vNIC is named the same on each Fabric Director, but each HA vNIC pair on each Fabric Director should not have the same name.

In Windows Clusters, Set Persistent vHBA Device IDs with `-local-id` Argument

When using Windows cluster resources, the numbering of vHBAs and their disks is changed when a Server Profile is disconnected, then reconnected. In this situation, when the Server Profile reconnects, new device IDs are assigned to the vHBAs and their disks. However, Windows cluster resources expect the same device IDs, and the new device IDs can cause the cluster resources to occasionally fail for the affected vHBAs.

To keep consistent device IDs in the Windows cluster, Xsigo recommends using the `-local-id=` qualifier when creating a vHBA with the `add vhba` command. This qualifier allows the same device ID to persist through a Server Profile disconnect and reconnect, and in turn, provides a predictable vHBA device ID for Windows cluster resources. When creating vHBAs in a Windows cluster, always use the `add vhba <name> | * -local-id=` command.

Support for Pillar Data Storage with Windows Hosts

Xsigo vHBAs support connecting to Pillar Data storage. Pillar's AxiomONE Path Manager (APM) 3.2 is required for supporting multipathing on Windows 2008 and Windows 2003 hosts.

Supported Update Paths

With this version of host drivers, upgrading the installed drivers is supported if the previous version of installed host drivers is either 2.7.4 or later, or 2.7.4-PVS and later. If your servers are running this version of host driver and you want to upgrade to 3.0.6 host drivers, you can run `setup.exe` and select the upgrade option. For PVS deployments, run `setup.exe /citrix` and select the upgrade option.

If your servers are running a version of host drivers older than either 2.7.4 or 2.7.4-PVS, you cannot upgrade. Instead, you must uninstall the old drivers and install the 3.0.6 host drivers.

Upgrading Software for Servers



Note

If you do not want to upgrade the host drivers, you can always remove (uninstall) the older host drivers and install the new host drivers. Be aware that uninstalling and re-installing host drivers will require you to reconfigure any IP configuration, and also remove and recreate any Hyper-V switches using Xsigo vNICs.

However, if you want to upgrade (not uninstall and re-install the host drivers), use this procedure as a best practice:

- Step 1** For a non-SAN Booted server, disconnect any Server Profiles for the host by issuing the `set server-profile <name> | * disconnect` command. This command removes the virtual resources in the Server Profiles.



Note

In 3.0.6 Windows host drivers, use the disconnect command instead of setting the Server Profile down. In host driver versions later than 3.0.6, you will need to set the Server Profile down.

- Step 2** Allow the traffic to halt on the servers you will be upgrading.
- Step 3** When the Server Profile is in down/down state, run the *setup.exe* installer and select the *Upgrade* option to install the new host drivers.
- Step 4** Reboot the server.
- Step 5** When the server has rebooted and after the post-install scripts have completed, reconnect the Server Profile(s) and allow the Server Profile to return to the up/up state.
- ```
set server-profile <name> connect
```
- Step 6** When the Server Profile all vNICs and vHBAs have transitioned to up/up, resume the halted I/O on the server.

## Virtual Resources Supported per Windows Server

Table 1 shows the number of virtual resources tested and supported on each type of Windows server.

Table 1 Virtual Resources Supported per Windows Server

| Virtual Resource Type                  | Windows Server 2003 |        | Windows Server 2008, 2008 R2, 2008 R2 SP2 and later |        |
|----------------------------------------|---------------------|--------|-----------------------------------------------------|--------|
|                                        | 32- Bit             | 64-Bit | 32-Bit                                              | 64-Bit |
| vNIC                                   | 16                  | 16     | 16                                                  | 16     |
| HA vNIC                                | 8                   | 8      | 8                                                   | 8      |
| vHBA                                   | 16                  | 16     | 16                                                  | 16     |
| Multipath vHBA (8 vHBA from each path) | 8                   | 8      | 8                                                   | 8      |

Be aware that updating a fully loaded Windows server can take approximately 30 minutes (sometimes longer). If your Windows server contains the listed maximum numbers of Xsigo virtual resources, be patient and allow for at least 30 minutes to complete the upgrade. If the upgrade runs longer than approximately 48 minutes, contact Xsigo Technical Support. For information, see [Technical Support Contact Information](#).

## Set Automatic Operating System Updates to “Manual”

Xsigo recommends setting automatic host operating system (OS) updates to “manual.” Automatic updates can download host OS patches that might be incompatible with your Xsigo Systems host drivers. Check with Xsigo Systems Customer Support before applying host OS updates.

## User Guides

User guides are available on CD for shipments to new customers, and by download from the Xsigo Technical Support web portal.

Xsigo Systems provides the following Fabric Director product documentation in PDF format:

- *Fabric Director Hardware and Host Drivers Installation Guide*
- *XgOS Software Upgrade Guide*
- *XgOS Command-Line User Guide*
- *XgOS Remote Booting Guide*
- *Fabric Manager User's Guide*
- *XgOS vNIC Switching Configuration Guide*

You can download these manuals by logging in to the Xsigo Support page ([www.xsigo.com/support](http://www.xsigo.com/support)) and clicking the “Documentation” tab the toolbar at the top of the page. You will need a login and password to access the Xsigo Support page. See [page 28](#).

## Documentation Erratum

The text in this section describes errors in the currently shipping Xsigo product documentation.

### The `xg_fwupdate.vbs` Script Is Still Documented

The `xg_fwupdate.vbs` script is no longer supported starting with host driver version 3.0.6. For more information, see [The `xg\_fwupdate.vbs` Utility is No Longer Supported](#) on page 14.

However, this script is currently documented in the “Working with Window Host Software” chapter of the *Xsigo Fabric Director Hardware and Host Drivers Install Guide, 3.8.0*. Despite being documented, do not use `xg_fwupdate.vbs`.

## Supported Host Drivers

Version 3.0.6-Windows contains updated Windows host drivers which include support for both Windows Server 2008 and Windows Server 2003 hosts. Version 3.0.6-Windows supports the following host drivers:

- `hostdrivers_windows_3.0.6_FREE.zip`

## Considerations for Windows Server 2008 and Hyper-V

Be aware of the following considerations:

- If your network contains Windows Server 2008 hosts, they must be running Windows Server 2008 SP2 or Windows Server 2008 R2.
- Windows 2008 R2 hosts connected to iSCSI storage might crash to a blue screen and display the following error message:

```
0x0000000A (<parameter1>, <parameter2>, <parameter3>, <parameter4>)
IRQL_NOT_LESS_OR_EQUAL
```

This issue is a Microsoft problem (not Xsigo). Microsoft is aware of this issue and has addressed it through a hot fix that you can request from Microsoft. More information can be found at:

<http://support.microsoft.com/kb/979711/en-us>

- Removing a vNIC from a Hyper-V server that has been assigned to a VM through the “Virtual Network Manager” will cause the VM’s network adapter to change to type “Internal”. Adding the same vNIC back without removing the configuration for that network adapter from the “Virtual Network Manager” prevents the network adapter from passing traffic.

You must remove the setting from the “Virtual Network Manager” before adding the vNIC back. After the vNIC has been added back, you may add it once again to the “Virtual Network Manager” then assign it to the VM. This is a Microsoft limitation occurring with physical NICs that have been “uninstalled” and added back again by using hardware rescan in the Device Manager.

- When adding vNICs to the “Virtual Network Manager” you should make sure all Network Adapter setting dialogs are closed before:

- adding any vNICs
- modifying “Virtual Network Manager”

To ensure the network properties are not opened by the system, you can open one adapter’s properties to see if Windows alerts you that an Adapter Properties dialog is already open and no changes can be made until the other dialog is closed. After you have done this check, it is safe to make “Virtual Network Manager” changes or add more vNICs.

- Hyper-V “Virtual Network Manager” can fail with an “adapter already bound to switch” message if too many vNICs are added to the “Virtual Network Manager” at the same time. Simultaneously adding 4 or fewer vNICs is reliable. If more than 4 vNICs are required, add them in groups of 4 or less and allow each batch of vNICs to be successfully added before attempting to add the next batch.

If the “adapter already bound” message is displayed, open the network properties of each remaining Xsigo Failover Adapter and uncheck (deselect) “Microsoft Virtual Network Switch Protocol”.

This will need to be done for each vNIC left on the system because if the “adapter already bound” message is displayed, protocols are bound, and the vNICs will not function properly in that state.

## Considerations for Windows Server 2003

You can check the version of the Windows drivers by selecting *Control Panel->Add Remove Programs*, locating the Xsigo host driver, then selecting the driver, and clicking “Click here for support information” link.

Be aware of the following Windows host driver considerations for this release:

- Windows hosts must be running a minimum of Microsoft Windows Enterprise Server 2003 R2 SP2.
- The default Windows registry setting supports TCP. However, you can increase TCP performance by setting the **TcpMaxConnectRetransmissions** and **TcpMaxDataRetransmissions** values to the maximum settings. Go to the following URL for the recommended registry values:

<http://msdn2.microsoft.com/en-us/library/ms884976.aspx>

- An issue with the Windows PnP manager sometimes causes creating, migrating, or deleting a vNIC or vHBA to take approximately 1 to 2 minutes for each virtual resource. For example, creating 10 vNICs can take 10 to 20 minutes. You can reduce the amount of install time by adding one vNIC or vHBA, then waiting for the device installation to complete before adding the next vNIC or vHBA.

## Downgrading the Xsigo Host Drivers on Windows Servers

Downgrading Xsigo drivers is not supported. As a result, to load an older version of host drivers, you need to uninstall the newer version and re-install the older version. Be aware that when you uninstall and re-install the host drivers, you will need to recreate the host-side IP configuration.

To revert to an earlier version of the drivers, the general procedure is as follows:

- Step 1** For a non-SAN Booted server, disconnect any Server Profiles for the host by issuing the `set server-profile <name> | * disconnect` command. This command removes the virtual resources in the Server Profiles.



Note

In 3.0.6 Windows host drivers, use the disconnect command instead of setting the Server Profile down. In host driver versions later than 3.0.6, you will need to set the Server Profile down.

- Step 2** Wait for any virtual resources to be removed from the host.
- Step 3** Remove the Xsigo host drivers.
- Step 4** Reboot the server.
- Step 5** Install the earlier driver version.
- Step 6** When the server has rebooted and after the post-install scripts have completed, reconnect the Server Profile(s) and allow it to return to up/up state.
- ```
set server-profile <name> connect
```
- Step 7** When the Server Profile all vNICs and vHBAs have transitioned to up/up, resume the halted I/O on the server.

Known Issues with the Windows Host Drivers

This section describes behaviors and problems that you may experience with version 3.0.6 of the Xsigo Windows host drivers.

In Certain Situations, Adding Multiple vNICs Can Cause the Windows Device Manager to Fail

Problem Description: This problem occurs in the following situations:

- **Adding a series of vNICs, or removing then immediately adding vNICs, without waiting for each vNIC to successfully start before adding the next, can cause all of the vNIC installations to fail.** If the “Found New Hardware Wizard” window appears, all subsequent attempts to create new vNICs will fail. The failed vNIC icons may appear in the Device Manager under “System Devices”, “Network Adapters” or “Other Devices”, with yellow exclamation points next to them. See the examples in [Figure 15](#) and [Figure 16](#) on page 21.
- **Sometimes adding multiple vNICs can be halted because the Windows “Found New Hardware” popup dialog is displayed on a Windows host.** You can check the state of vNICs on the Fabric Director by issuing the `show vnic` command for the newly created vNICs. If the vNICs are in the up/initializing state for more than 2 to 3 minutes, this problem can be delaying their creation.



These problems can also occur with high availability vNIC pairs and vHBAs in Windows servers.

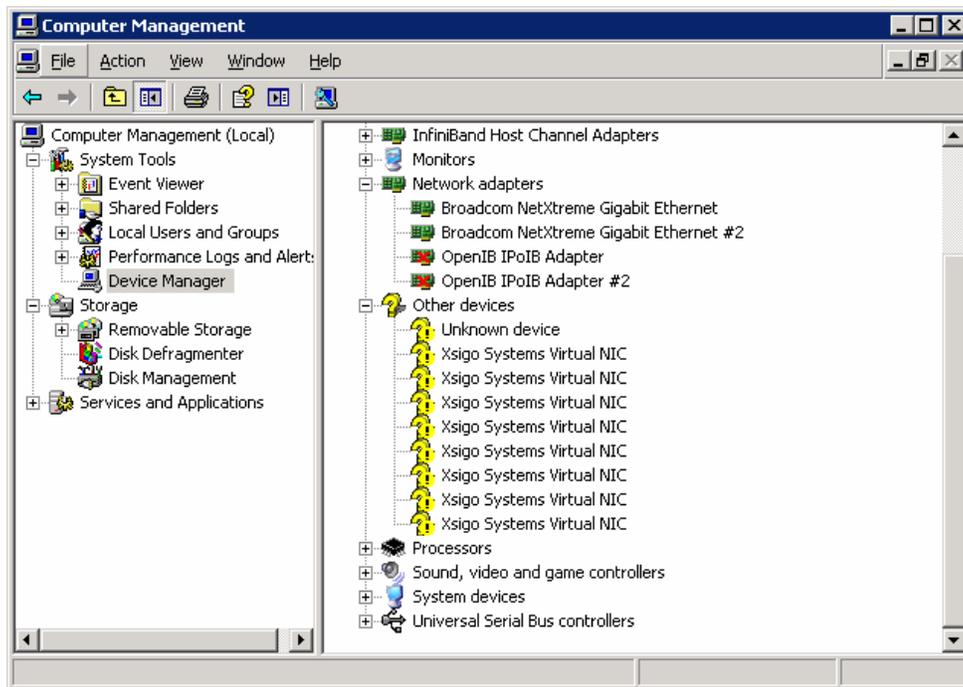


Figure 15 Computer Management Dialog — vNICs Failed to Add (1)

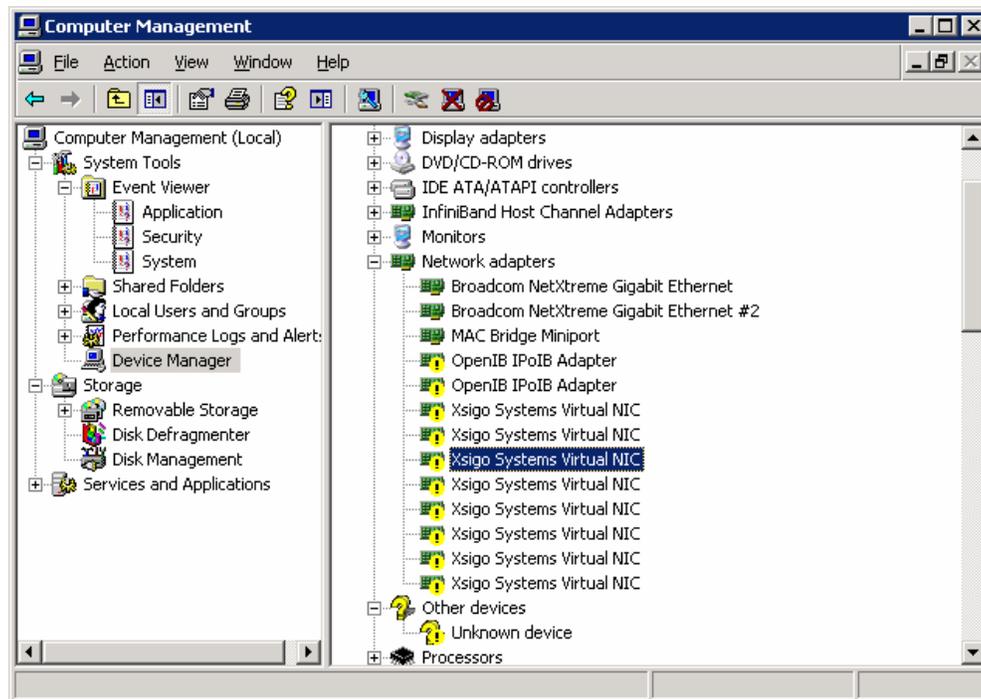


Figure 16 Computer Management Dialog — vNICs Failed to Add (2)

Suggested Action: As a workaround, choose one of the following:

- **For adding (or removing, then immediately adding) multiple vNICs or vHBAs:** Before adding multiple vNICs or vHBAs and committing the transactions for the Windows host on the Fabric Director, wait 5 minutes or longer. This pause ensures that all of the vNIC or vHBA instances have been successfully added or deleted.
- **For the “Found New Hardware” dialog:** Log on to the Windows host as console admin (`mstsc /v <windows host name> /console`). When the “Found New Hardware” dialog is displayed, click *Next* or *Finish* until the dialog is cleared. After the dialog is cleared, the new vNICs or vHBAs install and begin functioning.

Reason: The Windows PnP component installs or uninstalls PnP devices in a synchronous manner. Because one device is installed at a time, the Xsigo Windows co-installer might still be busy adding the new vNICs in the Windows PnP Manager while they are being deleted (or are busy with some other pending installation). The Xsigo device co-installer for adding or removing vNIC or vHBA devices will not be able to run until the device installations are complete. The result may be that the devices are not completely un-installed or installed due to the “Found New Hardware” popup dialog. User intervention is required to clear the dialog and complete the pending PnP operation.

Erroneous Error Message from DCOM Source

Problem Description: In the **Computer Management->System Tools->Event Viewer->System** event log, you may see an error message logged from the DCOM source. See [Figure 17](#) on page 22.

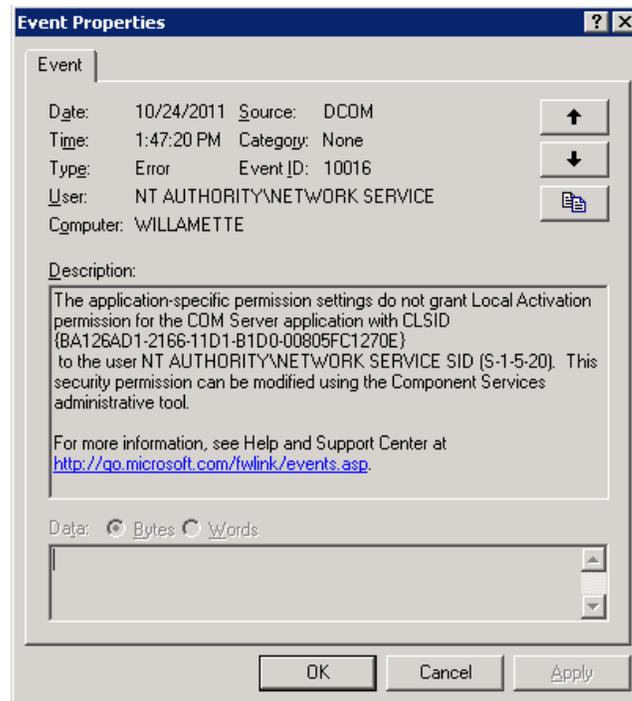


Figure 17 Event Properties

Suggested Action: None. The error message can be safely ignored.

Reason: The application-specific permissions are incorrectly set. This issue is being addressed.

If the Windows Host Server has *Driver Verifier* Enabled, Xsigo Device Performance May Degrade

Suggested Action: Do not run Windows Driver Verifier on any of the Xsigo devices.

Reason: The Window's Driver Verifier application is only used by driver developers. It should not be enabled unless you are specifically testing driver stability.

Known Problems

Table 2 shows the known problems in this release of Xsigo Windows host drivers.

Table 2 Known Problems in Version 3.0.6-Windows

Number	Description
9927	<p>In extremely rare cases under unknown conditions, you may receive a Windows event log error ID 10016. This error indicates that the NETMAN component in the DCOM configuration requires these permissions:</p> <pre>"Local Activation" permission for the COM Server application with CLSID {BA126AD1-2166-11D1-B1D0-00805FC1270E}</pre> <p>Granting the "Local Activation" to the user NT AUTHORITY\NETWORK SERVICE SID (S-1-5-20) repairs the error.</p> <p>This error has been seen only on Windows 2003 servers.</p>
10124	<p>For chassis-managed VLANs, dynamic changing of a vNIC with VLANs back to a standard vNIC is not supported. You must delete the vNIC and recreate it without a VLAN:</p> <p>Step 1 Run <code>xginste32 showphantom *vnic*</code>. If you have 64-bit servers, run <code>xginste64 showphantom *vnic*</code></p> <p>Step 2 Locate the vNIC in the resulting list.</p> <p>Step 3 Run <code>xginstdev32 phantomremove @"xsigobus\vnic\</code> and provide the vNIC name. Of, if you have 64-bit servers, run <code>xginstdev32 phantomremove</code></p> <p>For example, assuming vnic1 is the vNIC you want to change:</p> <pre>xginstdev32.exe phantomremove @"xsigobus\vnic\vnic1"</pre> <p>or</p> <pre>xginstdev32.exe phantomremove @"xsigobus\vnic\vnic1"</pre> <p>Step 4 Recreate the vNIC through the XgOS CLI.</p>
11795	<p>A display problem causes the netmask to show the incorrect number of bits when the IP address for a vNIC is passed to Hyper-V to assign. The IP address is correctly assigned, and traffic does pass across the affected vNIC(s), but the IP address is displayed as 0.0.0/32, and the netmask is incorrectly displayed. This problem occurs only when the vNIC IP address is host-managed through Hyper-V.</p>
11903	<p>On Windows 2008 hosts that are connected to EMC storage if a LUN Mask is applied to the vHBA, then the LUN Mask is changed to a target mask, the LUNs will remain on the Windows host even after a rescan on the vHBA. This problem has been seen on EMC storage only.</p> <p>You can work around this problem by:</p> <ol style="list-style-type: none"> 1. Removing the affected vHBA (<code>remove vhma <name></code>) 2. Re-adding the vHBA with the correct LUN mask (<code>add vhma <name> <slot> -lun-mask=<mask></code>)
12095	<p>Xsigo has observed a situation where Windows hosts that lost connectivity to the Fabric Director will regularly attempt to reconnect for a lengthy period of time, then eventually fail to connect.</p> <p>To work around this problem, you can reboot the server.</p>

Table 2 (continued) Known Problems in Version 3.0.6-Windows

Number	Description
12429	<p data-bbox="261 394 1398 453">For Windows Server 2003 64-bit servers that are configured for SAN Boot, the SAN Boot disk can crash if you disconnect the IB cable under a very specific condition. This problem has been seen:</p> <ul data-bbox="310 474 1398 575" style="list-style-type: none"> <li data-bbox="310 474 1398 506">• only when 64-bit Windows Server 2003 hosts are connected through 3Par MPIO software <li data-bbox="310 516 1398 575">• only when the SAN Boot vHBA is actively carrying reads and writes at the time the IB cable is disconnected <p data-bbox="261 600 1398 659">This problem is due to the 3PAR MPIO software, not due to Xsigo SAN Boot. In all other conditions, Xsigo SAN Boot is functional and operates predictably for Windows Server 2003 64-bit servers.</p> <p data-bbox="261 684 1143 711">To work around this problem, you must reconnect the IB cable and reboot the host.</p>
13150	<p data-bbox="261 730 1398 789">On a Windows 2008 host with 8 HA vNICs and no vHBAs, a race condition between a port-down event and vNIC removal can sometimes cause a blue-screen when uninstalling host drivers.</p> <p data-bbox="261 810 1398 869">You can work around this issue by setting the SAN Boot Server Profile on the physical server to “down” state before uninstalling the host drivers:</p> <p data-bbox="310 890 1398 949">Step 1 On the server where drivers will be uninstalled, set the SAN Boot Server Profile to admin state “down”:</p> <pre data-bbox="402 974 1122 1001">set server-profile <server-profile-name> down</pre> <p data-bbox="310 1022 1192 1050">Step 2 Verify that the SAN Boot Server Profile has transitioned to down state:</p> <pre data-bbox="402 1075 1057 1102">show server-profile <server-profile-name></pre> <p data-bbox="310 1123 1398 1182">Step 3 When the SAN Boot Server Profile is in the down/down state, proceed with uninstalling host drivers.</p>
15453	<p data-bbox="261 1199 1398 1291">When HA vNICs are configured on Windows 2008 64-bit servers, a very rare timing problem can cause secondary vNICs to stay in up/down state for a delayed amount of time (up to 16 minutes) on the Fabric Director if you issue the remove vnic command on the HA vNICs then upgrade the Fabric Director.</p> <p data-bbox="261 1312 1398 1371">You can work around this issue, you can either reboot the Windows host or unplug the IB cable for a minute and plug it back in.</p>
16258	<p data-bbox="261 1394 1398 1453">If vNICs were configured in chassis-managed trunk VLANs, and the Windows host drivers are removed and installed, traffic could take up to 15 minutes for traffic to pass over the vNIC.</p> <p data-bbox="261 1474 1398 1596">This 15-minute delay occurs because the Windows PnP component installs or uninstalls PnP devices in a synchronous manner. Because one device is installed at a time, the Xsigo Windows co-installer might still be busy adding the new vNICs in the Windows PnP Manager while they are being deleted (or are busy with some other pending installation).</p>
16536	<p data-bbox="261 1619 1398 1711">If you disable a host-managed VLAN through the Windows host (not through the Fabric Director) without also setting the VLAN tag value to 0, the VLAN is prevented from being removed from the chassis. As a result, the vNIC or VLAN appears to be working but does not actually pass traffic.</p> <p data-bbox="261 1732 1398 1791">You can work around this problem, by always setting the VLAN tag to 0 whenever you disable a host managed VLAN through the Windows console.</p>

Table 2 (continued) Known Problems in Version 3.0.6-Windows

Number	Description
17879	<p>On rare occasions, the silent install scripts fail the first time you attempt them on Windows 2003 hosts. When the problem occurs, the <code>setup.exe</code> script does execute, but it stops before any of the drivers or components (for example, the IB stack) are installed. This problem has been observed on Windows Server 2003 hosts only.</p> <p>To work around this problem you can do either of the following:</p> <ul style="list-style-type: none"> • Run <code>setup.exe</code> manually one time on the system. When prompted to disable driver updates click Yes and then Cancel. After completing this sequence, the Unattended script files will now run as desired. • Right-click <i>My Computer</i>, then select <i>Hardware</i> tab-><i>Windows Updates</i>-> to display the Connect to Windows Update dialog shown in Figure 18 below.



Figure 18 Connect To Windows Update

- Select ***Never Search Windows Update for Drivers*** then click **OK** on each dialog until all dialogs are closed.
- 18450 On very rare occasions, the Windows Server 2003 hosts running Windows. 3.0.6 host drivers can lose their system ID. The XgOS CLI shows the server present in the output of `show physical servers`, but displays (`no system ID`) for the affected hosts. However, when the system ID disappears, the host becomes no longer manageable through Fabric Manager.
- You can work around this problem by doing either of the following:
- For the XgOS CLI, reboot the server. When the server comes back online, the system ID will be populated in the output of `show physical-server`. It will take a few minutes for the server ID to be relearned and appear in the command's output. Please be patient.
 - For Fabric Manager, reboot the server. When the server has successfully rebooted, use the ***Scan for New and Remove Old Servers*** button (Server Resource Manager->Physical Server Summary) to rediscover the affected server and add it to Fabric Manager.

Fixed Problems

[Table 3](#) shows the fixes that are in version 3.0.6-Windows. This release also contains fixes from previous versions of Xsigo host drivers for Windows. The version in which the fix first appeared is noted in text.

Table 3 Fixed Problems in Version 3.0.6-Windows

Number	Description
21455	The usage of the vNIC or HA vNIC MTU has been changed. Now, there are two MTUs that can be used—either the MTU set for the vNIC (or HA vNIC) device on the Windows host, or the MTU set through the XgOS. How the MTU is determined is different than in previous versions. For more information, see MTU Usage on Host-Side vNIC Devices Has Been Enhanced on page 2.
21361	For Windows hosts running Pillar Axiom Path Manager software (APM) that were connected to Pillar storage, the path management software was not correctly performing path failover and failback if Xsigo host drivers were installed. This problem was observed when either the Fabric Director or Fibre Channel I/O modules were reset. This problem is fixed in version 3.0.6 host drivers for Windows.
19949	If you used the <code>xg_fwupdate.vbs</code> script to query for HCA information, a problem sometimes caused queue pairs on the HCA to flap for an indefinite amount of time, which led to service interruption on the server where the script was run. This problem is fixed in version 3.0.6 host drivers by no longer attempting to execute the script. Instead, if the script is attempted, the version information for the VBS shell script utility is displayed. Be aware that the <code>xg_fwupdate.vbs</code> script is no longer supported starting in version 3.0.6 as documented in The <code>xg_fwupdate.vbs</code> Script Is Still Documented on page 17.
17630	Windows 2008 Server R2 hosts running Citrix PVS Xen client experienced a problem that sometimes caused a blue screen crash (BSOD) in the InfiniBand bus driver. This problem is fixed in version 3.0.6 of Xsigo host drivers for Windows.
19895	A problem occurred that caused individual blades within a blade server to use the UUID of the blade server enclosure instead of the UUID of the individual blades themselves. As a result, the multiple blades shared the same UUID. In this situation, the blades were not seen as individual entities, and were not individually accessible. This problem is fixed in 3.0.0-Windows host drivers by providing a work around for affected blades. For information, see Procedure to Set Correct UUIDs on Blades in Blade Servers on page 8.
19421	A problem in the Windows vNIC driver caused the vNIC link speed to be reported as 0 even when the vNIC was up and configured for a valid, non-zero link speed. This problem is fixed in 3.0.0-Windows host drivers.
19288	The XsigoMonitor utility was not reporting information to the xsgo-support tool. This problem is fixed in 3.0.0-Windows host drivers.
14008	When a direct-attached vHBAs was created on a Windows server through Windows Create Disk Wizard, then vHBA was attached to NetApp SnapDrive, only one vHBA was usable per server. This restriction occurred because Xsigo exposed the port WWPN to the OS, and Xsigo could register more than one unique WWN per host. This problem is fixed in 3.0.0-Windows.
13760	The state of HA vNICs was not correctly displayed after the administrative or operational state was changed on the host. As a result, the vNIC state displayed on the host side was sometimes different than the vNIC state displayed on the Fabric Director. This problem is fixed in 3.0.0-Windows host drivers.

Table 3 (continued) Fixed Problems in Version 3.0.6-Windows

Number	Description
12546	In a multi-chassis configuration, if you issued the system clear config command on an Fabric Director that was the XDS standby, a problem caused XDS table entries on the XDS master to become stale. When the XDS standby came back online, any attached Windows Server 2003 hosts queried the XDS master and the stale entries prevented Server Profiles for Windows 2003 hosts from coming back online. This problem is fixed in 3.0.0-Windows.
10125	On a Windows Server 2003 R2 SP2 or Windows Server 2008 SP2 host, the default gateway was not completely deleted when the Server Profile is removed. This problem is fixed in 3.0.0-Windows.
9381	When showing the interface speed of a vNIC through a Windows host (for example, <i>Start->Control Panel ->Network Connections->Properties</i>), the vNIC properties displayed the speed as 1 Gbps even when the interface was 10 Gbps. This problem is fixed in 3.0.0-Windows host drivers.

Technical Support Contact Information

Xsigo Systems is a wholly owned subsidiary of Oracle. Xsigo Customer Support is willing to help solve any reported issues 24 hours a day, 7 days a week, 365 days a year. The Xsigo Technical Assistance Center (TAC) is open 9:00 a.m. to 6:00 p.m. PST Monday through Friday. If you need assistance, you can contact the Xsigo Technical Assistance Center (TAC) in any of the following ways:

- Email

You can send an email to Xsigo at support@xsigo.com and we will respond within 24 hours (Monday through Friday).

- Web Access

You can create a Service Request through the Support Web interface (<http://support.xsigo.com/>) and we will respond within 24 hours (Monday through Friday). If you do not have a login we will provide you with access to create, view, update and close Service Requests. You can also open RMA cases via the Web.

- Phone Contact

If you require a faster response for any reason, Xsigo provides response to all phone calls in a maximum of 30 minutes (24 hours a day, 7 days a week, 365 days a year).

- You can reach us through the Xsigo switchboard by dialing +1 408-329-5600 and selecting option “2”
- You can reach us through a direct line, by dialing +1 408-736-3013 (24 hours a day, 7 days a week)
- For our US customers, you can call us through our toll-free number, by dialing 866-974-4647

Gathering Information for Xsigo Technical Support — Windows

If Oracle’s Xsigo Fabric Director is supporting Windows hosts and problems are encountered, please gather the information in the following sections before contacting Xsigo Technical Support or filing a case through the support website.

On the Xsigo Fabric Director

- Type and number of servers connected (brand, model, number of CPUs, size and type of memory)
- Output from the `get-log-files -all` command (for the Xsigo Fabric Director), which will gather the `show tech-support` information plus all log files, and place this information into `xsigo-logs-<chassis-name>-tar.gz`

In addition to this general information, follow the procedures in the following sections. This information will be required by Xsigo Technical Support.

On the Windows Server

Collecting information from the Windows host is supported through one or two visual basic scripts. The type of problem you encounter determines whether you will run one or both scripts:

- For reproducible problems, you will run both the Xsigo Trace script (`XsigoTrace.vbs`) and the XsigoSupport script (`Xsigosupport.vbs`). To run both scripts, see [Running the Xsigo Trace Script](#).
- For non-reproducible problems, you will run only the Xsigo Support script. To run the Xsigo Support script (`Xsigosupport.vbs`), see [Running the Xsigo Support Script](#).

Gathering Windows host server information consists of:

- running the appropriate scripts
- configuring the Windows host server to generate complete kernel dump information for “blue-screen” events



The following sections document how to gather troubleshooting information on a Windows Server 2003 host. For Windows 2008, the procedure and information gathered is similar, but the dialogs and screen output will be different. For gathering troubleshooting information (for example, kernel memory dumps) on a Windows Server 2008 host, consult the help system topics on the Windows 2008 host.

Running the Xsigo Trace Script

For reproducible issues on a Windows host, you will run `XsigoTrace.vbs` to collect Xsigo trace information before running `XsigoSupport.vbs`.

- Step 1 Start a Windows command prompt by selecting *Type Start->Run->cmd*
- Step 2 From the command prompt, change to the Support directory, by entering the following command:
`cd %programFiles%\Xsigo Systems\Support`
- Step 3 Start trace collection on all Xsigo drivers running on the Windows host by using either of the following options:
 - If a blue-screen occurred on the server, run `cscrip Xsigosupport.vbs -d`
 - If no blue-screen occurred on the server, run `cscrip XsigoTrace.vbs`

The output of both options contains similar information, but `cscrip XsigoSupport.vbs -d` has more detailed output. The following is a partial capture of the output

```
C:\Program Files\Xsigo Systems\Support>cscrip XsigoSupport.vbs -d Microsoft (R)
Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Create Xsigo Support directory: XsigoSupport_IBM-1-5-12-2011_11-16-2

Start collecting Network, IB and All XgInstDev Devices information (may take
several minutes)...

route print
=====
Interface List
 29...00 13 97 09 80 09 .....Xsigo VNIC FailOver Heartbeat.IBM-1 MAC:[00:13:97:
09:80:09]
 28...00 13 97 09 80 07 .....Xsigo VNIC FailOver Labnet.IBM-1 MAC:[00:13:97:09:
80:07]
 27...00 13 97 09 80 0d .....Xsigo VNIC FailOver Domain.IBM-1 MAC:[00:13:97:09:
80:0d]
 26...00 13 97 09 80 0b .....Xsigo VNIC FailOver Traffic.IBM-1 MAC:[00:13:97:09:
80:0b]
 17...02 13 97 09 80 09 .....Microsoft Failover Cluster Virtual Adapter
 11...00 1a 64 33 c7 6a .....Broadcom BCM5708S NetXtreme II GigE (NDIS VBD Client)
#2
 10...00 1a 64 33 c7 6c .....Broadcom BCM5708S NetXtreme II GigE (NDIS VBD Client)
 1.....Software Loopback Interface 1
 20...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 21...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 12...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 14...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
 15...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
```

```

22...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #7
=====
<...>

```



Note

The **cscrip XsigoTrace.vbs** command toggles the script on and off. The first time you issue the command, the script starts. After you reproduce the issue, you will need to issue the command a second time to halt the script.

- Step 4** When the script is running, reproduce the issue affecting the Windows host server.
- Step 5** After reproducing the issue, return to the command prompt change directory back to Support by issuing the following command:

```
cd %programFiles%\Xsigo Systems\Support
```

- Step 6** Stop trace collection on all Xsigo drivers running on the Windows host by entering the following command again:

cscrip XsigoTrace.vbs

When you enter this command the second time, the script halts and the following output is displayed:

```

C:\Program Files\Xsigo Systems\Support>cscrip XsigoSupport.vbs
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Create Xsigo Support directory: XsigoSupport_IBM-1-5-12-2011_11-16-2

Start collecting Network, IB and All XgInstDev Devices information (may take
several minutes)...

route print
=====
Interface List
29...00 13 97 09 80 09 .....Xsigo VNIC FailOver Heartbeat.IBM-1 MAC:[00:13:97:
09:80:09]
28...00 13 97 09 80 07 .....Xsigo VNIC FailOver Labnet.IBM-1 MAC:[00:13:97:09:
80:07]
27...00 13 97 09 80 0d .....Xsigo VNIC FailOver Domain.IBM-1 MAC:[00:13:97:09:
80:0d]
26...00 13 97 09 80 0b .....Xsigo VNIC FailOver Traffic.IBM-1 MAC:[00:13:97:09
:80:0b]
17...02 13 97 09 80 09 .....Microsoft Failover Cluster Virtual Adapter
11...00 1a 64 33 c7 6a .....Broadcom BCM5708S NetXtreme II GigE (NDIS VBD Client)
#2
10...00 1a 64 33 c7 6c .....Broadcom BCM5708S NetXtreme II GigE (NDIS VBD Client)
1.....Software Loopback Interface 1
20...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
21...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
15...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
22...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #7
=====
<...>

```

At this point, the issue affecting the Windows host server should be captured.

- Step 7** You must now run the Xsigo Support script. Proceed to [Running the Xsigo Support Script](#).

Running the Xsigo Support Script

The Xsigo Support script (`Xsigosupport.vbs`) captures and packs data into a .ZIP file in the `%programFiles%\Xsigo Systems\Support` directory, which is the same directory where you run the script. The .ZIP file name has the following format:

`XsigoSupport_mm_dd_year_hrs_min_sec.zip`

For example, `Xsigosupport_11_22_2007_13_30_30.zip` is the Xsigo Support file created on November 22, 2007 at 1:30 and 30 seconds in the afternoon. The script is time-stamped with 24-hour time. Each time you run the script a new .ZIP file will be created.



Caution

If your problem is reproducible, you must run the Xsigo Trace script before running the Xsigo Support script.

Xsigo recommends that you run `Xsigosupport.vbs` in kernel dump mode by using the `-d` argument. This mode will capture kernel dump information if any blue-screen crash has occurred on the Windows host server, even if the current problem did not result in a blue-screen crash. For more information about kernel dump mode, see [Configure the Windows Host Server to Collect a Complete Kernel Memory Dump](#).

To run `Xsigosupport.vbs`, follow this procedure:

- Step 1 Start a Windows command prompt by selecting *Type Start->Run->cmd*
- Step 2 From the command prompt, change to the Support directory, by entering the following command:
- Step 3 Start the Xsigo Support script in kernel dump mode, by entering the following command:

```
cd %programFiles%\Xsigo Systems\Support
```

```
cscript Xsigosupport.vbs -d
```

When you enter this command, the script starts collecting the required information and packing it into the .ZIP file. While the script is running, the following output is displayed:

```
C:\Program Files\Xsigo Systems\Support>cscript XsigoSupport.vbs -d Microsoft (R)
Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Create Xsigo Support directory: XsigoSupport_IBM-1-5-12-2011_11-16-2
```

```
Start collecting Network, IB and All XgInstDev Devices information (may take
several minutes)...
```

```
route print
=====
Interface List
 29...00 13 97 09 80 09 .....Xsigo VNIC FailOver Heartbeat.IBM-1 MAC:[00:13:97:
09:80:09]
 28...00 13 97 09 80 07 .....Xsigo VNIC FailOver Labnet.IBM-1 MAC:[00:13:97:09:
80:07]
 27...00 13 97 09 80 0d .....Xsigo VNIC FailOver Domain.IBM-1 MAC:[00:13:97:09:
80:0d]
 26...00 13 97 09 80 0b .....Xsigo VNIC FailOver Traffic.IBM-1 MAC:[00:13:97:09:
80:0b]
 17...02 13 97 09 80 09 .....Microsoft Failover Cluster Virtual Adapter
 11...00 1a 64 33 c7 6a .....Broadcom BCM5708S NetXtreme II Gige (NDIS VBD Client)
#2
```

```

10...00 1a 64 33 c7 6c .....Broadcom BCM5708S NetXtreme II GigE (NDIS VBD Client)
1.....Software Loopback Interface 1
20...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
21...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
15...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
22...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
18...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #7
=====
<...>

```



Note

Unlike the Xsigo Trace script, you do not need to explicitly turn the Xsigo Support script on, then off. Issue the **cscript XsigoSupport.vbs -d** command once. When the script completes, it shuts off and the .ZIP file is created.

Step 4 Copy all .ZIP files present in the %programFiles%\Xsigo Systems\Support directory, and send them to Xsigo Customer Support.



Note

The .ZIP file can be large (for example, greater than 1 GB) because it might contain system kernel memory dump information if the Windows host server has experienced a blue-screen crash.

Step 5 Proceed to the next section.

Configure the Windows Host Server to Collect a Complete Kernel Memory Dump

Kernel memory dump information can be gathered from the Windows host in addition to running the Xsigo Support script in kernel dump mode. Kernel memory dump information occurs if the Windows host server encounters a blue-screen crash. For more information about the Windows blue-screen crash, see the following links to Microsoft's web site:

- To manually generate a Windows crash dump on a running server (which can be useful in deadlock situations), see:
 - <http://support.microsoft.com/?id=244139>
 - http://www.microsoft.com/technet/scriptcenter/guide/sas_cpm_klll.mspx?mfr=true
- For details about different types of memory dump, see: <http://support.microsoft.com/kb/254649/>

The procedure in this section configures the Windows host to gather a proper kernel memory dump the next time that a blue-screen crash occurs.

To configure the Windows server to gather complete kernel memory dump information, follow this procedure:

Step 1 Follow this menu path:

Start->Settings->Control Panel->System

The System Properties dialog is displayed.

Step 2 Click the *Advanced* tab. See [Figure 19](#).



Figure 19 System Properties Dialog

- Step 3 In the Startup and Recovery section, click the *Settings* button. The Startup and Recovery dialog is displayed.
- Step 4 In the System Failure section, click the following check boxes:
- Send an Administrative Alert
 - Automatically Restart

See [Figure 20](#).



Figure 20 System Failure Checkboxes

- Step 5 From the *Write Debugging Information* dropdown menu, select Kernel Memory Dump.
- Step 6 Click the *Overwrite any existing file* check box. See [Figure 21](#) on page 33.



Figure 21 Write Debugging Information Options

-
- Step 7** Click *Apply* to configure the server for gathering kernel dump information the next time it crashes with a Windows blue-screen error. The configuration is complete at this point. Do the next two steps if the server crashes.
- Step 8** If a Windows blue-screen crash occurs, after the server reboots, run Explorer and copy the kernel dump file from the directory `%systemRoot%\memory.dmp` to your temp directory.
- Step 9** Send the kernel dump file to Xsigo Technical Support.