Tiger
Technology

Tiger ST⬤RE

Tiger Store 2.9 Release Notes

This document provides release information for Tiger Store version 2.9. It discusses new features in this release as well as best practices, fixed and known issues.

What's New

Complete Tiger Bridge Integration

Version 2.9 provides complete integration of Tiger Bridge. While you can still perform manual data lifecycle operations in the Tiger Store Volume Browser, configuring automatic data replication and archiving, as well as space reclaiming is no longer performed through the Replication & Tiering menu of the Tiger Store interface, but directly through the Tiger Bridge interface. On a Tiger Store appliance, you can access the graphic user interface of Tiger Bridge by establishing remote connection to your storage server through Tiger Bridge Configuration application, which is available for download in the Tiger Store 2.9 bundle.

For more information, refer to the Tiger Store 2.9 Administration Guide.

Support for Windows Server 2019

You can install version 2.9 of Tiger Store or Tiger Client on a computer running Windows Server 2019.

Support for macOS Mojave on Tiger Clients

You can install Tiger Client 2.9 on a computer running macOS Mojave (10.14).

See also "Displaying Volumes Part of a Pool in the Finder of macOS Mojave" on page 17.

New Kernels Supported on Red Hat Enterprise Linux/ CentOS Linux 7.x

You can now install the Tiger Client driver on a computer running any of the following Red Hat Enterprise Linux/CentOS Linux 7.x kernels:

- 3.10.0-693.el7.x86_64

- 3.10.0-693.11.6.el7.x86_64

- 3.10.0-862.3.2.el7.x86_64

- 3.10.0-862.9.1.el7.x86_64

New Kernels Supported on Red Hat Enterprise Linux/ CentOS Linux 6.x

You can now install the Tiger Client driver on a computer running any of the following Red Hat Enterprise Linux/CentOS Linux 6.x kernels:

- 2.6.32-642.3.1.el6 (64-bit)

- (CentOS Linux 6.x only) 2.6.32-642.3.1.el6.centos.plus (64-bit)

- 2.6.32-642.15.1.el6 (64-bit)

Support for NTFS Cluster Size above 64KB

Tiger Store 2.9 introduces support for NTFS volumes with cluster size above 64KB as long as the operating system of the storage server and the Tiger Client allows creating and mounting such volumes. Currently, this option is available in Microsoft Windows 10/Server 2016 (version 1709) and later.

This change allows you to manage through Tiger Store NTFS volumes with size up to 2 PB.

Importing RAID on Appliances Exporting Their Own Storage

On hardware model 3 of Tiger Store appliances exporting their own storage, Tiger Store allows you to import the RAID if for some reason the chassis RAID controller reports its disks as Foreign. For more information about importing the RAID, refer to the Tiger Store 2.9 Administration Guide.

View Private Volume Information

In the Volumes page of Tiger Store 2.9 you can view details about volumes set to Private such as volume capacity, used and free space.

Removed Support for Mac OS X Lion

You will not be able to upgrade a Tiger Client computer running Mac OS X Lion to version 2.9.

Removed Support for Red Hat Enterprise Linux/CentOS Linux 5 and SUSE Linux 10

You will not be able to upgrade a Tiger Client computer running Red Hat Enterprise Linux/CentOS Linux 5 or SUSE Linux 10 to version 2.9.

Fixed Known Issues in Version 2.9

Improved Support for Red Hat Enterprise Linux/CentOS Linux 7

Version 2.9 provides many stability fixes Red Hat Enterprise Linux/CentOS Linux 7 as well as improved data cache handling on write operations.

Improved Support for Volume Pooling on Mac Tiger Clients

Version 2.9 provides the following improvements on Mac Tiger Clients when smart storage pooling is enabled:

• improved performance of file operations on a volume pool.

• preventing the access to the individual volumes in the pool (see also "Displaying Volumes Part of a Pool in the Finder of macOS Mojave" on page 17).

• the pool is accessible in the Finder after restarting or logging on/off the Tiger Client computer.

Support for Hard Links on Linux Tiger Clients

Version 2.9 provides improved support for hard links created from a Linux Tiger Client on the shared storage volumes. Now, hard link are reported properly even after remounting the shared storage volumes.

No E-mail Notification when the ATTO RAID Controller Performs Media Scan

With version 2.9 on appliances exporting their own storage, Tiger Store no longer sends a false e-mail notification about problems, when the ATTO RAID controller scans the disk drives for media errors and parity errors.

Unlocking Files on the Shared Volumes in the Finder

Version 2.9 resolves a problem, which could prevent you from unlocking a file stored on a shared storage volume in the Finder.

Restarting Add-on Services

With version 2.9 the add-on services running on your Tiger Store appliance are properly restarted through the web interface.

Disconnecting Mac Tiger Clients When Volumes Are Hidden through Tiger Spaces

Version 2.9 resolves a problem, which could prevent a Mac Tiger Client from disconnecting from the storage server through the web interface, when shared volumes are hidden through Tiger Spaces.

Exporting a SMB Share When Volume Pooling Is Enabled

With version 2.9 network clients can normally access and work with SMB network shares exported from a volume pool.

Upgrade to Version 2.9

Important: *All computers on your Tiger Store network must run the same version of the software.*

To upgrade your Tiger Store storage server to version 2.9 from version 2.8 or above:

• (software-only installation) Without uninstalling version 2.8 or above, run the installation for version 2.9 and follow the on-screen instructions.

• (appliances) Contact Tiger Technology support for instructions about uploading version 2.9 as a firmware update.

Upgrade from Version 2.7.3 or Below

To upgrade your storage server to version 2.9 from version 2.7.3 or below, you need to:

• uninstall the previous version of the product from the storage server.

• perform a clean installation of version 2.9 on the storage server.

• deactivate Tiger Store on the storage server and then activate it anew.

On storage servers running the software-only version of the product, follow the steps provided below. On Tiger Store appliances, contact Tiger Technology support for assistance on upgrading to version 2.9.

To upgrade your Tiger Store storage server to version 2.9 from version 2.7.3 or below:

1. On the storage server computer display the Control Panel.

2. Double-click Programs and Features.

3. Right-click Tiger Store and select Uninstall.

4. Confirm that you want to uninstall Tiger Store.

5. When the Deactivation Wizard appears, select "Yes, return the license to server," click Next and then choose the desired deactivation method, following the steps described in the Tiger Store Administration Guide.

6. When prompted, restart the computer.

7. When the storage server computer starts, log on to it using an account with administrative privileges.

8. In a web browser go to:
https://license.tiger-technology.com

9. In the home page of the licensing server, enter your order name and password in the corresponding fields, and click Log in.

10. In the Licensing Server menu, click Current Version and download the Tiger Store server installation and the Tiger Client bundle installations for version 2.9.

11. Double-click the Tiger Store installation file.

12. When the installation starts, click Next.

13. If the wizard suggests the installation of additional prerequisites, accept and click Next.

14. Select where to install the product, accept the terms of the software license agreement and click Install.

15. When the installation finishes, click Finish and select not to restart the computer, when prompted.

16. Double-click the Tiger Client bundle installation file.

17. When the installation starts, click Next.

18. Select where to install the clients bundle, accept the terms of the software license agreement and click Install.

19. When the installation finishes, restart the computer.

20. When the storage server computer starts, access the Tiger Store web interface.

21. .In the web interface, click System and then About.

22. Click Manual Activation.

23. In the License Activation dialog, copy the serial number and in a web browser go to:
https://license.tiger-technology.com

24. In the home page of the licensing server, enter your order name and password in the corresponding fields, and click Log in.

25. In the Licensing Server menu, click Activate License.

26. In Activate License, paste the serial number for your copy of Tiger Store and click Generate Activation Key.

27. In the License Activation dialog, paste the keys generated for your copy of Tiger Store, and click OK.

Upgrade Tiger Clients to Version 2.9

Aside from upgrading your storage server, you must also upgrade all Tiger Client computers to version 2.9. On Apple Mac and Linux, to upgrade the client driver to version 2.9 you must first uninstall the previous version of the Tiger Client software and then install the new version. On Windows Tiger Clients, you can upgrade the client driver to version 2.9 without uninstalling the previous version.

To upgrade Windows Tiger Client to version 2.9:

1. Access the web interface of the storage server.

2. Find the Tiger Client installation for your operating system and click Download.

3. Once the installation downloads to your computer, run it, following the installation steps described in the Tiger Store Administration Guide.

To upgrade Apple Mac Tiger Client to version 2.9:

1. Go to Applications | Tiger Client.

2. Double-click Uninstall.

3. Provide administrator's user name and password.

4. When prompted, confirm that you want to uninstall the Tiger Client software.

5. When the computer starts, open the web interface of the storage server.

6. Find the Tiger Client installation file for your operating system and click Download.

7. When the installation file downloads to your computer, double-click it to start the installation.

8. Follow the on-screen instructions and when prompted, restart your computer.

To upgrade a Linux Tiger Client to version 2.9:

1. Log on to the Linux system as root.

2. In command-line, execute the following:
```
rpm −e Tiger−Client
```

3. In the web interface of the Tiger Store, find the Tiger Client installation file for your operating system and click Download.

4. When the installation file downloads to your computer, log on to the Linux system as root.

5. In command-line, execute:
```
rpm –i <path to the Tiger Client software .rpm file>
```

6. In command-line, execute the following as root:
```
/etc/init.d/tboxd start
```

Best Practices

Avid File System Emulation and Avid Versions Without Bin Locking

Tiger Store's Avid file system emulation allows you to mount one and the same Avid project with Read & Write permissions on multiple Tiger Client computers simultaneously, letting Avid restrict accesses to the bins that are currently in use.

Still, when you use an Avid version, which does not provide bin locking (like Avid Media Composer | First, for example) even though Avid file system emulation may be enabled on the volumes, Tiger Store cannot prevent users on different computers from accessing the same bin and from overwriting each other's changes.

Change the TCP Port for Access to the Web Interface

By default, TCP port 80 is designated for access to the web interface of Tiger Store. If this port is already in use by another service or you simply want to access the Tiger Store's web interface through another port, you can assign a different port for the purpose. To do this, you should create a new string value in the Tiger Store registry on the storage server. On a storage server running the software-only installation of Tiger Store, follow the steps below. On Tiger Store appliances, contact Tiger Technology support for assistance.

Once you assign a different TCP port for access to the web interface of Tiger Store, each time you want to access it in your web browser, aside from providing the IP address/domain name of the storage server, you must also provide the number of the new TCP port as well. For example, if your storage server uses IP address 10.200.6.33 and you have assigned TCP port 8380 to be used instead of the default port 80, to access the web interface of Tiger Store you must enter the following in the address bar of the web browser:
```
10.200.6.33:8380
```

Important: *Even if you assign a new TCP port for access to the web interface of Tiger Technology, accessing the web interface from Tiger Client computers using the tray*

application (Windows) or the menulet (Mac OS X) will always redirect the request through TCP port 80.

To assign new TCP port for access to Tiger Store's web interface:

1. On the storage server, start the Registry Editor.

> **Tip:** *To start Registry Editor, on the Start menu click Run and in the dialog type regedit.*

2. Navigate to:
HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tbox\tboxmaster\settings\

3. Right-click in the right pane and select New | String Value.

4. Rename the new REG_SZ value to:
`webui_port`

5. Right-click the `webui_port` value and select Modify.

6. In Value Data enter the number of the TCP port to be used for access to Tiger Store's web interface and then click OK.

7. Restart the storage server.

8. Make sure the new TCP port is not blocked by the firewall on the storage server.

Installing Tiger Spaces after Tiger Store

In case you want to install Tiger Spaces on your storage server, to ensure the normal functionality of both products, you must first install Tiger Store software and only after that Tiger Spaces.

Configure a DNS Reverse Lookup Zone to use Active Directory in Heterogeneous Environment

When Tiger Store operates in cross-platform environment (with Linux and Mac Tiger Clients), to benefit from Active Directory support, DNS reverse lookup zone must be configured on the domain controller. Otherwise, the domain permissions will not be respected by the Unix based client systems.

For information about configuring DNS reverse lookup zone, refer to your Active Directory domain controller documentation.

Extending Volumes Managed by Tiger Store

Unlike most disk management operations that can be executed while in Maintenance mode, extending a volume is a rather complex task that functions on low level and may not be cleanly performed while the Tiger Store drivers are loaded, even if the storage server operates in Maintenance mode.

With this in mind, the recommended procedure for extending a SAN volume managed by Tiger Store is to first change the volume's status to Offline and then uninstall Tiger Store from the storage server. Once the storage server is rebooted and the volume can be mounted and accessed as a private NTFS volume, you can perform the extend operation.

Detaching Shared Volumes from Tiger Store for Use on Another Computer

To protect volumes from data corruption that could occur when multiple computers have access to them simultaneously, Tiger Store marks the volumes it manages. To be able to mount a volume without Tiger Store, this volume needs to be unmarked. Tiger Store automatically unmarks all volumes with Offline status. If you intend to physically disconnect a volume for use on another computer, you must first change the status of this volume to Offline. If you fail to set the volume to Offline, you need to contact Tiger Technology support for assistance on unmarking the volume.

Avoid Backing Up the Settings Configuration in Maintenance Mode

Tiger Store cannot ensure the consistency of the settings configuration backup, when you save it while in Maintenance mode. To avoid possible problems, it is advisable to always back up and restore the settings configuration when the appliance is not running in Maintenance mode.

Granting Full Control to the System Account

In Windows, the built-in System account, used by the operating system and by services, by default has Full Control to all files on an NTFS volume. To provide for the normal operation of Tiger Store, it is advisable not to change the Full Control permissions of this account.

For details about displaying the System account when setting permissions and granting Full Control to it, refer to your Windows documentation.

Assigning IP Addresses to Network Ports

IP Addresses Limitations

When assigning IP addresses to the network ports of Tiger Store, make sure that you avoid the following IP addresses as they are either link-local addresses or are in use by Tiger Store services:

- Link-local addresses in the range 169.254.0.0 - 169.254.255.255

- IPMI addresses in the range 1.1.1.0 - 1.1.1.255

IP Addresses on Tiger Store with High-Availability

It is sometimes possible a request from a LAN Tiger Client to be redirected through the 1GbE port instead of a faster connection (through a 10GbE port, for example). The problem can be observed with Tiger Store storage servers with high-availability and is reproducible when the node you have added to your storage servers list tries to redirect you to the other server node, which is currently playing the role of a primary node. To avoid the problem, it is highly advisable to set the IP addresses of the ports on the faster network connection between the storage server and the LAN Tiger Client to be on a separate LAN or on a subnet of the LAN used by the Public port.

For example, if the Public port uses IP address 172.16.1.1 (with subnet mask 255.255.255.0), set the IP address of the first 10GbE port to 172.16.2.1 (with subnet mask 255.255.255.0) and change the IP address of the Tiger Client 10GbE port to be on the same subnet. For the next 10GbE port of the storage server, set IP address 172.16.3.1 (with subnet mask 255.255.255.0) and respectively change the IP address of the 10GbE port of a Tiger Client to be on the same subnet.

Another important thing is to add Tiger Store to the storage servers list on each LAN Tiger Client using the IP address set for the faster network connection and not the Public port.

Synchronization of IP Settings Between High-Availability Nodes

To guarantee the failover between the two server nodes of a storage server with high-availability, the network ports with identical names on both nodes (the Public ports, for example) must use consecutive IP addresses and identical settings for subnet, router and DNS server. In case you cannot meet these requirements, the failover between server nodes cannot take place. When you configure the IP settings of one node, as long as the other node is also online, Tiger Store attempts to automatically synchronize the IP settings and assigns the same settings for subnet, router and DNS server and a consecutive IP address of the port with the same name on the other server node. If the consecutive IP address on the network is already taken, Tiger Store will assign a random IP address to the identical port of the other server node and failover between the two nodes will not be possible.

When one of the nodes is offline while you change the IP configuration settings of the other node, you must synchronize the IP settings of the two nodes manually, in order not to obstruct failover between server nodes. You can do this in the Node view of the respective server node.

Using a DHCP Server on Your Tiger Store Network

A Dynamic Host Configuration Protocol (DHCP) server automatically assigns and leases IP addresses to computers as they are added to a network. While you can allow run-time configuring of IP addresses of both the Tiger Store server and the Tiger Clients, to ensure the proper cross-network communication, there should be a DNS server on the network that resolves the IP address of each connected computer to its domain name. Additionally, each Tiger Client should add the Tiger Store server to its storage servers' list using its domain name instead of the IP address with which it is currently identified.

In case there isn't a DNS server on the network, you should configure your DHCP server to use static allocation of IP addresses to the Tiger Store server and Tiger Clients.

Note: *Non Tiger Client computers can still benefit from dynamic allocation of IP addresses by the DHCP server.*

Migrating Replicated Data

Migrating Replicated Data from One Replication Target to Another

While the Replication & Tiering mechanism of Tiger Bridge doesn't restrict you about changing the replication target, to avoid problems, you should set a new replication target with caution and after careful planning. If you need to set a new replication target to which files to be copied, you should keep in mind that all already replicated files will be inaccessible from the new replication target. Additionally, offline files (replicated files that have a copy only on the replication target) cannot be retrieved unless they have a counterpart on the new replication target.

When changing the replication target of your shared storage, it is recommended to migrate all already replicated data from the previous replication target to the new one. The safest workflow to do this is to let the Replication & Tiering mechanism replicate it again on the new replication target. For the purpose, you have to make sure that:

• all already replicated files are available on the shared storage (note that lack of free space on your shared storage may hamper the process).

• the status of all already replicated files is not "replicated" but "normal" as the Replication and Tiering mechanism will skip files on the shared storage that are with "replicated" status and will not copy them to the new replication target.

You can achieve this following these steps:

1. To ensure that each replicated file has an offline counterpart on the shared volume(s), in the drop-down box of the Volume Browser, select a volume with enabled replication and then click Rescan Volume.

2. Repeat the above step for each volume on which replication is enabled.

3. In the left pane of the Volume Browser, select the root of the volume and in the right pane select a folder and click Restore.

   Note: *You have to manually select all offline files in the root of the volume and click Restore.*

4. Repeat the above step for each folder on each volume with enabled replication in order to restore all replicated files to their original locations.

5. In the Replication & Tiering page of the web UI, specify a new replication target.

6. In the Replication Options dialog, select "Do not replicate" and leave the Exceptions list empty.

7. In the left pane of the Volume Browser, select the root of the volume and in the right pane select a folder and click Make Offline, to revert all files from "Replicated" status to "Normal" status.

Note: *You have to manually select all restored file in the root of the volume and click Make Offline to revert their status to "Normal".*

Important: *Clicking Make Offline transfers the status of replicated files to "normal" only if the Replication & Tiering mechanism detects that the selected files don't have copies on the replication target. If you issue the command for a file with "replicated" status, which actually has a copy on the replication target, the command will replace the file on the shared storage with a stub file pointing to its copy on the replication target.*

8. Repeat the above step for each folder on each volume with enabled replication.

9. Set replication policy parameters for the new replication target to let the Replication & Tiering mechanism to copy all files.

Migrating Replicated Data to a New Volume

When you need to reformat a volume from which data has been replicated or to replace it with a volume with bigger capacity, instead of manually moving data between volumes in order to restore data on the new volume, you can use the Replication & Tiering mechanism to automate the process. Following the steps below, you will be able to restore all already replicated data from the replication target to the new volume. Data will be restored in the form of stub files, which you can make online in the Volume Browser or on demand (by accessing them) in your file browser.

To ensure that all needed data is copied to the replication target, you may have to manually replicate files or whole folders in the Volume Browser of your appliance:

1. In the web interface of your appliance, go to System | Replication & Tiering and click Browse.

2. In the Volume drop-down box, select the old volume.

Note: *If you are migrating Tiger Spaces data, in the Volume Browser select the "Workspaces" check box to display all project folders.*

3. In the right pane, select a file or folder with Normal status and click Replicate.

Note: *In the Volume Browser a folder is with Normal status if it contains even just one file, which is not yet replicated.*

When all files/folders you want to migrate to the new volume are with replicated status in the Volume Browser, you are ready to proceed with the migration steps below.

Important: *If you're using a Private volume as replication target, before you reformat or detach the volume from which data has been replicated, you must get its GUID as well as the GUID of the volume, on which you will restore data. For the purpose you can*

access the web interface of your storage server through port 9125, typing the following in the address bar of a web browser:

```
[IP address of the storage server]:9125/volumes
```

The storage server lists information about each shared volume. Search the list for the label of the respective volume and copy its GUID from the "guid" field of the list.

To restore replicated data on a new volume:

1. If you are migrating Tiger Spaces data, enable support for Tiger Spaces on the new volume.

2. In the Replication & Tiering page, enable replication on the new volume, by setting exactly the same replication target as for the old volume (the same WOS policy, private volume, folder on the SMB/CIFS share, bucket on target, etc.).

3. (for replication on a Private volume only) Disable replication (select "No Replication") and share the private volume, then in your file browser go to the .tt_rt folder in the root of the volume and rename the folder with the GUID of the old volume with the GUID of the new volume, then enable replication again using the same settings as in the step above.

4. In the Replication & Tiering page, click Browse to open the Volume Browser.

5. In the Volume drop-down box, select the new volume and then click Rescan Volume.

The Replication & Tiering module creates a stub file for each replicated file on the replication target, which it cannot find on the volume i.e. all files that have been replicated from the old volume.

6. (for migrated Tiger Spaces data only) Convert all restored files from offline to replicated: in the Volume Browser, select the new volume in the drop-down box and select the "Workspaces" check box, then one by one select each workspace and click Restore.

7. (Tiger Spaces only) Log on to Tiger Spaces, log on as administrator and rescan each workspace, to regenerate its information such as size, users, application type, number of files, etc. as well as to queue proxy media generation.

Restarting A Server Node While in Maintenance Mode

When you enter Maintenance mode, Tiger Clients are automatically disconnected from both server nodes of your Tiger Store appliance, until you exit Maintenance mode in the web UI or restart the appliance. It is advisable not to restart just one server node (in node view) as it will exit Maintenance mode and will attempt to supervise the volumes managed by Tiger Store, while the other node is in Maintenance mode and performs a maintenance operation.

Setting Up the SAN Policy on Windows Tiger Clients

By default, on Tiger Client computers running Windows operating system all shared disks visible to the computer are delivered as offline and read-only. You can bring these disks to online mode in

Disk Management, still, there's a possibility on the next boot of the system the disks to be offline again. To change this behaviour, you should make sure that the SAN policy of the operating system is set to "Online All". To view and set the SAN policy of your computer you can use diskpart.exe command-line utility that is stored in the system drive of your computer.

To view and change the SAN policy of your computer:

1. Run command prompt as administrator.

2. In command prompt, start diskpart utility by typing:
   diskpart

3. To view the current SAN policy, type this followed by return:
   SAN

   The utility displays one of the following:

   • Offline Shared - all newly discovered disks that do not reside on a shared bus are brought online and made read-write.

   • Offline - all newly discovered disks remain offline and read-only.

   • Online All - all newly discovered disks are brought online and made read-write.

4. Do one of the following:

   • If the SAN policy of your computer is "Online All", exit diskpart utility and command prompt.

   • If the SAN policy of your computer is not "Online All", proceed with the steps below.

5. Run command prompt as administrator.

6. In command prompt, start diskpart utility by typing:
   diskpart

7. Execute the following:
   san policy=OnlineAll

Using Identical Time and Date Settings

It is advisable to use identical settings for time and date on all computers on your Tiger Store network (the storage server and all client computers). Using different time and date settings may hamper communication with the storage server and the Traffic and Events reports may display incorrect information.

Disabling Mac OS X Time Machine for Shared Volumes

It is highly advisable to exclude all volumes shared by Tiger Store from the list of locations Time Machine is set to back up on your Mac OS X. Keeping this feature turned on for shared volumes may hamper performance.

To exclude a shared volume from Time Machine's backup:

1. In Time Machine preferences, click the Options button.

2. In the sheet with locations, select a shared Tiger Store volume and click the "-" button.

3. Repeat the above step for each shared Tiger Store volume.

4. Click Save.

Calculating Folder Size (Mac OS X)

Use the Calculate Sizes option, available in List view of the Finder, to calculate sizes per folder and per window. Activate this option only for folders on your local disks. Do not enable it for folders on the shared storage volumes, as this will temporarily slow down performance. If you enable this option on a shared volume, network computers that see the volume will be unable to work on it.

For details about managing the "Calculate Sizes" option, refer to your Mac OS X® documentation.

File Systems Behaviour and Files Compatibility

The three operating systems (Windows, Mac OS X and Linux) on which you can install the Tiger Client software differ in the way they manage files. On Windows, files can have many streams, in contrast to Mac OS X (only 2 streams - data fork and resource fork), and Linux (only data stream). In addition, files created by Mac OS X also have extended attributes (such as the Finder Info, for example) that are not available on the other two platforms.

These peculiarities of the file systems lead to partial loss of information when transferring a file created on one platform through a machine running on another platform.

For instance, when on Mac OS X you copy a file with 50 streams created by Windows, all file streams' information is lost, except the information of the data stream. The result will be the same when a Linux computer copies a 50-stream Windows file. A Mac OS X file copied by Linux will also lose its resource fork's info.

Streams' information is not lost when copying Mac OS X or Linux files by a Windows computer, but in this case a Mac OS X file will lose the extended attributes information.

There is another problem with files sharing common file format. For example, a movie file created with Final Cut Pro on Mac OS X is playable by QuickTime. If a Windows workstation copies this file, it will not recognize it as QuickTime-playable until adding the *.mov extension to it.

See also "Final Cut Pro X Project Names on the Shared Volumes" on page 17.

Avoiding Long File Names

By default, on Windows the length of file names is limited to 260 characters and on Mac OS X - to 1024 characters. On both Windows and Mac OS X, the full path to the file is also included in the

character count. That is why it is possible to receive errors when attempting to create or copy a file with long file name. For this reason it is advisable to avoid long file names in order to ensure that file operations on the shared storage are normally processed.

Final Cut Pro X Project Names on the Shared Volumes

It is advisable that the Final Cut Pro X projects you create on the shared volumes have names that do not exceed 31 symbols.

Using Antivirus on the SAN

It is advisable to use an antivirus software (like ESET NOD32, for example) on your shared storage only when needed or if inevitable for your workflow. Additionally, to avoid decreased performance, it is advisable to run the checks only from the storage server computer.

New Known Issues

Automatic Defragmentation Disabled on Storage Servers Running Windows Update 1809

Due to possible problems when automatic volume defragmentation is performed from a storage server running Windows update 1809, this option is disabled. On all storage servers running other than Windows update 1809, you can enable/disable Tiger Store's automatic volume defragmentation.

Displaying Volumes Part of a Pool in the Finder of macOS Mojave

When smart storage pooling is enabled, the Finder on macOS Mojave Tiger Client may display not only the volume pool, but also the individual volumes. Still, users on the Tiger Client computer can access only the pool and attempting to access the contents of the individual volumes returns error.

Unresolved Known Issues

Disconnecting Tiger Clients from the Storage Server

When the "Restrict client actions" check box is enabled, Apple Mac and Linux clients may fail to manually disconnect from the storage server (through the menulet or the command-line interface, respectively) as the field for providing an administrator's password may not appear.

Prevent Replicated Data Loss After Upgrading to Tiger Bridge

Due to incompatibility between version 2.7.3 and earlier of Tiger Store's replication & tiering mechanism and Tiger Bridge, it is possible after upgrading to Tiger Bridge to lose data from the replication target. To avoid this problem, before upgrading to Tiger Bridge you must contact Tiger Technology support for assistance on converting the attributes of replicated and offline files, which will prevent data loss.

Activating the High-availability Add-on

After activating the high-availability add-on on your storage server, you need to restart the storage server to be able to view the HA Nodes page in the web interface.

Duplicated Files on Spectra Logic BlackPearl

When the Tiger Bridge add-on is set to replicate on a Spectra Logic BlackPearl appliance, it is possible duplication of files to occur on both the replication tier and the shared volume(s). As the BlackPearl appliance cannot tell that an already replicated file is moved to another directory on the shared volume, it perceives it as a new file to replicate and keeps both its copy in its previous location and the new one. Similarly, should you attempt to restore a replicated file that has been moved, the mechanism will restore two copies of the file - one in its original location and another in the location to which it has been moved.

File Moved to Another Volume in the Pool After Modifying It

If you use an application that creates a temporary file when modifying an existing file on the volume pool, after you save the file it might be moved to another volume in the pool (the one on which the distribution policy in the pool creates new files).

Connecting to a Newly Added Secondary Node from Tiger Clients

In case you have added a Tiger Store appliance to your storage servers list when only one of its nodes has been online, when the other server node is also online and an IP address is assigned to it, you may have to remove the appliance from the list and add it anew, in order to ensure that in case of failover you can connect to it.

Support for Hard Links Limitations

The support for hard links on volumes shared by a Tiger Store storage server is provided with the following exceptions:

- as on NTFS hard links to the same file have identical file IDs, the Finder may not show them properly. For example, if a file has two hard links in the same directory, when you browse this directory in the Finder only one of the hard links will be shown;

- you cannot use hard links on pooled volumes (smart storage pooling);

Support for Fast User Switching Known Issues

The Fast User Switching option allows switching between users on a single machine without quitting applications and logging out. It lets users leave their applications running and their files open when another user needs to log in.

While operations on the shared volumes are not interrupted when you switch users on a Tiger Client computer, the Tiger Client tray application/menulet may not be present when a new user logs on, thus preventing that user from controlling the available Tiger Client commands. A workaround to this problem is to force display the Tiger Client tray icon/menulet by restarting it.

Note: *As users on Linux computers use the command-line interface to manage the Tiger Client driver, you can use fast user switching without problems.*

To restart the Tiger Client tray application on a Windows computer:

1. Run the Task Manager as administrator.

2. In the Processes tab, right-click smct.exe and select End Process.

3. In the Run command (press Windows logo key+R to display it), execute this:
   `C:\Program Files\Tiger Technology\Tbox\smct.exe`

   Note: *Where C: is the drive, on which the Tiger Client driver is installed.*

To restart the Tiger Client menulet application on Mac OS X:

1. Start the Activity Monitor (go to Applications | Utilities | Activity Monitor).

2. In the Disk tab, in the Process name column select smct.

3. Click End Process in the Activity Monitor task bar.

4. Provide an administrator's user name and password.

5. On the drive, on which the operating system is installed, go to /Library/Application Support/ embedded/smct and double-click it.

Teaming Network Ports Known Issues

After enabling/disabling the setting for teaming of network ports, the web interface may display error, whereas the setting is actually applied. Additionally, on a Tiger Store appliance with 2 server nodes, the default IP address assigned to the team is identical on both server nodes. Note that

manually assigning an IP address to the team in cluster view, synchronizes the setting on both server nodes if they are online and there's no need to assign it in node view.

Restoring Deleted Tiger Spaces Workspace from the Replication Target

When you delete a replicated workspace in the Tiger Spaces web interface, Tiger Spaces automatically moves it to a temporary Trash folder in the workspaces depot. Should Tiger Bridge happen to replicate the Trash folder before Tiger Spaces deletes it, the deleted workspace is automatically moved to a Trash folder on your replication target.

Note: *Currently the replication on Spectra Logic BlackPearl doesn't support paths synchronization when renaming the containing folder and the deleted workspace will be present in both the depot and the Trash folder on the replication target. Thus, you will be able to restore the deleted folder directly from the depot.*

To restore the workspace in the depot on your main storage from the Trash folder on a Private volume, SMB/CIFS network share or a DDN Web Object Scaler as a replication tier, you should:

• (SMB/CIFS network share) Manually move the project from the Trash folder to the Workspaces folder and then rescan the Volume in order to re-generate the deleted files as stub files, which you can then restore.

• (Private volume) Disable Tiger Bridge's replication & tiering on the Private volume and share it to Tiger Clients, then unhide the .tt_rt folder in the root of the volume and manually move the deleted workspace from the Trash folder to the Workspaces folder. Make the volume Private again and enable Tiger Bridge's replication & tiering on it, then rescan the shared volume in the Volume Browser in order to re-generate the deleted files as stub files, which you can then restore.

• (DDN Web Object Scaler) Rescan the volume and regenerate the deleted data as stub files and then contact Tiger Technology support for assistance on moving the data from the hidden Trash folder to the Workspaces folder.

Regardless of the replication target you use, the final step to allow Tiger Spaces to detect and let you work with the workspace in Tiger Spaces is to restart the add-on services in the Maintenance page of Tiger Store.

Only Automatic Defragmentation of Volumes Available

Currently, you cannot perform manual defragmentation of your volumes. To keep your volumes defragmented it is advisable to enable the automatic defragmentation.

Renaming a Volume

You may have to rename a volume twice in the web interface of Tiger Store in order to permanently change its name.

Volume Status not Preserved after Exiting Maintenance Mode

Note: *This issue cannot be observed on Tiger Store appliances with two server nodes.*

Volumes that have been shared before entering Maintenance mode may become Private after exiting Maintenance mode even though its tile shows Shared status. That is why after exiting Maintenance mode, it is advisable to check the status of all volumes seen by the storage server and manually change it. If the status of the volume is Shared, but it cannot be mounted on Tiger Clients, first set it to Private and then set it to Shared to let client computers mount it.

LAN Clients Taking Up SAN Client Licenses

When a Tiger Client sends a request to Tiger Store for connection to the shared volumes, the storage server checks the number of currently available licenses for this type of connection (SAN or LAN) and if a license is available, lets the Tiger Client computer mount the volumes. If all connections for this type are already in use, the storage server lets the Tiger Client mount the volume(s) using another type of connection as long as such is available. While this lets Fibre Channel clients mount the volumes over the Ethernet when there's a problem with the FC HBA or port, or all SAN connections are already in use, it is possible a LAN client to take up a SAN connection and thus prevent a SAN computer from mounting the volumes, because all SAN connections are already taken up. A workaround to this problem is to manually free the connection, by disconnecting the LAN computer in the Clients page of the web interface.

Mac OS X Clients Mounting NTFS Stripe Partitions over the LAN

Currently, Mac OS X client computers can mount just the first partition of a striped NTFS volume over the Fibre Channel and all other partitions are mounted over the Ethernet.

Label of SAN Disks Missing in Windows Explorer of Windows Tiger Clients

On some Windows Tiger Clients, the label of shared volumes mounted over the Fibre Channel may be missing in Windows Explorer.

To attempt to resolve the problem restart the Tiger Client computer or disconnect and then reconnect to Tiger Store:

1. Click the Tiger Client tray application and then click Connect/Disconnect.

2. In the list of all storage servers, click the Tiger Store appliance to disconnect from it.

3. Again click Connect/Disconnect and click the Tiger Store appliance in the list to connect to it.

It is possible the above workaround to be inapplicable on Windows 10 Tiger Clients. If this is the case, you can still identify volumes in Windows Explorer by their drive letter or use command-line to list their labels (using diskpart utility, for example).

Specifying Name and Preferred Mount Location of a Volume Pool

You cannot rename a smart storage pool or set preferred mount location on Windows Tiger Clients.

Volume Disappears from Web UI during Check and Repair Procedure

While you perform the Check & Repair procedure on a Tiger Store volume, it is not listed in the web UI. Once the procedure finishes, you can manage the volume in the web interface again.

Exporting a SMB Share in Domain Environment

To ensure that Tiger Store can export a SMB share to computers without the Tiger Client software, when your appliance is deployed in an Active Directory domain, the domain account "Everyone" must have at least Read Only access to the root of the volume from which the share is exported.

Mounting a Storage Pool on Tiger Client in Domain Environment

In case you have deployed Tiger Store in Active Directory domain and smart storage pooling is enabled, Windows Tiger Clients may fail to mount the storage pool unless the group 'Everyone' has Read access to the virtual volume.

Incorrect Connection Status on Tiger Clients Running Mac OS X

The Tiger Client software on Mac OS X may sometimes fail to correctly display the connection status to the Tiger Store appliance. For example, the Settings dialog of the Tiger Client menulet may display that the Tiger Store is online, when it is actually offline. Another example is when the Tiger Client loses its Fibre Channel connection to the appliance and mounts the volume(s) over the LAN, while the volume icons in the Finder and on the desktop are not of volumes mounted over the Ethernet. Additionally, in this case Tiger Clients running Mac OS X may fail to disconnect from the volume(s).

Allowing smct.app and vpd During Tiger Client Installation on Mac OS X

During installation of Tiger Client on Mac OS X, even if you specify that smct.app and the vpd daemon must be added as firewall exceptions, you should manually allow them in the firewall database of your computer. Note that as long as the firewall of your computer is turned on, you will have to add them to the firewall database after each reboot of the computer.

Applying New Network Environment Settings

It is possible when changing the settings for network environment (domain or workgroup) of your appliance after clicking the Apply button in the Settings page an error to be displayed, when in fact the changes have been applied. It is advisable to refresh the web UI of Tiger Store in order to verify whether the new settings have been applied.

Renaming the Appliance

Should you rename your Tiger Store appliance after it has been added to an Active Directory domain, Tiger Clients may fail to browse the volumes it shares even if they re-add it to their storage servers list. It is advisable before renaming the appliance, to set the network environment to workgroup and manually delete the records about the appliance from the domain controller. It is advisable to do this each time you switch the network environment of your Tiger Store from domain to workgroup.

Alternatively, you can manually change the DNS record for the Tiger Store appliance in the respective DNS Zones in your domain so they can match the new name of the appliance. For details about configuring DNS services, refer to your Windows documentation.

Moving Replicated or Offline Files/Folders

If you move a replicated or offline file/folder from its original location to a folder that is not subject to Tiger Bridge's replication on the shared storage, this folder will also appear on the replication target, but will contain just the files/folders that are subject to replication. For example, if you move an offline file "Report" from its original folder "April" to folder "Drafts" that is not subject to replication and contains other files as well, the replication and tiering mechanism of Tiger Store will create on the replication target a folder "Drafts", but containing just the file "Report".

Importing Offline Dynamic Disks in Maintenance Mode

Offline dynamic disks cannot be imported when your Tiger Store appliance operates in Maintenance mode. To import offline disks, you have to exit Maintenance mode.

Incorrect LAN Traffic Statistics

If you monitor the LAN traffic statistics of Tiger Store with high-availability add-on activated by accessing its web interface through the secondary node (the server node that is in standby mode), the graph will display no LAN traffic. To view the actual statistics, open the web interface using the IP address of the current primary node.

Errors When Entering/Exiting Maintenance Mode

When entering/exiting Maintenance mode, the web UI of Tiger Store may display errors, when in fact the operation has succeeded. To verify that you have entered/exited Maintenance mode, refresh the browser. If on exiting Maintenance mode the error persists, restart the storage server.

Executing Operation on the Tiger Store Volume from Terminal

When Tiger Store is deployed in an Active Directory domain, you won't be able to execute certain operations on the Tiger Store volume(s) from the Terminal of a Mac OS X client computer even if you have logged on as a user that has Full Control. These security mapping issues are not valid for operations performed in the file browser.

Support for Mirrored/Spanned Volumes

No Support for Software Mirrored Volumes

Currently, Tiger Store doesn't provide support for software mirrored volumes. You can use hardware mirrored volumes as part of your shared storage, but with some limitations (see "Mirrored/Spanned Volumes Mounted Over LAN on Mac OS X and Linux" on page 24).

Mirrored/Spanned Volumes Mounted Over LAN on Mac OS X and Linux

Currently mirrored/spanned SAN volumes can be mounted on Mac OS X/Linux SAN Tiger Clients only over the LAN. Such volumes are mounted normally on Windows SAN Tiger Clients.

No Support for Spotlight Indexing

Currently, Spotlight Indexing is not supported on Mac OS X clients. To index and search through shared volumes from Tiger Clients running Mac OS X, use Spotlight alternatives.

No Support for Indexing Service on Shared Volumes

Currently, Tiger Store does not support the Windows indexing service on shared volumes mounted on Tiger Clients.

No Support for Sparse Files

Tiger Store does not provide support for sparse files on SAN volumes.

No Authorization Required When Removing Tiger Store from the Domain

If you decide to switch your Tiger Store from domain to workgroup environment, the domain controller does not require that you authenticate yourself as a user authorized to remove computers from the domain.

Manually Refreshing the Contents of a Directory

The contents of a directory may not be automatically refreshed on Tiger Clients and some file operations may fail. For instance if a Linux Tiger Client tries to copy a directory that is deleted by a Windows Tiger Client, the Linux computer may not be notified about this, and the copy operation will result in error.

To overcome such problems you may have to manually refresh the contents of the disks/directories you are working with.

Changing Volume's Icon on Mac OS X

You can change the appearance of a shared volume's icon on a Mac OS X client computer, but the original icon of the volume will be restored immediately after restarting the storage server and your personal icon will be deleted.

Compressing or Encrypting Folders on Shared Volumes

You will not be able to compress or encrypt any folder on a shared volume. If you try to complete any of these operations, the system displays an error message.