

## Motorola Solutions Technical Notification (MTN)

**TITLE:** DAS (Direct Attached Storage) 4525 firmware update fixes multiple issues.

**TECHNOLOGY:** ASTRO 25

**SYMPTOMS:**

1. ESXi loses connection to DAS 4525 unexpectedly.
2. DAS 4525 is reporting false positive Temperature warning to UEM. A subcomponent of this component is unhealthy.
3. DAS 4525 is reporting degraded Enclosure 0, Ops Panel Ambient Temperature-Degraded
4. Critical alarm clears after approximately 10 minutes.  
[UEM] (Critical) The Overall status of the connectivity unit is Unknown. Unit state is Online.  
[UEM] (Clear) The overall status of the connectivity unit is Ok. Unit state is Online.

Messages mentioned in point 2-4 above are false positive and only displayed on UEM (not visible in DAS logs).

**MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:**

DAS 4525  
ASTRO A7.18; A2019.2; A2020.HS; A2021.1

**SEVERITY RECOMMENDATION:**

**Medium / Operational** - Schedule to implement

**ROOT CAUSE / DEFINITIVE TEST:**

OEM Firmware defects.

**WORKAROUNDS AND CORRECTIVE ACTIONS:**

**RESOLUTIONS AND REPAIR PROCEDURES:**

Use the procedure in Appendix A.

**To obtain software:**

- 1) Initiate a software request case through Motorola Solutions, Inc. Centralized Managed Support Operations (CMSO) at 800-MSI-HELP (800-674-4357) or 302-444-9800
- 2) Await confirmation email from Motorola Solutions Software Factory (MSSF) with instructions
- 3) Complete the Motorola Solutions Software Factory Software Order Form:
  - a) Reference **MTN-0007A-22-NA** in the 'Reason for Software/Hardware Change' section of the software order form.
  - b) List the part number (**KC #** as listed under "**PARTS REQUIRED (HARDWARE/SOFTWARE)**" below) in the 'Part # or Version #' section of the software order form.
- 4) Email completed Software Order Form to MSSF for processing

ANY USE NOT APPROVED BY MOTOROLA SOLUTIONS IS PROHIBITED. This Motorola Technical Notification (MTN) is issued pursuant to Motorola's ongoing review of the quality, effectiveness, and performance of its products. The information provided in this bulletin is intended for use by trained, professional technicians only, who have the expertise to perform the service described in the MTN. Motorola disclaims any and all liability for product quality or performance if the recommendations in this MTN are not implemented, or not implemented in compliance with the instructions provided here. Implementation of these recommendations may be necessary for the product to remain compliant with applicable laws or regulations. Please be advised that failure to implement these recommendations in the manner instructed may also invalidate applicable warranties, or otherwise impact any potential contractual rights or obligations. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. ©2021 Motorola Solutions, Inc. All rights reserved.

DOCUMENT NUMBER: MTN-0007A-22-NA  
APC: 877  
ISSUE DATE: Dec-2022  
EXPIRATION DATE: 31-Dec-2023  
Bulletin Type: Informational Only

**TIME TO IMPLEMENT/SYSTEM IMPACT:**

Estimated time to implement - per machine - 5 hours to install the DAS (including backup). (DAS Will be unavailable 2 hours)

High - Loss of functionalities/audio/downtime

**PARTS REQUIRED (HARDWARE/SOFTWARE):**

mot-csr-das-06.17.04-01 / KC877V0B0000210105 or newer

This MTN supersedes MTN-0007-22-NA. In case MTN-0007-22-NA was already applied there is no need to apply the updated version.

**REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:**

[Virtual Management Server Software User Guide](#)

[Backup and Restore Services Feature Guide](#)

**WHEN TO APPLY RESOLUTION:**

After failure

After (re)installation

During maintenance

**LABOR ALLOWANCE:**

This is an informational bulletin. No labor warranty is implied, intended or authorized for U.S. Domestic Partners/Customers. Other regions should follow their own standard procedures.

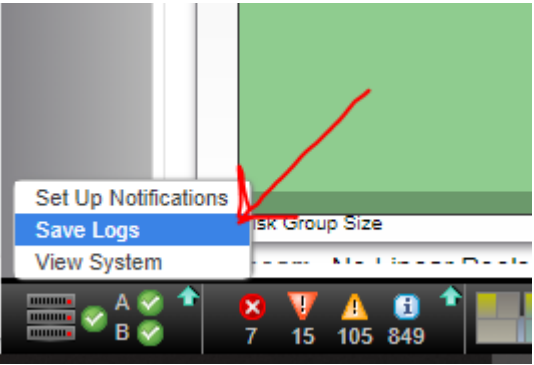
For assistance with this bulletin please contact your MSI Technical support center

[https://www.motorolasolutions.com/en\\_us/support.html](https://www.motorolasolutions.com/en_us/support.html)

## Appendix A - Update Procedure

<b>Before You Begin:</b>	<p>Before replacing DAS Controller, execute an offline backup of every VM hosted by DAS. Backup procedures are included in the "Backup and Restore Service Feature Guide " GCD document.</p> <ol style="list-style-type: none"> <li>1. At the beginning follow the procedure: "Scheduling a One-Time Backup of a BAR Client," for each virtual machine placed on the DAS.</li> <li>2. If the customer system does not include a NAS device, then follow the procedures: "Creating an ISO Archive to Store Offline" for each virtual machine hosted on DAS and "Transferring Files to or from the BAR Server". After transferring the backup file (ISO) to the NM Client local or attached drive, archive these files or burn them on a DVD .</li> <li>3. If the customer system includes a NAS device, follow the procedure: "Exporting a Data Archive from the BAR Server to the Offline Storage NAS"</li> </ol> <p><b>IMPORTANT NOTE:</b> Depending on the extent of problems found, the system may be required to reboot both VMS servers. This may require VM shutdowns as well as switchover of the Zone Controllers as each server is rebooted.</p>
--------------------------	---

1	Insert the <b>mot-csr-das disc</b> into the optical drive of the Windows device.
2	Update DAS firmware to GT280R009-03 or the latest. (for more details go to "Appendix B – Update DAS Firmware") After upgrading firmware check the midplane firmware version ( <a href="#">Appendix C</a> ) if the version is correct, this procedure is complete. Else continue this procedure.
3	<p>To log in to the DAS, do the following:</p> <ol style="list-style-type: none"> <li><b>3.1</b> Run a web browser.</li> <li><b>3.2</b> In the web browser address field, type <b>https://&lt;controllerA-address&gt;</b> and press Enter.</li> <li><b>3.3</b> Type <b>manage</b> in the <b>User name</b> field.</li> <li><b>3.4</b> Type an appropriate password in the <b>Password</b> field.</li> <li><b>3.5</b> Click the <b>Sign In</b> button.</li> </ol> <p><b>Result:</b> You are login into user web interface</p>
4	In the left bottom corner, click on the field with A and B characters.

	 <p><b>Result:</b> Drop-down list appears</p>
5	<p>From drop-down list choose <b>Save Logs</b></p> <p><b>Result:</b> Save Logs windows appears</p>
6	<p>In <b>Save Logs</b> window fill in the required fields (with red star) following</p> <p><b>Your Name:</b> &lt;Enter your first and last name &gt;</p> <p><b>Your Email Address:</b> &lt;Enter your email address&gt;</p> <p><b>Your Phone Number:</b> &lt;Enter any numbers e.g.: 3456356&gt;</p> <p><i>INFO: The data you entered will be saved to the log file</i></p> <p>And click <b>OK</b></p> <p><b>Result: Progress of Get Logs</b> window appears. (Wait until <b>Save As</b> window will appears)</p>
7	<p>In the <b>Save As</b> window choose temporary localization and click <b>Save</b></p> <p><b>Result:</b> File with logs was saved on the disk</p>
8	<p>In the right-top corner click on field with System name and Version of firmware</p> <p><b>Result:</b> Drop-down list appears.</p>
9	<p>From drop-down list choose <b>Set Up System Services</b></p> <p><b>Result: System Setting</b> appears.</p>
10	<p>In <b>Manage Users</b> tab select <b>manage user</b> and check <b>FTP in Interfaces</b></p> <p>Click <b>Apply and Close</b></p> <p><b>Result:</b> The manage user can use the SFTP service.</p>

11	<p>Launch the web browser and in the address bar, enter:</p> <pre>https://&lt;esxi-mgmt-ip-address&gt;</pre> <p>where: &lt;esxi-mgmt-ip-address&gt; is the IP address of ESXi management network interface (please refer to «IP plan» document).</p> <p><b>Result:</b> VMware ESXi Embedded Host Client authentication page is open.</p>
12	<p>Authenticate by performing the following steps:</p> <p>In the User name field, enter the name of the user with administrator privileges.</p> <p>In the Password field, enter the password.</p> <p>Click <b>Log in</b> button.</p> <p><b>Result:</b> VMware ESXi Embedded Host Client home page opens.</p>
13	<p>Disable applications that need to be disabled before Shutting down.</p> <p>See: “<b>Private Network Management Servers Feature Guide</b>”, chapter “<b>Enabling/Disabling PNM Server Applications</b>”.</p> <p><b>Result:</b> All virtual machines may be safely shut down (except Zone Controller VM).</p>
14	<p>At the <b>Navigator</b> pane on the left, click on <b>Virtual Machines</b>.</p> <p>Check all virtual machines located on DAS (Do not power off <b>ZC</b>).</p> <p>Click the <b>Shut down</b> button on the top of the menu.</p> <p>Wait until all process in <b>Recent tasks</b> menu in <b>Result</b> column will be <b>Completed successfully</b>.</p> <p><b>Result:</b> All virtual machines located on DAS were shut down.</p>
15	<p>On the NM Client,</p> <p>If you are using Windows 7, open the start menu and type <b>Command</b> in the Search programs and files text field.</p> <p>If you are using Windows 10, type <b>Command</b> in the Search Windows text field from the launch bar.</p> <p><b>Result: Command Prompt</b> terminal window appears.</p>
16	<p>In <b>Command Prompt</b> window, enter the following:</p> <p>11.1 Type the drive letter of the optical drive that contains the mot-csr-das disc followed by a colon (example: E:) and press <b>Enter</b>.</p> <p>11.2 Type <code>cd addins</code> and press <b>Enter</b>.</p> <p><b>Result:</b> The directory is changed to the addins directory of the mot-csr-das disc.</p>
17	<p>Enter following comment:</p> <pre>sftp -P 1022 manage@&lt;ip address to DAS controller&gt;</pre> <p>where “&lt;ip address to DAS controller&gt;” is the IP address of DAS controller A (please refer to «IP plan» document).</p> <p>for example: <code>sftp -P 1022 manage@10.2.233.42</code></p>

	<p>and press <b>Enter</b></p> <p><b>Result:</b> Prompt with asking about the user appears.</p>
18	<p>Enter password to manage user account and press <b>Enter</b>.</p> <p><b>Result:</b> A command prompt is displayed on terminal window <b>sftp&gt;</b></p>
19	<p>Enter following command:</p> <pre>put 1026619_sp3224a_12g_vpd_v13_crc_a1796e3d.gff encl:00:127</pre> <p><b>Result:</b> The 1026619_sp3224a_12g_vpd_v13_crc_a1796e3d.gff was uploaded to the controller A</p>
20	<p>Do the following steps to shut down the storage system.</p>
21	<p>Establish the ssh connection to DAS Controller A management interface IP address by using a <b>PuTTY</b> terminal emulator software.</p> <p>In to <b>Host Name (or IP address)</b> enter &lt;ip address to DAS controller A &gt; is the IP address of DAS controller A (please refer to «IP plan» document).</p> <p>Click <b>Open</b></p> <p><b>Result:</b> A command prompt is displayed on <b>PuTTY</b> terminal emulator window.</p>
22	<p>Log on as the <code>manage</code> user.</p> <p><b>Result:</b> You are logged in as a manage user.</p>
23	<p>Execute following command:</p> <pre>shutdown both</pre> <p><b>IMPORTANT !!!</b></p> <p>Wait till Cache LED on both the controllers to go OFF and for it to shutdown completely (may take 20 minutes). After the controllers shut down, the blue OK to Remove LED on the controller illuminates.</p> <p><b>Result: The Storage Controllers in a controllers module were shut down.</b></p>
24	<p>Power OFF the DAS chassis by pulling power cables and wait for <u>5 minutes or more for the drives to spin-down completely</u>.</p> <p>Power ON the DAS chassis by connecting the power and wait several minutes for the boot to complete.</p> <p><b>Verify the boot completion by performing the following steps.</b></p>

25	<p>Establish the ssh connection to DAS Controller A management interface IP address by using a <b>PutTY</b> terminal emulator software.</p> <p>In to <b>Host Name (or IP address)</b> enter &lt;ip address to DAS controller A &gt; is the IP address of DAS controller A (please refer to «IP plan» document).</p> <p>Click <b>Open</b></p> <p><b>Result:</b> A command prompt is displayed on <b>PutTY</b> terminal emulator window.</p>		
26	<p>Log on as the <code>manage</code> user.</p> <p><b>Result:</b> You are logged in as a <code>manage</code> user.</p>		
27	<p>Execute following command:</p> <pre>show system</pre> <p>check if Health is OK</p> <p>example: Health: OK</p> <p>If Health is NOT “OK”, wait a few more minutes and repeat the <code>show system</code> command.</p> <p><b>Result:</b> System boot and health verification is complete</p>		
28	<p><b>NOTE:</b> Perform the following steps for both VMS servers connected to the DAS.</p> <p>Launch the web browser and in the address bar, enter:</p> <pre>https://&lt;esxi-mgmt-ip-address&gt;</pre> <p>where: &lt;esxi-mgmt-ip-address&gt; is the IP address of ESXi management network interface (please refer to «IP plan» document).</p> <p><b>Result:</b> VMware ESXi Embedded Host Client authentication page is open.</p>		
29	<p>Authenticate by doing the following:</p> <p>In the User name field, enter the name of the user with administrator privileges .</p> <p>In the Password field, enter the password.</p> <p>Click the <b>Login</b> button.</p> <p><b>Result:</b> <b>VMware ESXi Embedded Host Client</b> home page opens.</p>		
30	<p>At the <b>Navigator</b> pane on the left, click on <b>Storage</b>→ <b>Devices</b></p> <p>Check if all devices are <b>Normal</b> in the <b>Status</b> column.</p> <table border="1" data-bbox="217 1663 1523 1717"> <tr> <td data-bbox="217 1663 415 1717">IF</td> <td data-bbox="415 1663 1523 1717"><b>SEAGATE Serial Attached SCSI Disk</b> have Error in the <b>Status</b> column.</td> </tr> </table>	IF	<b>SEAGATE Serial Attached SCSI Disk</b> have Error in the <b>Status</b> column.
IF	<b>SEAGATE Serial Attached SCSI Disk</b> have Error in the <b>Status</b> column.		

THEN	<p><b>NOTE:</b> During this task, the site trunking may occur during ZC switchover required only when server with active ZC has this error.          Rebooting should be done only on servers with the error.</p> <ol style="list-style-type: none"> <li>1. If the error is present on the server with standby ZC, perform the shutdown of standby ZC following Appendix D and reboot of that server following Appendix E.</li> <li>2. If the error is present on the server with active ZC, perform planned ZC switchover followed by shutdown of the newly standby ZC following Appendix D and reboot of the server following Appendix E.</li> </ol>						
OTHERWISE	Go to next step						
<p><b>Result:</b> VMS was rebooted successfully.</p>							
31	<table border="1"> <tr> <td data-bbox="672 869 415 928">IF</td> <td data-bbox="415 869 1539 928">VMS reboot was required.</td> </tr> <tr> <td data-bbox="672 928 415 1150">THEN</td> <td data-bbox="415 928 1539 1150"> <ol style="list-style-type: none"> <li>1. Wait for the automatic powerup of the virtual machines. This may take several minutes per virtual machine. Observe the Tasks window at the bottom of the Host Client.</li> <li>2. Make sure that all required virtual machines are powered up. Troubleshoot and powerup manually if needed.</li> </ol> <p>Enable the Linux based applications if they were disabled previously. Refer to procedure in step 13.</p> </td> </tr> <tr> <td data-bbox="672 1150 415 1339">OTHERWISE</td> <td data-bbox="415 1150 1539 1339"> <p>Power On all virtual machines one by one, by right clicking the virtual machine and selecting <b>Power</b> → <b>Power On</b>.</p> <p><b>NOTE: Do not power on all virtual machines at the same time.</b></p> <p>Enable the Linux based applications if they were disabled previously. Refer to procedure in step 13.</p> </td> </tr> </table> <p><b>Result:</b> All virtual machines work correctly.</p>	IF	VMS reboot was required.	THEN	<ol style="list-style-type: none"> <li>1. Wait for the automatic powerup of the virtual machines. This may take several minutes per virtual machine. Observe the Tasks window at the bottom of the Host Client.</li> <li>2. Make sure that all required virtual machines are powered up. Troubleshoot and powerup manually if needed.</li> </ol> <p>Enable the Linux based applications if they were disabled previously. Refer to procedure in step 13.</p>	OTHERWISE	<p>Power On all virtual machines one by one, by right clicking the virtual machine and selecting <b>Power</b> → <b>Power On</b>.</p> <p><b>NOTE: Do not power on all virtual machines at the same time.</b></p> <p>Enable the Linux based applications if they were disabled previously. Refer to procedure in step 13.</p>
IF	VMS reboot was required.						
THEN	<ol style="list-style-type: none"> <li>1. Wait for the automatic powerup of the virtual machines. This may take several minutes per virtual machine. Observe the Tasks window at the bottom of the Host Client.</li> <li>2. Make sure that all required virtual machines are powered up. Troubleshoot and powerup manually if needed.</li> </ol> <p>Enable the Linux based applications if they were disabled previously. Refer to procedure in step 13.</p>						
OTHERWISE	<p>Power On all virtual machines one by one, by right clicking the virtual machine and selecting <b>Power</b> → <b>Power On</b>.</p> <p><b>NOTE: Do not power on all virtual machines at the same time.</b></p> <p>Enable the Linux based applications if they were disabled previously. Refer to procedure in step 13.</p>						
32	<p>Verify if the VPD CRC version is correct.  <b><u>Appendix C – How to check the correct firmware version of the midplane</u></b></p> <p><b>Result:</b> VPD CRC version verification is complete</p>						

33	<p>To log in to the DAS, do the following:</p> <ol style="list-style-type: none"><li>2.1 Run a web browser.</li><li>2.2 In the web browser address field, type https://&lt;controllerA-address&gt; and press Enter.</li><li>2.3 Type <b>manage</b> in the User name field.</li><li>2.4 Type an appropriate password in the Password field.</li><li>2.5 Click the Sign In button.</li></ol> <p><b>Result:</b> You are login into user web interface</p>
34	<p>In the right-top corner click on field with System name and Version of firmware</p> <p><b>Result:</b> Drop-down list appears.</p>
35	<p>From drop-down list choose <b>Set Up System Services</b></p> <p><b>Result:</b> <b>System Setting</b> appears.</p>
36	<p><b>!!!IMPORTANT !!!</b></p> <p>In <b>Manage Users</b> tab select <b>manage user</b> and uncheck <b>FTP</b> in <b>Interfaces</b> Click <b>Apply and Close</b></p> <p><b>Result:</b> <b>SFTP settings have been restored to those prior to the procedure.</b></p>
37	<p>Procedure is complete.</p>

## **Appendix B – Update DAS Firmware**

1	Insert the DotHill DAS Firmware disc into the optical drive of the Windows device.
2	Open the start menu.
3	Type command in the Search programs and files text field. <b>Result:</b> The Command Prompt appears in the list of available programs and files.
4	Right-click Command Prompt and select Run as administrator. <b>Result:</b> The Command Prompt window appears.
5	At the command prompt, type powershell and press Enter. <b>Result:</b> The powershell prompt is displayed.
6	At the powershell prompt, type the drive letter of the optical drive that contains the DotHill DAS Firmware disc followed by a colon (example: E:) and press Enter. <b>Result:</b> The directory is changed to the root directory of the DotHill DAS Firmware disc.
7	At the powershell prompt, type cd bin and press Enter. <b>Result:</b> The directory is changed to the bin directory of the DotHill DAS Firmware disc.
8	At the powershell prompt, type .\Update-ASTRODas.ps1 and press Enter. <b>Result:</b> The user is prompted to “Configure for DSR?(n,y)”
9	If the system is configured for DSR, type y and press Enter. Otherwise, type n and press Enter and skip to step 11. <b>Result:</b> The user is prompted to “DSR Core(1-2):”
10	Type the number corresponding to the correct core type and press Enter. <b>Result:</b> The user is prompted to “Zone ID(1-7):”
11	Type the number corresponding to the Zone and press Enter. <b>Result:</b> The user is prompted to “Enter “manage” user password:”
12	Type the password for the manage user for the DAS to be updated and press Enter. <b>Result:</b> The user is prompted to “Enter “monitor” user password, or press enter to use current password:”
13	Type the password for the monitor user for the DAS to be updated and press Enter. <b>Result:</b> The user is prompted to “Confirm the password”
14	Type again the password for the monitor user and press Enter. <b>Result:</b> The user is prompted to “Enter SNMP Security Level(1-3):”

15	Type the number corresponding to the correct SNMP Security level for this system and press Enter. <b>Note:</b> If the security level selected was for noauthnopriv, skip to step 20. Otherwise, continue to the next step. <b>Result:</b> The user is prompted to "Enter the "MotoMaster" authentication password:"
16	Type the authentication password for the MotoMaster user on the DAS and press Enter. <b>Result:</b> The user is prompted to "Confirm the password"
17	Type again the authentication password for the MotoMaster user and press Enter. <b>Result:</b> The user is prompted to "Enter the "MotoMaster" privacy password:"
18	Type the privacy password for the MotoMaster user on the DAS and press Enter. <b>Result:</b> The user is prompted to "Confirm the password"
19	Type again the privacy password for the MotoMaster user and press Enter. <b>Result:</b> The user is prompted to "Enter IP of Centralized Syslog Server (optional):"
20	If the system has a Centralized Syslog server, enter its IP address and press Enter. Otherwise, just press Enter. <b>Result:</b> The user is prompted to "Are the inputs correct(n,y):"
21	Type y and press Enter. <b>Result:</b> The DAS firmware image and settings update is performed and the user is prompted to "Press enter to exit".
22	Verify that there are no messages stating "[FAILED]" in the output of the script on the screen and then press Enter. <b>Result:</b> The powershell command prompt appears.
23	Enter exit and press Enter. <b>Result:</b> The Windows command prompt appears.
24	Enter exit and press Enter. <b>Result:</b> The procedure is complete.

### **Appendix C – How to check the correct firmware version of the midplane**

1	<p>Establish the ssh connection to DAS Controller A management interface IP address by using a <b>PuTTY</b> terminal emulator software.</p> <p>In <b>Host Name (or IP address)</b> enter &lt;ip address to DAS controller A &gt; is the IP address of DAS controller A (please refer to «IP plan» document).</p> <p>Click <b>Open</b></p> <p><b>Result:</b> A command prompt is displayed on <b>PuTTY</b> terminal emulator window.</p>
1	<p>Log on as the <code>manage</code> user.</p> <p><b>Result:</b> You are logged in as a manage user.</p>
2	<p>Execute following command</p> <pre>show configuration</pre> <p>find: <b>VPD CR in Midplane Version</b></p> <p>example:</p> <pre>Midplane Versions ----- VPD Format Version: 13 <b>VPD CRC: A1796E3D</b> Config Mismatch Version: 01 CPLD Version: 14 FRU Descriptor: 79</pre> <p>If <b>VPD CRC is A1796E3D</b> the Midplane Version is correct.</p>
3	<p>Procedure is complete.</p>

## **Appendix D - Switchover and Shutdown of Zone Controller Virtual Machine**

1	Before shutdown of an active ZC, perform the switchover. See: “ <b>Zone Controller Feature Guide</b> “, chapter: “ <b>Zone Controller Redundancy and Switchover</b> ”
2	At the <b>Navigator</b> pane on the left, click on <b>Virtual Machines</b> . Check the <b>Zone Controller</b> Virtual Machine. Click the <b>Shut down</b> button on the top of the menu. Wait until all processes in the <b>Recent tasks</b> menu in the <b>Result</b> column will be <b>Completed successfully</b> . <b>Result:</b> All virtual machines located on DAS were shut down.

## **Appendix E - Rebooting of VMS server**

1	Launch the web browser and in the address bar, enter: <code>https://&lt;esxi-mgmt-ip-address&gt;/ui</code> where <esxi-mgmt-ip-address> is an IP address of the ESXi management network interface (please refer to « <i>IP plan</i> » document). Note If a certificate warning appears, continue to the page. The form of the warning and steps to ignore it depend on the web browser. <b>Result: VMware ESXi Embedded Host Client</b> authentication page is open.
2	Authenticate by do the following: 1. In the <b>User name</b> field, enter user name with administrator privileges 2. In the <b>Password</b> field, enter the password 3. Click <b>Log in</b> button. <b>Result: VMware ESXi Embedded Host Client</b> home page opens.
3	At the <b>Navigator</b> pane on the left side, right-click on <b>Host</b> and select “ <b>Reboot</b> ”. <b>Result:</b> The “ <b>Reboot</b> ” window appears.
4	Click “ <b>OK</b> ” to start rebooting the ESXi server. Wait until the ESXi hypervisor reboot is complete. (It may take about 10 minutes) <b>Result:</b> The ESXi reboot is completed.