Smarter technology for all

ThinkSystem problem determination

ES41759C

October 2024

Lenovo

Prerequisites

- ThinkSystem architecture introduction
- ThinkSystem V2 architecture introduction
- ThinkSystem V3 architecture introduction
- Introducing ThinkSystem tools
- ThinkSystem tools for the ThinkSystem V3 platform
- The three things you need to do technical support

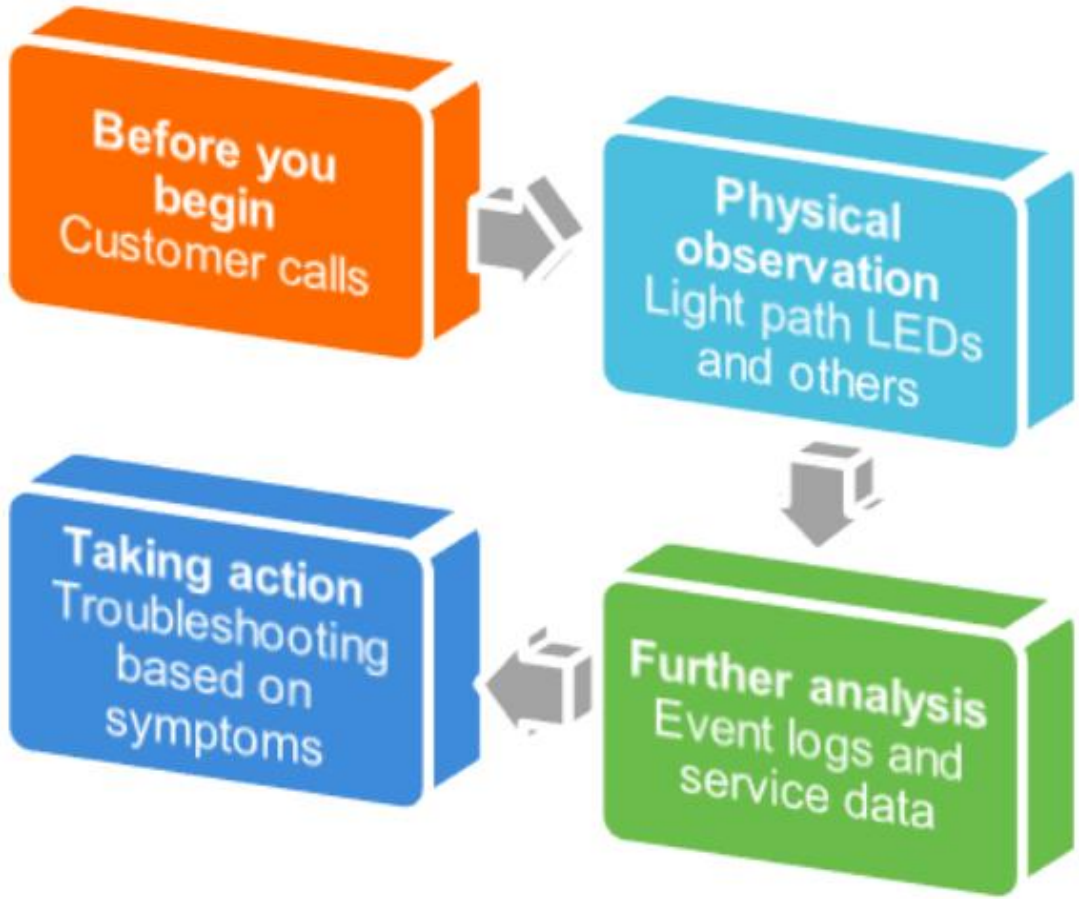
Objectives

After completing the course, you will be able to:

- Describe how to perform physical observation actions for problem determination
- Describe how to collect event logs and service data
- Describe the log parsing procedure
- Describe how to troubleshoot issues with each component based on symptoms
- Describe the problem determination steps and explain how to troubleshoot issues with ThinkSystem servers

Problem determination concept

The concept of ThinkSystem problem determination (PD) can be divided into four steps:



Lenovo

Before you begin

Before starting the problem determination process, check the following:

- Prior system use – has the system worked properly in the past? Have there been any recent hardware or software changes?
  - Return the server to the condition it was in before the problem occurred.
  - Where possible, reverse any hardware, software, or firmware changes that took place directly before the problem occurred.
  - Check the ServerProven and Configuration and Options Guide websites to verify that any newly added devices are supported by the server.
- Supported firmware levels on the current system
  - Fixes or workarounds for many problems might be available in updated versions of BIOS, UEFI firmware, device firmware, or device drivers.
  - Before installing a firmware or device driver update, refer to the README file and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure used to install it; this includes any special procedures that should be followed when updating firmware or a device driver to the latest version.
  - Check https://servicetools.lenovo.com/techtips/out/webhelp/ for any tech tips related to the issue.
- Possible location changes
  - Make sure the cables are functioning and seated correctly.
  - Shut down the server and reseat server components including the hot-swap power supply, drives, fans, riser cards, PCIe adapters, DIMMs, and, if applicable, the second CPU board. These components might vibrate and move position during a relocation.

What’s new

LXPM4, XCC2, and the Firmware and RoT Security Module

Lenovo

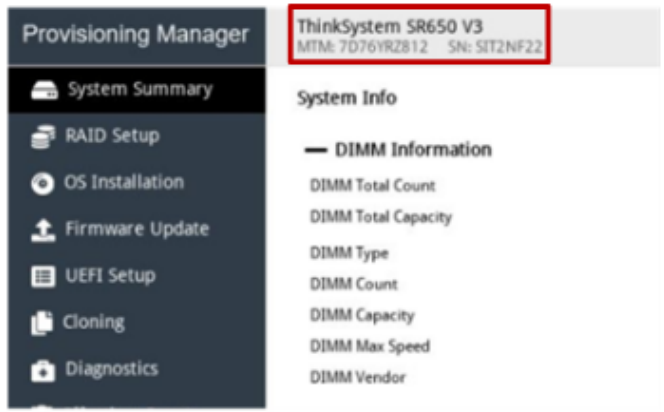
Update overview

Management software tools such as Lenovo XClarity Provisioning Manager (LXPM) and XClarity Controller (XCC) have been updated to accompany the new ThinkSystem V3 platform. The updates include:

- LXPM4: An enhanced GUI, QR codes for user access, and QR codes for events – click HERE for examples
- XCC2: A new service log for collection

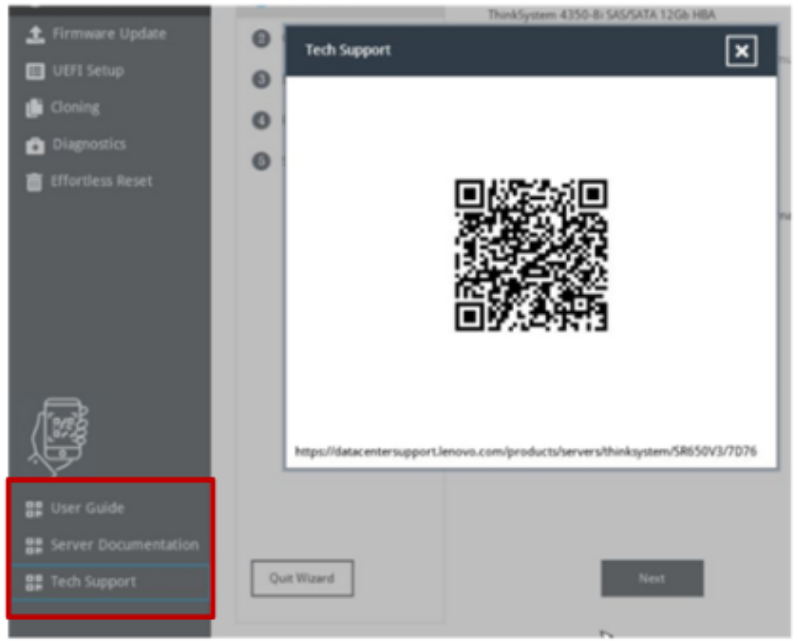
V3 servers and the SE450 are also equipped with the new Firmware and Root of Trust (RoT) Security Module, which provides an additional layer of security.

Enhanced GUI



Product name, machine type, and serial number at the top of the page

QR codes for user access



In the left navigation menu, users can find QR codes for the following functions:

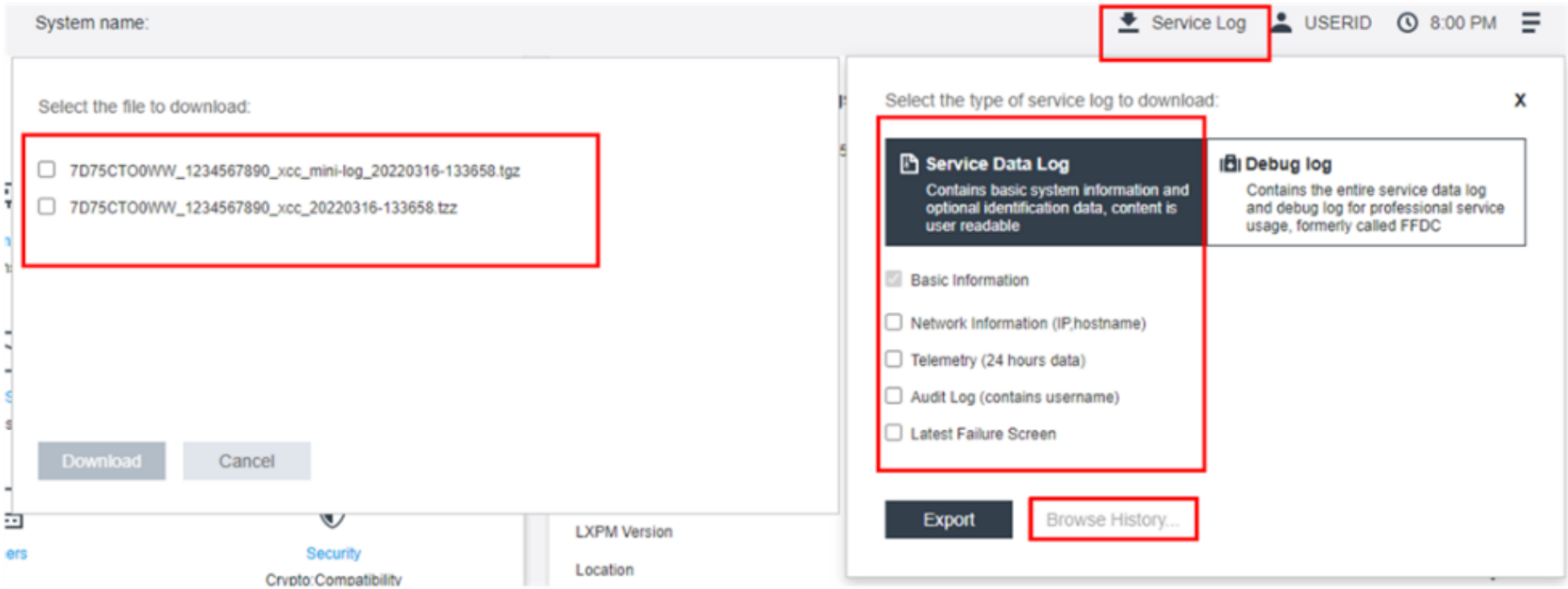
- User guides
- Server documentation
- Technical support

QR codes for events

If a user encounters an issue on the LXPM function page, they will be given a QR code for the event

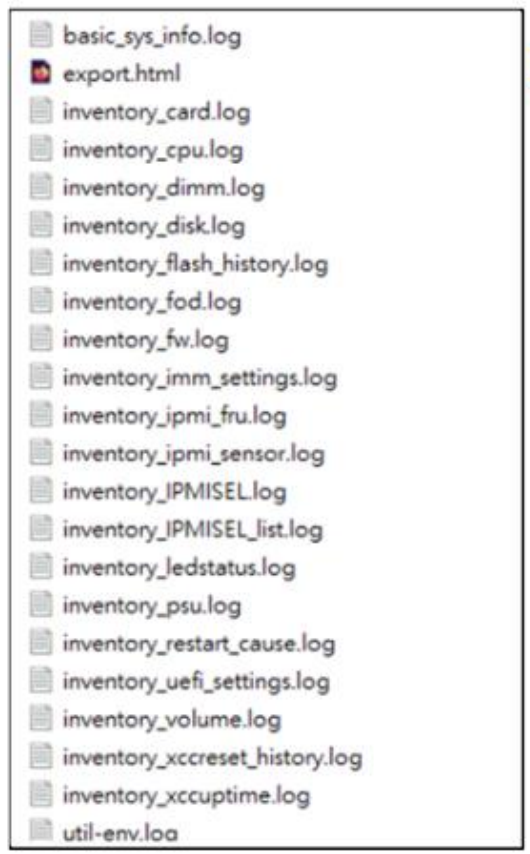
Collecting mini-logs (Service Data Logs) from the XCC2 web interface -1

The mini-log is a new type of service log with a smaller file size than the FFDC. When users encounter server issues and request field servicing, the field engineer should ask them to collect the service log from XCC. The service log is in HTML and JSON format, which can be readable in a text editor or browser, and a complete service log history is also available for download. There is an additional Debug log, formally called the FFDC, which is for PE engineers if the issue is escalated.



Collecting mini-logs (Service Data Logs) from the XCC2 web interface -2

After downloading the service log, unzip it in your local directory. You can select each log file to see different system information or open the export.html file in a browser to see all the logs.



System information

current_time	2022-07-10 19:20:31 UTC+00:00
hostname	XCC-7D72-SDVJWM11
hw_revision	4
ipv4_address	10.245.62.217
location	
lowest_u	1
machine_name	ThinkSystemNY1 SR630 V3
machine_typemodel	7D72GV7324
manufactureid	LNVO
power_state	1
rack_id	
room_id	
serial_number	SDVJWM11
server_state	7
system_name	
uuid	F2E6A79CA14311EC8111000EC6877222

Active Events

Firmware

index	type	version	build	release_date
1	BMC(Active)	0.42	ESX303E	2022-06-22
2	BMC(Primary)	0.42	ESX303E	2022-06-22
3	BMC(Backup)	0.42	ESX303E	2022-06-22
4	UEFI	1.00	ESE103U	2022-06-13
5	LXPM	4.00	EAL103M	2022-07-04
6	LXPM Windows Drivers	4.00	EAL301H	2022-06-12

Firmware and RoT Security Module troubleshooting

V3 servers and the SE450 cannot boot without the Firmware and RoT Security Module. If the system does not start, work through the following troubleshooting methods to identify whether the module or system board has failed.

Note: The power-control button will not function for approximately five to 10 seconds after the server has been connected to power.

Click each number in turn to see the procedure.

Step 1 2

Firmware and RoT Security Module troubleshooting

If an additional optional device has recently been installed, remove it and turn on the server again. If the server now starts, it indicates that the optional device uses more power than the system can afford.

Check the power button LED:

- If the power button LED is lit, check the system event log.
  - If there is a readable system event log without UEFI errors, replace the system board.
  - If there is a readable system event log with UEFI errors, replace the Firmware and RoT Security Module.
  - If there is no readable system event log, but the power button LED is still lit, run diagnostic isolation on the replacement units listed below, and replace the faulty parts:
    - System board
    - Firmware and RoT Security Module

Step 1—2

Firmware and RoT Security Module troubleshooting

- If the power button LED is not lit:
  - Disconnect and reconnect the power cable.
  - Make sure the power supplies are of the same type (the system-error LED would be lit if the power supply units do not match) and reseat all the units.
  - Check if any power supply error LEDs are lit and replace any faulty units.
  - If the problem persists, run diagnostic isolation on the replacement units listed below, and replace the faulty parts:
    - Power backplane
    - System board
    - Firmware and RoT Security Module

Common questions about the Firmware and RoT Security Module

Scroll down for more information

Question	Answer
Can V3 servers or the SE450 boot without the Firmware and RoT Security Module ?	The UEFI and XCC flash chips are on this module, and systems cannot boot without it.
Which configurations are on the Firmware and RoT Security Module, and which configurations are on the system board? For example, XCC, UEFI, Intel VROC RAID configuration, hardware VPD	• The UEFI and XCC flash chips are on the Firmware and RoT Security Module. • The VROC configuration is stored in the VROC member disks. • Hardware VPD is on system board.
Can you back up configurations from the Firmware and RoT Security Module ?	• The UEFI and XCC flash chips are on this module. UEFI stores the system UEFI configuration in XCC, and you can back up and restore these configurations while the system is normal. The procedure used to back up and restore UEFI and XCC configurations is the same as on ThinkSystem servers. Refer to the Lenovo XClarity Controllers guide for more information. • Hardware VPD is on the system board. • The VROC configuration is stored in the VROC member disks. Unless there has been data corruption of the NVMe drives, the VROC configuration will not be lost. **Attention**: For the VROC configuration, users should keep VMD on. If the VMD is disabled and the OS is rebooted, it might trigger an OS data recovery mechanism that corrupts the VROC configuration/metadata, especially with a Windows OS.

Common questions about the Firmware and RoT Security Module

Scroll down for more information

Question	Answer
configuration, hardware VPD	
Can you back up configurations from the Firmware and RoT Security Module ?	• The UEFI and XCC flash chips are on this module. UEFI stores the system UEFI configuration in XCC, and you can back up and restore these configurations while the system is normal. The procedure used to back up and restore UEFI and XCC configurations is the same as on ThinkSystem servers. Refer to the Lenovo XClarity Controllers guide for more information. • Hardware VPD is on the system board. • The VROC configuration is stored in the VROC member disks. Unless there has been data corruption of the NVMe drives, the VROC configuration will not be lost. **Attention**: For the VROC configuration, users should keep VMD on. If the VMD is disabled and the OS is rebooted, it might trigger an OS data recovery mechanism that corrupts the VROC configuration/metadata, especially with a Windows OS.
Which service action should be taken after replacing the Firmware and RoT Security Module but not the system board?	Restore the UEFI/XCC user configuration manually or by using OneCLI script.
Which service action should be taken after replacing the system board but not the Firmware and RoT Security Module ?	Restore the necessary data in VPD.