Lenovo & Veeam Hardened Repository Hardware Setup Quick Guide

Planning / Implementation

Introduction to Veeam Hardened Repository

Achieve radical resilience that can only come from complete confidence in your protection, response and recovery. Built on the principles of Data Security, Data Recovery and Data Freedom, Veeam Data Platform provides the confidence you need to take a stand against cyberattacks.

- Detect and identify cyberthreats
- Respond and recover faster from ransomware
- Secure and compliant protection for your data

Key capabilities include:

- **Early threat detection**: AI-powered, built-in Malware Detection Engine performs low-impact inline entropy and file-extensions analysis during backup for immediate detection.
- **Avoid reinfection**: Content analysis helps pinpoint identified ransomware strains to prevent the reintroduction of malware into your environment.
- **Guarantee survival**: Prevent accidental or malicious deletion or encryption of backups by employing a zero-trust architecture, “Four-Eyes” admin protection and immutable backups.
- **Proactive threat hunting**: Backup anomalies are instantly reported into ServiceNow and other SIEM tools of your choice, so you can immediately perform triage and reduce further risk to your data.
- **Automate clean recovery**: Perform orchestrated recovery of an entire environment using malware-free restore points.
- **Verify security and compliance**: Ensure recovery success with automated scans using the Security & Compliance Analyzer, leveraging infrastructure hardening and data protection best practices.
- **Get a second opinion**: Let your cyberthreat tool report infections directly into the Veeam Incident API, marking existing restore points as infected or trigger backup
- **Recover with precision**: Perform point-in-time recovery to the moment prior to infection with the I/O Anomaly Visualizer, ensuring the lowest possible data loss thanks to Veeam CDP.
- **Put the spotlight on malware**: Highlight threats, identify risks and measure the security score of your environment in the Veeam Threat Center.

For more information on the Hardened Repository, see the following Veeam help page:
https://helpcenter.veeam.com/docs/backup/vsphere/hardened_repository.html?ver=120

Introduction to the SR650 V3 and SR630 V3

Combining performance and flexibility, the SR630 V3 and SR650 V3 servers are a great choice for enterprises of all sizes. The servers offer a broad selection of drive and slot configurations and offers numerous high-performance features. Outstanding reliability, availability, and serviceability (RAS) and high-efficiency design can improve your business environment and can help save operational costs.

Figure 1. Lenovo ThinkSystem SR630 V3

Figure 2. Lenovo ThinkSystem SR650 V3

For details about the SR630 V3 and SR650 V3, see the Lenovo Press product guides:

- SR630 V3 Product Guide
- SR650 V3 Product Guide

The Red Hat hardware certification list (HCL) pages for the servers are as follows:

- Red Hat Certification for SR630 V3
- Red Hat Certification for SR650 V3

Server documentation links:

- SR630 V3 User Guide
- SR650 V3 User Guide

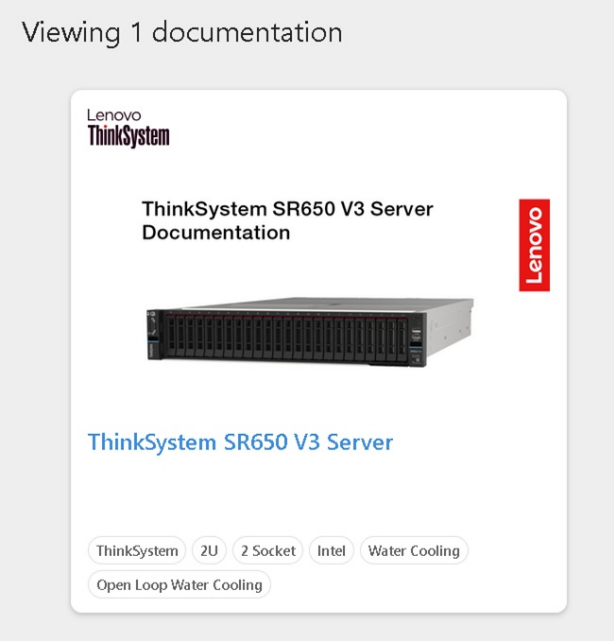

Figure 3. SR650 V3 documentation

Firmware update procedures

Updating the firmware and drivers on a regular schedule is the recommended best practice for several reasons:

- Achieves the highest-level hardware availability
- Enables you to proactively apply the latest bug fixes before your systems are affected by them
- Increases security, compatibility, and system uptime

For guidance on how to update the firmware of Lenovo ThinkSystem V3 servers, see the following documents:

- Lenovo ThinkSystem Firmware and Driver Update Best Practices - An Introduction
- Lenovo ThinkSystem V3 and V4 Server Firmware and Drivers Update Best Practices - Advanced Guide

Recommendations for updates

To have a successful firmware update consider these recommendations:

- Use of UpdateXpress System Packs
- Lenovo recommends that you update the entire system to the latest UpdateXpress System Pack (UXSP) level before you deploy the server into a production environment. This includes system firmware, all adapter and hard-drive firmware, and the corresponding device drivers in the operating system.

Tip: Install all the hardware components (modules, adapters, and drives) and power on the system at least once before updating the entire system, so that everything will be activated, detected, and updated together.

Installing system firmware

If new system management controller firmware (IMM or XCC) is applied, either a system management controller restart (via the XCC/IMM web interface or CLI) or a full power cycle (unplug the server) will be required to activate the pending updates. A virtual reseat will also restart the controller (if the function is available in your server).

If new UEFI firmware is applied, a server reboot is required to activate the updates. If delayed activation is being used, such as in XClarity Administrator, then the updates will remain as pending (unapplied) on the system until server is restarted.

If the system management controller firmware update package also includes updated FPGA firmware (as indicated in the change history for the update), then both the system management controller will need to be restarted (via XCC/IMM web interface/CLI) and the server will need to be rebooted before the FPGA change becomes effective. A full power cycle (unplug the server) will achieve both.

Additional recommendations

Some additional recommendations when applying firmware updates:

- When installing new hardware

  If you install or upgrade hardware components later, make sure that you perform a full system update to ensure that the system can handle the new hardware, and that the newly installed components have the proper firmware and drivers.

- Updating firmware manually

  If you are updating individual firmware manually or via your own script but are not using the XClarity tools mentioned above, you should always update the BMC (XCC or IMM) first, restart the BMC and wait 5 minutes, then update UEFI, reboot the server, then update the rest of the system. This order ensures that critical dependencies are satisfied.

- Subscribe to updates on the Lenovo support site

  Make sure that you visit the Lenovo Support web site regularly, or that you subscribe to product notifications to be informed of critical updates for your devices. Then, plan your maintenance schedule accordingly.

Update process flow

Use the following flow chart to determine the best tool to be used when updating the firmware and device drivers, based on your environment.

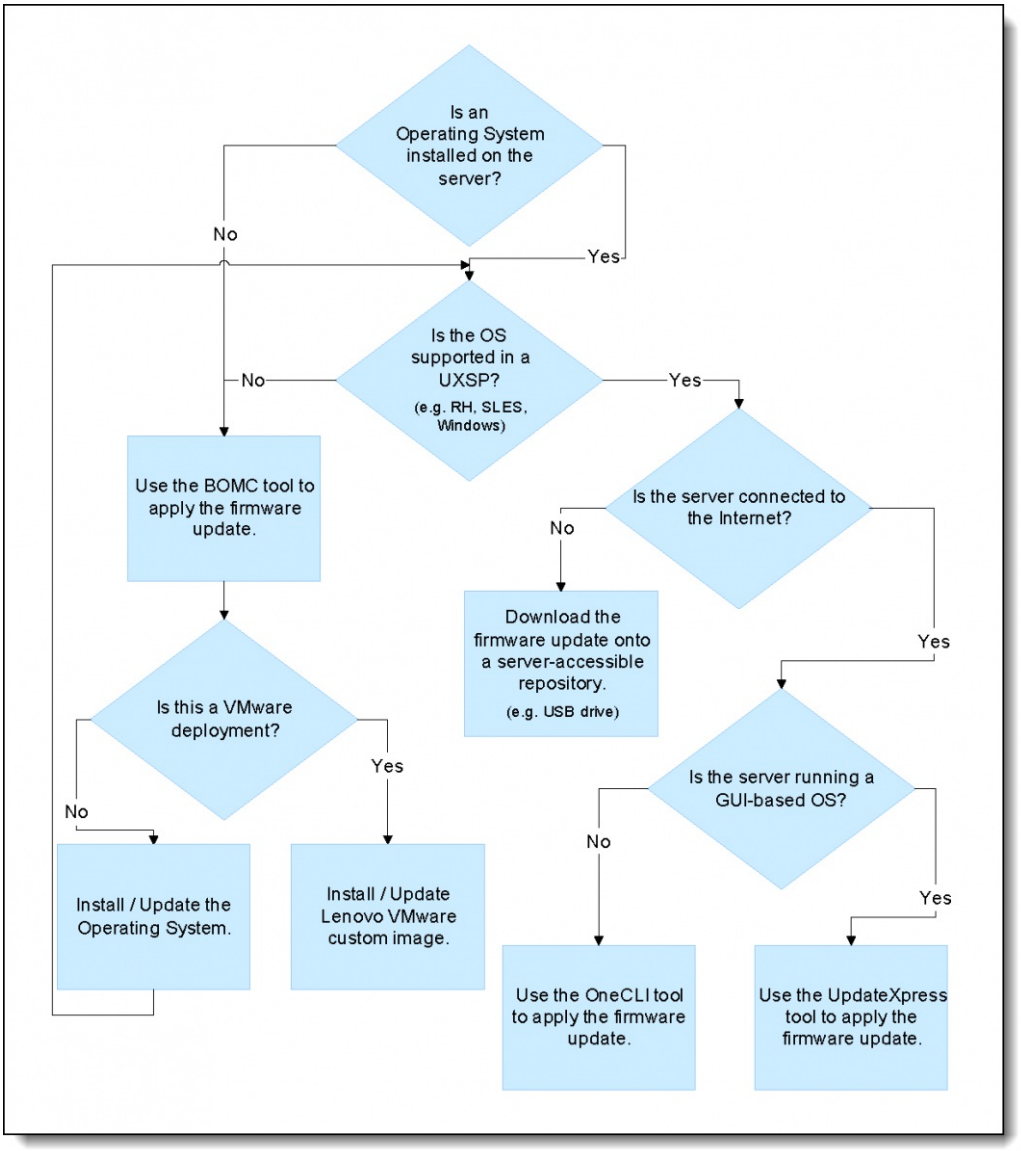

Figure 4. Update process flow

RAID setup for logical drives

For information on setting up RAID arrays on the SR630 V3 and SR650 V3, see the following pages on the Lenovo Docs web site:

- ThinkSystem SR630 V3 RAID Configuration
- ThinkSystem SR650 V3 RAID Configuration

Using RAID to store data remains one of the most common and cost-efficient methods to increase server's storage performance, availability, and capacity. Supported RAID levels varies by the storage controller configured in the server. For the RAID level supported by SR630 V3 and SR650 V3, see Technical specifications.

To create a RAID array in the XCC web interface, first select the RAID level as shown below.

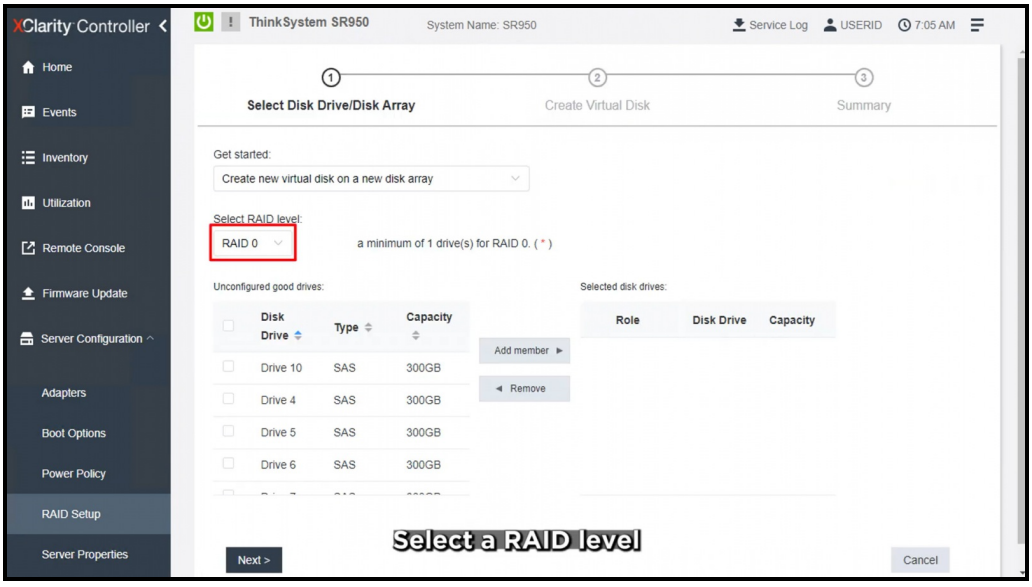

Figure 5. Select a RAID level

Follow the prompts, then click Start Creating to create the array.

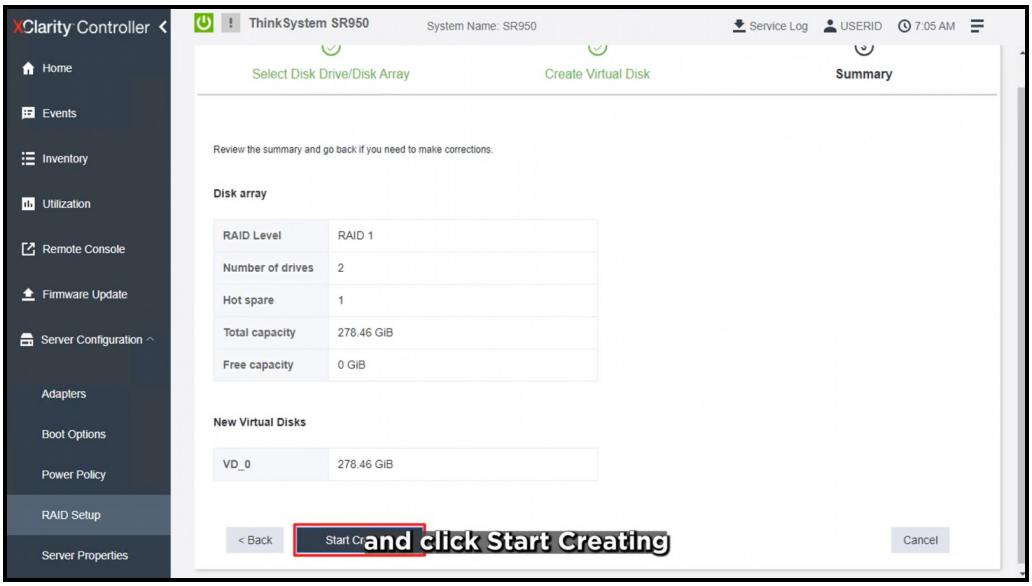

Figure 6. Click Start Creating

Once completed, a message will be displayed indicating that the virtual disk has been created.

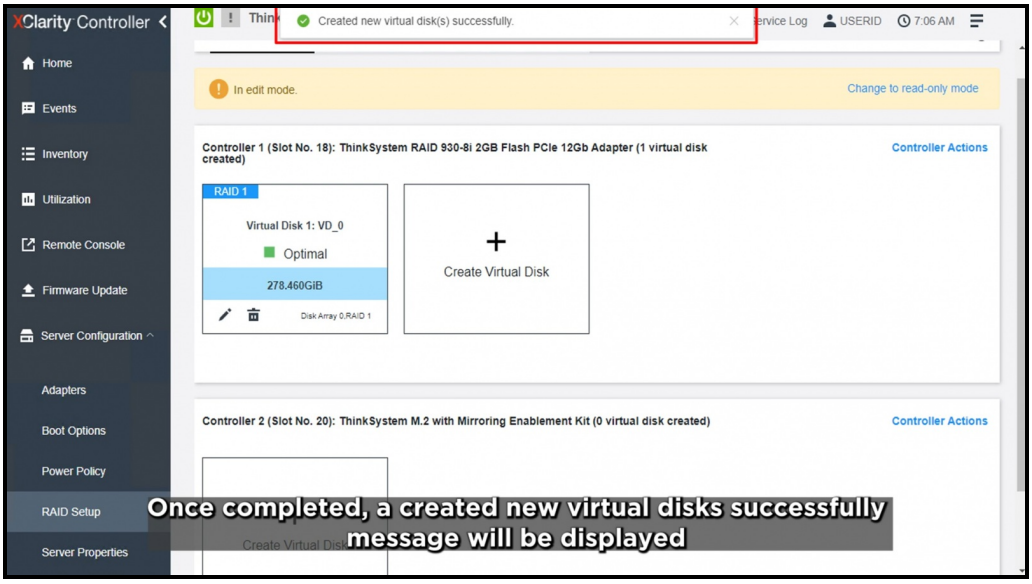

Figure 7. RAID array created

You could also follow this interactive guideline in our Youtube Channel: How to update firmware on Lenovo XClarity controller

You can configure RAID on the SR650 V3 and SR630 V3 using Lenovo XClarity Provisioning Manager V4. Details are at this documentation page:
https://pubs.lenovo.com/lxpm-v4/RAID_setup

You can also configure RAID on these servers using the XClarity Controller Web UI. Details on this documentation page:
https://pubs.lenovo.com/xcc2/dw1lm_c_ch6_configuringthestorage

The XCC2 Command Line Interface also supports RAID configuration. Details at this page:
https://pubs.lenovo.com/xcc2/dw1lm_c_ch7_commandlineinterface.html

Security procedures

To ensure your server is secure, following the guidance in the following paper:

How to Harden the Security of your ThinkSystem Server and Management Applications
https://lenovopress.lenovo.com/lp1260-how-to-harden-the-security-of-your-thinksystem-server

Topics in the paper:

- Hardening UEFI
- Hardening Lenovo XClarity Controller
- Hardening Lenovo XClarity Administrator
- Hardening Lenovo XClarity Orchestrator

XClarity Redfish integration

The Lenovo XClarity Controller provides a Redfish compliant set of easy-to-use REST APIs that can be used to access Lenovo XClarity Controller data and services from applications running outside of the Lenovo XClarity Controller framework.

This allows for easy integration of Lenovo XClarity Controller capabilities into other software, whether the software is running on the same system as the Lenovo XClarity Controller server, or on a remote system within the same network. These APIs are based on the industry standard Redfish REST API and are accessed via the HTTPS protocol.

Details about the Lenovo XClarity Controller Redfish REST API can be found at the following documentation page:
https://pubs.lenovo.com/xcc/rest_api

Lenovo provides open-source sample Redfish scripts that can be used as reference for developing software that communicates with Lenovo Redfish REST API. These sample scripts can be found here:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

DMTF specifications related to the Redfish API are available at: https://redfish.dmtf.org/. This website provides general specifications and other reference material on the Redfish REST API.

Alternative health monitoring using XCC

The XClarity Controller UI offers a system status page where you can view the server hardware status, event and audit logs, system status, maintenance history and alert recipients.

The following documentation links describe the available functions.

- Viewing the Health Summary/Active System Events
  Use the information in this topic to understand how to view the Health Summary/Active System Events.
- Viewing the System Information
  This topic explains how to obtain a summary of common server information.
- Viewing the System Utilization
  By clicking Utilization in the left pane, a summary of common server utilization information is provided.
- Viewing Event Logs
  The Event Log provides a historical list of all hardware and management events.
- Viewing Audit Logs
  The Audit Log provides a historical record of user actions, such as logging in to the XClarity Controller, creating a new user, and changing a user password.
- Viewing the Maintenance History
  The Maintenance History page includes information about the firmware update, configuration and hardware replacement history.
- Configuring Alert Recipients
  To add and modify email and syslog notifications or SNMP TRAP recipients, use the information in this topic.
- Capturing the latest OS failure screen data
  Use the information in this topic to capture and view an operating system failure screen.

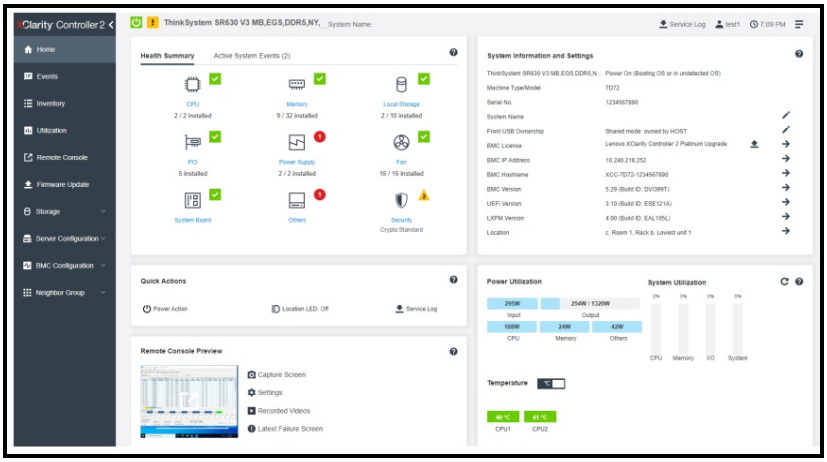

Figure 8. Health Summary page of XCC2

XClarity use of remote console for ISO installation

For guidance, see the following page in the Lenovo documentation, Enabling the remote console functionality.

XClarity Controller remote console functionality is available only in the XClarity Controller Advanced and XClarity Controller Enterprise features. If you do not have the privilege to operate the remote console, you will see a lock icon.

After you have purchased and obtained the activation key for the XClarity Controller Advanced upgrade install it using the instructions under Installing an activation key.

To use the remote console functionality, complete the following steps:

1. Click the image with a white diagonally pointing arrow in the Remote Console section of the XClarity Controller homepage or the Remote Console web page.
2. Select one of the following modes:
   - Start remote console in single-user mode
   - Start remote console in multiuser mode
3. Select whether or not to allow others to request to send a disconnection request to a remote console user when someone wishes to use the remote console feature and the feature is already in use in Single User Mode, or when the maximum number of users are using the remote console feature in Multi User Mode. The **No response time interval** specifies how long the XClarity Controller will wait before automatically disconnecting the user if no response is received to the disconnection request.
4. Select whether or not to allow record the latest three server boot videos, to allow record the latest three server crash videos, and to allow OS failure screen capture with HW error.
5. Click **Launch Remote Console** to open the remote console page in another tab. When all possible remote console sessions are in use, a dialog box will pop up. From this dialog box, the user can send a disconnection request to a remote console user who has enabled the setting to **Allow others to request my remote session disconnect**. The user can accept or deny the request to disconnect. If the user does not respond within the interval specified by the **No response time interval** setting, the user session will automatically be ended by the XClarity Controller.

todo: **these images are 6 years old**. The UEFI and LXPM screens don't look like this anymore. Please provide screenshots from the V3 servers.

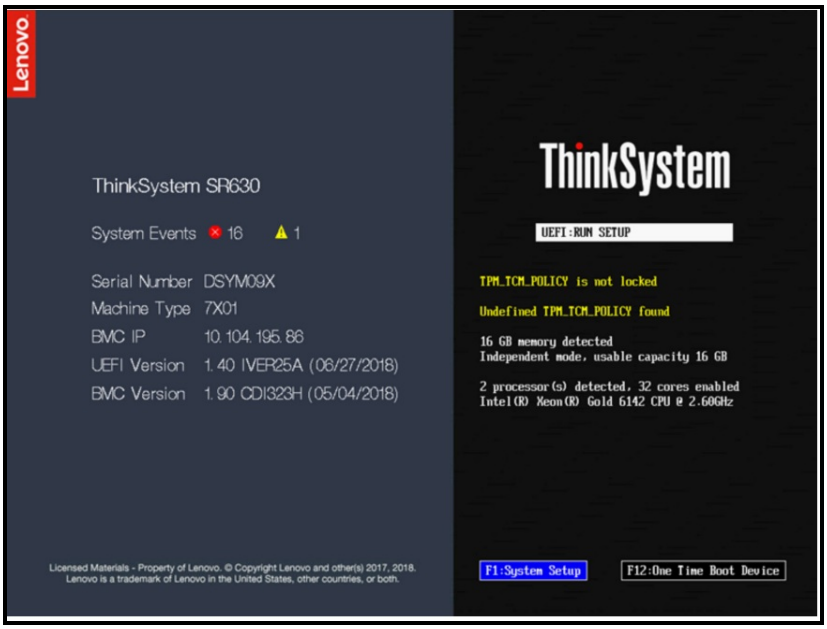

Figure 9. UEFI boot screen

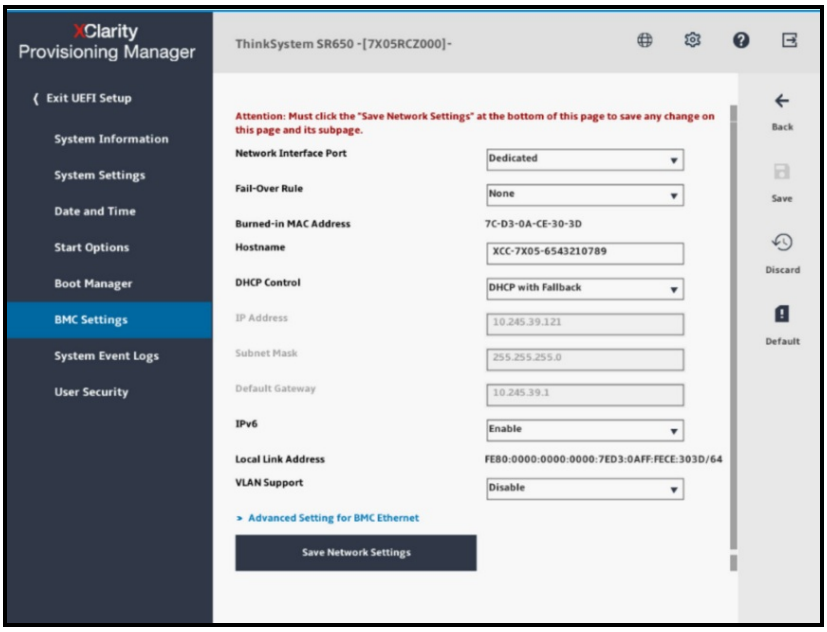

Figure 10. LXPM BMC Settings page

For more information

For more information about Veeam offerings from Lenovo, see the Veeam Software Solution Product Guide.

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, LP2100, was created or updated on November 26, 2024.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2100
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2100.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
ThinkSystem®
XClarity®

The following terms are trademarks of other companies:

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

PowerShell is a trademark of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.