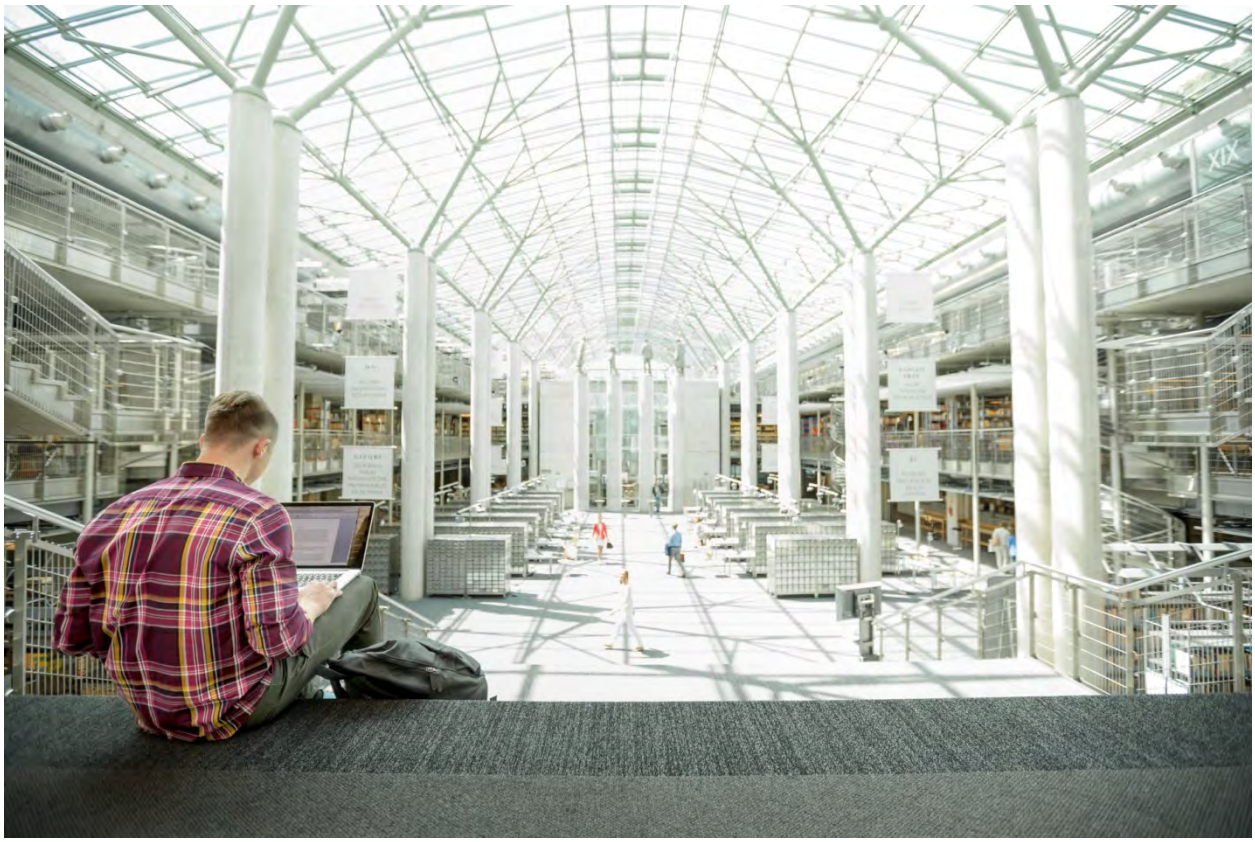
Cisco UCS Scale-Up Solution for SAP HANA on Cisco UCS M5 Rack Servers with SUSE Linux Enterprise Server for SAP Applications

Design and deploy a SAP HANA solution based on standalone Cisco UCS C-Series M5 rack servers with SUSE Linux Enterprise Server 12 SP4 for SAP Applications



Last Updated: May 16, 2019

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Contents

Executive summary 4
Solution overview 4
Introduction 4
Audience 4
Purpose of this document 5
What's new in this release? 5
Solution summary 5
Cisco UCS C480 M5 Rack Server 5
Cisco UCS C240 M5 Rack Server 6
Cisco UCS C220 M5 Rack Server 7
Infrastructure overview 8
Cisco UCS C480 M5 Rack Server 8
Cisco UCS C240 M5 Rack Server 9
Cisco UCS C220 M5 Rack Server 10
Solution design 12
SAP HANA system 12
Hardware requirements for the SAP HANA database 12
File system layout 12
Operating system 14
Deployment hardware and software 15
Preparing the SAP HANA scale-up node 16
Configuring the Cisco Integrated Management Controller 16
Launching the KVM console 20
Configuring BIOS settings 23
Rebooting the server to implement BIOS changes 30
Configuring RAID 30
Installing the operating system 42
Post-installation OS configuration 87
Configuring bonding for high availability 87
Preparing SAP HANA data, log, and shared file systems 92
Installing SAP HANA 98
Important SAP Notes 98
SAP HANA IMDB notes 98
Linux notes 98
Third-party software notes 98
SAP HANA virtualization notes 99
Performing an SAP HANA post-installation checkup 99
Commands for checking SAP HANA services 99
Tuning the SAP HANA performance parameters 100
Performing maintenance operations 100

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Maintaining the operating system 100
Prerequisites 100
Updating the OS 100
Updating SUSE online 101
Using YaST 101
Operating and maintaining SAP HANA 110
Monitoring SAP HANA 111
HDB info 111
Starting and stopping SAP HANA 112
HDB 114
Downloading revisions 114
For more information 114
Appendix: Solution variables used in this document 115

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Executive summary

Organizations in every industry are generating and using more data than ever before: from customer transactions and supplier delivery information to real-time user-consumption statistics. Without reliable infrastructure that can store, process, and analyze big data sets in real time, companies cannot use this information to their advantage. The Cisco® Scale-Up Solution for SAP HANA with the Cisco Unified Computing System™ (Cisco UCS®) using the Cisco UCS M5 rack server helps companies more easily harness information and make better business decisions that let them stay ahead of the competition. Our solutions help improve access to all your data to accelerate business decision making with policy-based, simplified management, lower deployment risk, and reduced total cost of ownership (TCO). Our innovations help enable you to unlock the intelligence in your data and interpret it with a new dimension of context and insight to help you gain a sustainable, competitive business advantage.

The Cisco solution for SAP HANA with the Cisco UCS C-Series M5 rack-mount server provides a robust platform for SAP HANA workloads in a single node.

Solution overview

This section introduces the solution discussed in this document.

Introduction

The Cisco UCS C480 M5 Rack Server supports a scale-up solution with pre-validated, ready-to-deploy infrastructure. Solution configuration and validation requires less time and is less complex than with a traditional data center deployment. The reference architecture discussed in this document demonstrates the resiliency and ease of deployment of an SAP HANA solution.

SAP HANA is SAP's implementation of in-memory database (IMDB) technology. The SAP HANA database takes advantage of the low-cost main memory (RAM), faster access, and data-processing capabilities of multicore processors to provide better performance for analytical and transactional applications. SAP HANA offers a multiple-engine, query-processing environment that supports relational data (with both row- and column-oriented physical representations in a hybrid engine) as well as graph and text processing for semi structured and unstructured data management within the same system. SAP HANA combines software components from SAP optimized for certified hardware. However, this solution has a preconfigured hardware setup and preinstalled software package that is dedicated to SAP HANA.

SAP HANA Tailored Datacenter Integration (TDI) offers a more open and flexible way to integrate SAP HANA into the data center by reusing existing enterprise storage hardware, thereby reducing hardware costs. With the introduction of SAP HANA TDI for shared infrastructure, the Cisco UCS Integrated Infrastructure solution provides the advantages of an integrated computing, storage, and network stack and the programmability of Cisco UCS. SAP HANA TDI enables organizations to run multiple SAP HANA production systems on a shared infrastructure. It also enables customers to run SAP application servers and an SAP HANA database hosted on the same infrastructure.

For more information about SAP HANA, see the SAP help portal: http://help.sap.com/hana/.

Audience

The intended audience for this document includes sales engineers, field consultants, professional services staff, IT managers, partner engineers, and customers deploying the Cisco solution for SAP HANA. External references are provided wherever applicable, but readers are expected to be familiar with the technology, infrastructure, and database security policies of the customer installation.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Purpose of this document

This document describes the steps required to deploy and configure a Cisco data center solution for SAP HANA. This document showcases one of the variants of Cisco's solution for SAP HANA. Although readers of this document are expected to have sufficient knowledge to install and configure the products used, configuration details that are important to the deployment of this solution are provided in this document.

What's new in this release?

Design and deploy a SAP HANA scale-up solution based on the standalone Cisco UCS C480 M5 Rack Server with SUSE Linux Enterprise Server (SLES) 12 SP4 for SAP Applications.

Solution summary

This section briefly describes the components of the solution.

Cisco UCS C480 M5 Rack Server

The Cisco Scale-Up Solution for SAP HANA uses the Cisco UCS C480 M5 Rack Server. Tables 1, 2, and 3 summarize the server specifications and show proposed disk configurations for the SAP HANA use case.

Table 1. Overview of Cisco UCS C480 M5 Rack Server configuration

CPU specifications	2.70-GHz Intel® Xeon® Platinum 8280L processor: Quantity 2 or 4	
Possible memory configurations	Analytics: • 16-GB DDR4: Quantity 12 (192 GB) • 32-GB DDR4: Quantity 12 (384 GB) • 32-GB DDR4: Quantity 24 (768 GB) • 64-GB DDR4: Quantity 24 (1.5 TB) • 128-GB DDR4: Quantity 24 (3 TB)	SAP Business Suite on SAP HANA (SoH): • 16-GB DDR4: Quantity 12 (192 GB) • 32-GB DDR4: Quantity 12 (384 GB) • 32-GB DDR4: Quantity 24 (768 GB) • 64-GB DDR4: Quantity 24 (1.5 TB) • 128-GB DDR4: Quantity 24 (3 TB) • 128-GB DDR4: Quantity 48 (6 TB)
Hard-disk drive (HDD) type and quantity	Any of the following: 1.8-TB 10,000-rpm SAS drive: Quantity 20 3.8-TB solid-state disk (SSD): Quantity 8 3.8-TB SSD: Quantity 3 (for up to 1.5-TB memory configurations)	
BIOS	C480M5.4.0.4b.0.0407190307	
Cisco Integrated Management Controller (IMC) firmware	4.0(4b)	
LSI MegaRAID controller	Cisco 12-Gbps SAS modular RAID controller	
Network card	• Cisco UCS Virtual Interface Card (VIC) 1385: Quantity 1 • For 10-Gbps connectivity: Onboard Intel 1 Gigabit Ethernet controller: Quantity 2 • Onboard Intel 10BASE-T Ethernet controller: Quantity 2	
Power supply	Redundant power supplies: Quantity 4	

Table 2. Cisco UCS C480 M5 proposed disk layout

Disk	Disk type	Drive group	RAID level	Virtual drive
Slot (1 through 20)	SAS HDD	DG0	50	VD0
Slot (1 through 8)	SSD	DG0	5	VD0
Slot (1 through 3; up to 1.5 TB of RAM)	SSD	DG0	5	VD0

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 3. Cisco UCS C480 M5 proposed disk configuration

Drives used	RAID type	Used for	File system
Any of the following: • 20 x 1.8-TB SAS HDD • 8 x 3.8-TB SSD • 3 x 3.8-TB SSD	Any of the following: • RAID 50 • RAID 5 • RAID 5	Operating system	Ext3
		Data file system	XFS
		Log file system	XFS
		SAP HANA shared file system	XFS

Cisco UCS C240 M5 Rack Server

The Cisco Scale-Up Solution for SAP HANA can also be deployed on the Cisco UCS C240 M5 Rack Server. Tables 4, 5, and 6 summarize the server specifications and show proposed disk configurations for the SAP HANA use case.

Table 4. Overview of Cisco UCS C240 M5 Rack Server configuration

CPU specifications	2.70-GHz Intel Xeon Platinum 8280L processor: Quantity 2
Possible memory configurations	Analytics: • 16-GB DDR4: Quantity 12 (192 GB) • 32-GB DDR4: Quantity 12 (384 GB) • 32-GB DDR4: Quantity 24 (768 GB) • 64-GB DDR4: Quantity 24 (1.5 TB) • 128-GB DDR4: Quantity 24 (3 TB)
HDD type and quantity	Any of the following: • 1.8-TB 10,000-rpm SAS drive: Quantity 20 • 3.8-TB SSD: Quantity 8 • 3.8-TB SSD: Quantity 8 • 3.8-TB SSD: Quantity 3 (for up to 1.5-TB memory configurations)
BIOS	C480M5.4.0.4b.0.0407190307
Cisco IMC firmware	4.0(4b)
Network card	Cisco UCS VIC 1385: Quantity 1 For 10-Gbps connectivity: • Onboard Intel 1 Gigabit Ethernet controller: Quantity 2 • Onboard Intel 10BASE-T Ethernet controller: Quantity 2
Power supply	Redundant power supplies: Quantity 2

Table 5. Cisco UCS C240 M5 proposed disk layout

Disk	Disk type	Drive group	RAID level	Virtual drive
Slot (1 through 20)	SAS HDD	DG0	50	VD0
Slot (1 through 8)	SSD	DG0	5	VD0
Slot (1 through 3; up to 1.5 TB of RAM)	SSD	DG0	5	VD0

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 6. Cisco UCS C240 M5 proposed disk configuration

Drives used	RAID type	Used for	File system
Any of the following: • 20 x 1.8-TB SAS HDD • 8 x 3.8-TB SSD • 3 x 3.8-TB SSD	Any of the following: • RAID 50 • RAID 5 • RAID 5	Operating system	Ext3
		Data file system	XFS
		Log file system	XFS
		SAP HANA shared file system	XFS

Cisco UCS C220 M5 Rack Server

The Cisco Scale-Up Solution for SAP HANA can also be deployed on the Cisco UCS C220 M5 Rack Server. Tables 7, 8, and 9 summarize the server specifications and show proposed disk configurations for the SAP HANA use case.

Table 7. Overview of Cisco UCS C220 M5 Rack Server configuration

CPU specifications	2.70-GHz Intel Xeon Platinum 8280L processor: Quantity 2
Possible memory configurations	Analytics: • 16-GB DDR4: Quantity 12 (192 GB) • 32-GB DDR4: Quantity 12 (384 GB) • 32-GB DDR4: Quantity 24 (768 GB) • 64-GB DDR4: Quantity 24 (1.5 TB) • 128-GB DDR4: Quantity 24 (3 TB)
HDD type and quantity	Any of the following: • 3.8-TB SSD: Quantity 8 • 3.8-TB SSD: Quantity 3 (for up to 1.5-TB memory configurations)
BIOS	C480M5.4.0.4b.0.0407190307
Cisco IMC firmware	4.0(4b)
Network card	Cisco UCS VIC 1385: Quantity 1 For 10-Gbps connectivity: • Onboard Intel 1 Gigabit Ethernet controller: Quantity 2 • Onboard Intel 10BASE-T Ethernet controller: Quantity 2
Power supply	Redundant power supplies: Quantity 2

Table 8. Cisco UCS C220 M5 proposed disk layout

Disk	Disk type	Drive group	RAID level	Virtual drive
Slot (1 through 8)	SSD	DG0	5	VD0
Slot (1 through 3; up to 1.5 TB of RAM)	SSD	DG0	5	VD0

Table 9. Cisco UCS C220 M5 proposed disk configuration

Drives used	RAID type	Used for	File system
Any of the following: • 8 x 3.8-TB SSD • 3 x 3.8-TB SSD	Any of the following: • RAID 5 • RAID 5	Operating system	Ext3
		Data file system	XFS
		Log file system	XFS
		SAP HANA shared file system	XFS

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Infrastructure overview

The Cisco Scale-Up Solution for SAP HANA uses the Cisco UCS M5 generation of Cisco UCS C-Series Rack Servers.

Cisco UCS C480 M5 Rack Server

The Cisco UCS C480 M5 Rack Server (Figure 1) can be deployed as a standalone server or in a Cisco UCS managed environment. When used in combination with Cisco UCS Manager, the C480 M5 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements. Cisco UCS Manager uses service profiles, templates, and policy-based management to enable rapid deployment and help ensure deployment consistency. It also enables end-to-end server visibility, management, and control in both virtualized and bare-metal environments.

The C480 M5 is a storage- and I/O-optimized enterprise-class rack server that delivers industry-leading performance for:

- IMDBs
- Big data analytics
- Virtualization and virtual desktop infrastructure (VDI) workloads
- Bare-metal applications

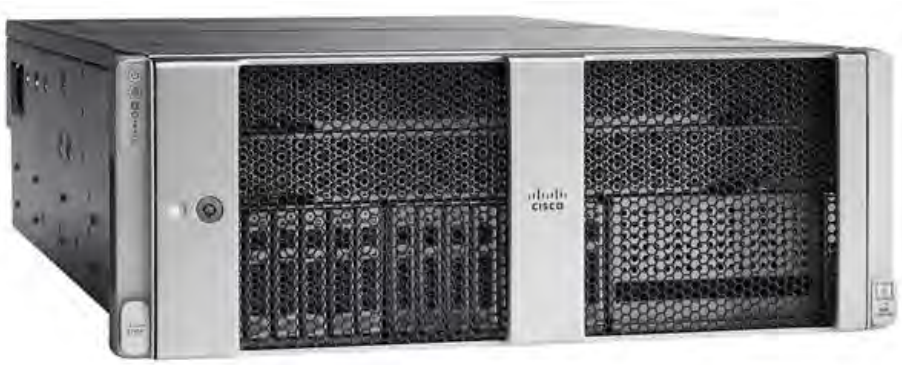
It delivers outstanding levels of expandability and performance for standalone or Cisco UCS managed environments in a 4-rack-unit (4RU) form factor. And because of its modular design, you pay for only what you need.

The C480 M5 offers these capabilities:

- Latest Intel Xeon Scalable processors with up to 28 cores per socket and support for two- or four-processor configurations
- 2933-MHz DDR4 memory and 48 DIMM slots for up to 6 TB of total memory
- 12 PCI Express (PCIe) 3.0 slots
- Six x8 full-height, full-length slots
- Six x16 full-height, full-length slots
- Flexible storage options with support up to 32 small-form-factor (SFF) 2.5-inch, SAS, SATA, and PCIe Non-Volatile Memory Express (NVMe) disk drives
- Cisco 12-Gbps SAS modular RAID controller in a dedicated slot
- Internal Secure Digital (SD) and M.2 boot options
- Dual embedded 10 Gigabit Ethernet LAN-on-motherboard (LOM) ports

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 1. Cisco UCS C480 M5 Rack Server



Cisco UCS C240 M5 Rack Server

The Cisco UCS C240 M5 Rack Server (Figure 2) is a 2-socket, 2RU rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, from big data and analytics to collaboration. Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of a Cisco UCS managed environment to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' TCO and increase their business agility.

In response to ever-increasing computing and data-intensive real-time workloads, the enterprise-class C240 M5 server extends the capabilities of the Cisco UCS portfolio in a 2RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, and five times more NVMe PCIe SSDs than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The C240 M5 delivers outstanding storage expandability with exceptional performance, with:

- Latest Intel Xeon Scalable CPUs with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Intel 3D XPoint-ready support, with built-in support for next-generation nonvolatile memory technology
- Up to 26 hot-swappable SFF 2.5-inch drives, including 2 rear hot-swappable SFF drives (up to 10 support NVMe PCIe SSDs on the NVMe-optimized chassis version), or 12 large-form-factor (LFF) 3.5-inch drives plus 2 rear hot-swappable SFF drives
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- Modular LOM (mLOM) slot that can be used to install a Cisco UCS VIC without consuming a PCIe slot, supporting dual 10- or 40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LOM ports
- Modular M.2 or SD cards that can be used for bootup
- High performance for data-intensive applications

The Cisco UCS C240 M5 Rack Server is well-suited for a wide range of enterprise workloads, including:

- Big data and analytics
- Collaboration

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- Small and medium-sized business (SMB) databases
- Virtualization and consolidation
- Storage servers
- High-performance appliances

C240 M5 servers can be deployed as standalone servers or in a Cisco UCS managed environment. When used in combination with Cisco UCS Manager, the C240 M5 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements.

Cisco UCS Manager uses service profiles, templates, and policy-based management to enable rapid deployment and help ensure deployment consistency. If also enables end-to-end server visibility, management, and control in both virtualized and bare-metal environments.

Figure 2. Cisco UCS C240 M5 Rack Server



Cisco UCS C220 M5 Rack Server

The Cisco UCS C220 M5 Rack Server (Figure 3) is among the most versatile general-purpose enterprise infrastructure and application servers in the industry. It is a high-density 2-socket rack server that delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications. The Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of Cisco UCS to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' TCO and increase their business agility.

The Cisco UCS C220 M5 server extends the capabilities of the Cisco UCS portfolio in a 1RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, 20 percent greater storage density, and five times more PCIe NVMe SSDs than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The C220 M5 server delivers outstanding levels of expandability and performance in a compact package, with:

- Latest Intel Xeon Scalable CPUs with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Intel 3D XPoint-ready support, with built-in support for next-generation nonvolatile memory technology
- Up to 10 SFF 2.5-inch drives or 4 LFF 3.5-inch drives (77 TB of storage capacity with all NVMe PCIe SSDs)
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- mLOM slot that can be used to install a Cisco UCS VIC without consuming a PCIe slot, supporting dual 10- or 40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LOM ports
- High performance for data-intensive applications

The Cisco UCS C220 M5 Rack Server is well-suited for a wide range of enterprise workloads, including:

- Big data and analytics
- Collaboration
- SMB databases
- Virtualization and consolidation
- Storage servers
- High-performance appliances

C220 M5 servers can be deployed as standalone servers or in a Cisco UCS managed environment. When used in combination with Cisco UCS Manager, the C220 M5 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements.

Cisco UCS Manager uses service profiles, templates, and policy-based management to enable rapid deployment and help ensure deployment consistency. If also enables end-to-end server visibility, management, and control in both virtualized and bare-metal environments.

Figure 3. Cisco UCS C220 M5 Rack Server



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Solution design

This section describes the SAP HANA system requirements defined by SAP and the architecture of the Cisco UCS solution for SAP HANA.

SAP HANA system

An SAP HANA scale-up system on a single server is the simplest of the SAP HANA installation types. You can run an SAP HANA system entirely on one host and then scale the system up as needed. All data and processes are located on the same server and can be accessed locally. For this option the network must have at least one 1 Gigabit Ethernet access network and one 10 Gigabit Ethernet storage network.

Hardware requirements for the SAP HANA database

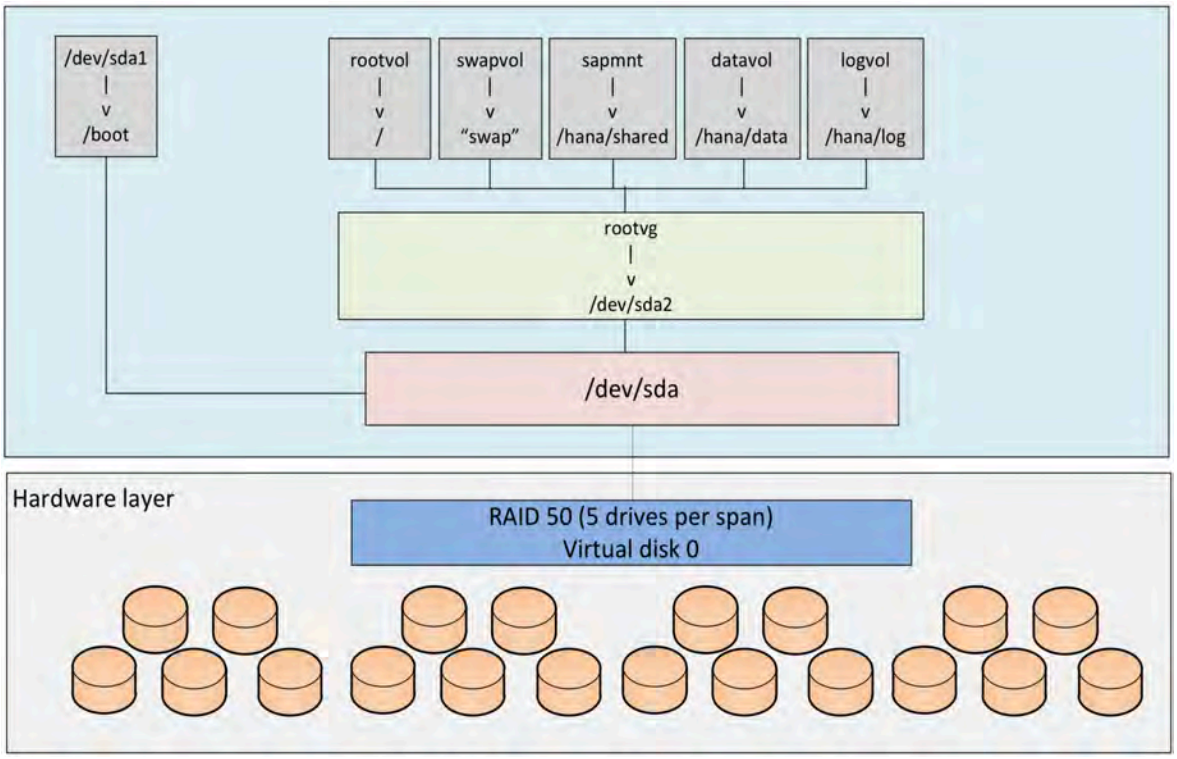
SAP defines hardware and software requirements for running SAP HANA systems. For the latest information about the CPU and memory configurations supported for SAP HANA, see https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/appliances.html.

Note: This document does not cover the updated information published by SAP. Additional information is available at http://saphana.com.

File system layout

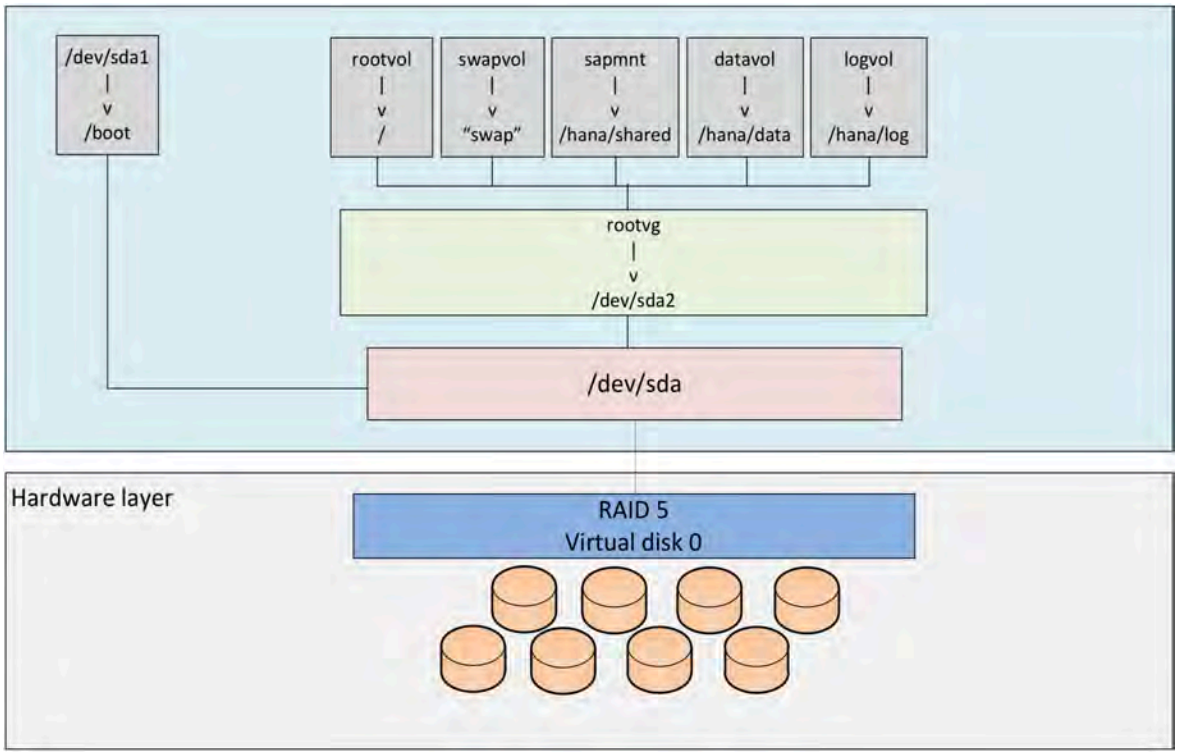
Figures 4, 5, and 6 show the file system layouts and the storage sizes required to install and operate SAP HANA. When installing SAP HANA on a host, specify the mount point for the installation binaries (/hana/shared/<SID>), data files (/hana/data/<sid>), and log files (/hana/log/<sid>), where sid is the instance identifier of the SAP HANA installation.

Figure 4. Proposed disk layout with partition mapping with 20 SAS drives



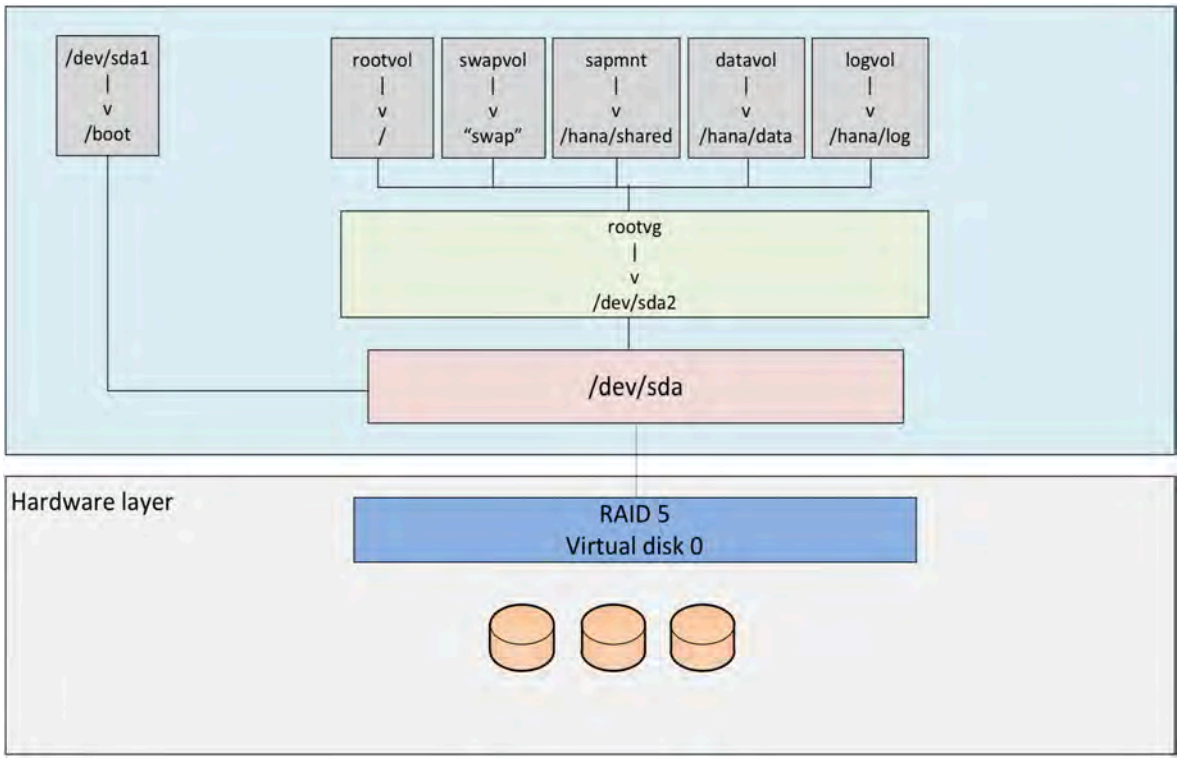
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 5. Proposed disk layout with partition mapping with 8 SSD drives



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 6. Proposed disk layout with partition mapping with 3 SSD drives (up to 1.5-TB memory configurations)



The storage size for the file system is based on the amount of memory on the SAP HANA host. Here are some sample file system sizes for a single-node system with 3 TB of memory:

- /hana/shared: 1 x memory (3 TB)
- /hana/data: 3 x memory (9 TB)
- /hana/log: 1 x memory (512 GB)

Note: For solutions based on the Intel Xeon Platinum processor, the size of the log volume (/hana/log) must be as follows:

- Half of the server memory for systems of 256 GB of memory or less
- Minimum of 512 GB for systems with 512 GB of memory or more

Operating system

SAP HANA supports the following operating systems:

- SUSE Linux Enterprise Server (SLES) for SAP Applications
- Red Hat Enterprise Linux (RHEL) for SAP Applications

Note: This document provides installation steps for SLES for SAP 12 SP2.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Deployment hardware and software

This section is intended to enable you to fully configure the customer environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. Table 10 lists the configuration variables that are used throughout this document. You can complete this table using your specific site variables and use it in implementing the configuration steps presented in this document.

Table 10. Configuration variables

Variable	Description	Customer implementation value
<<var_cimc_ip_address>>	Cisco UCS C480 M5 server's IMC IP address	
<<var_cimc_ip_netmask>>	Cisco UCS C480 M5 server's IMC network netmask	
<<var_cimc_gateway_ip>>	Cisco UCS C480 M5 server's IMC network gateway IP address	
<<var_raid50_vd_name>>	Name for virtual drive VD0 during RAID configuration	
<<var_hostname.domain>>	SAP HANA node's fully qualified domain name (FQDN)	
<<var_sys_root-pw>>	SAP HANA node's root password	
<<var_lvm_vg_name>>	SAP HANA node's OS logical volume management (LVM) volume group name	
<<var_mgmt_ip_address>>	SAP HANA node's management and administration IP address	
<<var_mgmt_nw_netmask>>	SAP HANA node's management network netmask	
<<var_mgmt_gateway_ip>>	Cisco UCS C480 M5 server's management and administrative network gateway IP address	
<<var_mgmt_netmask_prefix>>	Netmask prefix in Classless Inter-Domain Routing (CIDR) notation	

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Preparing the SAP HANA scale-up node

This section discusses how to prepare the SAP HANA scale-up node for the SAP HANA installation.

Configuring the Cisco Integrated Management Controller

To configure the on-board IMC, you should connect a keyboard, video, and mouse (KVM) switch to the server.

1. After everything is connected, turn on the power to the server (Figures 7 and 8).

Figure 7. BIOS POST screen



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

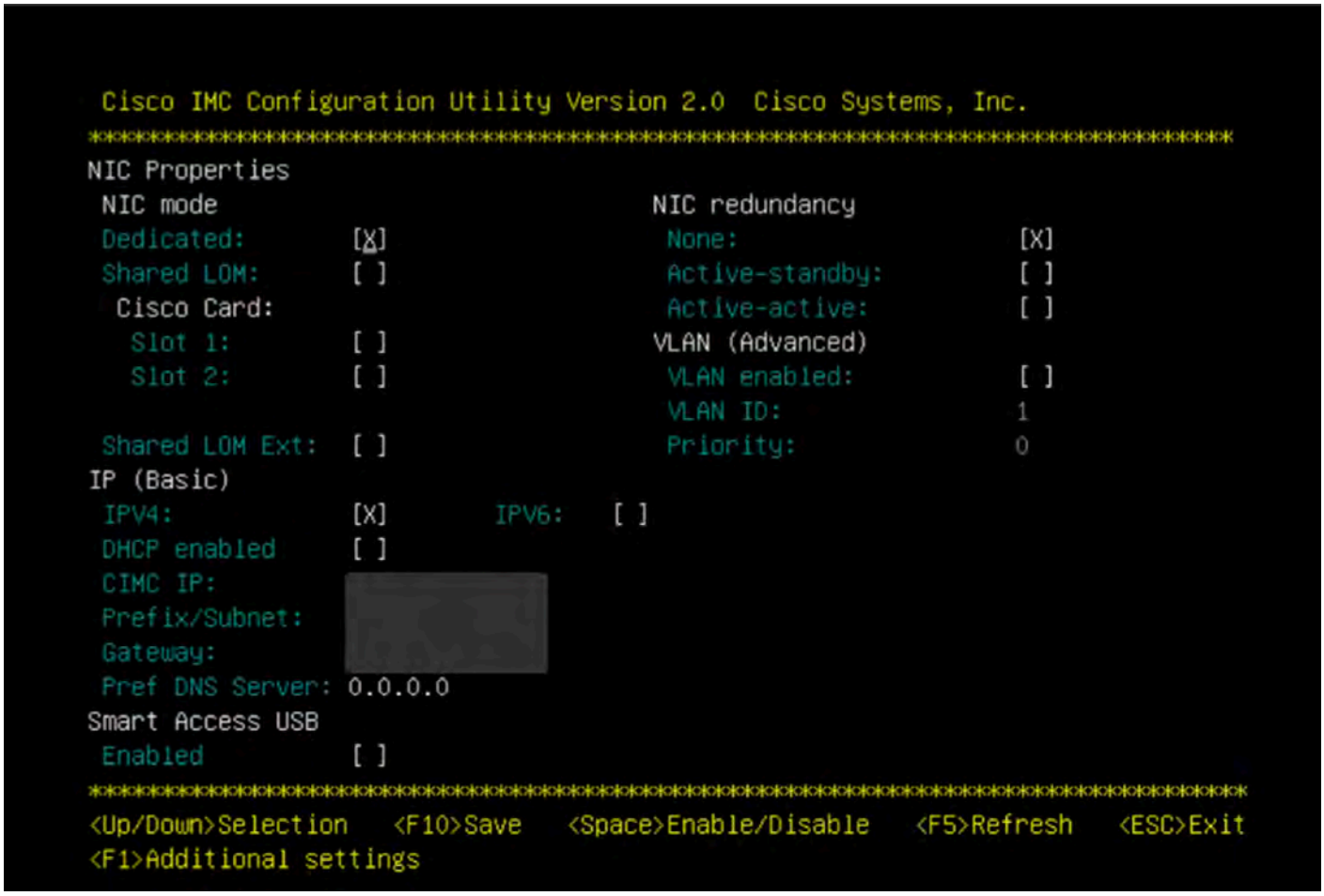
Figure 8. Bios POST screen (continued)



2. Press F8 to display the IMC configuration (Figure 9).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 9. Cisco UCS C480 IMC configuration view (local display)



3. Use the console network IP address <<var_cimc_ip_address>>, netmask <<var_cimc_ip_netmask>>, and gateway <<var_cimc_gateway>> for the IPv4 settings of the IMC. Select None for network interface card (NIC) redundancy.
4. Press F10 to save configuration and exit the utility.
5. Open a web browser on a computer on the same network with Java and Adobe Flash installed.
6. Enter the IMC IP address of the Cisco UCS C480 M5 server: http://<<var_cimc_ip_address>>.
7. Enter the login credentials as updated in the IMC configuration. The default user name and password are **admin** and **password** (Figure 10).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 10. Cisco IMC login screen

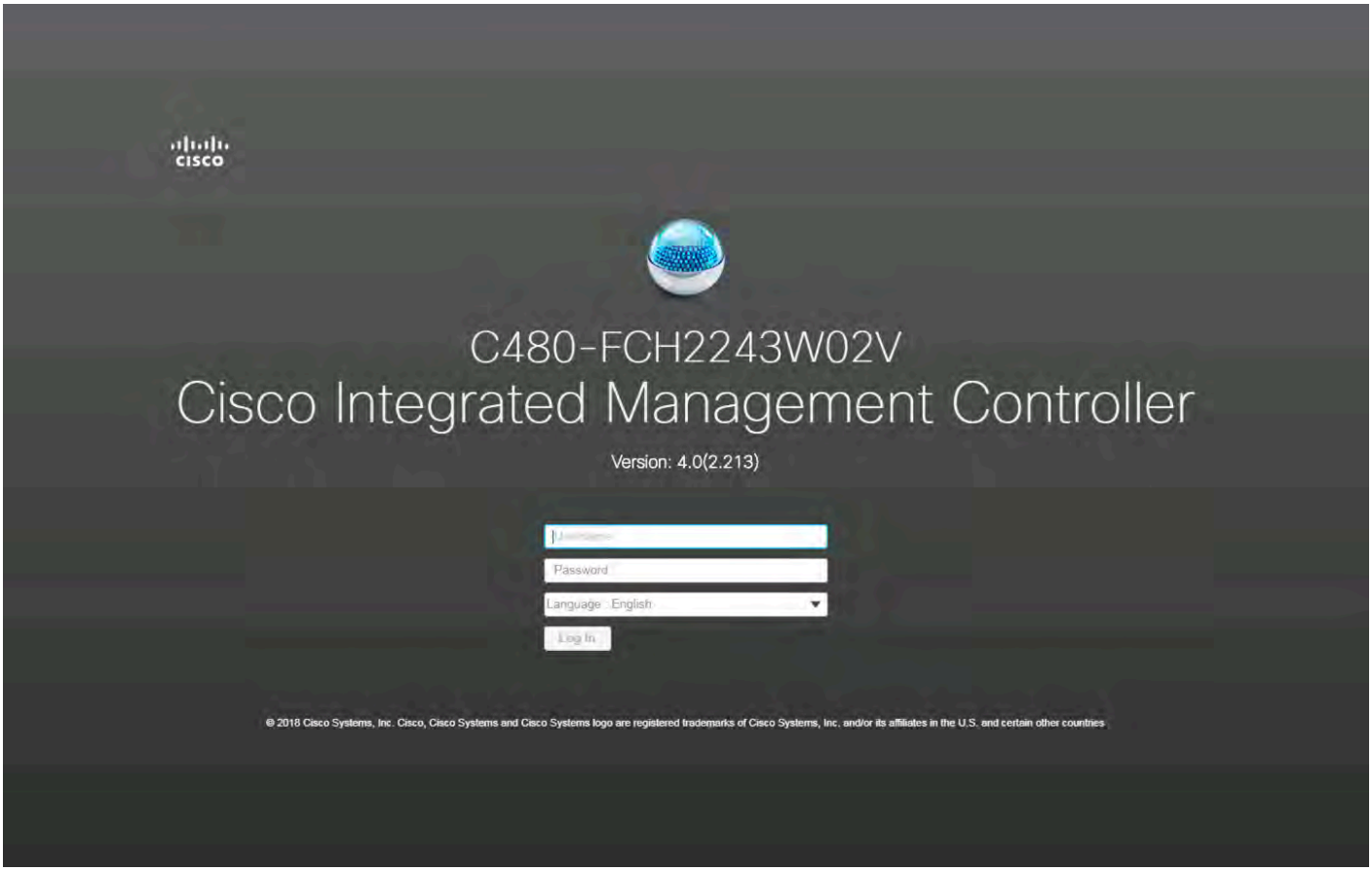
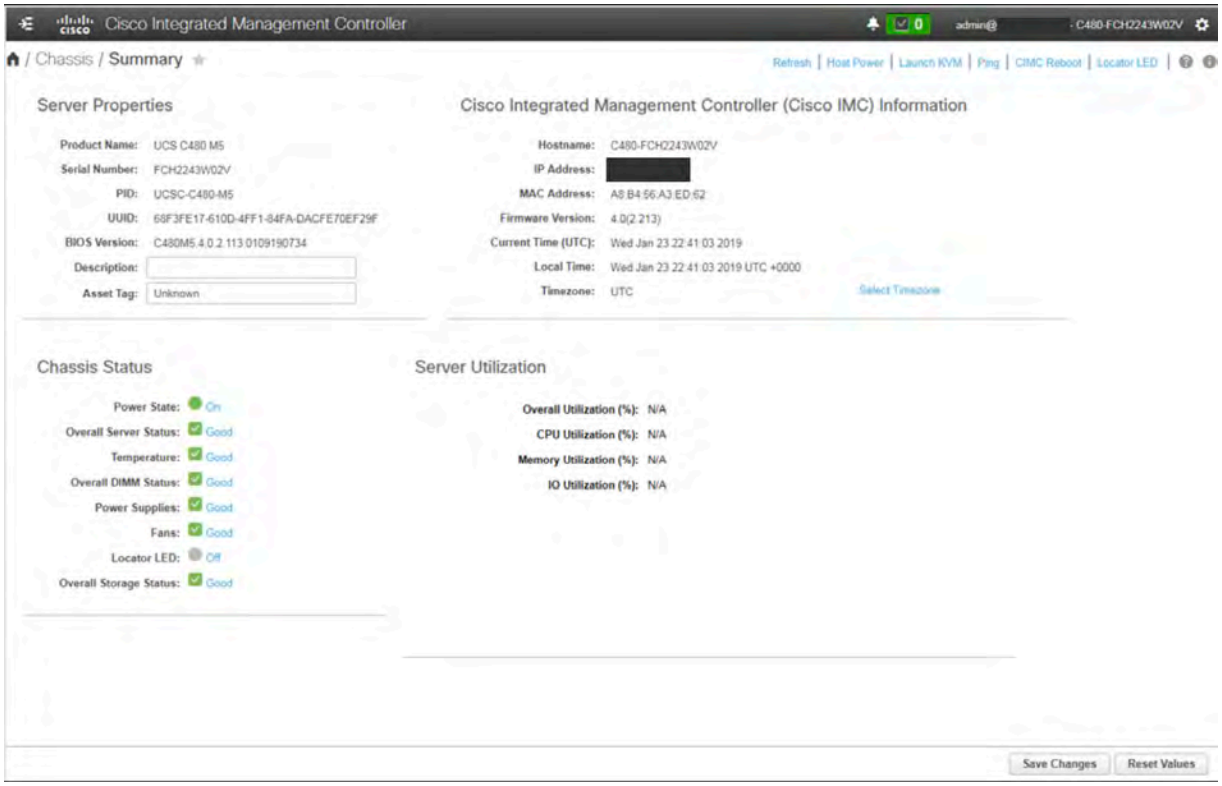


Figure 11 shows the results.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 11. Cisco IMC summary screen



Launching the KVM console

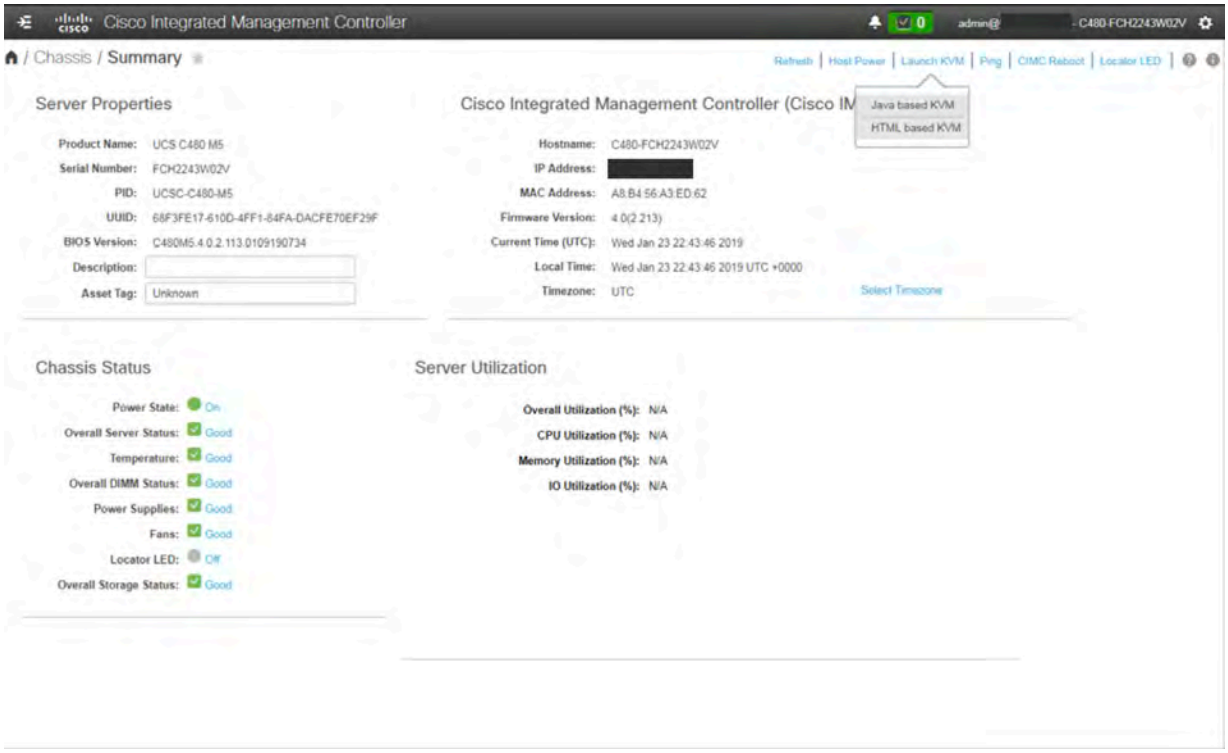
You next need to launch the KVM console and map the SLES 12 for SAP SP2 DVD ISO file for the installation.

1. Click Launch KVM in the top-left corner of the IMC home screen (Figure 12).

   Starting with Cisco IMC Release 3.0, two options are available for launching the KVM: one using the Java console and another using the browser-based HTML KVM console. In this example, the HTML KVM console has been used.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 12. Cisco IMC home screen



2. After you select the HTML-based console, a certificate confirmation window appears. Click the provided hyperlink to continue (Figure 13).

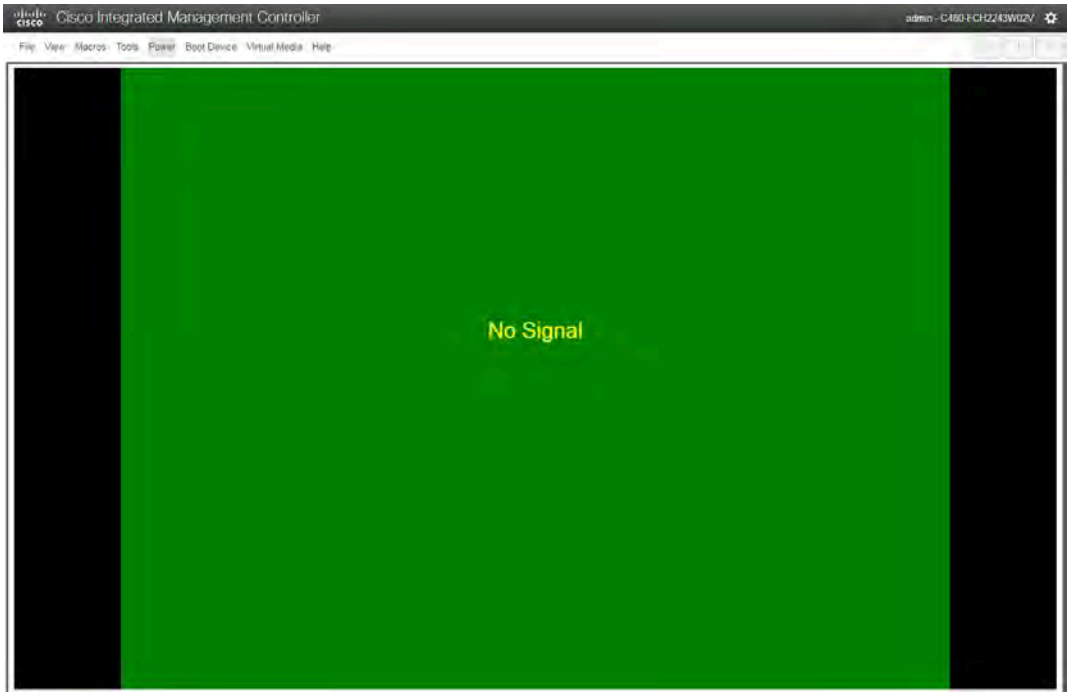
Figure 13. Click the hyperlink to load the KVM application



The KVM window will appear (Figure 14).

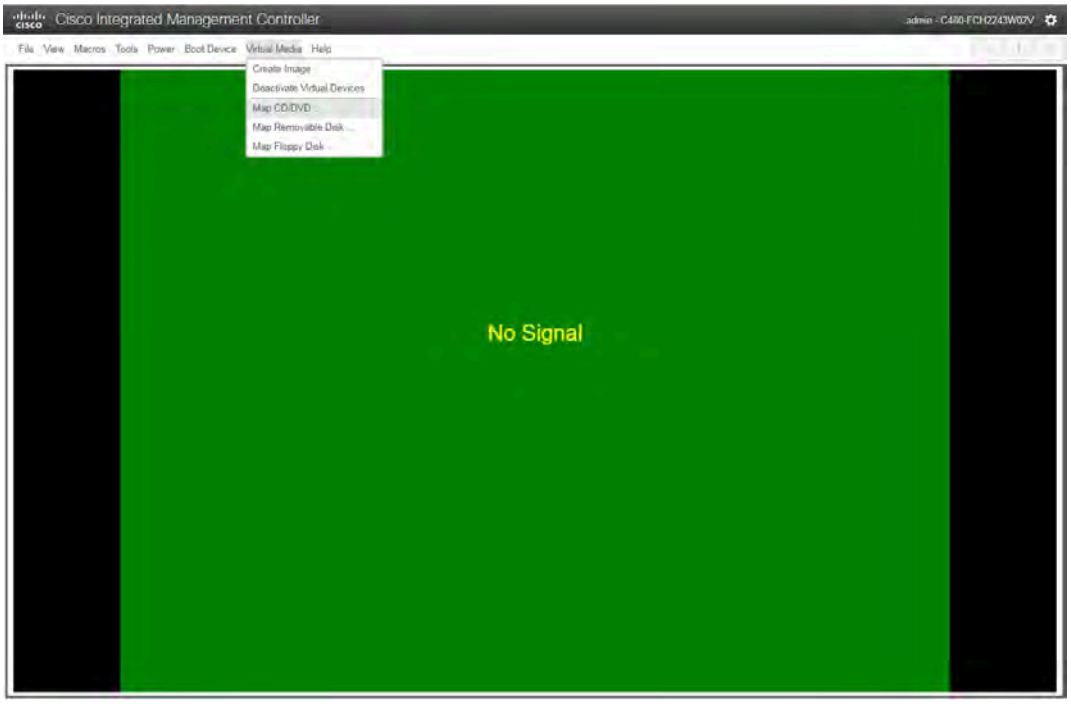
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 14. KVM window



3. In the menu bar at the top of the KVM window, choose Virtual Media > Activate Virtual Devices > Map CD/DVD (Figure 15).

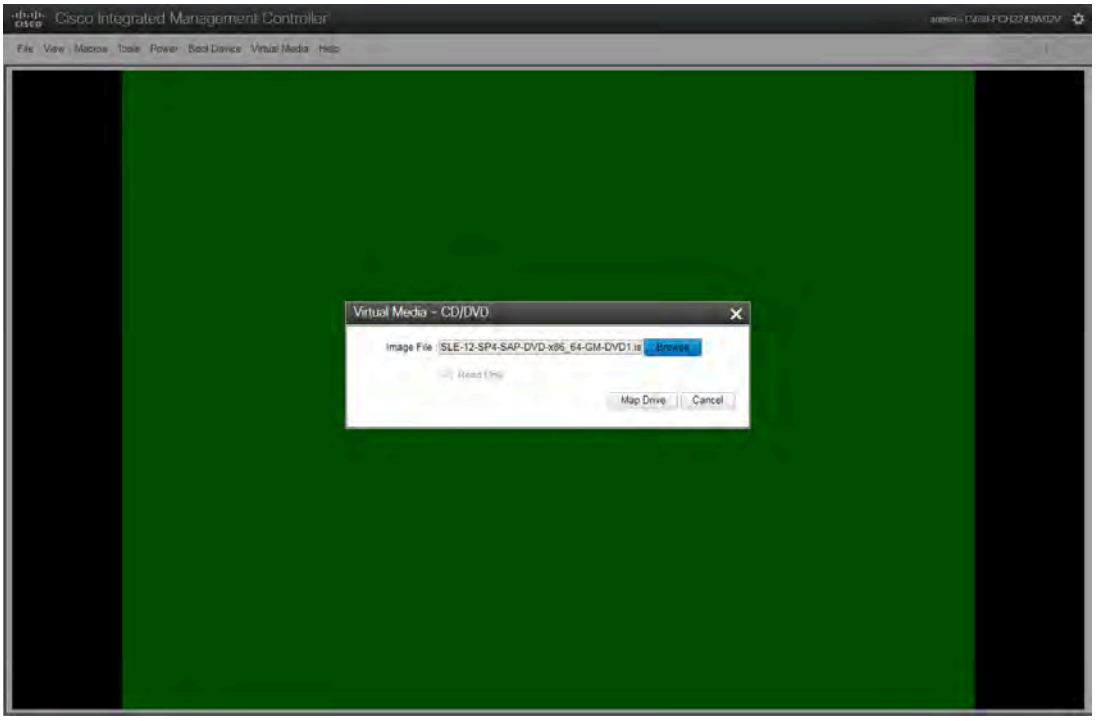
Figure 15. Beginning the CD/DVD mapping process



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

4. Browse for the SLES 12 for SAP SP4 DVD ISO file and click Map Drive (Figure 16).

Figure 16. Click Map Drive



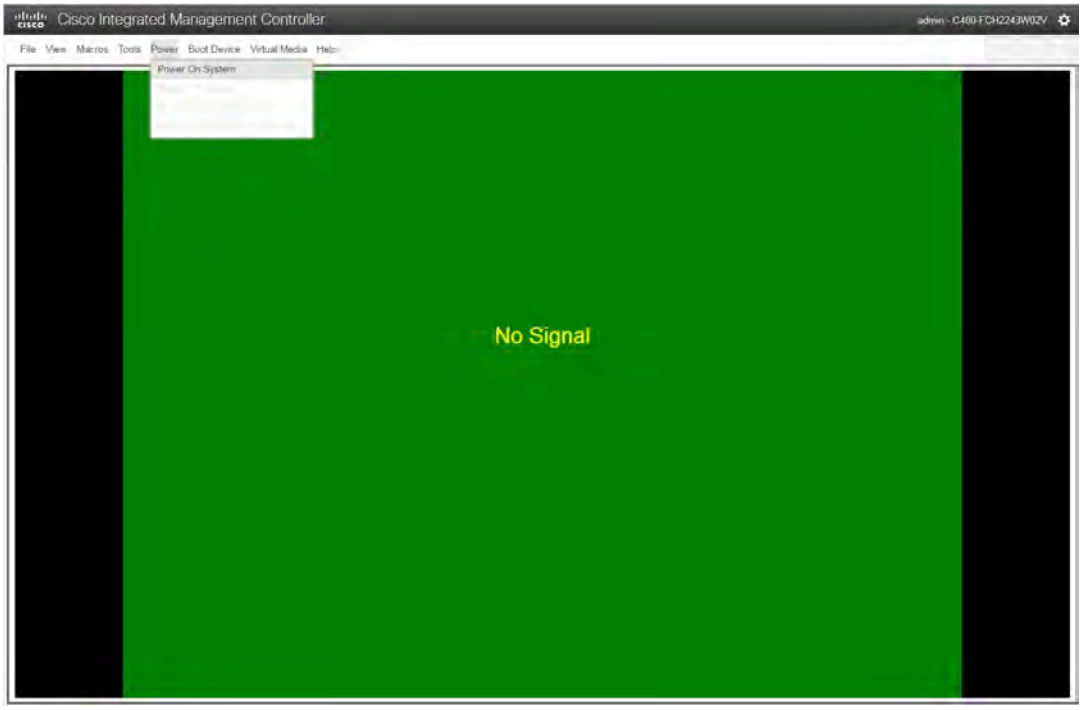
Configuring BIOS settings

You need to power on the server and configure some BIOS settings before proceeding with the RAID configuration.

1. From the menu bar at the top of the KVM window, choose Power > Power on System (Figure 17).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

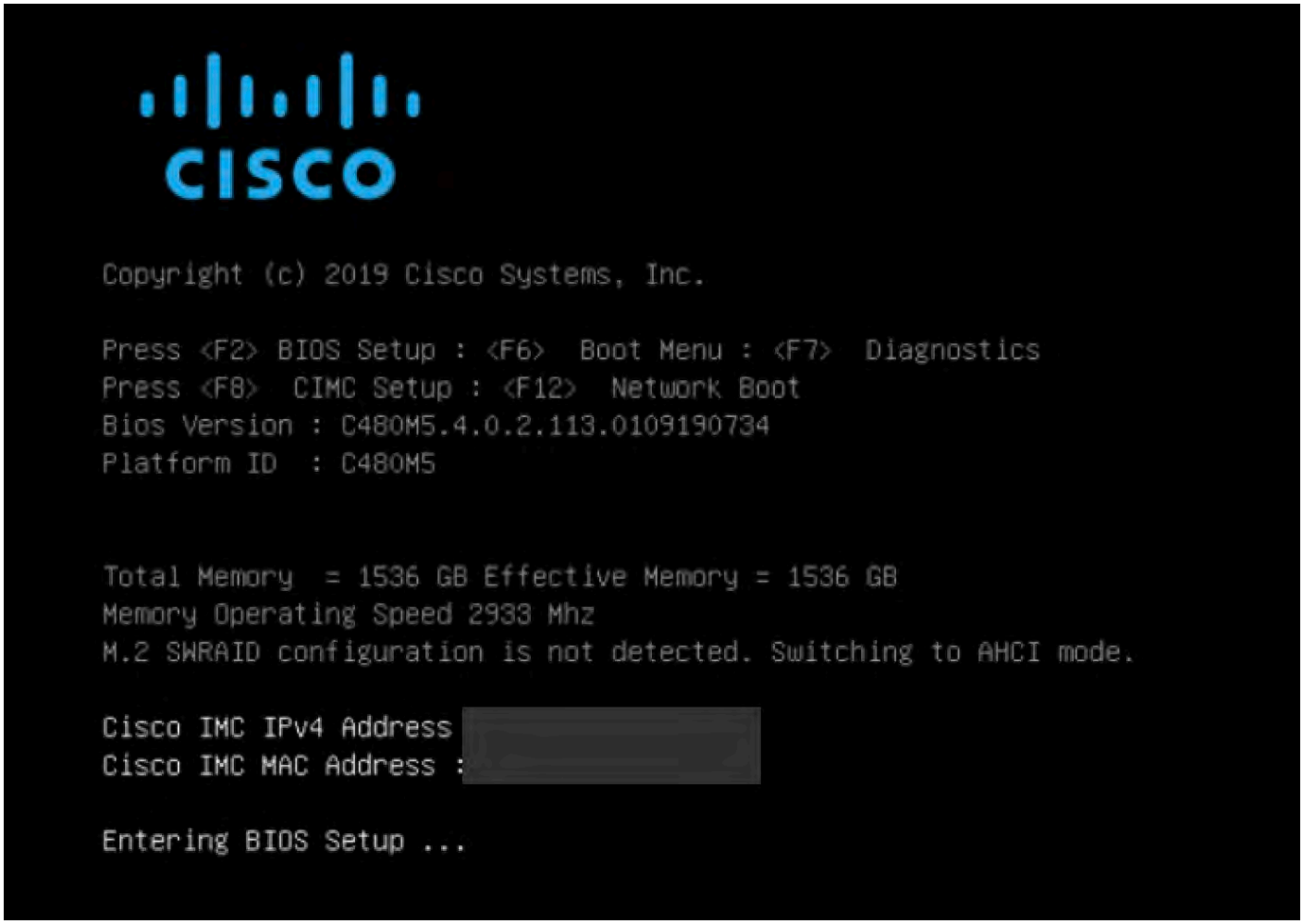
Figure 17. Power on the system



2. After the server has booted, press F2 to enter the BIOS menu (Figure 18).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

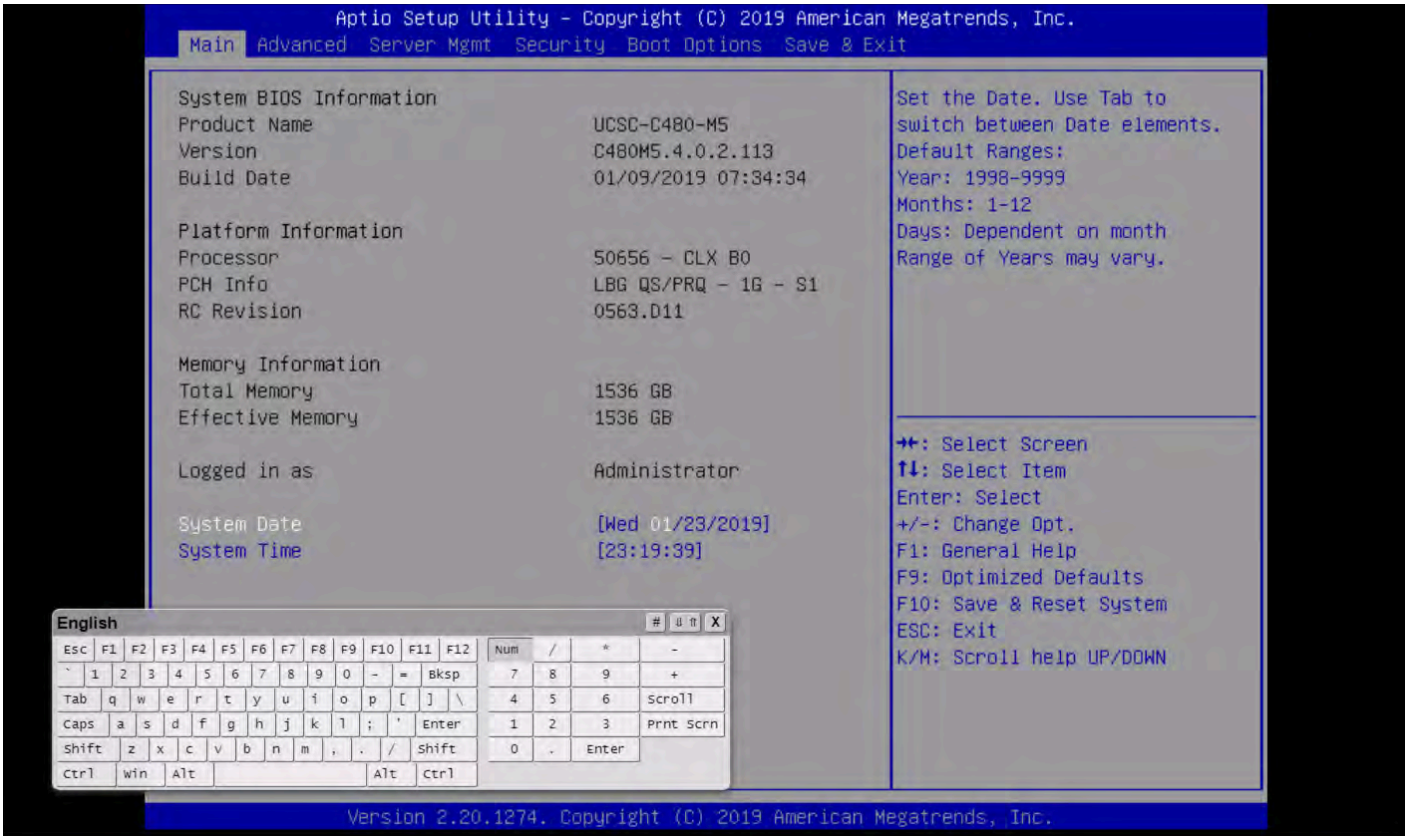
Figure 18. Press F2



3. For a better keyboard experience, from the View menu select the on-screen keyboard (Figure 19).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

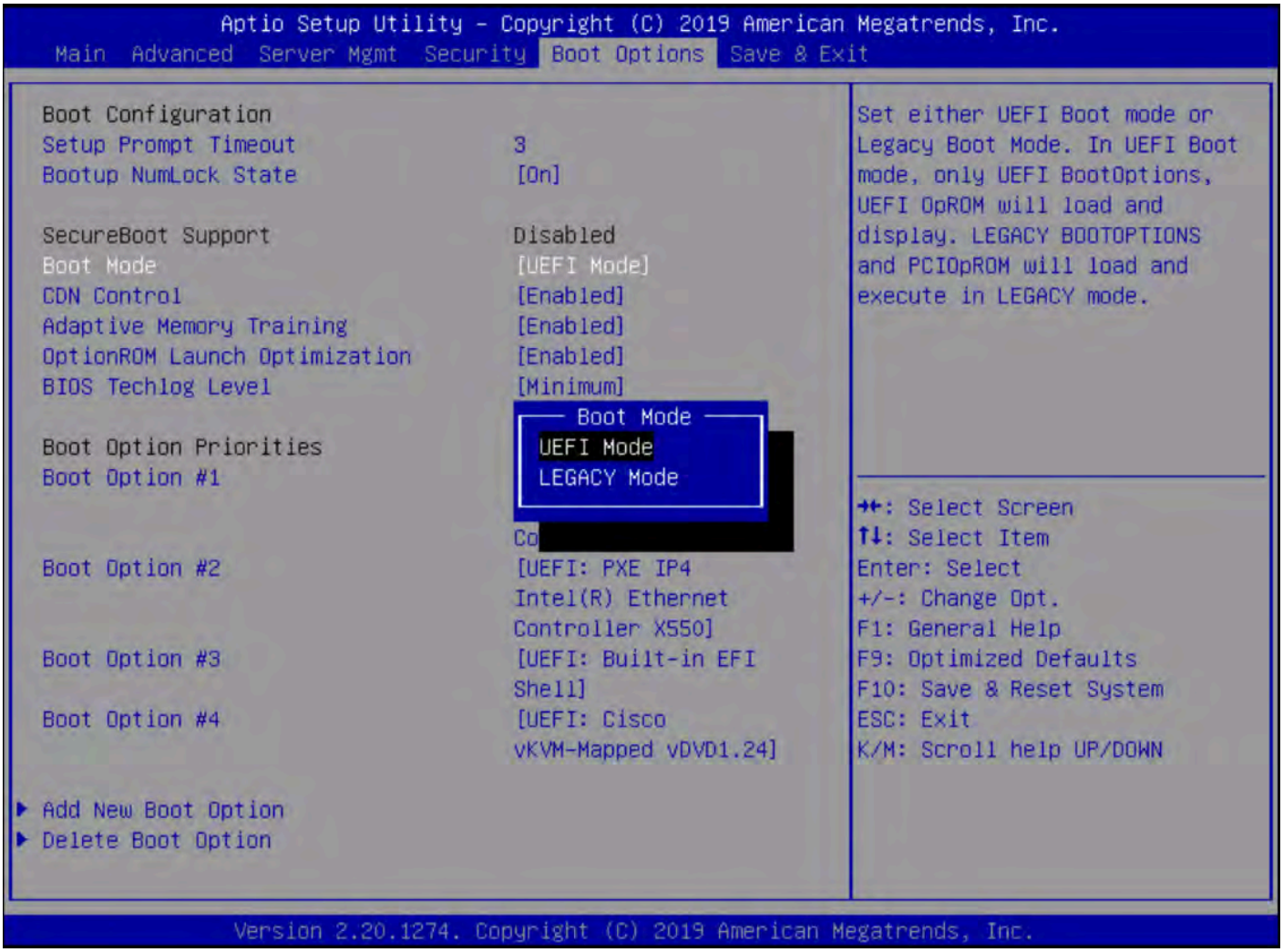
Figure 19. On-screen keyboard



4. From the BIOS menu, choose Boot Options > Boot Mode > UEFI Mode (Figure 20). This setting selects the Unified Extensible Firmware Interface (UEFI).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

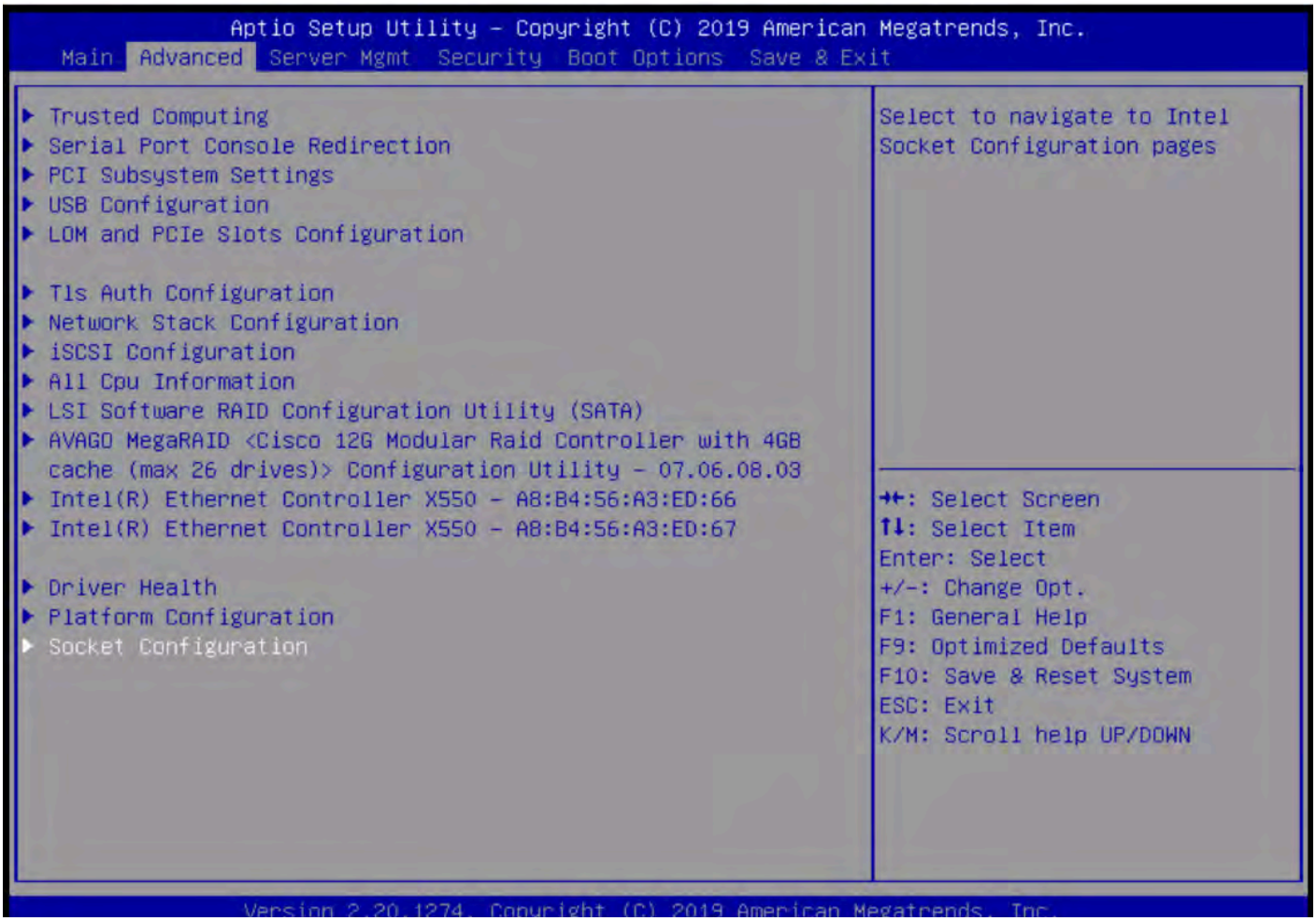
Figure 20. Choose UEFI Mode



5. Disable the C-states of the CPU as recommended in the SAP for HANA requirements. From the BIOS menu, choose Advanced > Socket Configuration (Figure 21).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

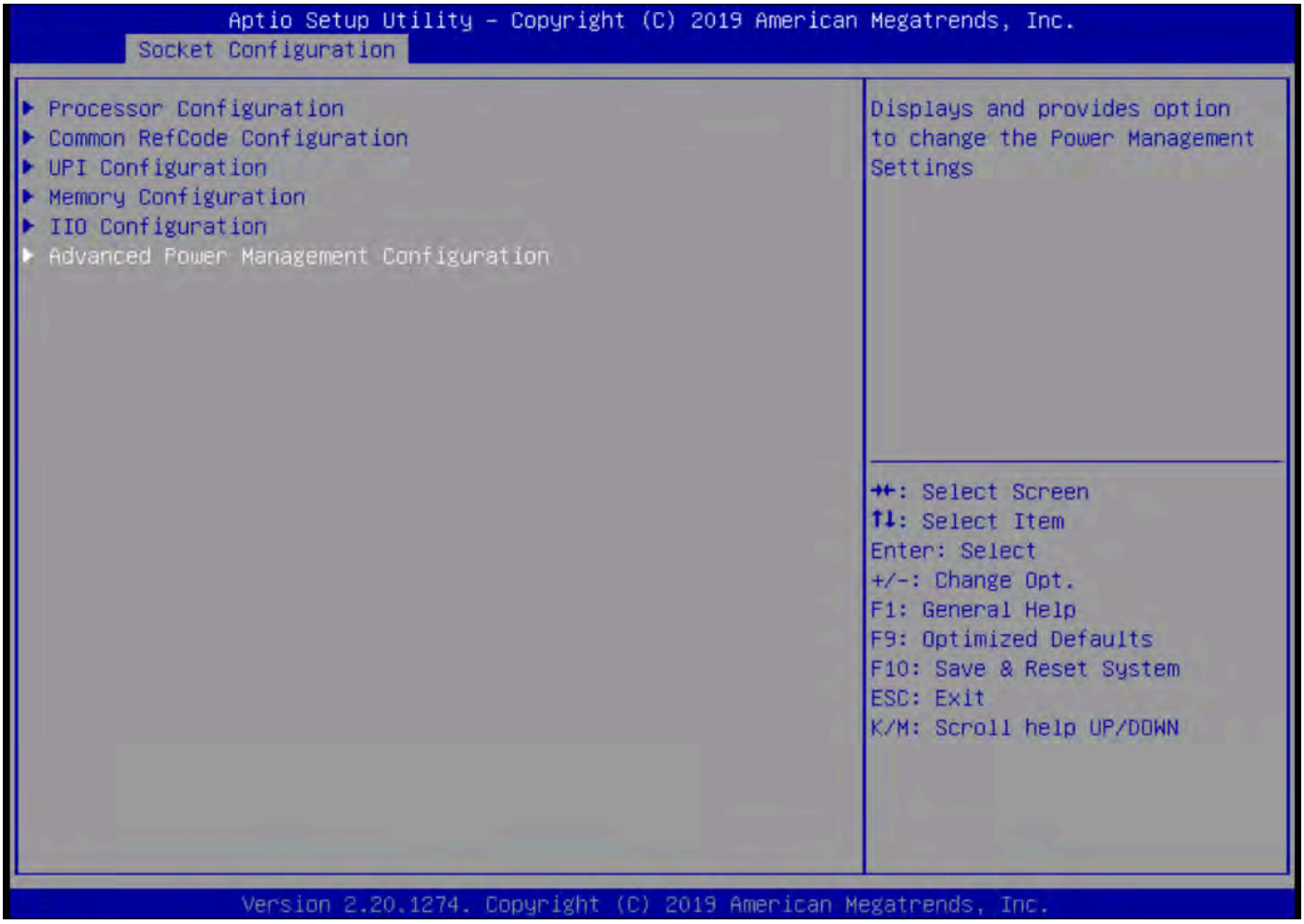
Figure 21. Choose Socket Configuration



6. Choose Advanced Power Management Configuration (Figure 22).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 22. Choose Advanced Power Management Configuration



7. Choose CPU C State control and then disable the C-states as shown in Figure 23.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 23. Disabling C-states



8. After disabling the C-states, press F10 and save the BIOS settings.

Rebooting the server to implement BIOS changes

To make the boot options and CPU C-states take effect, reboot the server.

You are now ready to configure RAID.

Configuring RAID

This document covers all scale-up solutions with 2- and 4-socket configurations of the Cisco UCS M5 platform.

Table 11 lists the RAID options and the available platforms.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Table 11. RAID options

Platform	SAS (20 drives)	SSD (3 or 8 drives)
Cisco UCS C480	RAID 50	RAID 5
Cisco UCS C240	RAID 50	RAID 5
Cisco UCS C220	-	RAID 5

Table 12 lists the settings that you need to configure when you create the virtual drives.

Table 12. RAID settings

RAID settings	RAID 50	RAID 5
Stripe size	256	256 (8 SSDs or 20 SAS drives) 128 (3 SSDs)
Read policy	Read ahead	Read ahead
Write policy	Write back	Write back
I/O policy	Cached	Default

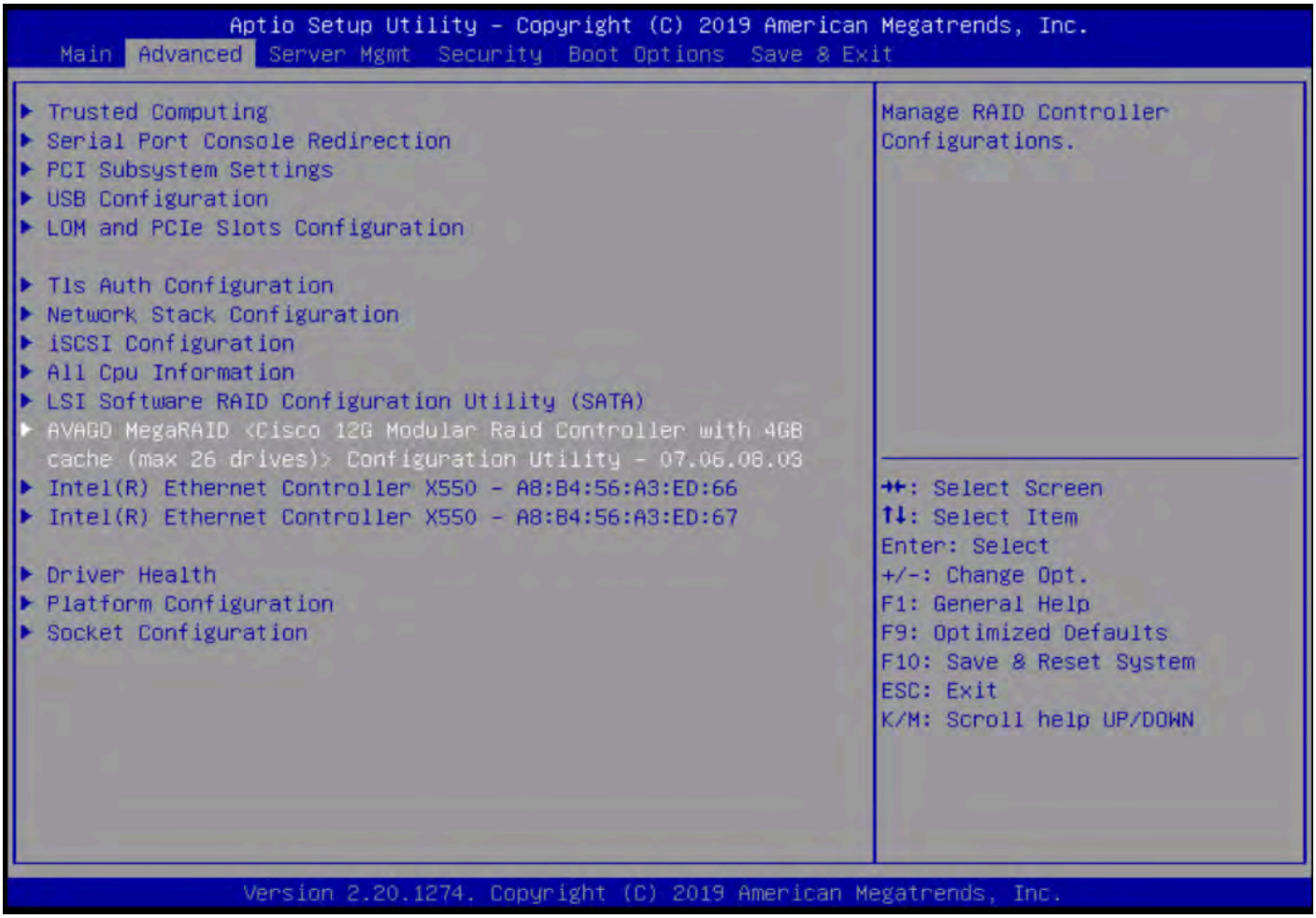
The following procedure shows the RAID 50 configuration with SAS drives on the Cisco UCS C480 M5 server used for SAP HANA.

The same procedure applies to the creation of RAID 5 virtual drives with SSD-based options except that the number of drives will be three or eight and the RAID level will be RAID 5.

1. Boot the server and press F2 to enter the BIOS menu.
2. Navigate to Advanced and select the Avago MegaRAID utility to proceed with the RAID configuration (Figure 24).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

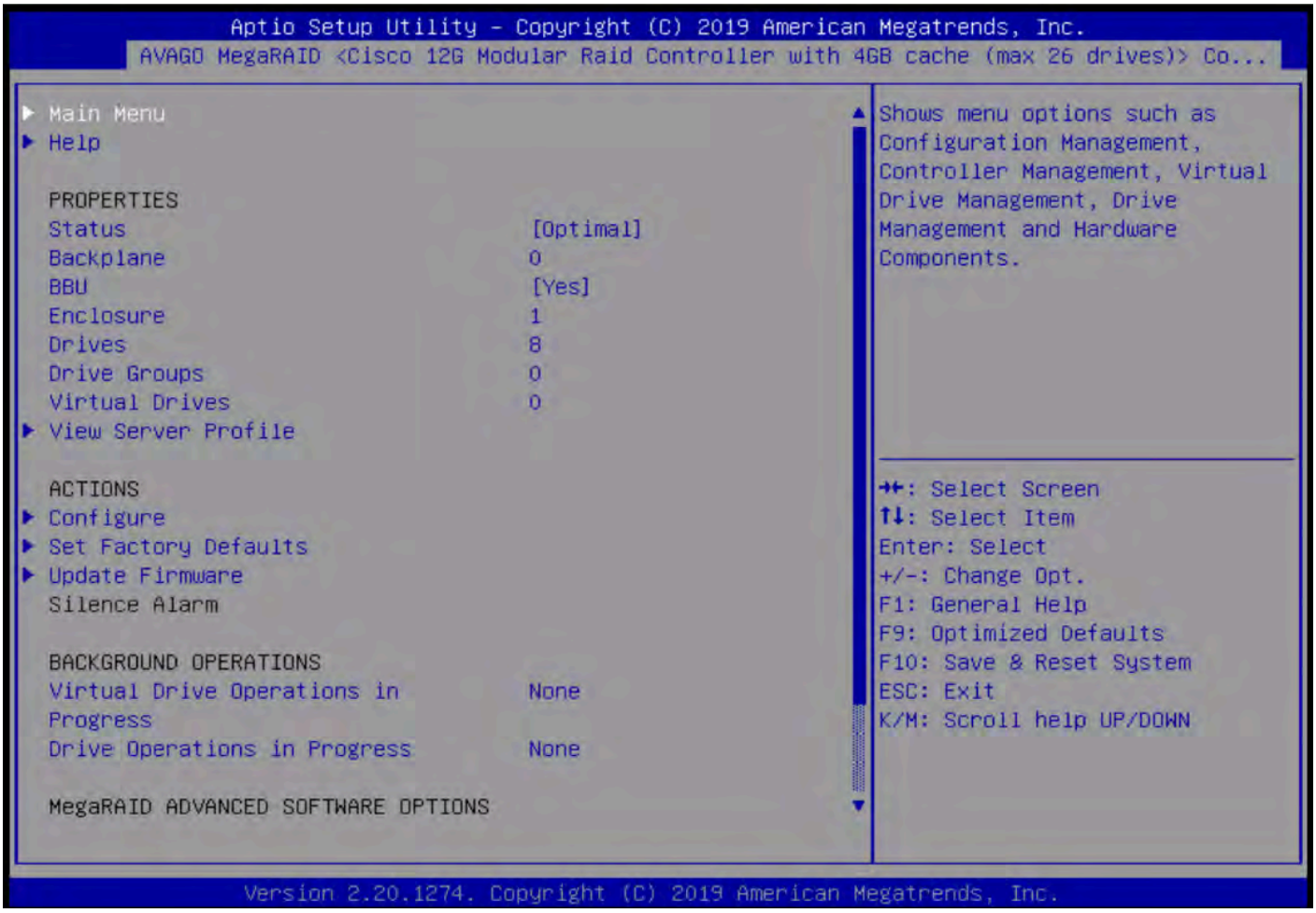
Figure 24. Select Avago MegaRAID



3. Choose Main Menu (Figure 25).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

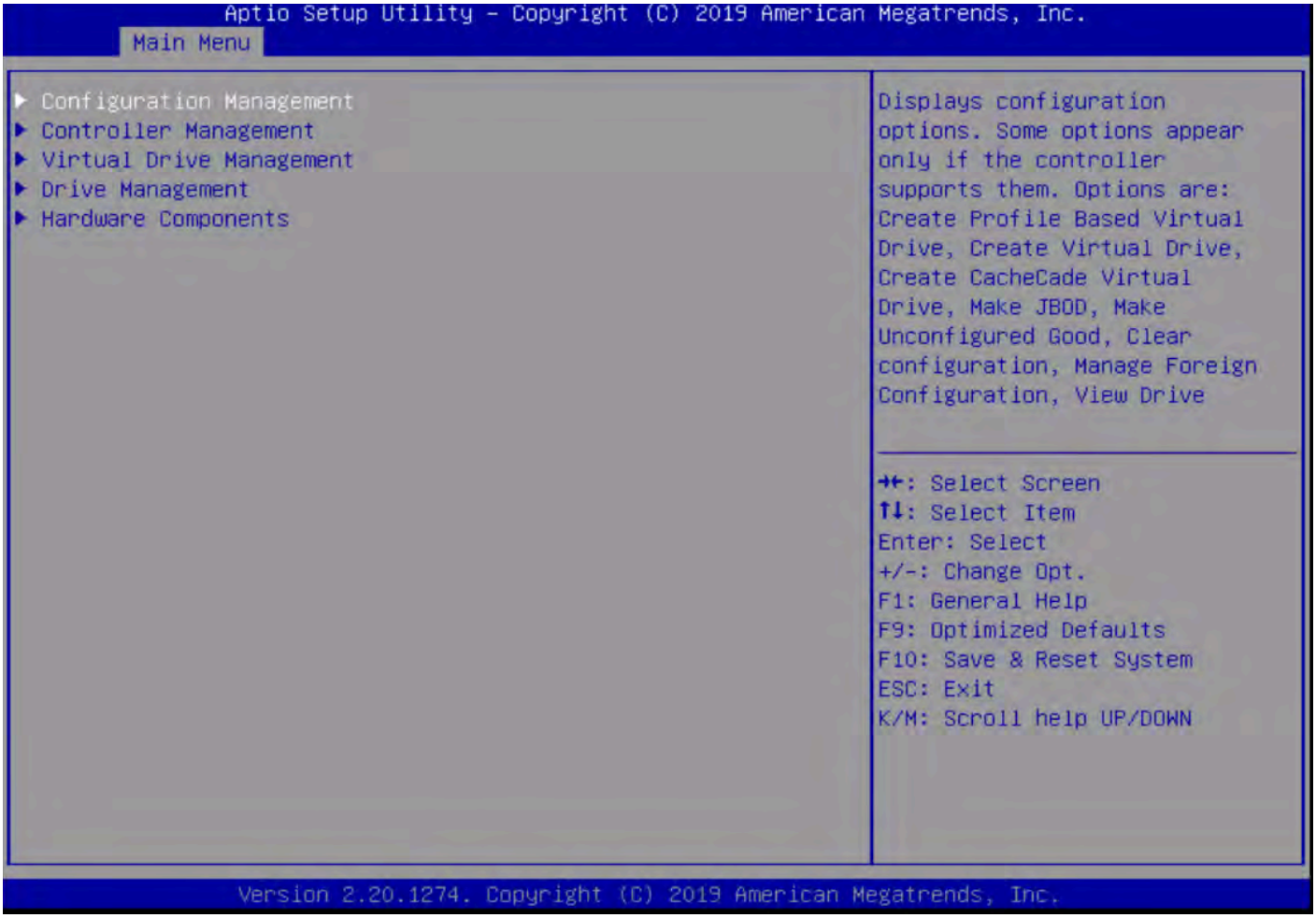
Figure 25. Choose Main Menu



4. Choose Configuration Management (Figure 26).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 26. Choose Configuration Management



5. Choose Create Virtual Drive (Figure 27).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

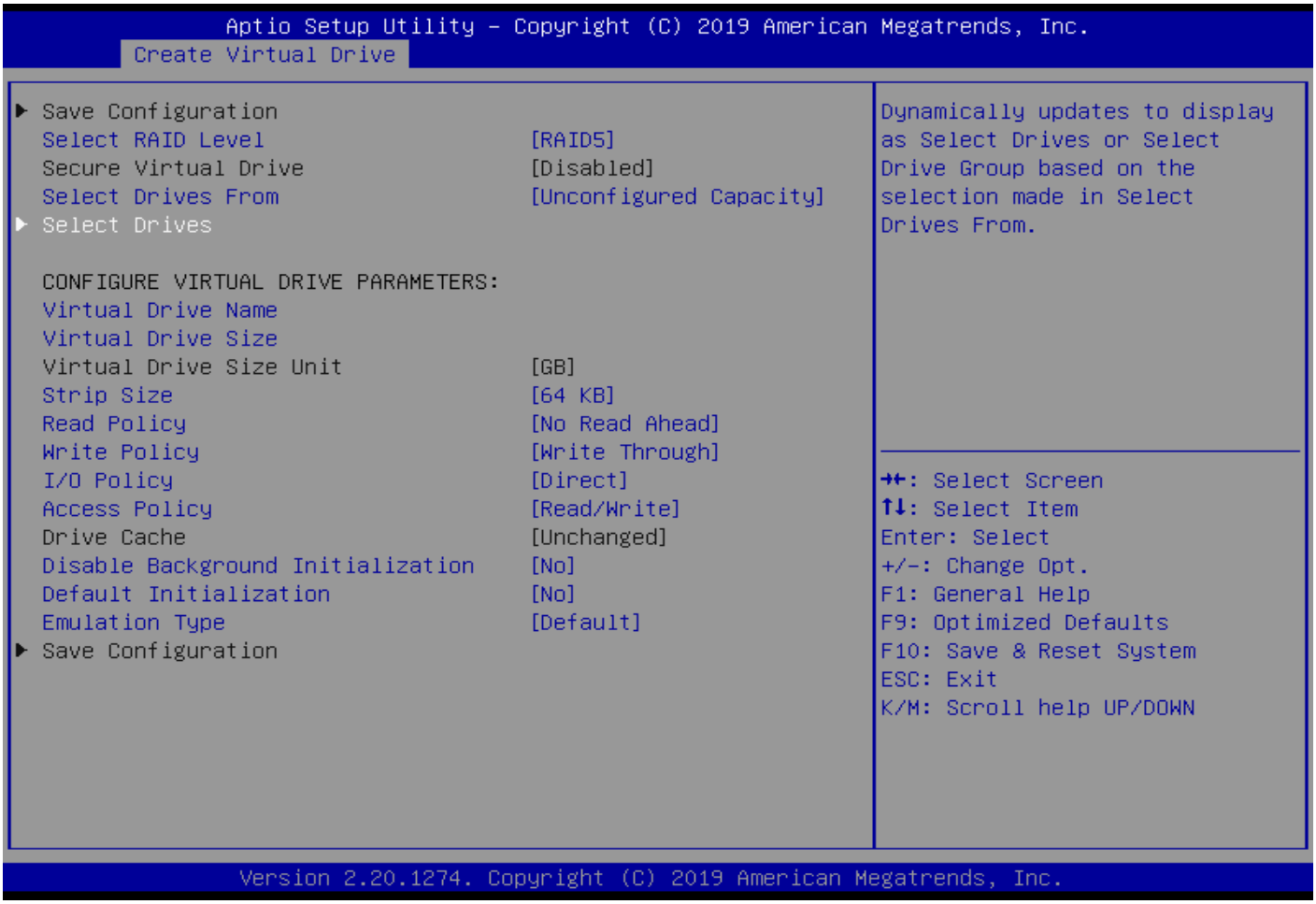
Figure 27. Choose Create Virtual Drive



6. Choose the following options to create a RAID 50 or RAID 5 virtual drive. With 20 disks, add five spans.
   a. For RAID Level, choose RAID 50 or RAID 5.
   b. Choose Select Drives (Figure 28).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

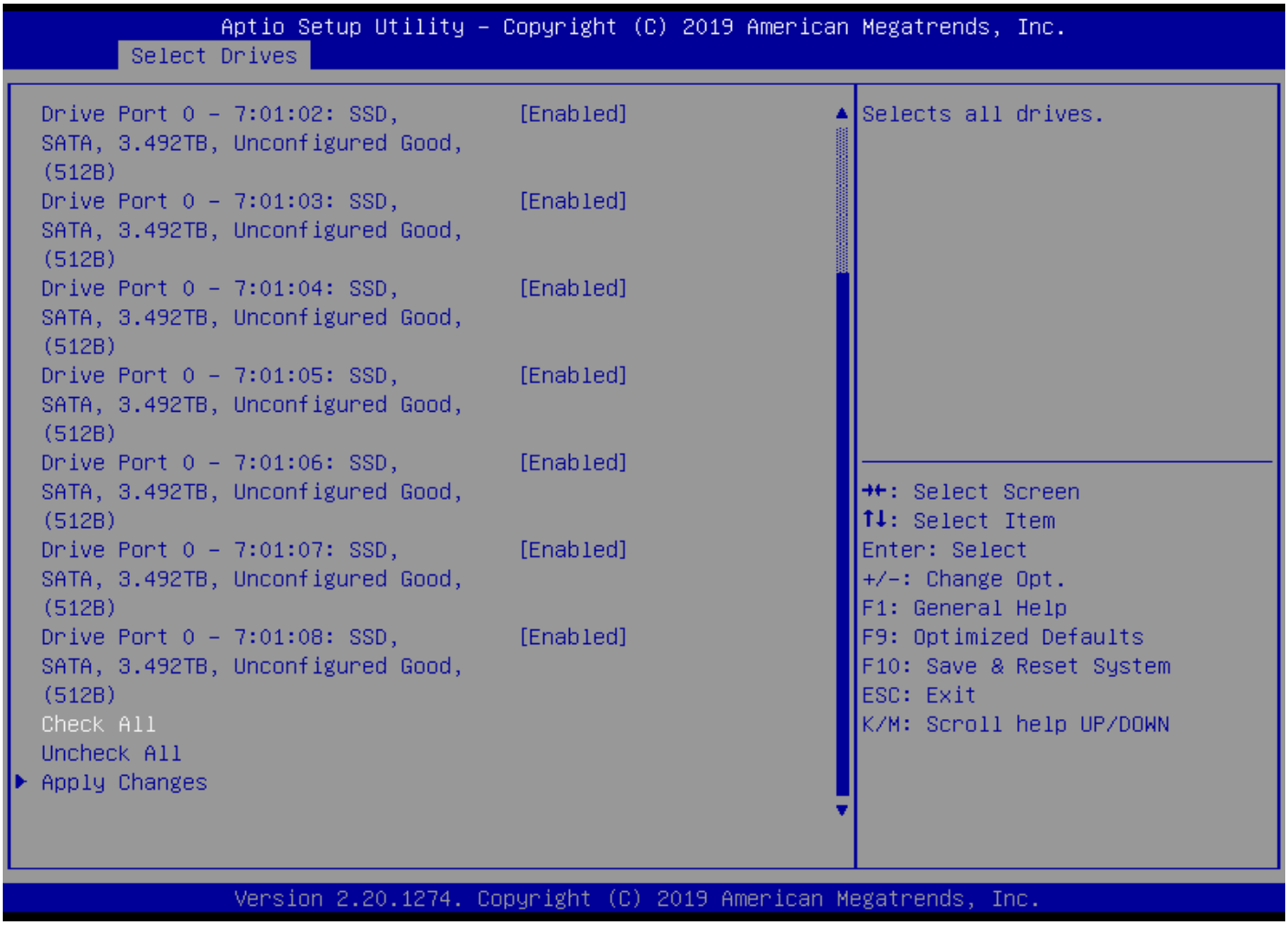
Figure 28. Choose RAID options



c. Choose Select Drives and then select the eight SSDs by choosing Enabled as shown in Figure 29.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

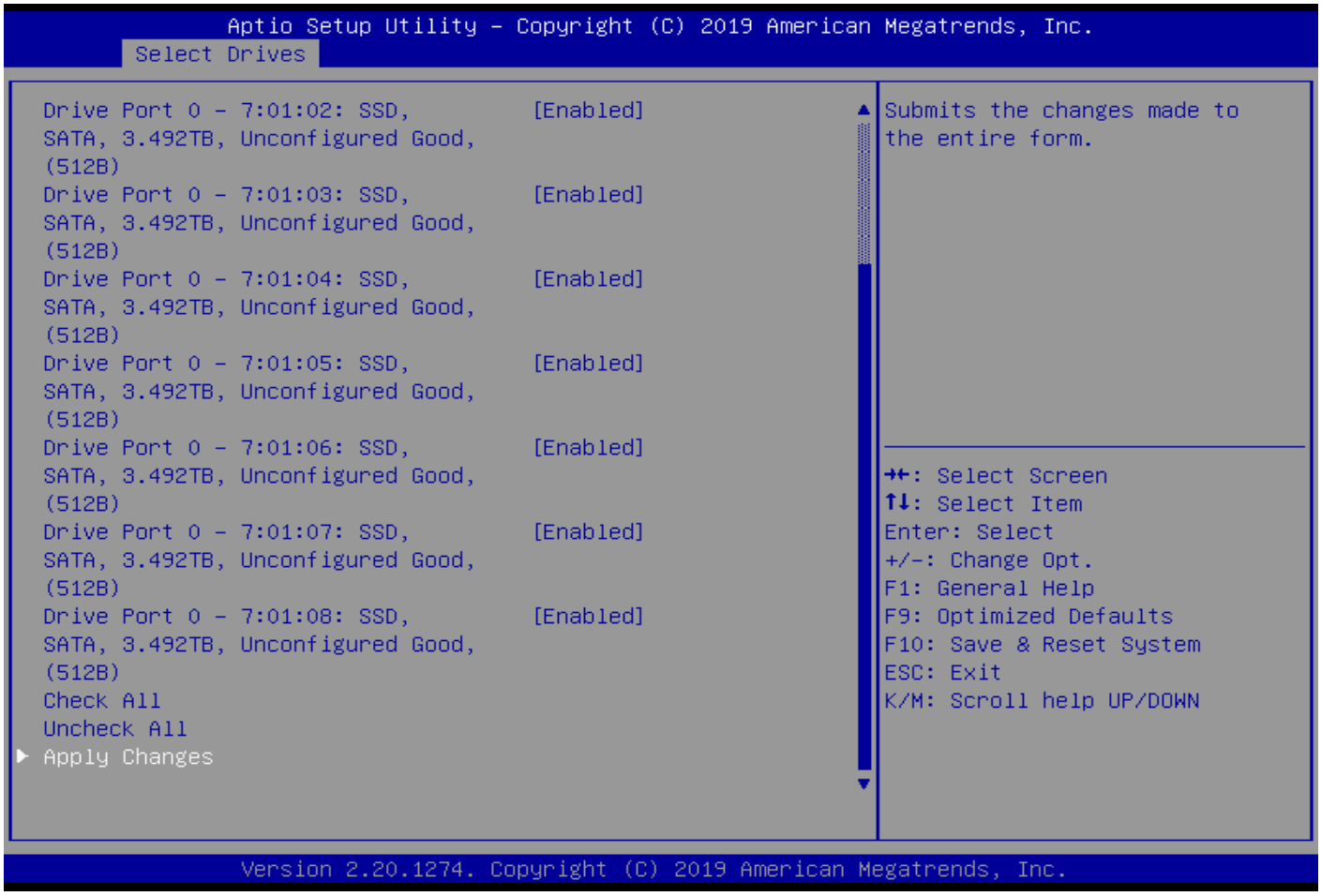
Figure 29. Choose Enabled



d. Scroll up or down and on the Select Drives screen and choose Apply Changes (Figure 30).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 30. Apply the changes

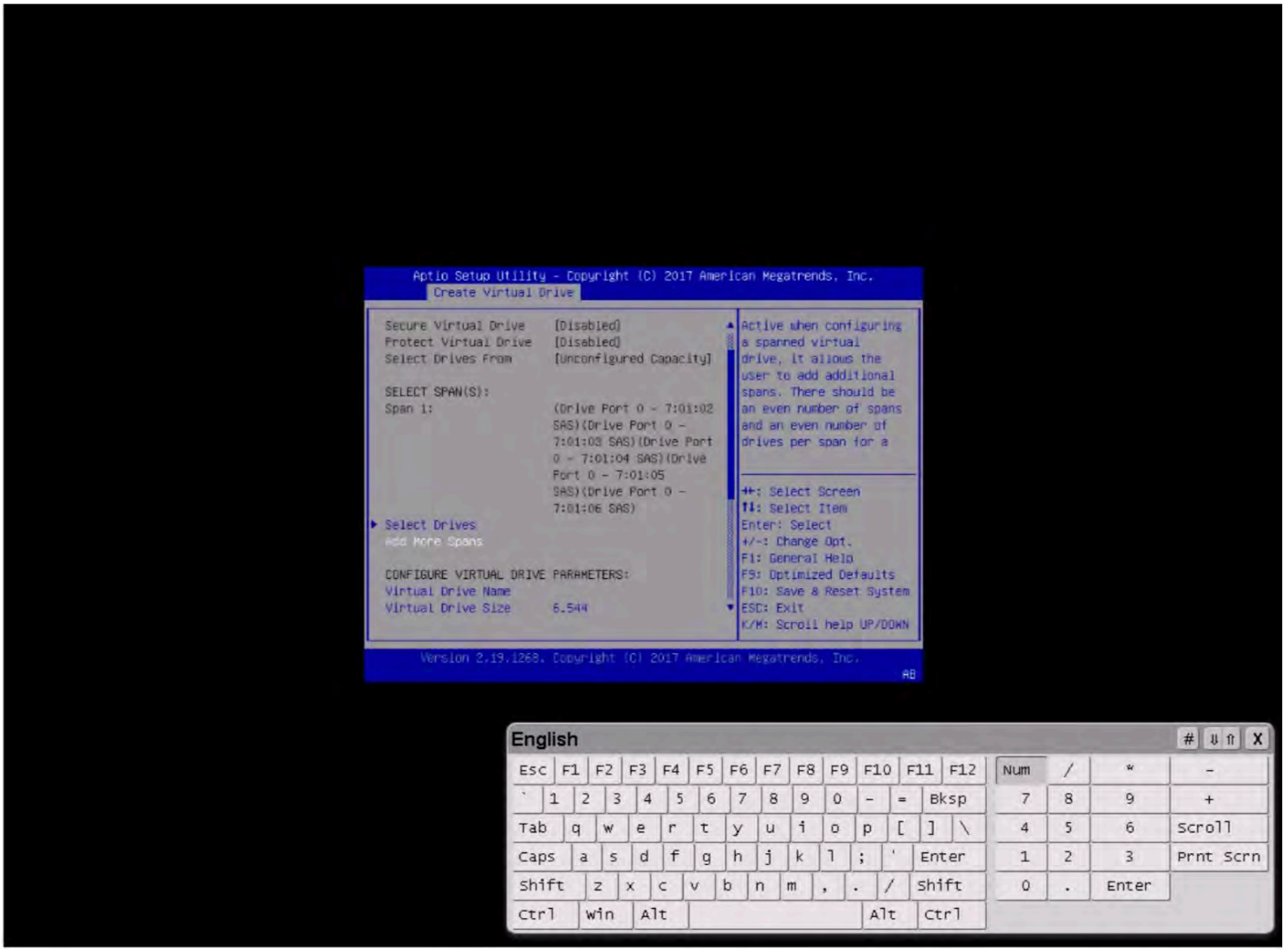


e. Choose OK in the confirmation window.

7. Add four more spans using the same process as in step 6 when configuring RAID 50 (Figure 31).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

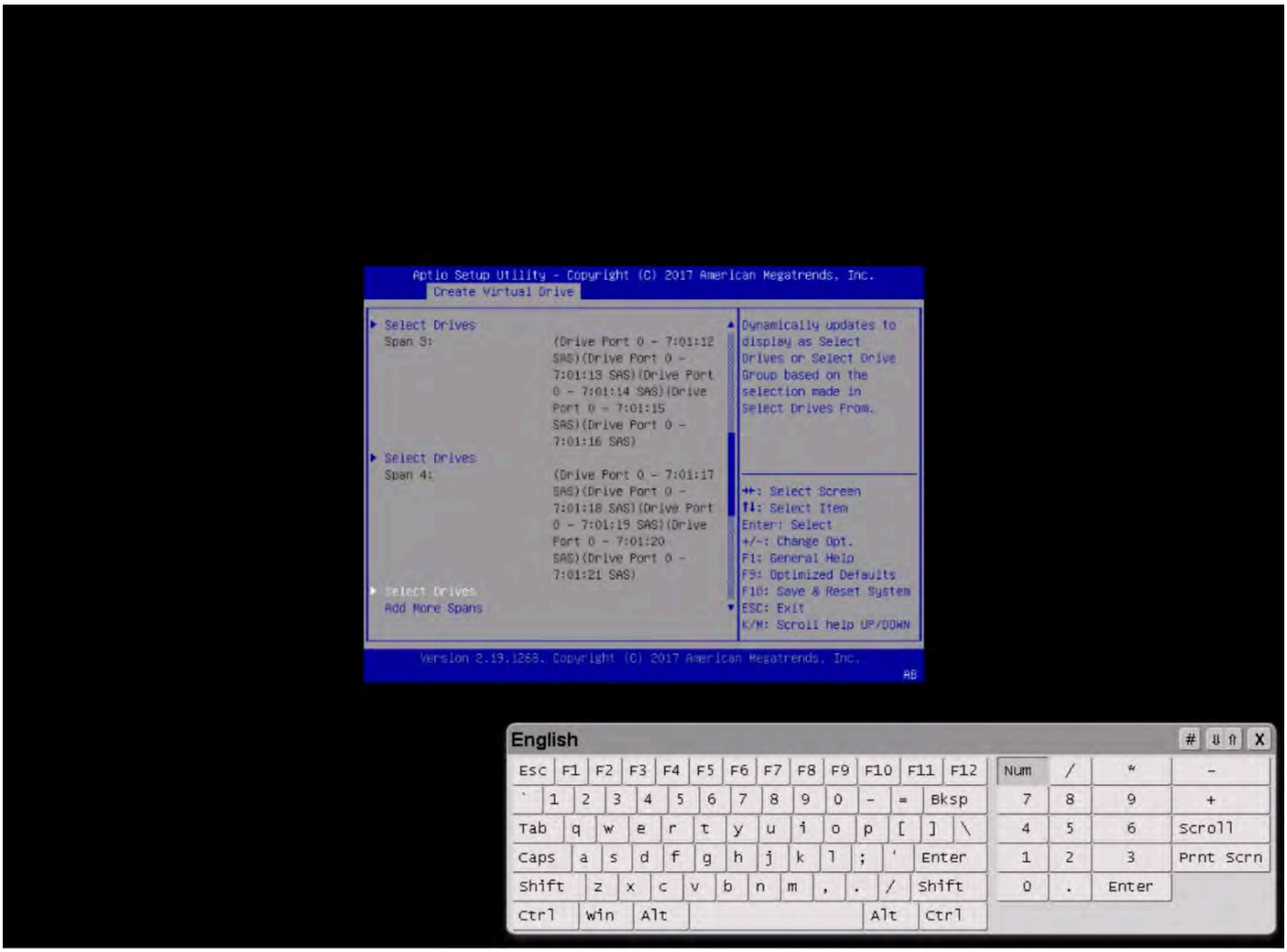
Figure 31. Add more spans



8. After repeating the steps to add spans and drives, verify that four spans with five drives per span have been added (Figure 32).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 32. Verify that spans and drives have been added

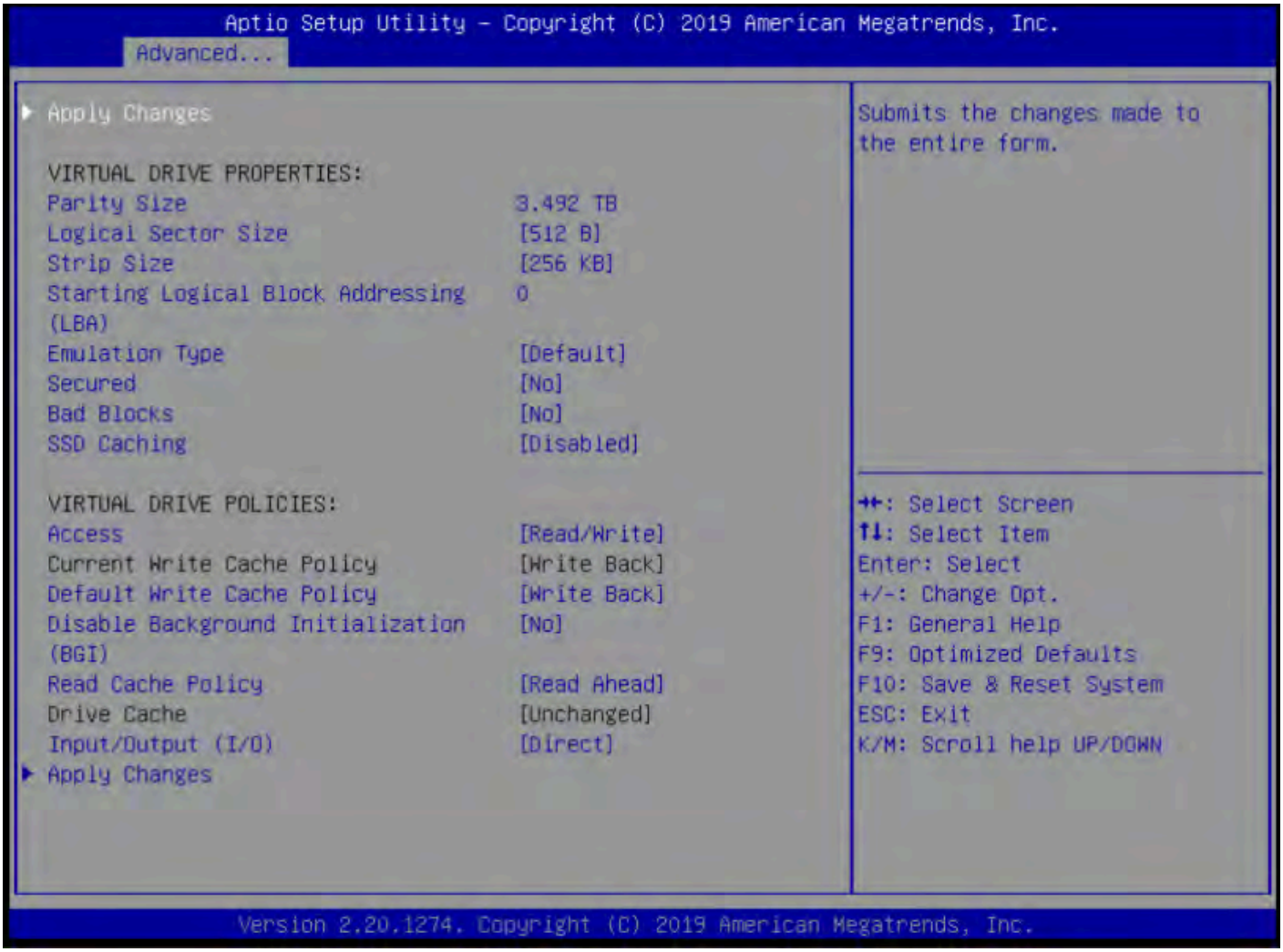


9. Configure the virtual drive parameters as shown in Figure 33.
   a. Name the virtual drive <<var_raid5_vd_name>>.
   b. For Strip Size, choose 256 KB.
   c. For Read Policy, choose Read Ahead
   d. For Write Policy, choose Write Back.

When you are done, choose Save Configuration and press Enter.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 33. Virtual drive parameters



10. In the next window, the utility will ask for confirmation. Choose OK to proceed.

Note: The RAID settings described here apply only to a configuration using 20 SAS drives with RAID 50. Refer to Table 12 for the RAID options for SSD drives with RAID 5 settings.

11. Wait for the initialization process for VD0 to complete, which may take several minutes.
12. Press Esc and choose OK to exit the RAID configuration utility.
13. Press Ctrl+Alt+Del to reboot the server.

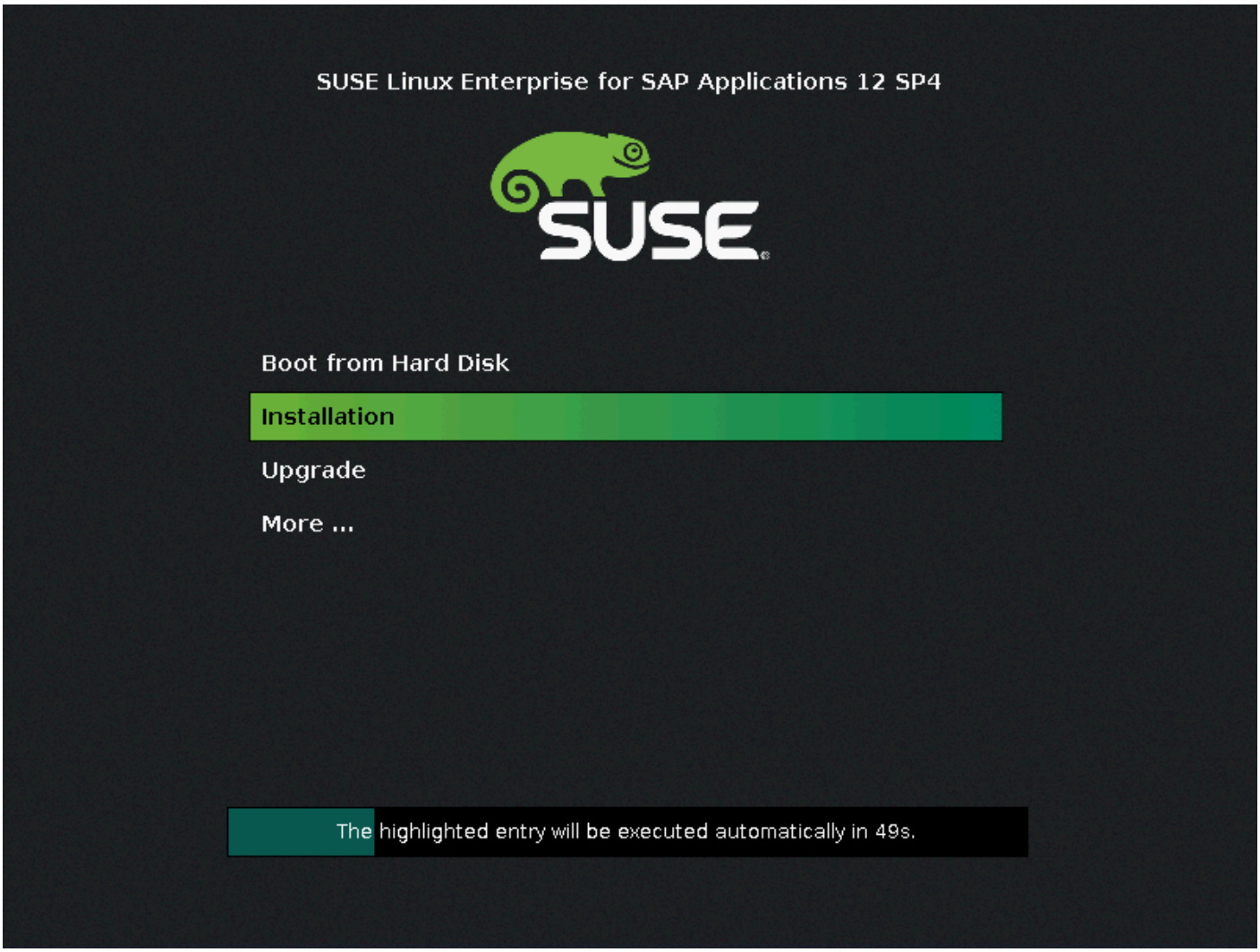
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Installing the operating system

This section shows the installation procedure for SLES 12 for SAP SP4 on local drives.

1. Follow the steps in the section “Launching the KVM console” to mount and boot the ISO image (Figure 34).

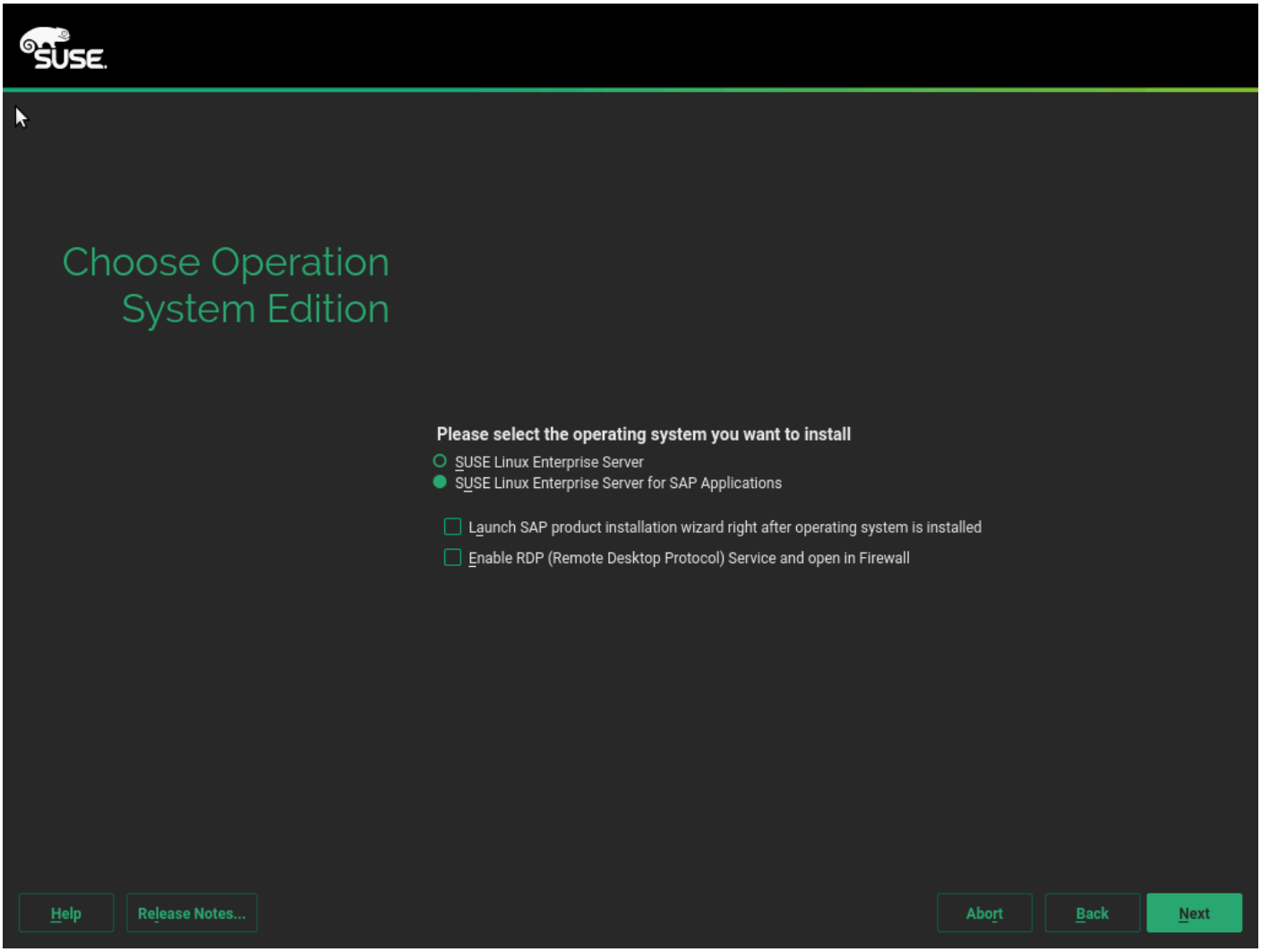
Figure 34. Booting to the ISO image



2. On the Language, Keyboard, and License Agreement page, select the English language and your preferred keyboard layout, agree to the license terms, and click Next.
3. On the Network Settings page, click Next. You will return to the network configuration as part of the post-installation tasks.
4. On the Registration page, click Skip Registration. You will register later as part of the post-installation tasks.
5. On the Choose Operating System Edition page, select the SUSE Linux Enterprise Server for SAP Applications option (Figure 35).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

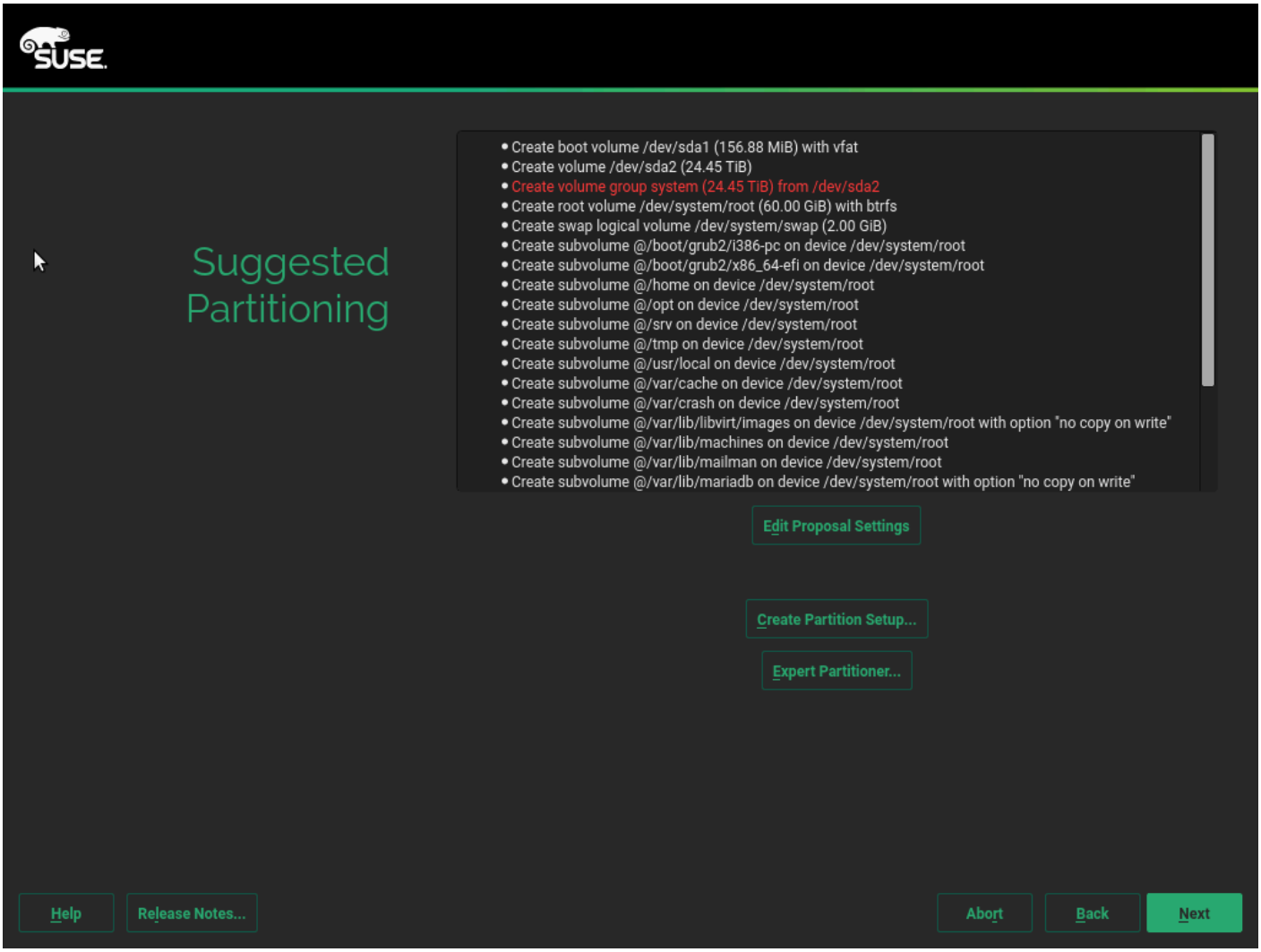
Figure 35. Select the product installation mode



6. On the Add On Product page, click Next. In this configuration example, there are no additional products to install.
7. On the Suggested Partitioning page, click Expert Partitioner (Figure 36).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

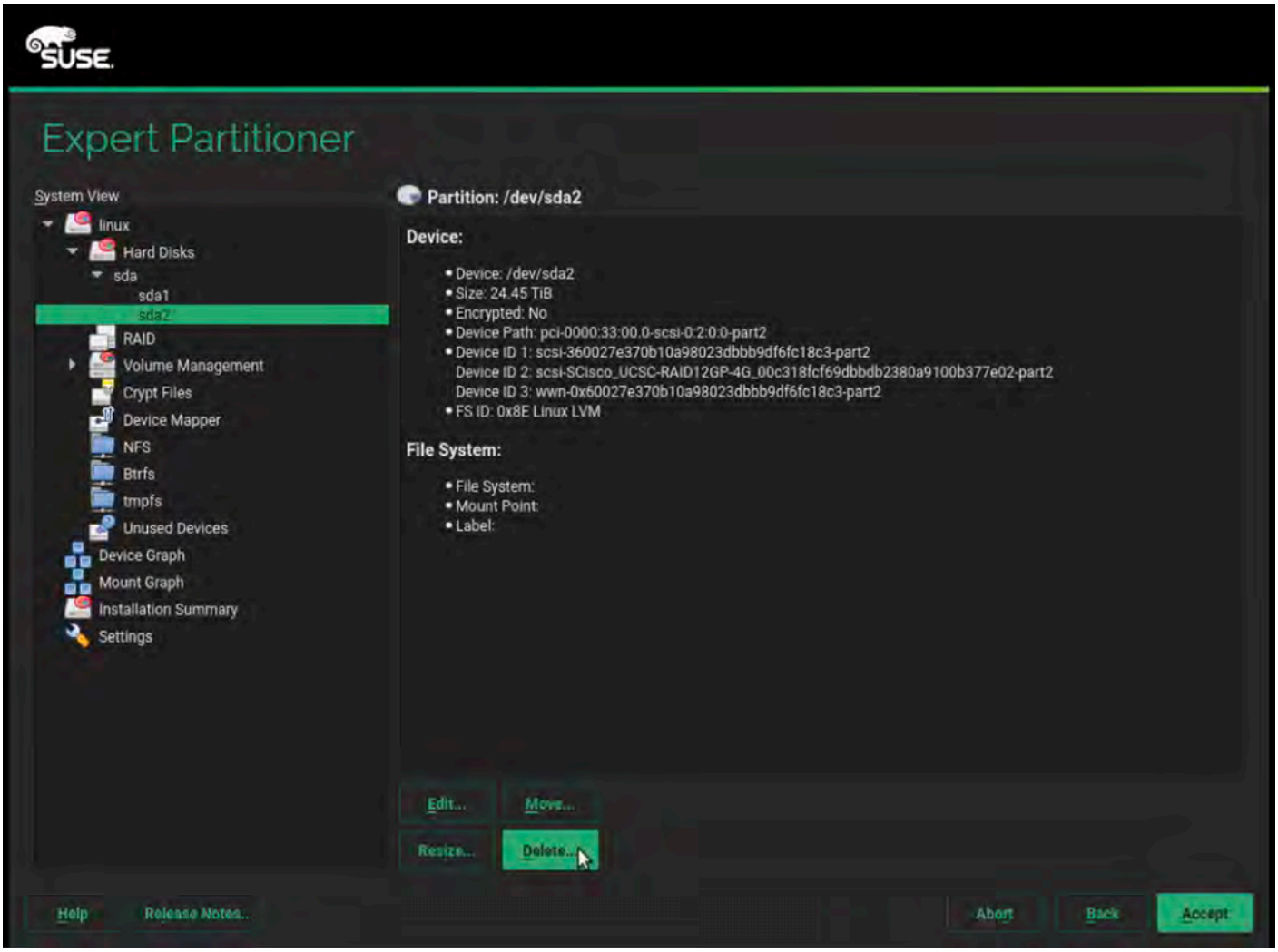
Figure 36. Suggested partitioning initial proposal: Select Expert Partitioner



8. At the left, choose System View > Linux > Hard Disks > sda.
9. Clear the suggested partitions. The example here shows two suggested partitions: sda1 and sda2. Use the following steps to delete sda1 and sda2.
   a. Delete partition sda2 (Figures 37 and 38).

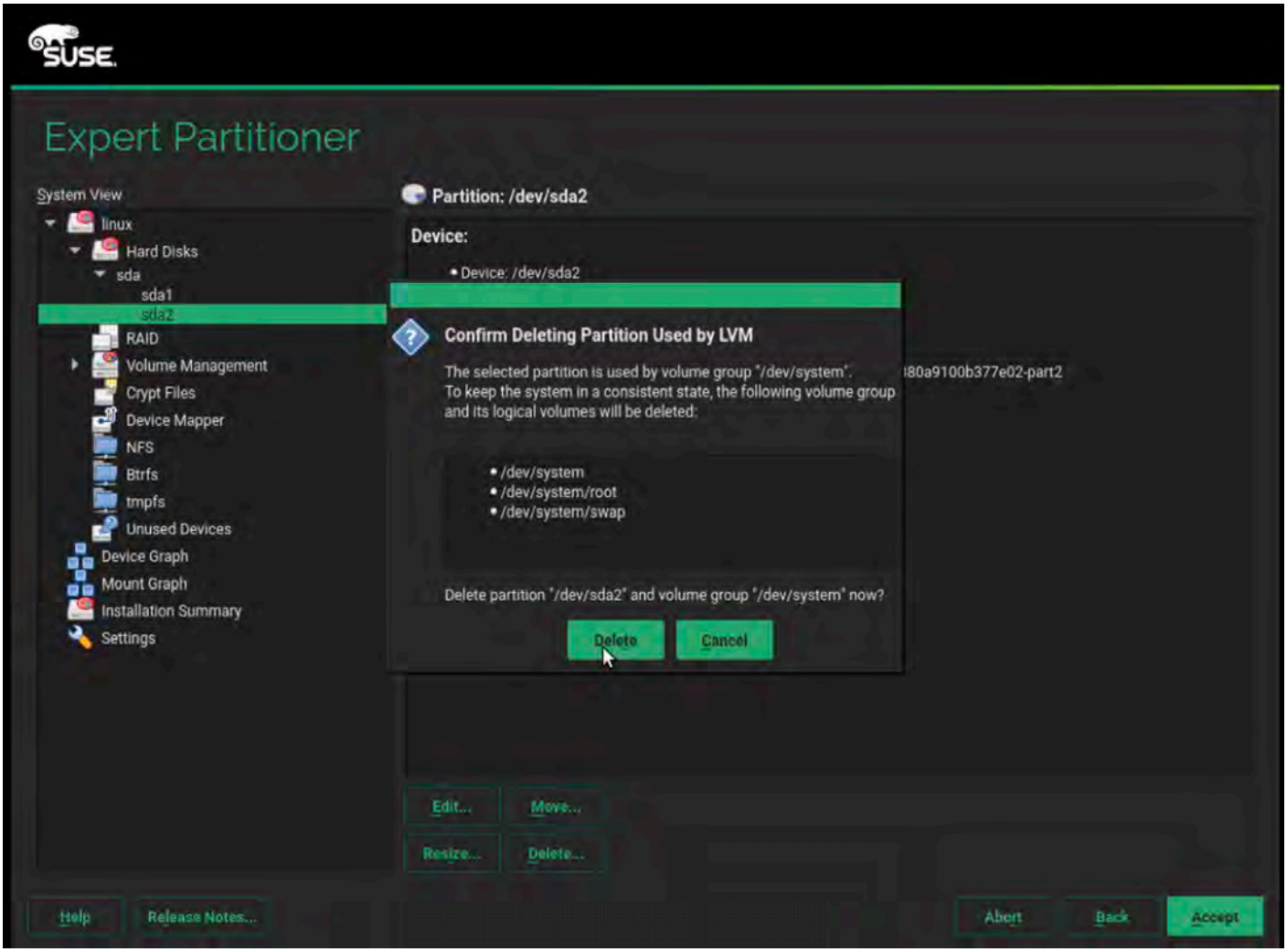
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 37. Expert Partitioner: Delete partition sda2



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

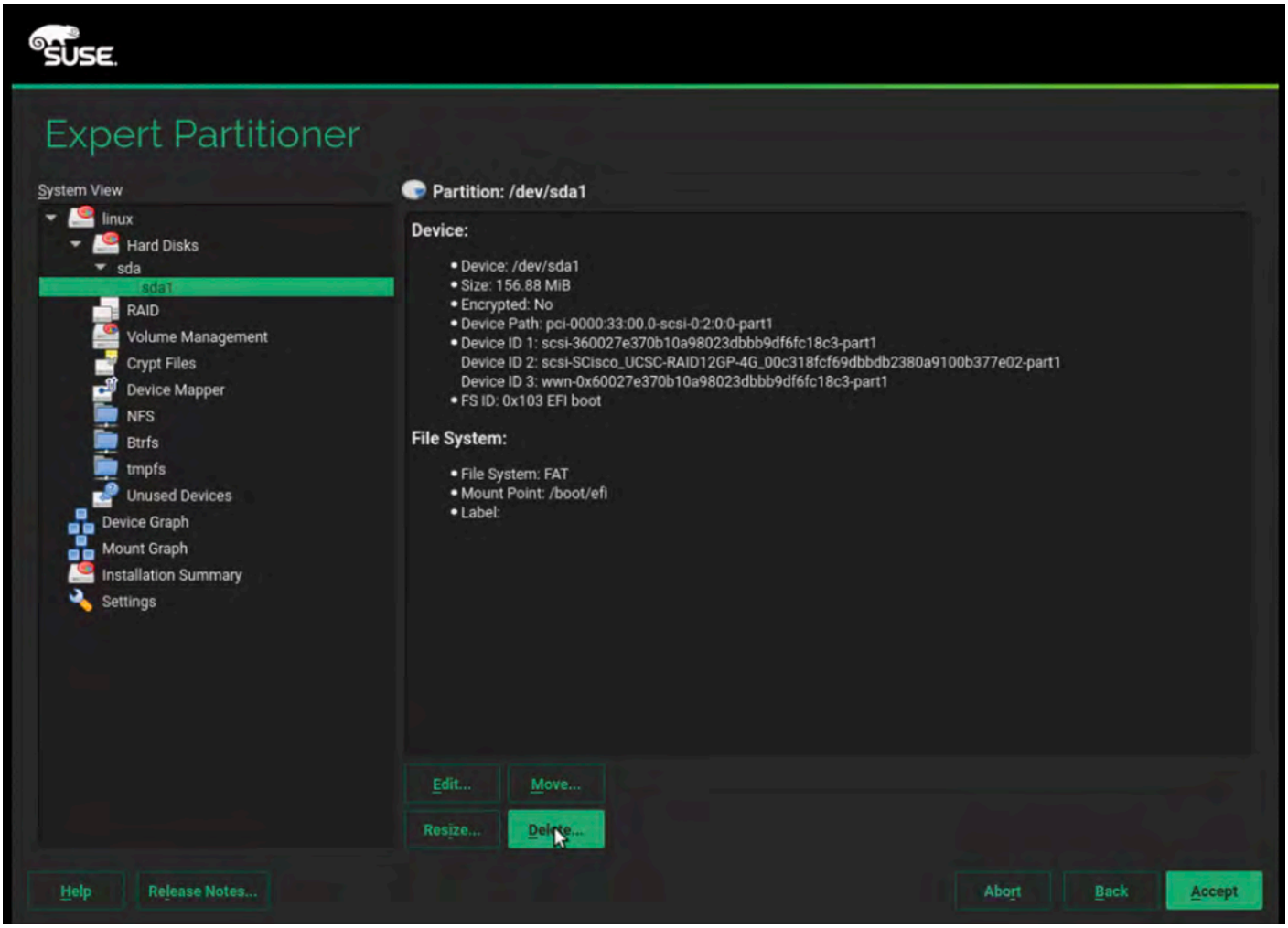
Figure 38. Expert Partitioner: Confirm deletion of partition sda2



b. Delete partition sda1 (Figures 39 and 40).

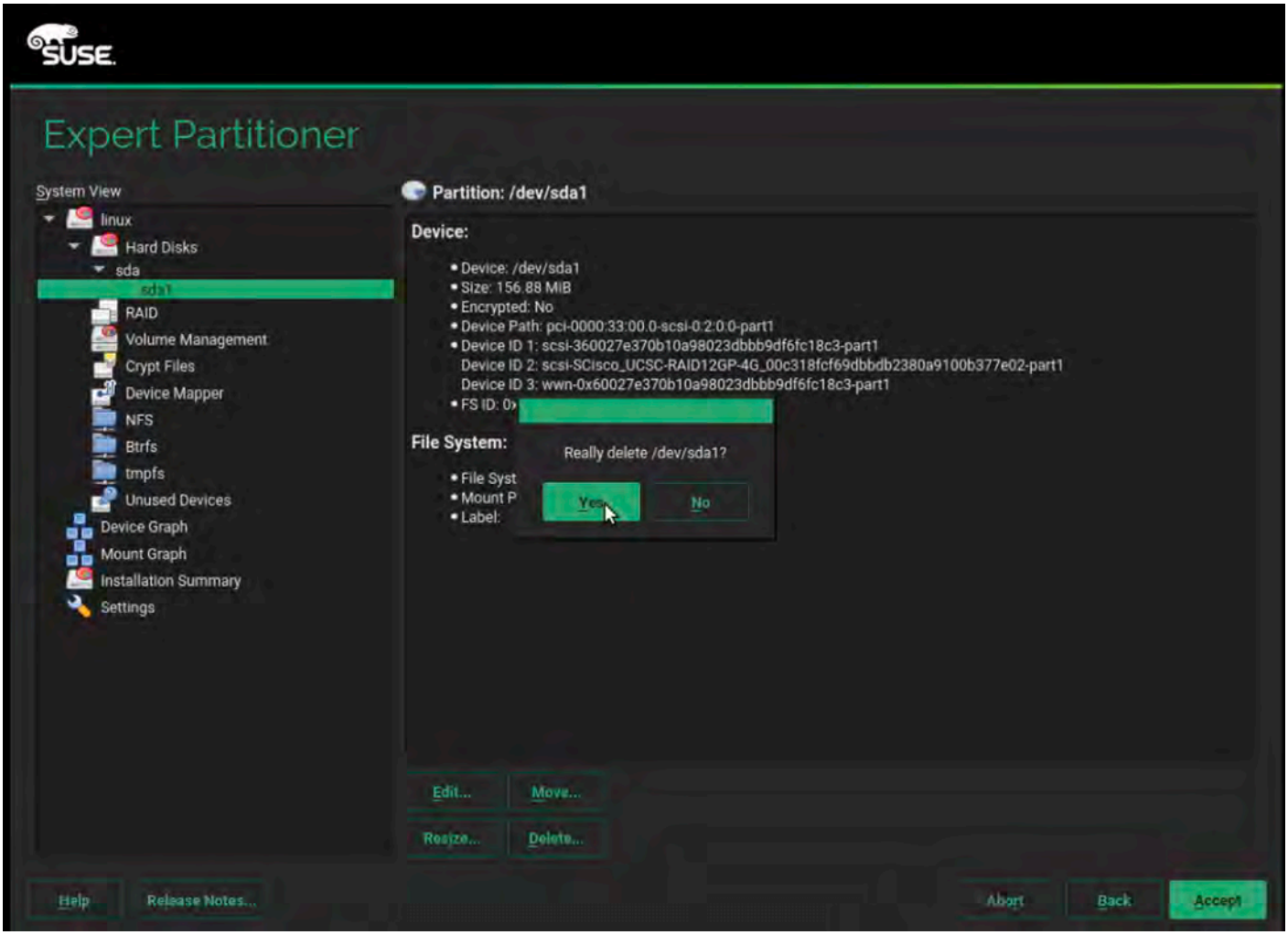
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 39. Expert Partitioner: Delete partition sda1



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 40. Expert Partitioner: Confirm deletion of partition sda1



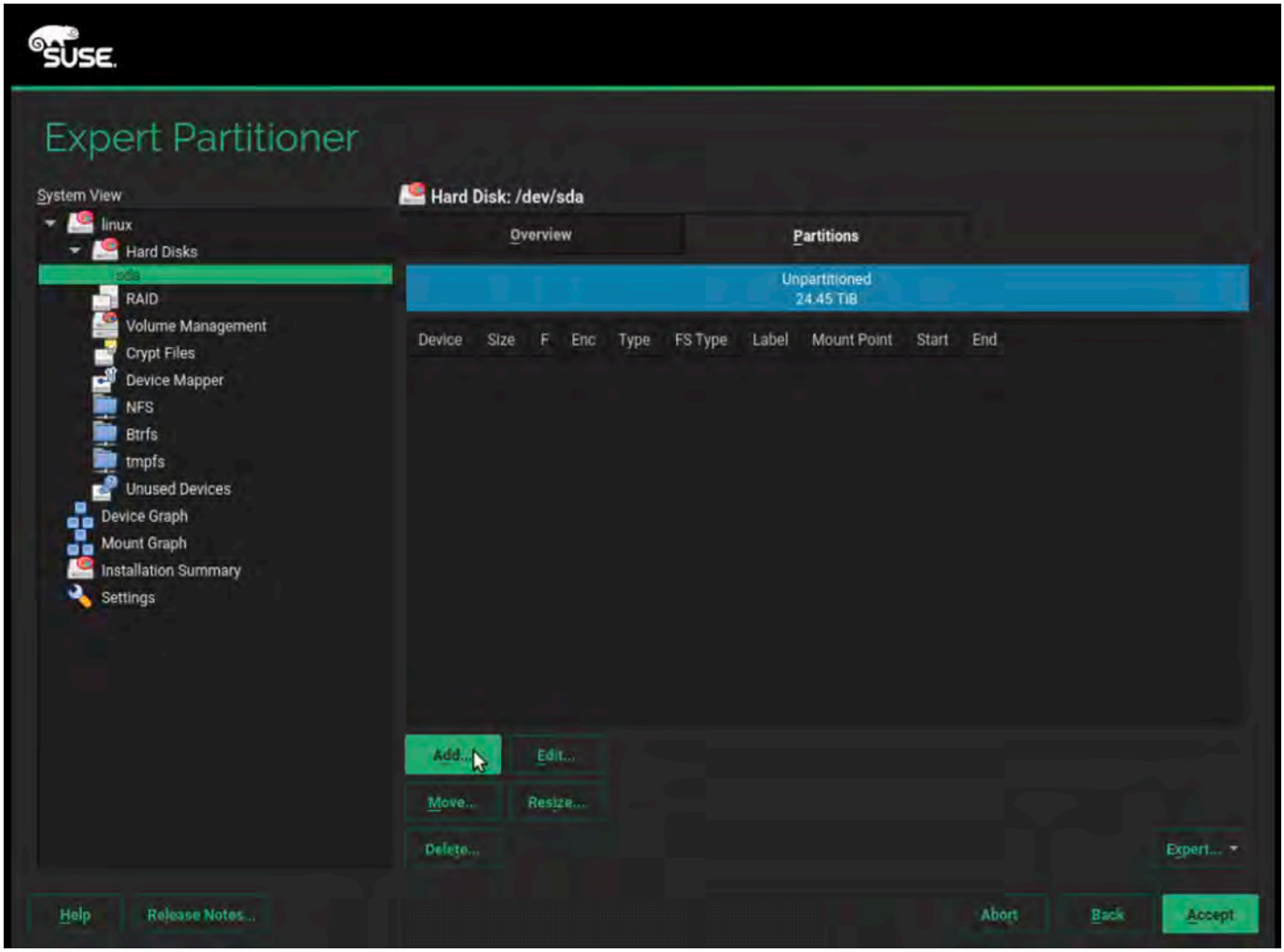
Now, from the unpartitioned device sda, you will use the steps here to do the following:

- Create a 200-MB /boot/efi partition (/dev/sda1) from the disk device available (/dev/sda).
- Create another partition (/dev/sda2), assigning the rest of the available space in the device (/dev/sda). Assign this partition to Linux LVM, thus making it a physical volume.
- Create a volume group (hanavg) and assign the available physical volume (/dev/sda2) to it.
- Create a logical volume for /filesystem with a size of 100 GB and using the Ext3 file system.
- Create a swap volume with a size of 2 GB.

10. In the Expert Partitioner, choose the device /dev/sda and click Add (Figure 41).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

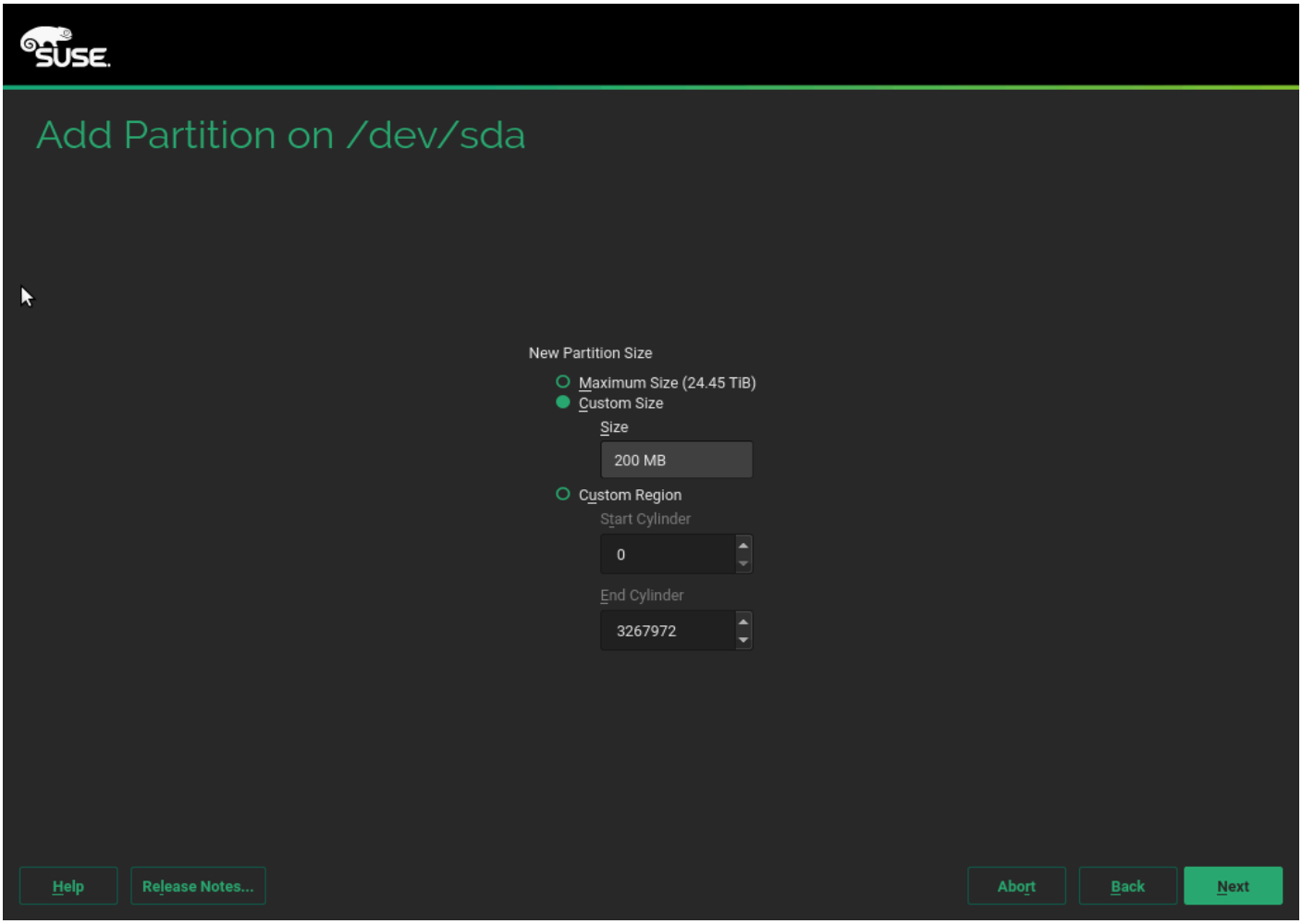
Figure 41. Add new partition



11. Create a partition with a size of 200 MB for /boot/efi (Figure 42).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

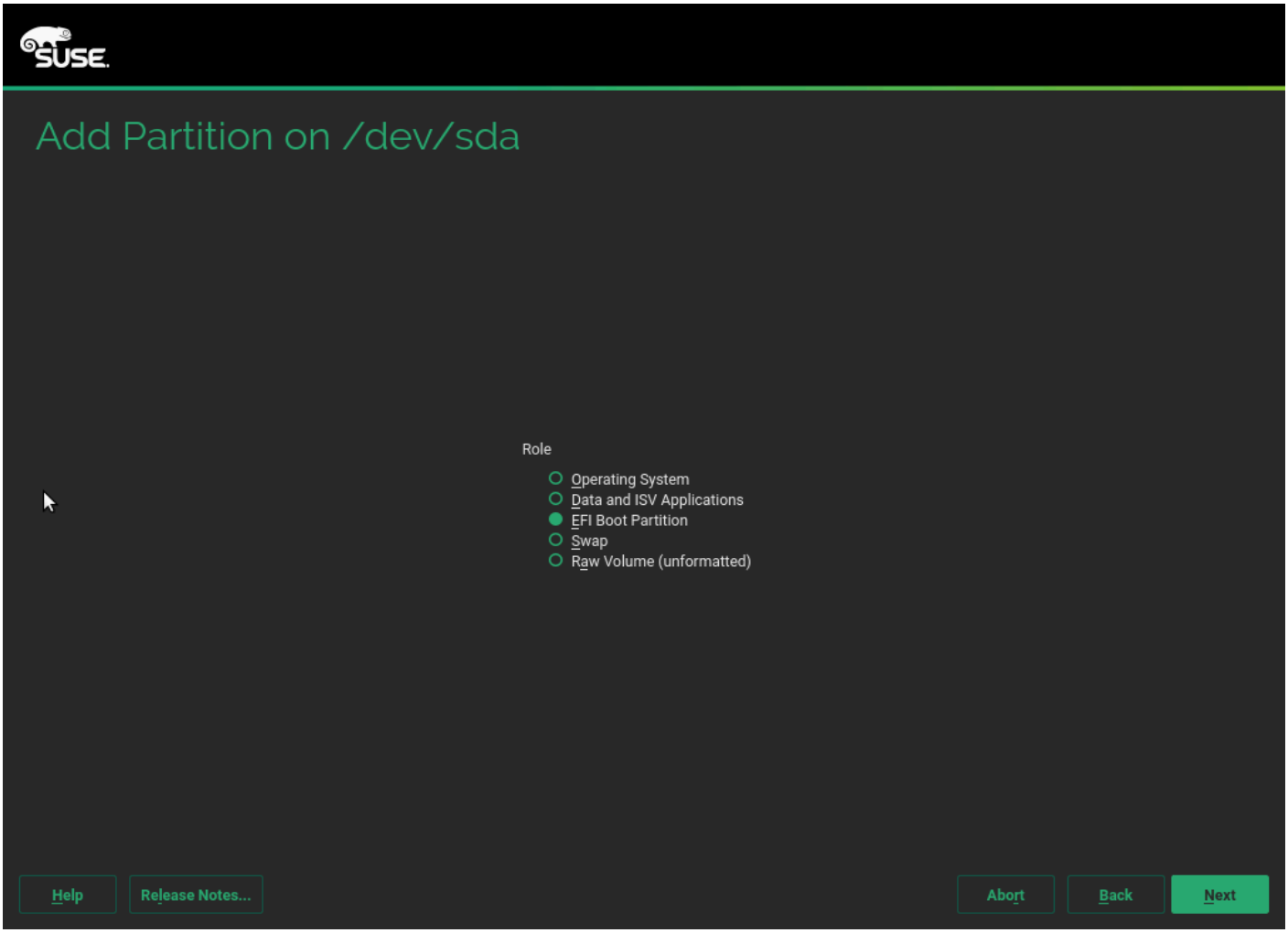
Figure 42. Adding a partition: Specify the new partition size



12. Click Next. For Role, select EFI Boot Partition (Figure 43).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

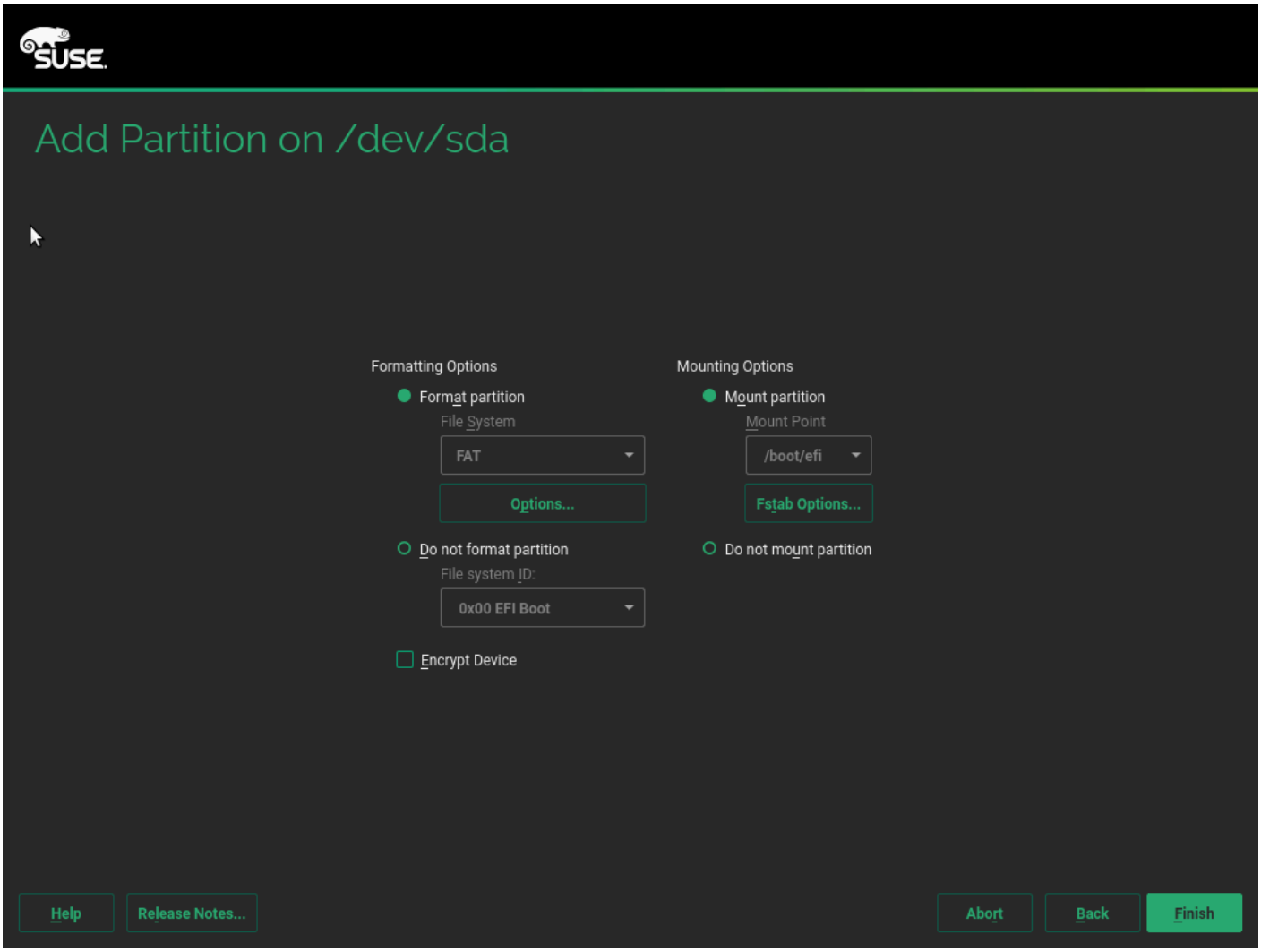
Figure 43. Adding a partition: Specify the role



13. Click Next. By default, the FAT file system is selected, and /boot/efi is selected as the mount point (Figure 44).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

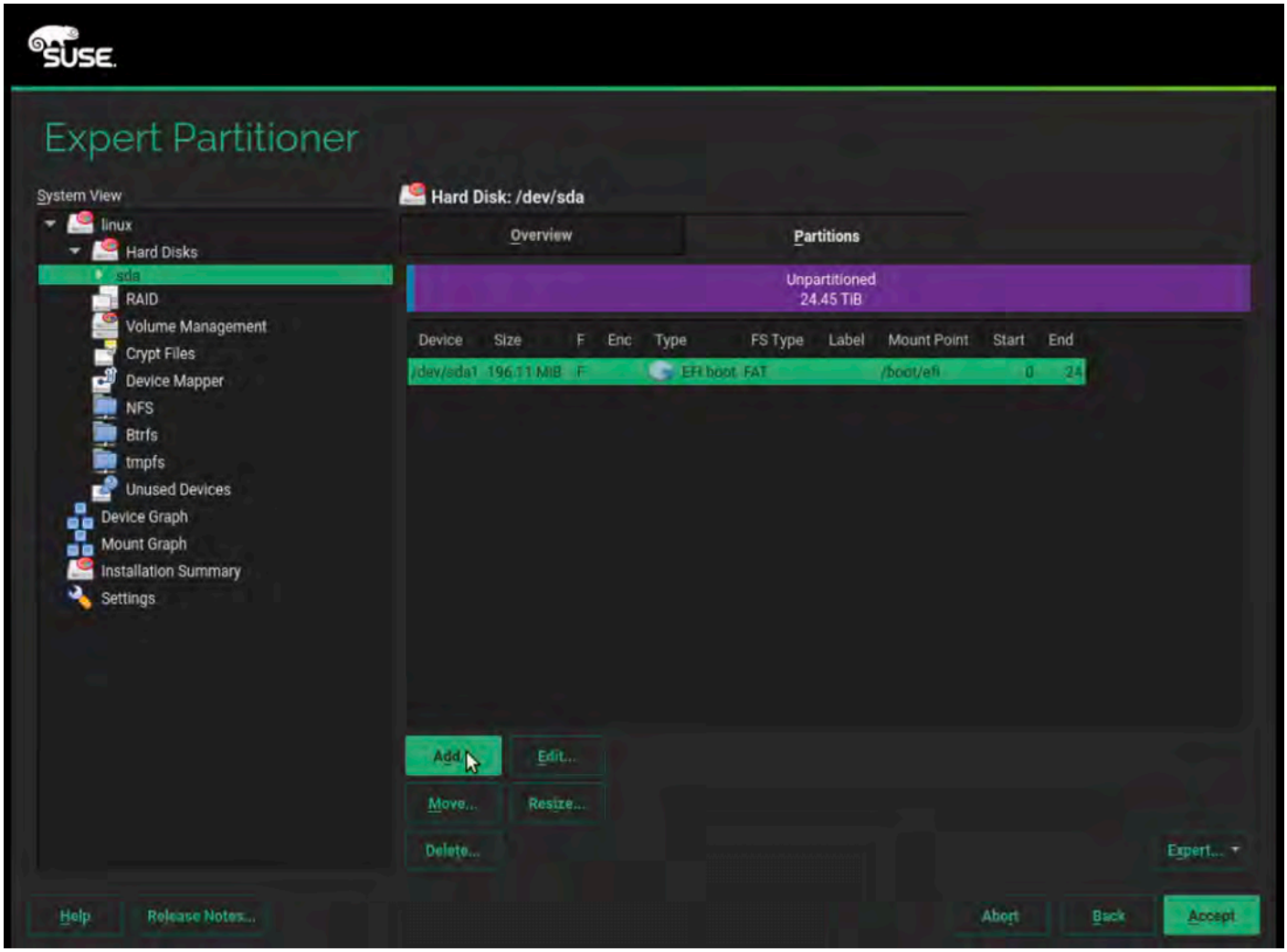
Figure 44. Adding a partition: Select formatting and mounting options



14. Click Finish. Then click Add to add another partition (Figure 45).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

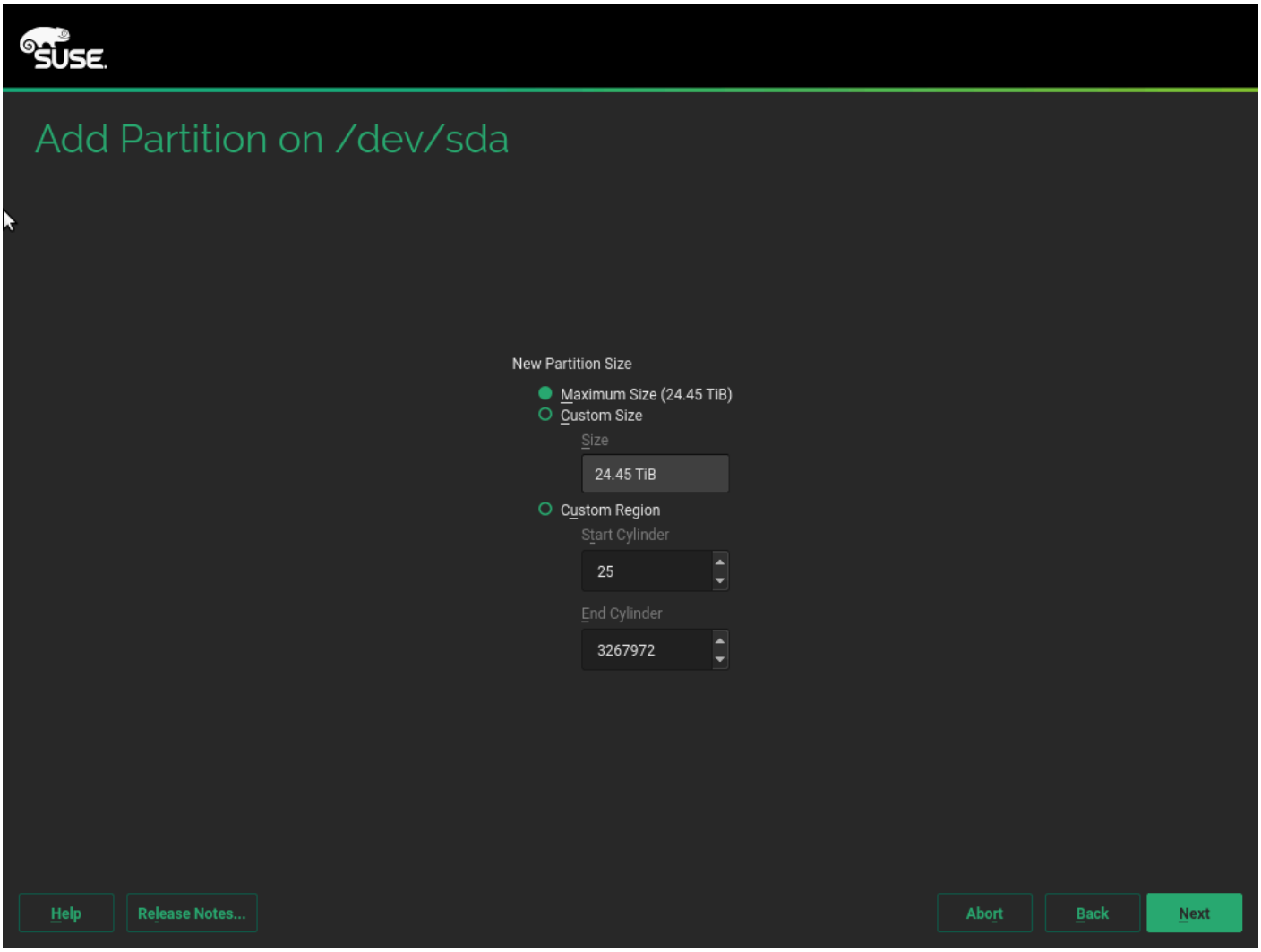
Figure 45. Expert Partitioner: Add another partition



15. Allocate the rest of available space to the partition (Figure 46).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

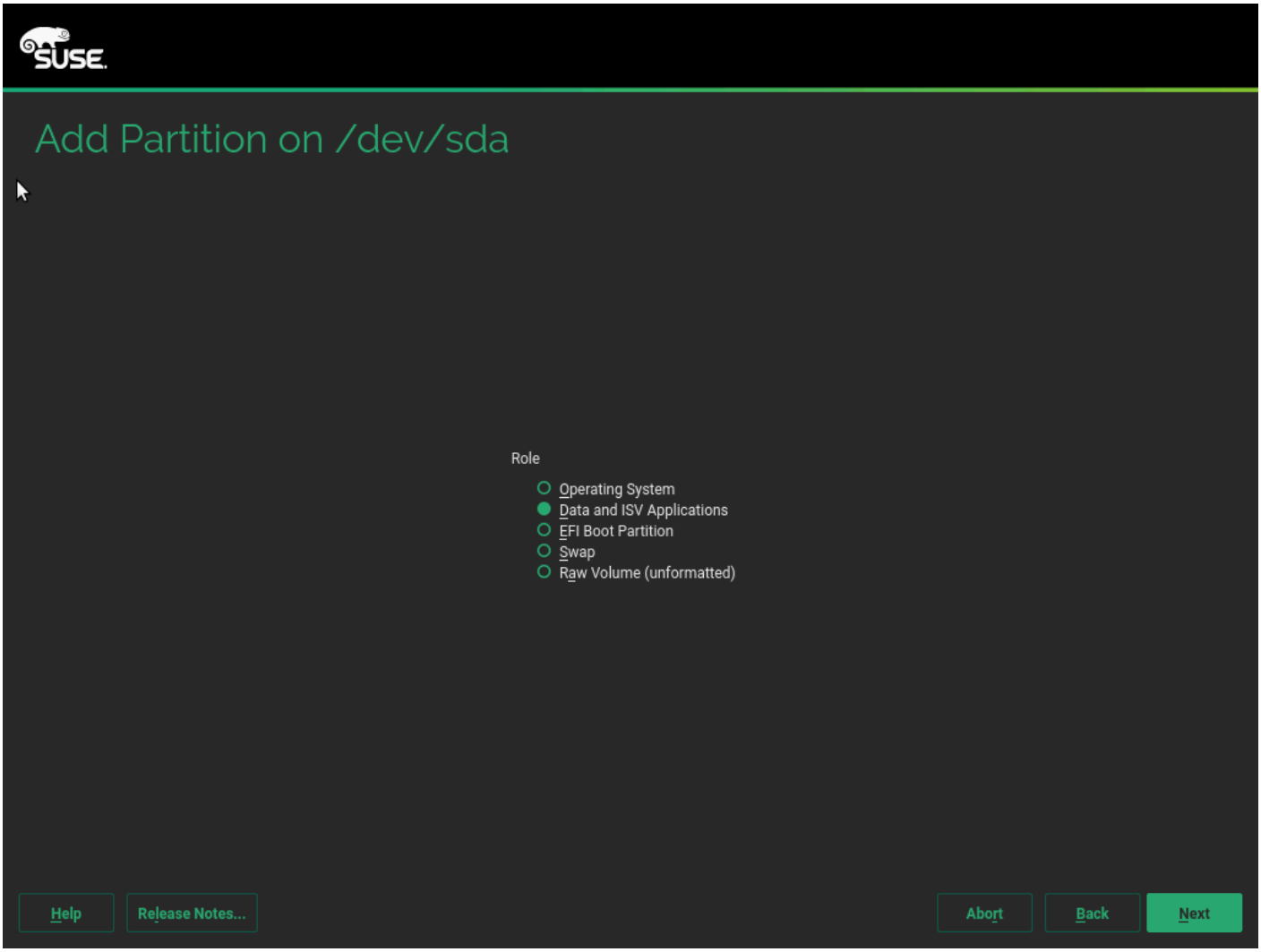
Figure 46. Another partition: Specify the partition size



16. Click Next. For Role, choose Data and ISV Applications (Figure 47).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

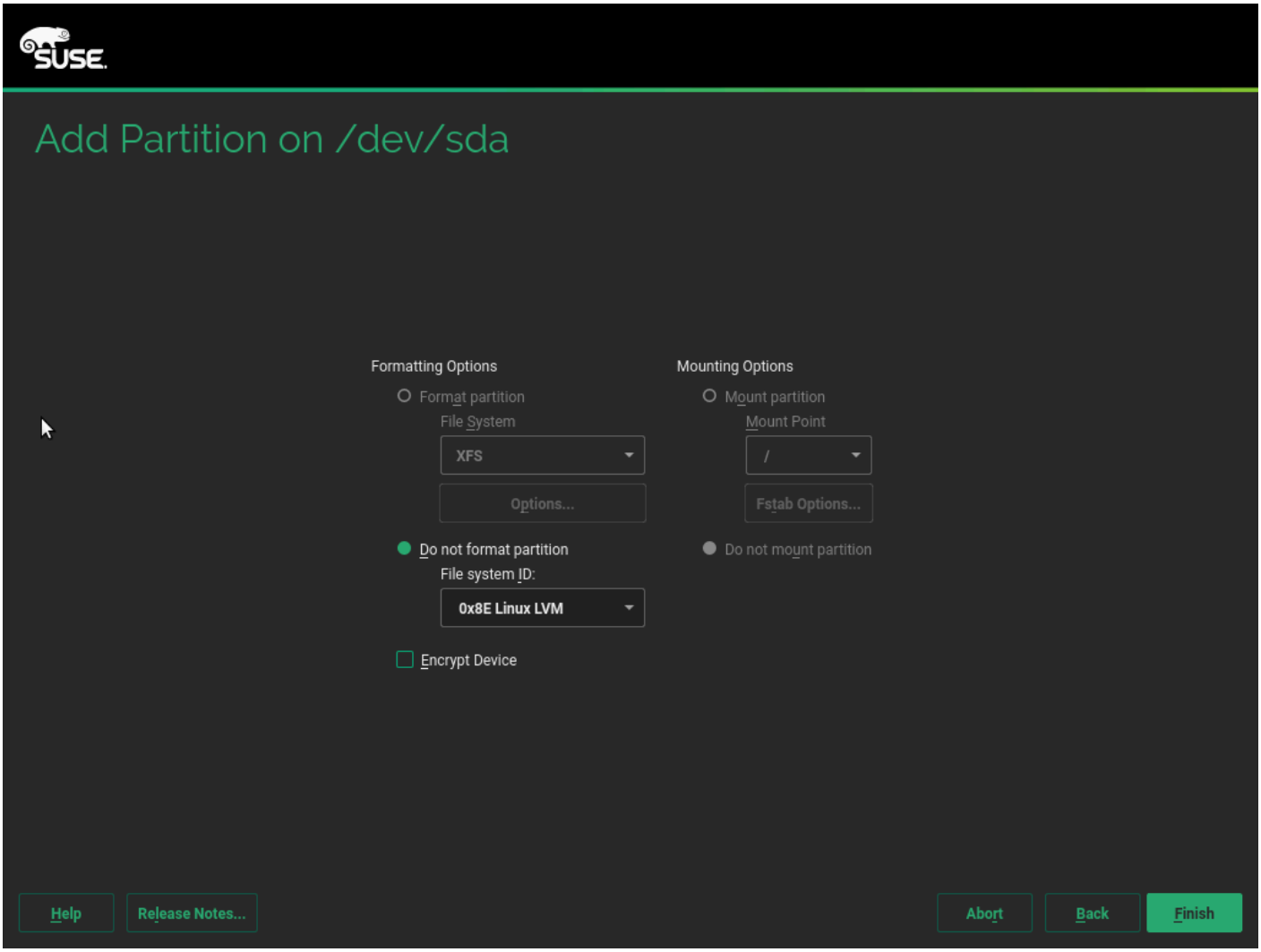
Figure 47. Adding another partition: Specify the role



17. Assign the partition with the file system ID 0x8E Linux LVM (Figure 48).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

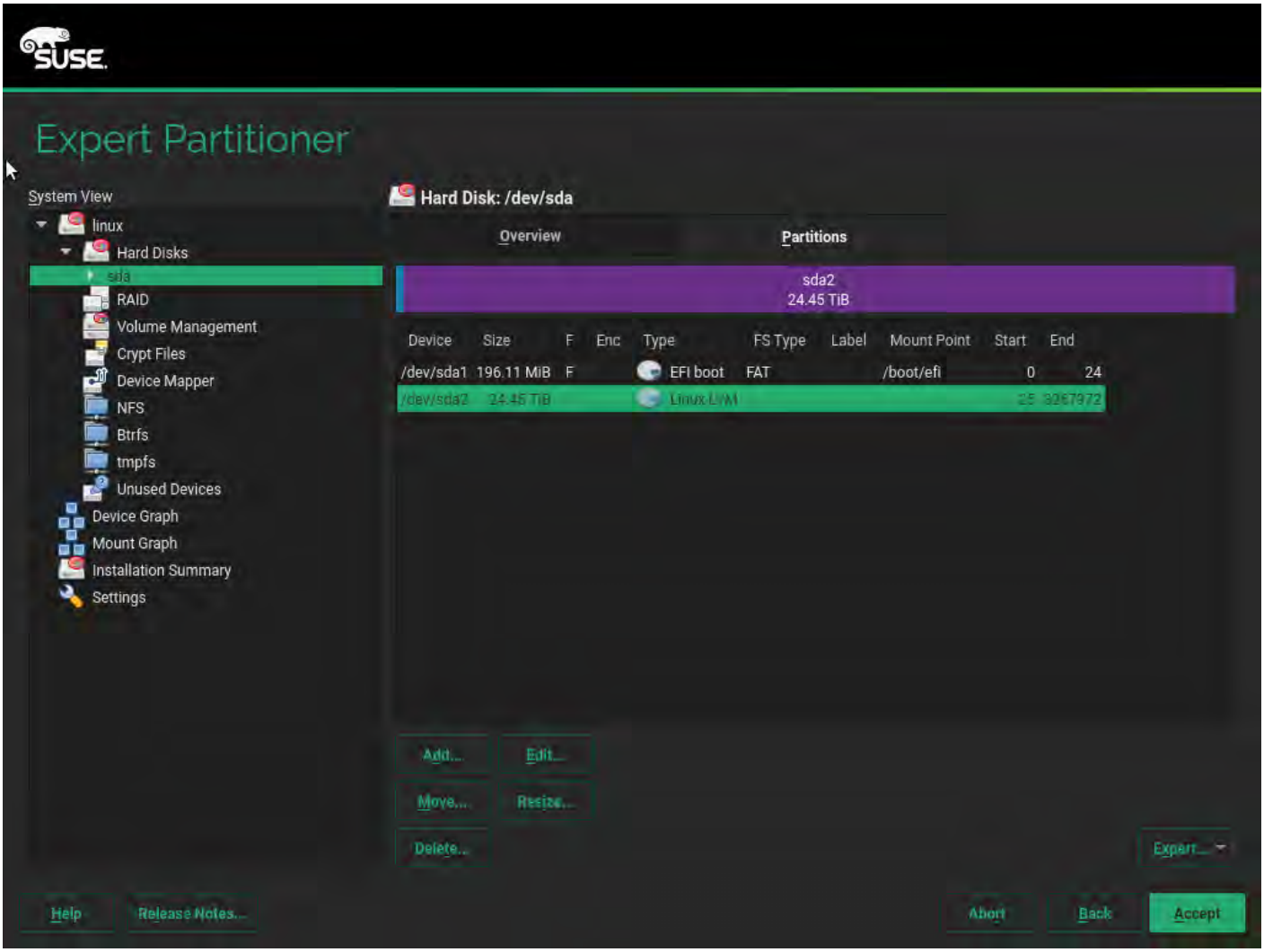
Figure 48. Adding another partition: Specify formatting and mounting options



18. Click Finish. You will see an overview of your partitions (Figure 49).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

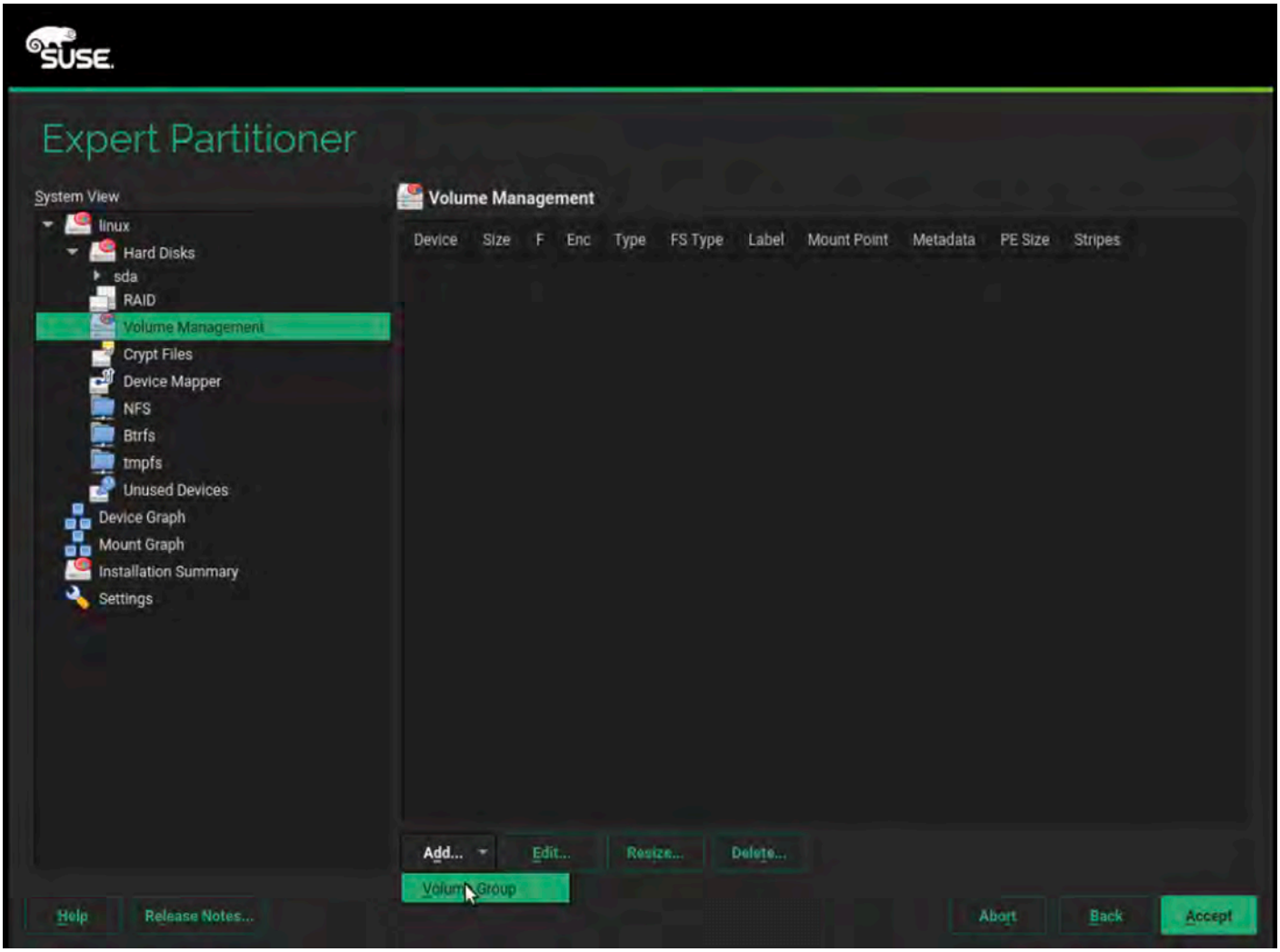
Figure 49. Expert Partitioner: Hard disk /dev/sda partitions overview



19. In the System View pane on the left, select Volume Management. Choose Add > Volume Group (Figure 50).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

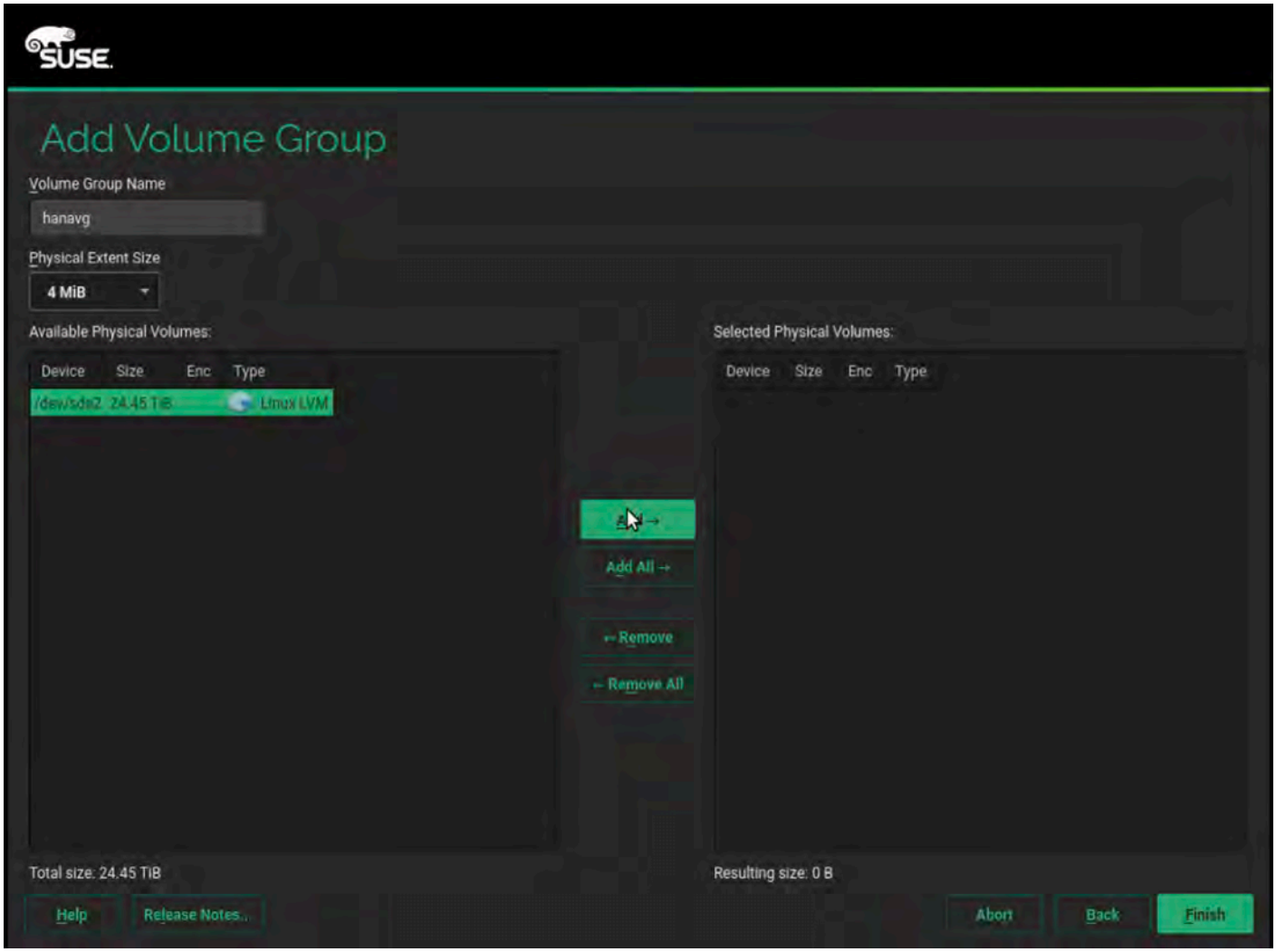
Figure 50. Expert Partitioner volume management: Add a volume group



20. Provide a name for the volume group, select /dev/sda2 from the list of available physical volumes, and click Add (Figures 51 and 52).

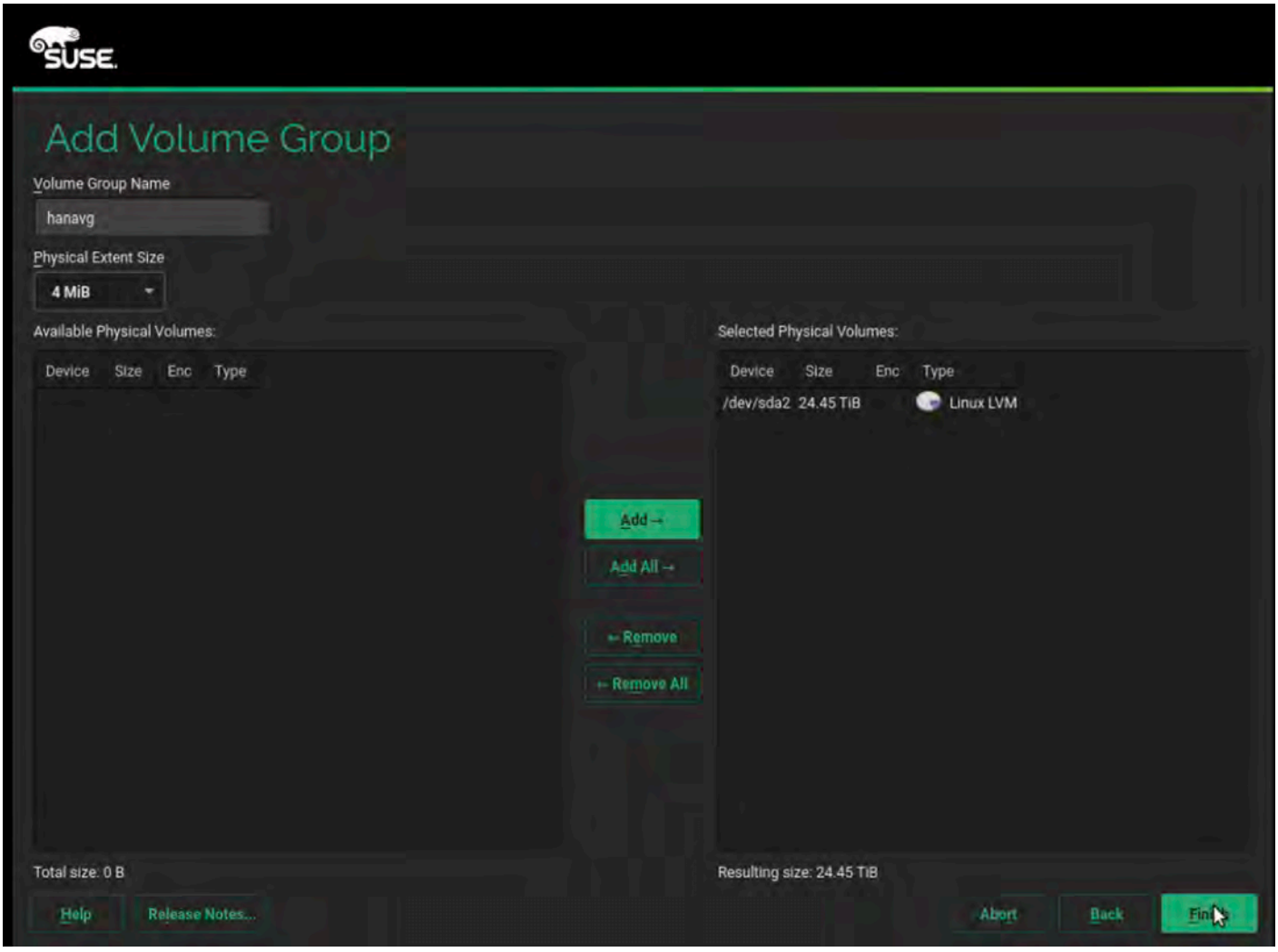
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 51. Add Volume Group: Select an available physical volume



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

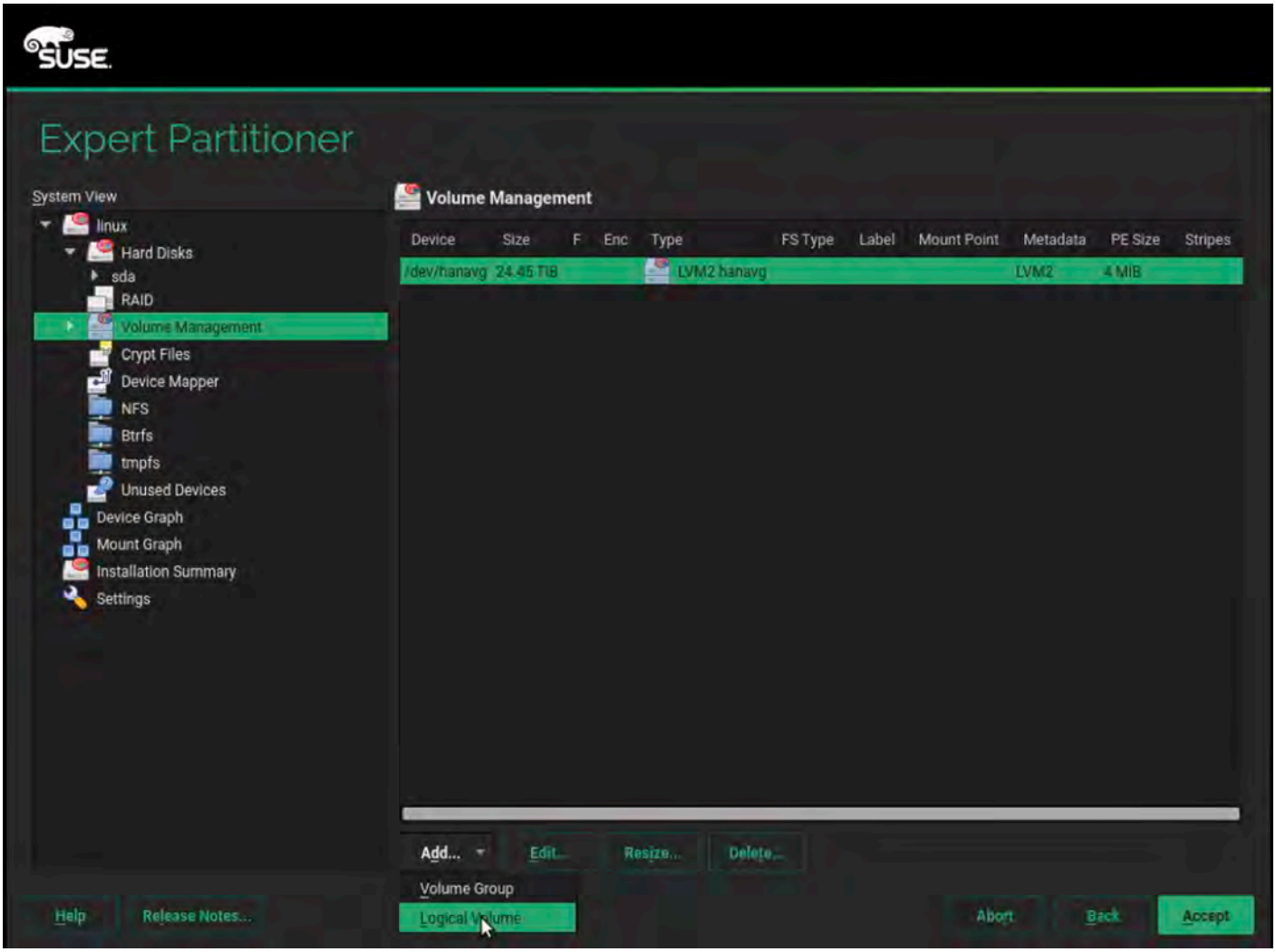
Figure 52. Add Volume Group (continued)



21. Click Finish.
22. Under Volume Management, click Add and select Logical Volume (Figure 53).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

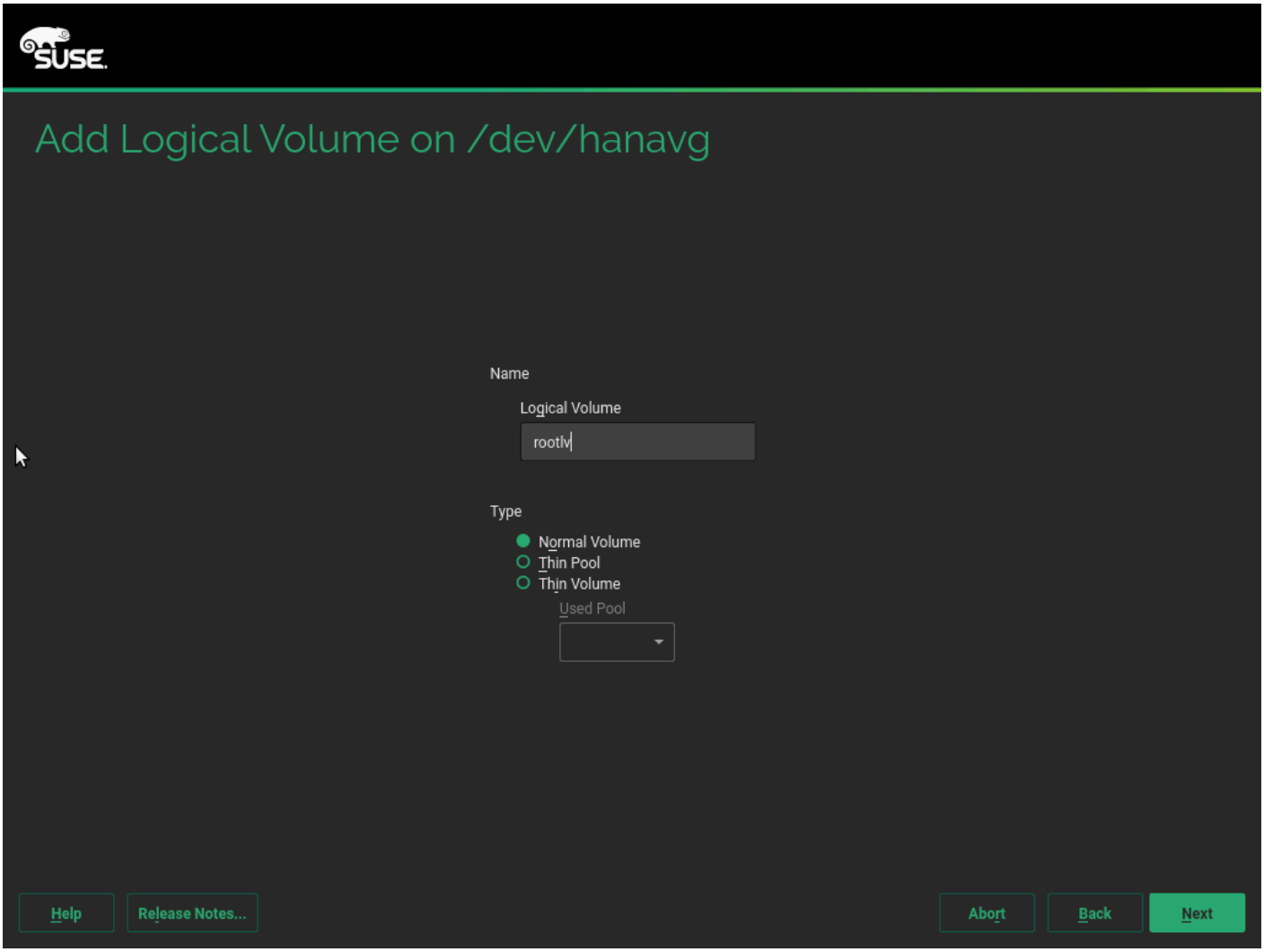
Figure 53. Expert Partitioner: Add a logical volume



23. Add a logical volume with the name **rootlv** in the volume group (Figures 54).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

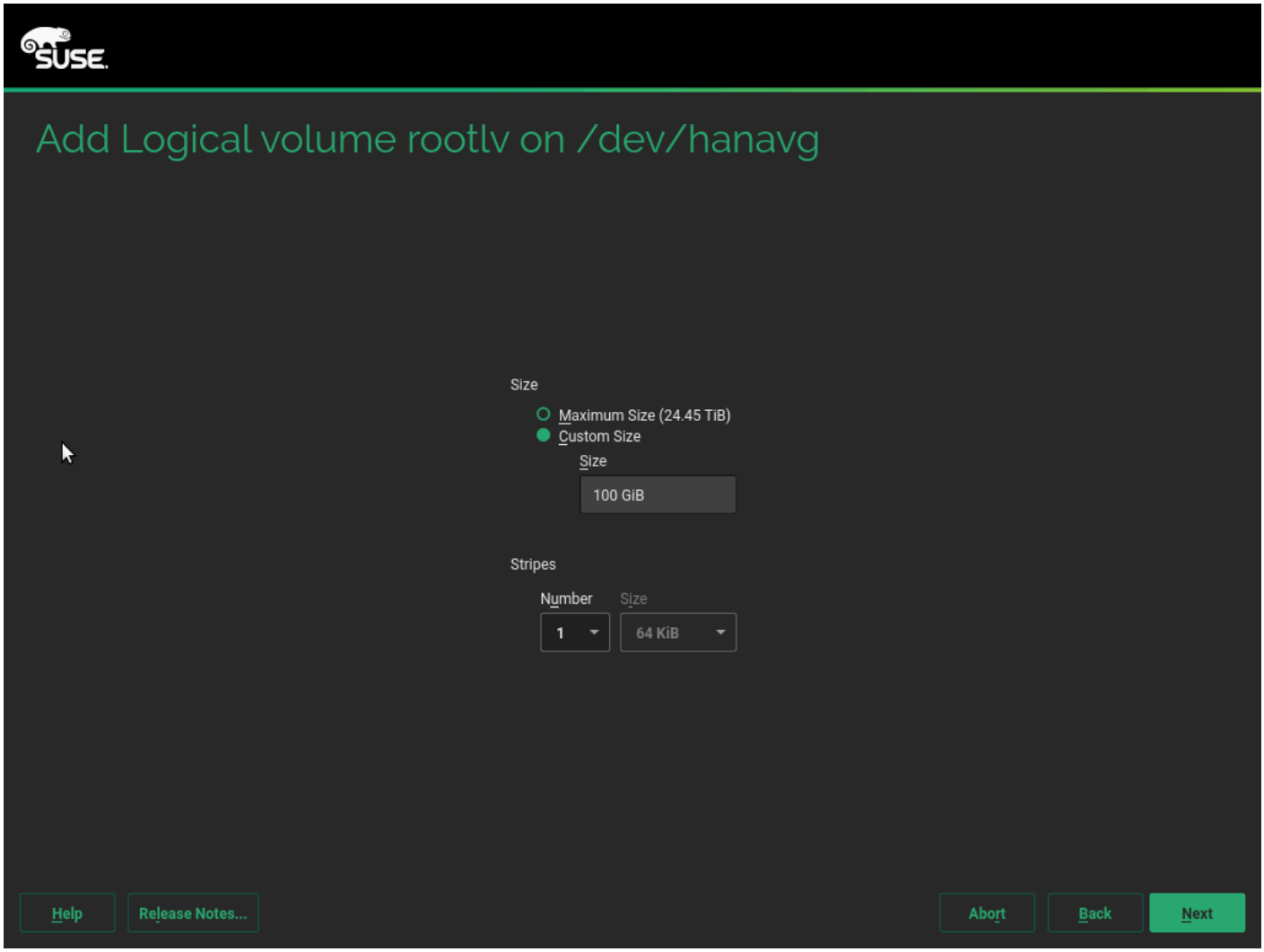
Figure 54. Adding a logical volume: Specify the name and type



24. Click Next. Specify a size of 100 GB and 1 stripe (Figure 55).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

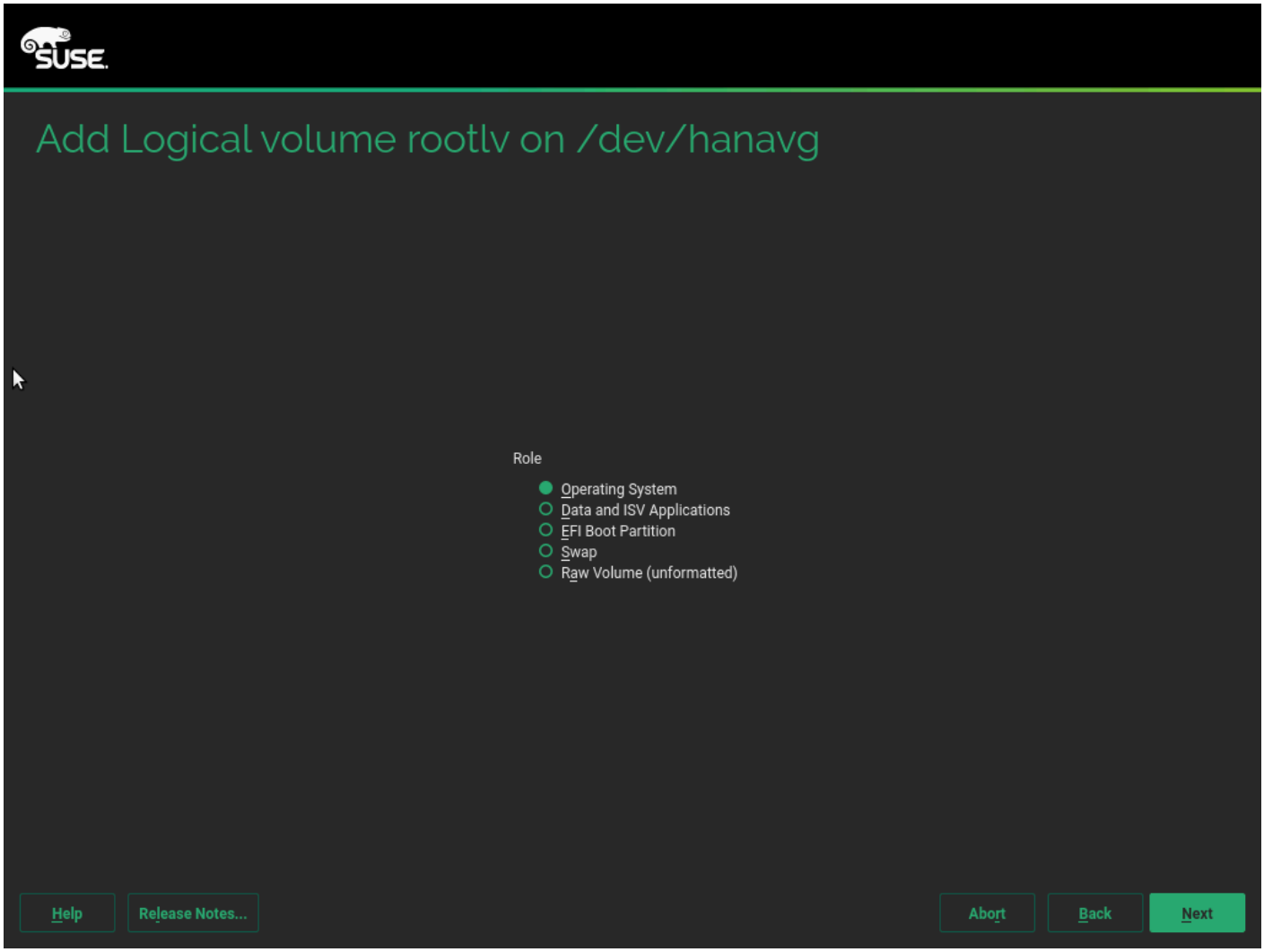
Figure 55. Adding a logical volume: Specify the size and stripe



25. Click Next. For Role, specify Operating System (Figure 56).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

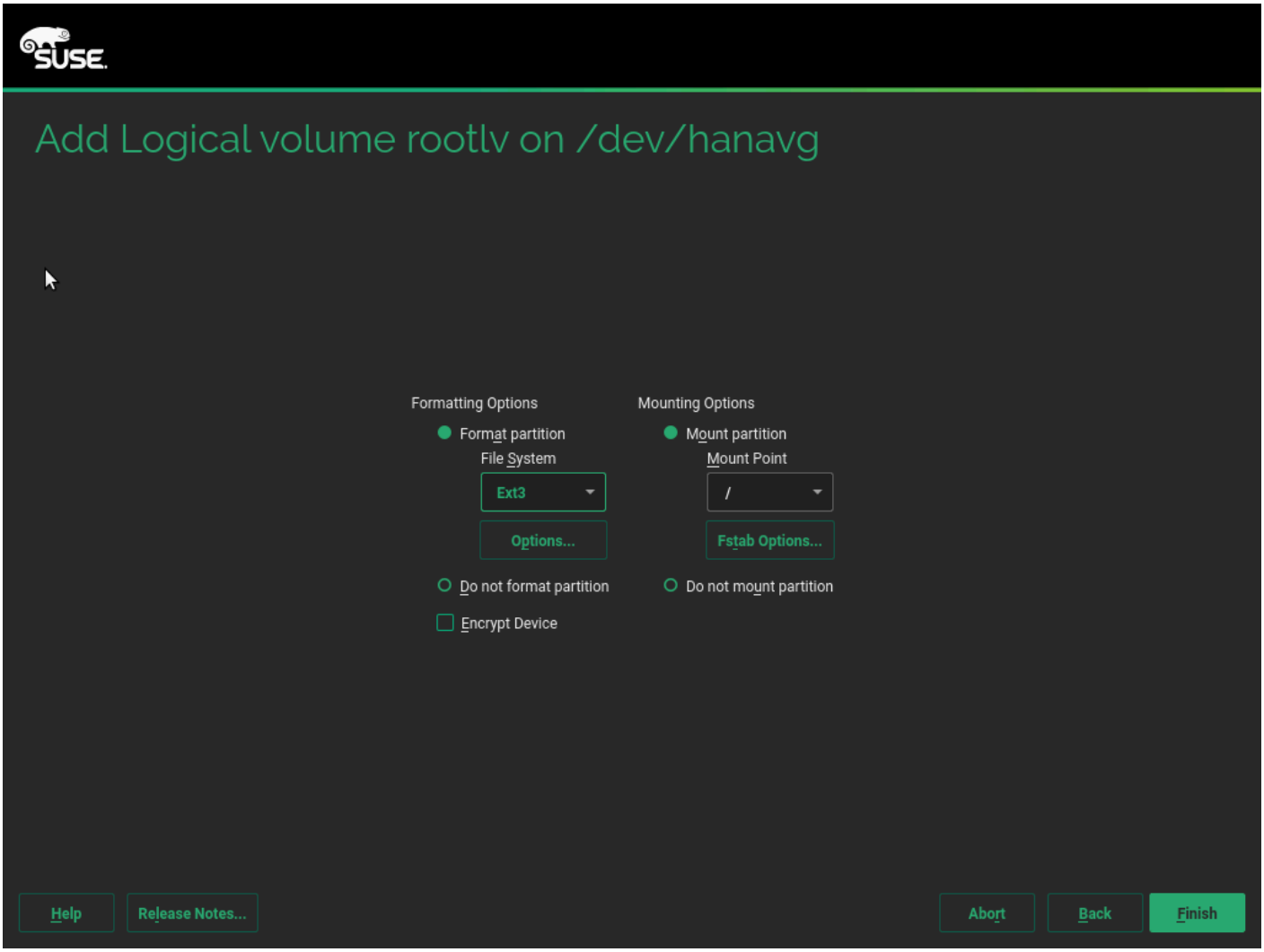
Figure 56. Adding a logical volume: Specify the role



26. Click Next. Specify the formatting and mounting options. Format the 100-GB logical volume rootlv with the Ext3 file system and assign the / mount point (Figure 57).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

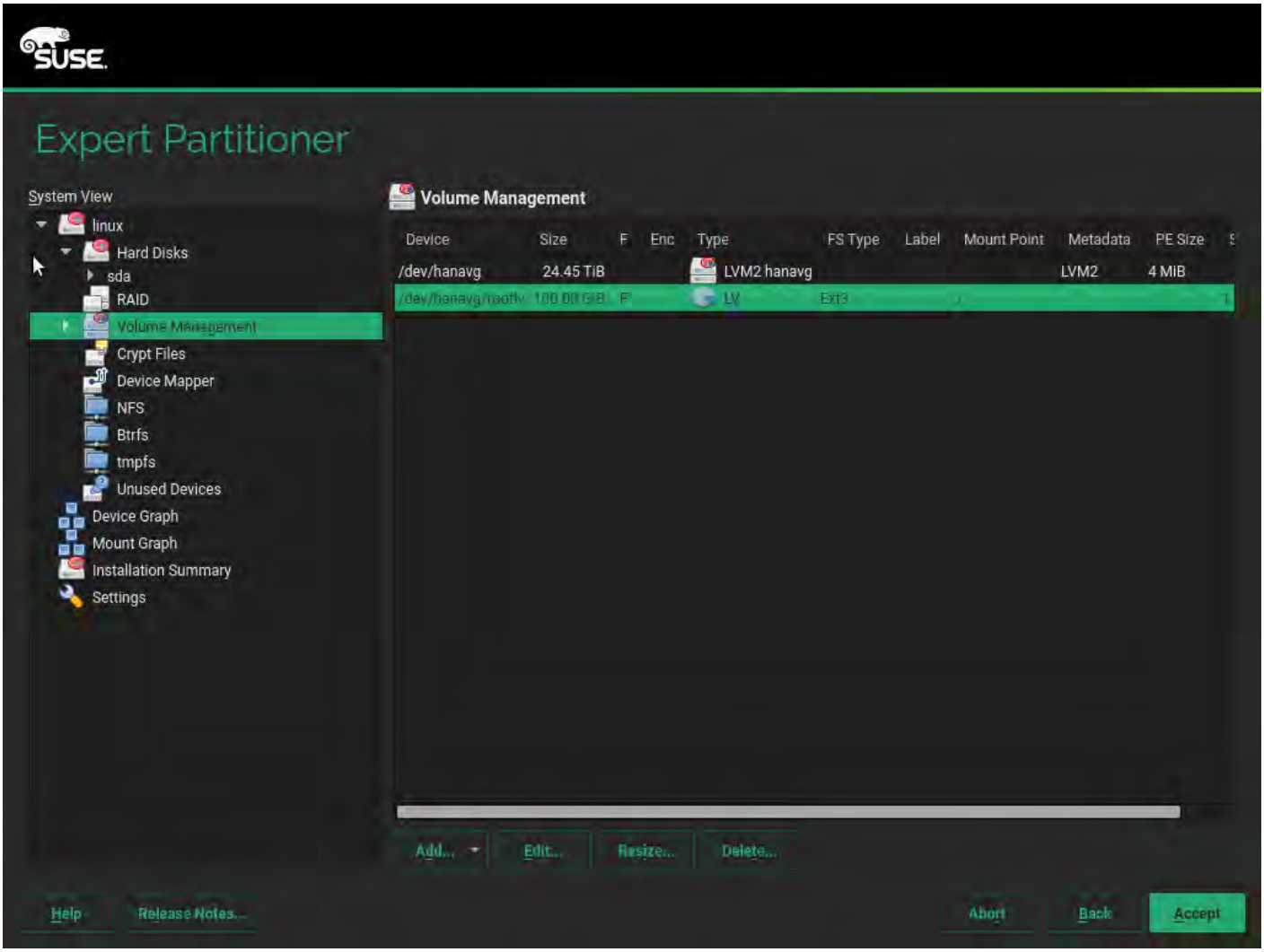
Figure 57. Adding a logical volume: Specify formatting and mounting options



27. Click Finish.
28. Create a swap volume with a size of 2 GB. Under Volume Management, click Add and select Logical Volume (Figure 58).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

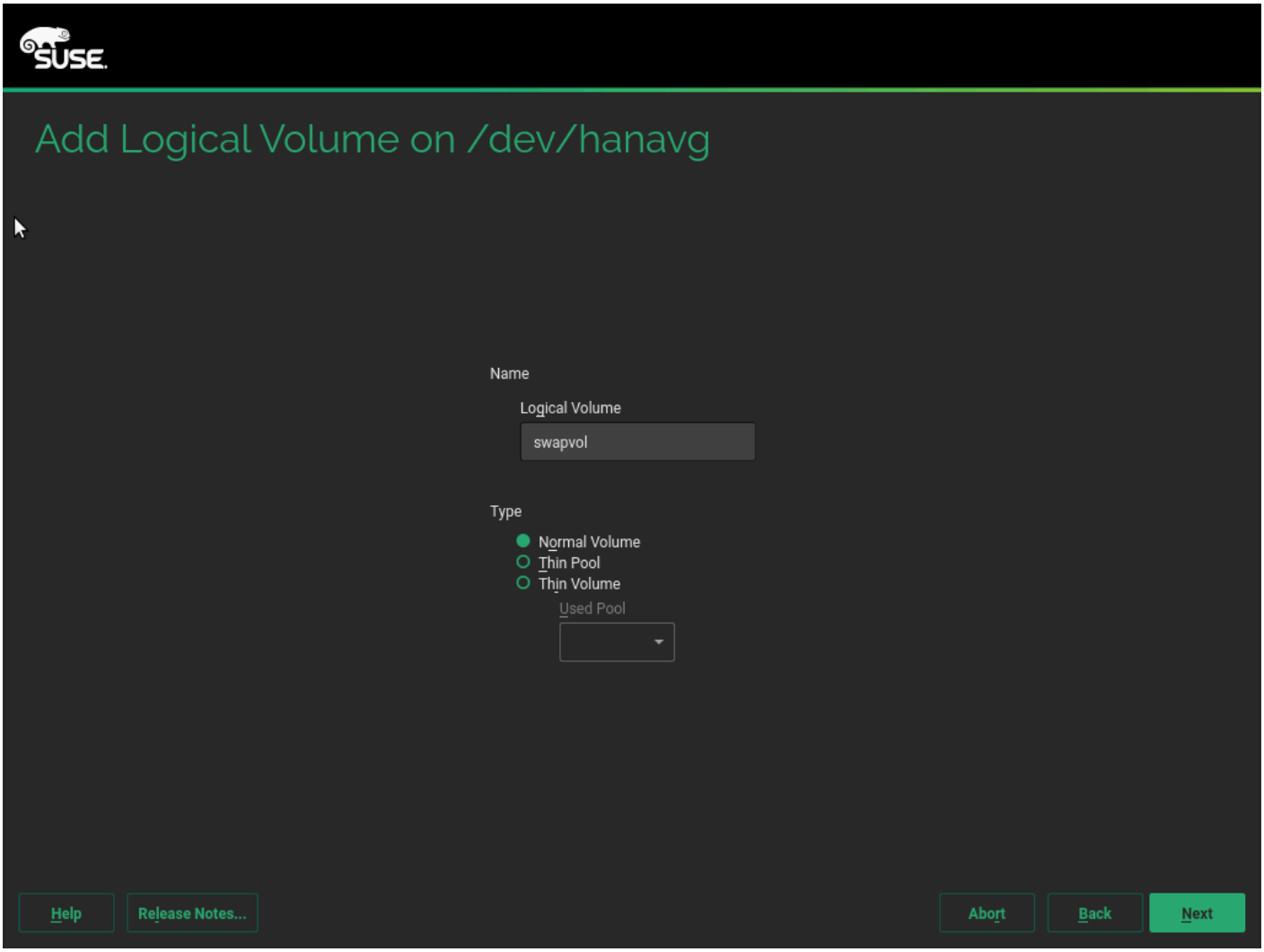
Figure 58. Expert Partitioner volume management: Add another logical volume



29. Add a logical volume for swapping with the name **swapvol** (Figure 59). Then click Next.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

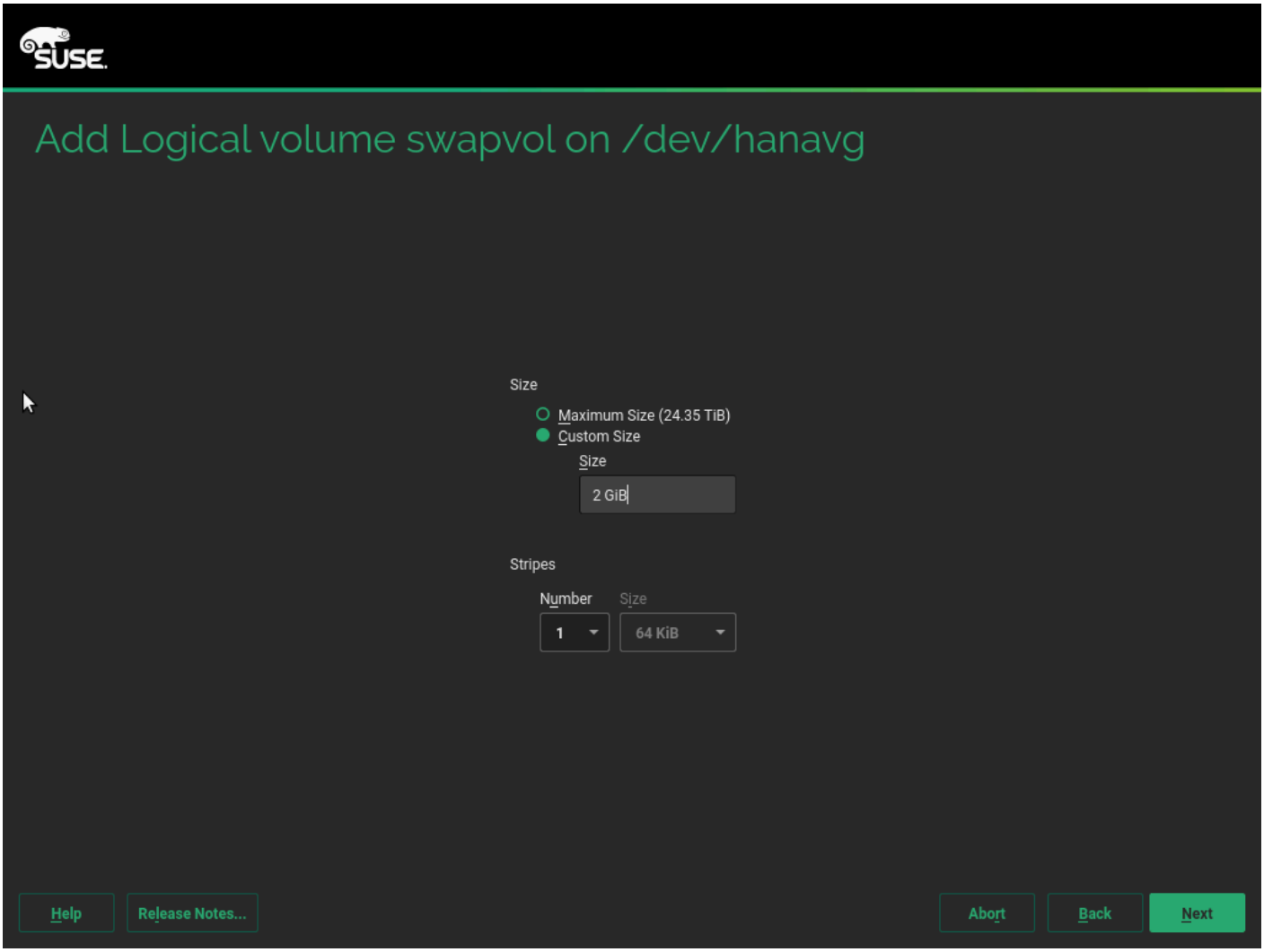
Figure 59. Adding another logical volume: Specify the name and type



30. Assign a space of 2 GB and one stripe (Figure 60). Then click Next.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 60. Adding another logical volume: Specify size and stripe information



31. For Role, select Swap (Figure 61). Then click Next.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

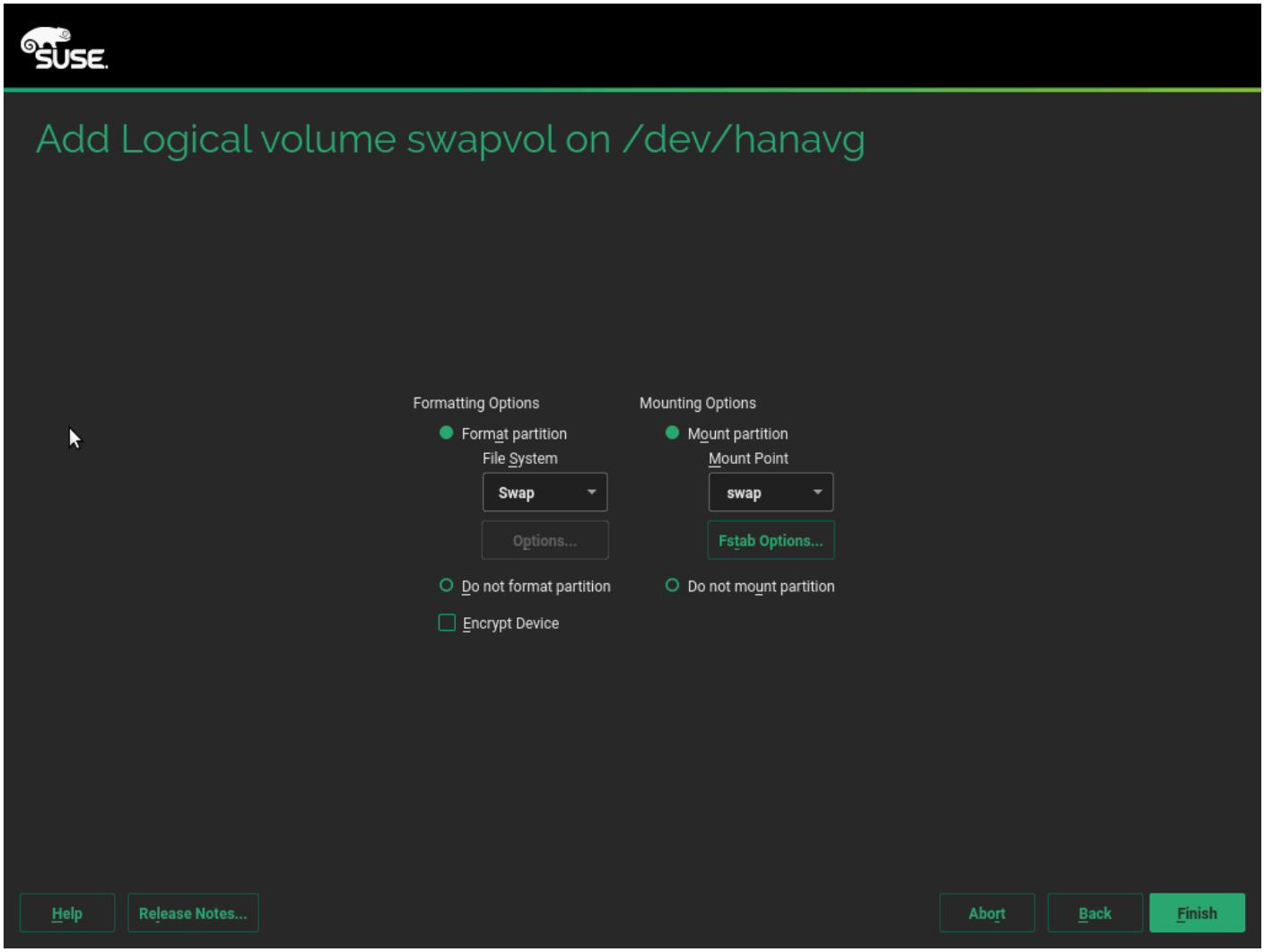
Figure 61. Adding another logical volume: Specify the role



32. Specify the formatting a mounting options (Figure 62).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

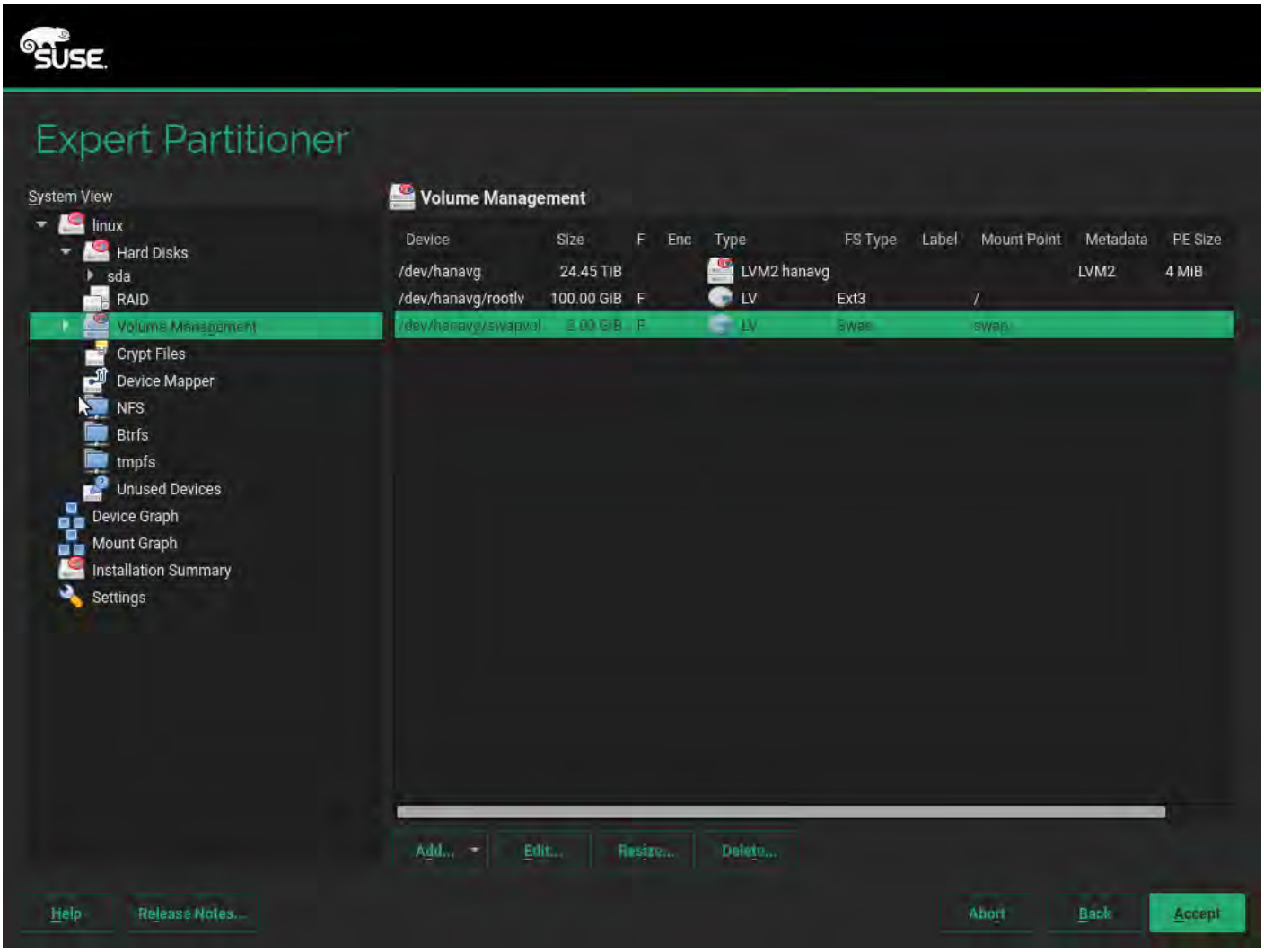
Figure 62. Adding another logical volume: Specify formatting and mounting options



33. Click Finish. A summary page appears (Figure 63).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

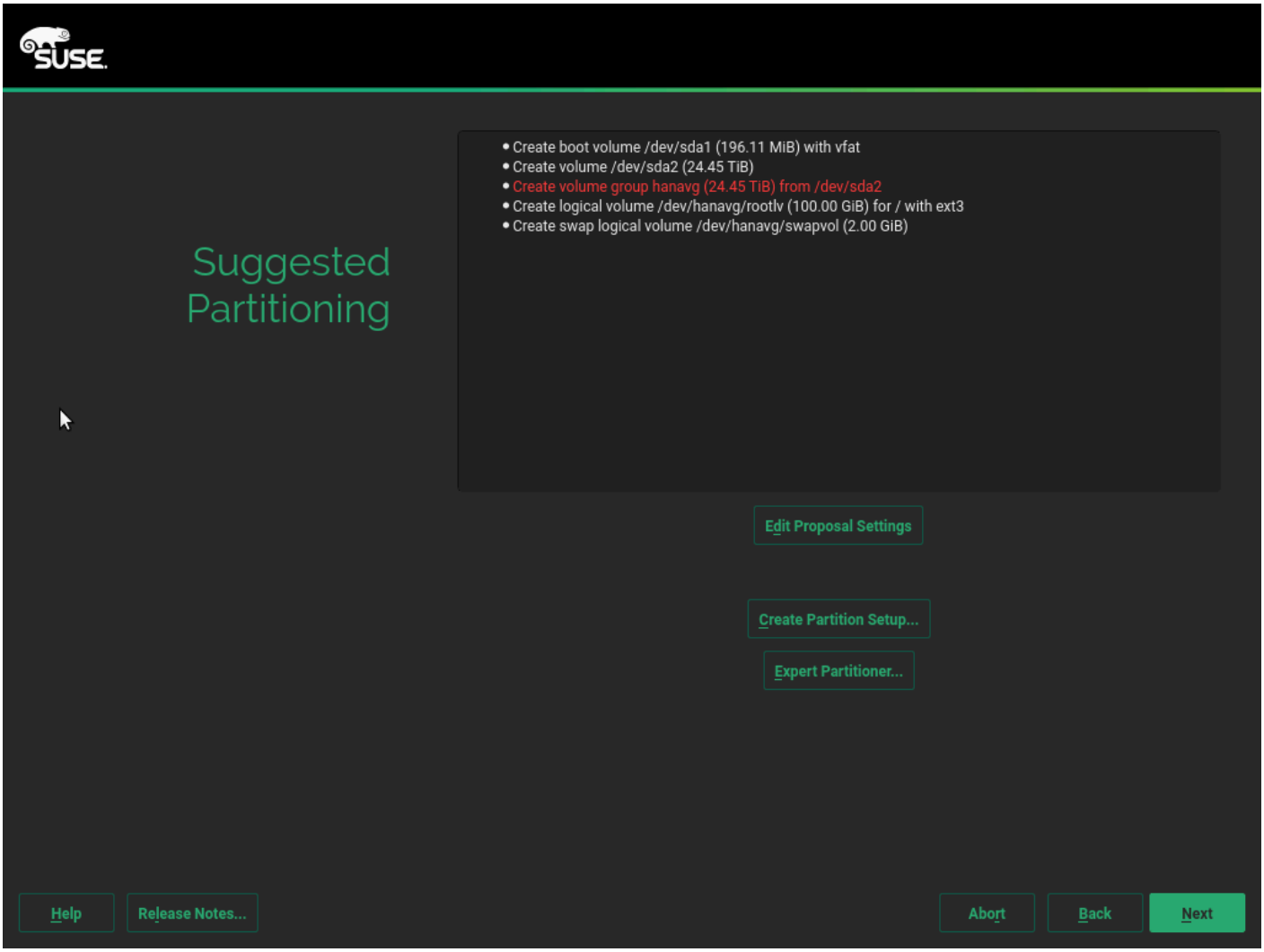
Figure 63. Expert Partitioner: Volume management summary page



34. Click Accept to return to the Installation Settings page.
35. Review the updated partition information (Figure 64). Then click Next.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

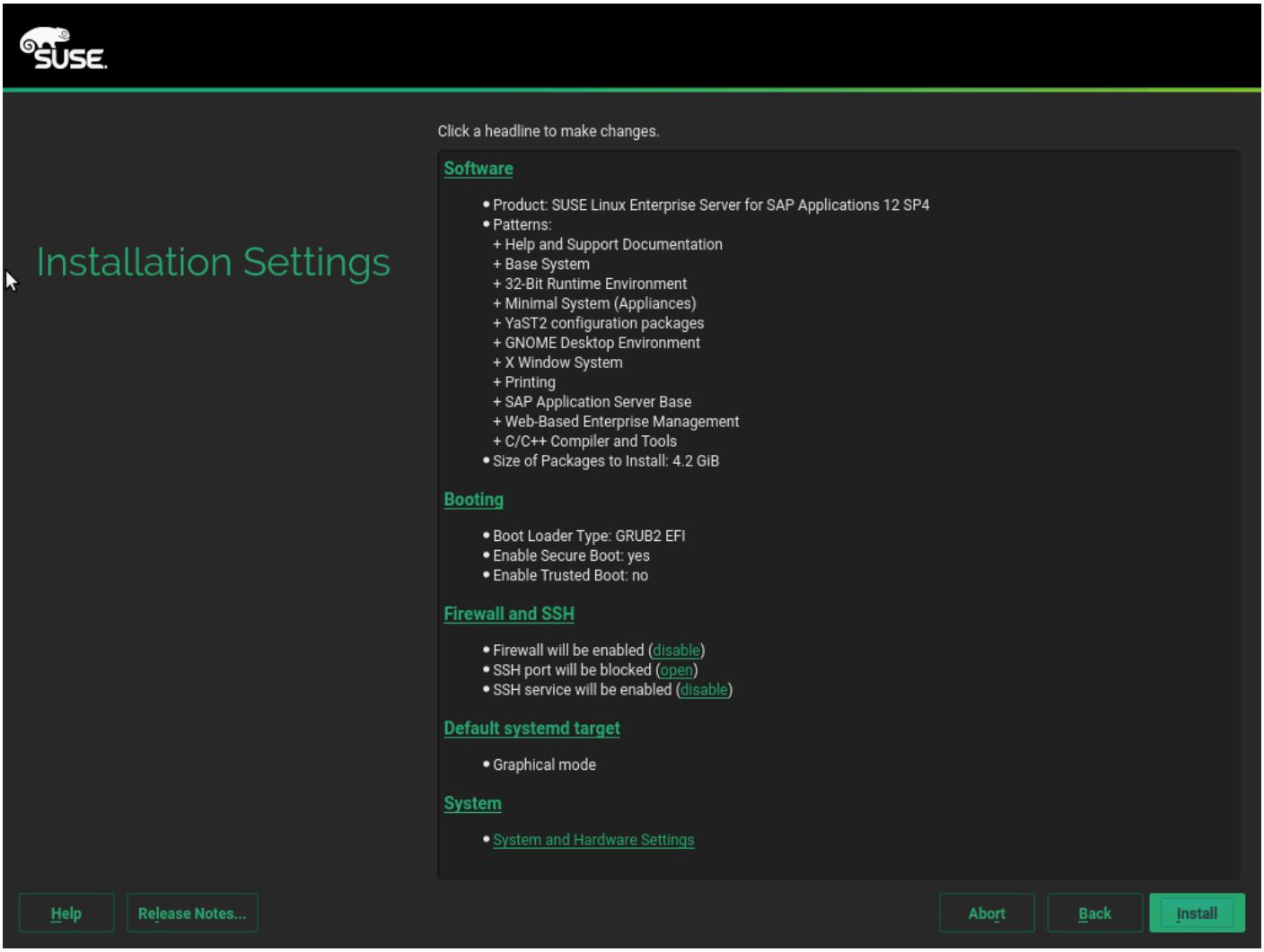
Figure 64. Updated partition information



36. For Clock and Time Zone, choose the appropriate time zone and select the hardware clock set to UTC.
37. For the password for the system administrator root, enter the appropriate password using <<var_sys_root-pw>>.
38. On the Installation Settings screen, review the default information (Figure 65).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

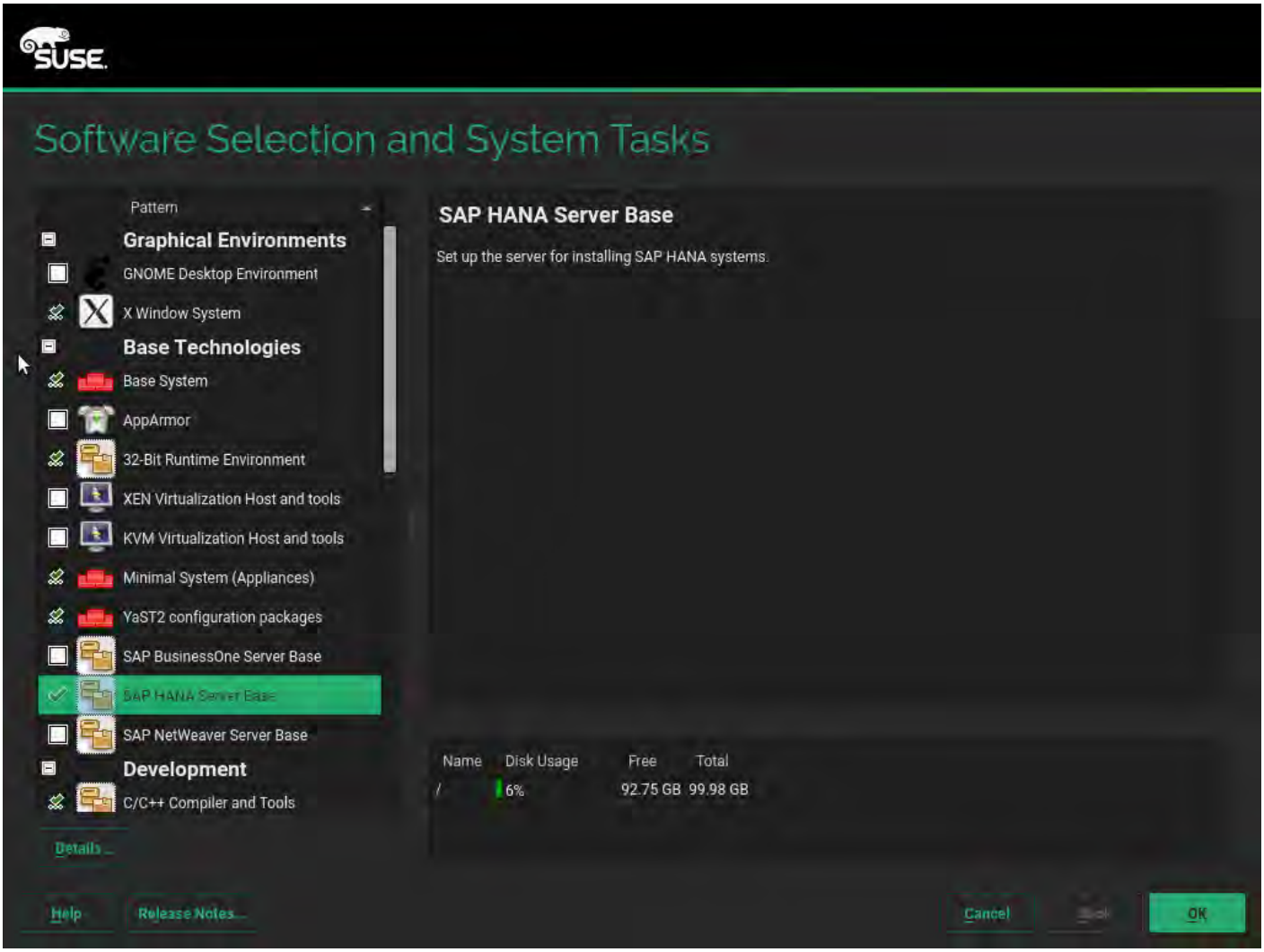
Figure 65. Installation Settings: Default proposal



39. Customize the software selection. Click the Software headline to make changes as shown in Figure 66.
    a. Deselect Gnome Desktop Environment.
    b. Deselect Web-Based Enterprise Management
    c. Select C/C++ Compiler and Tools.
    d. Select SAP HANA Server Base.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

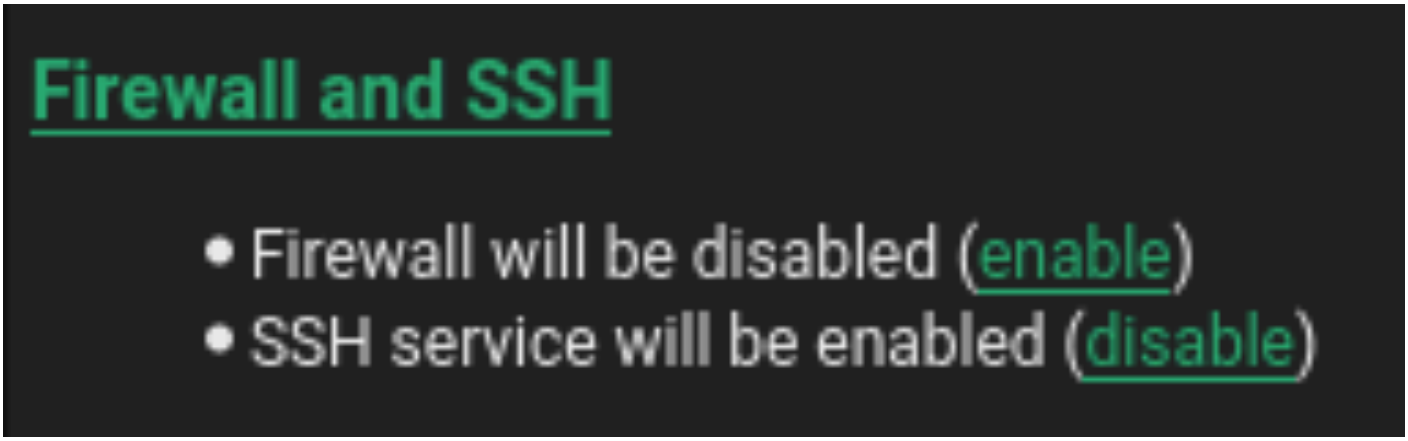
Figure 66. Software Selection and System Tasks: Customized settings



40. Click OK.
41. Under then Firewall and SSH headline, disable the firewall. This selection will automatically enable Secure Shell (SSH) service (Figure 67).

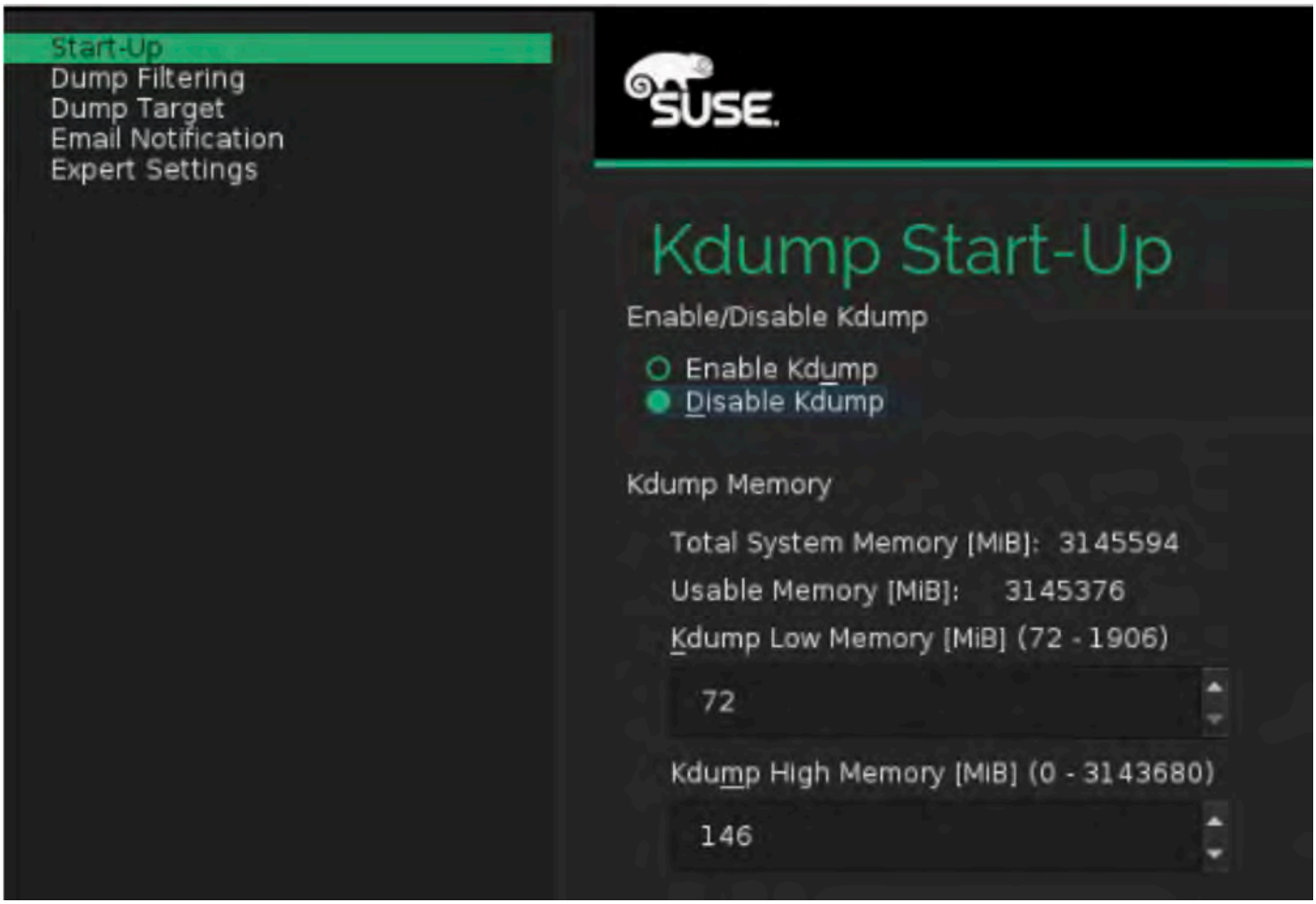
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 67. Firewall and SSH service customized



42. Click the Kdump headline and select Disable Kdump (Figure 68).

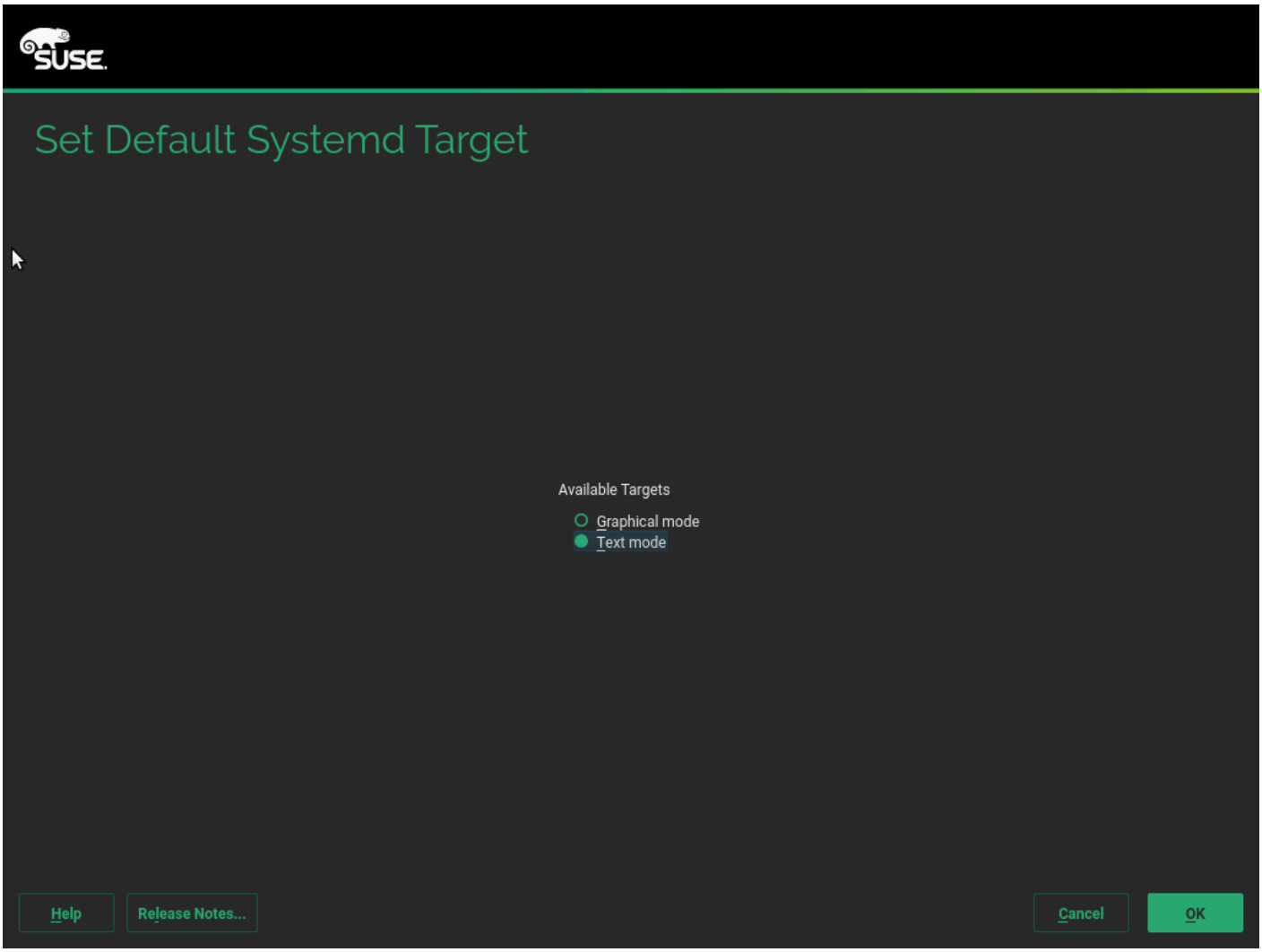
Figure 68. Disabling Kdump



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

43. Click OK.
44. Click the “Default systemd target” headline and choose “Text mode” (Figure 69).

Figure 69. Setting the default system target to Text mode



45. Click OK.
46. Click the Clone System Configuration headline and click “do not write it” (Figures 70 and 71).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 70. Clone system configuration selection

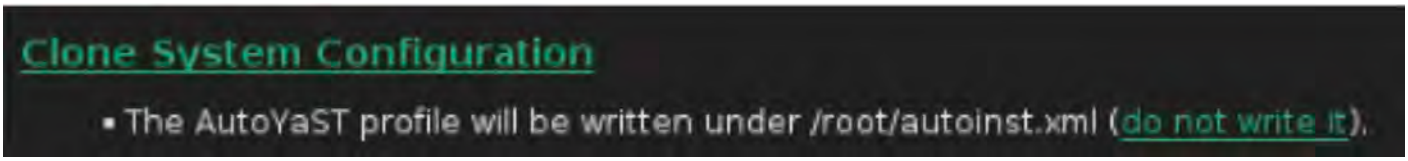
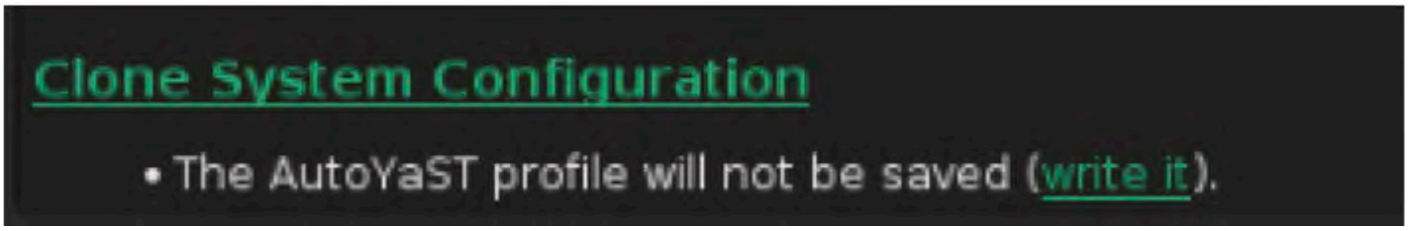


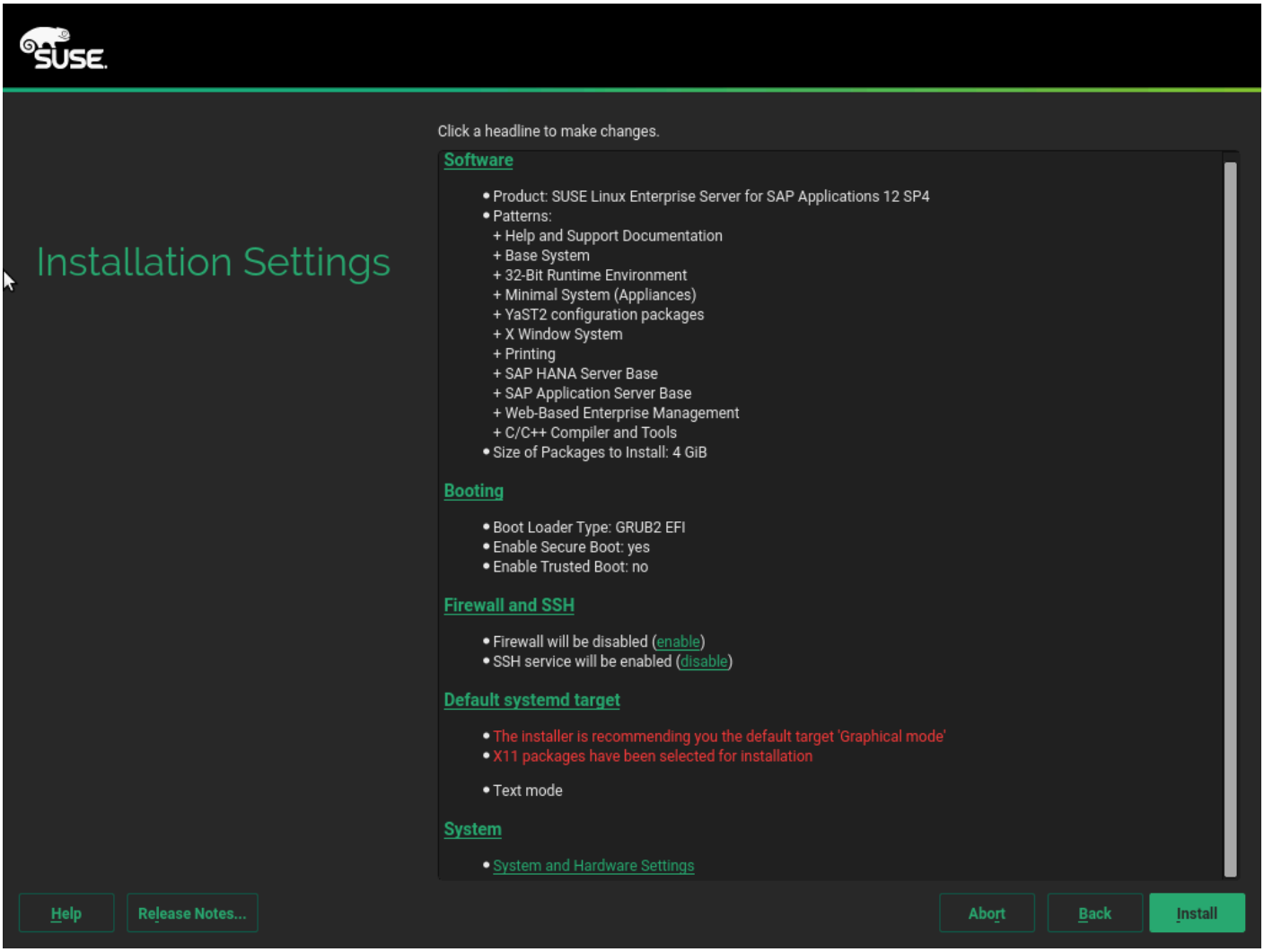
Figure 71. Clone system configuration selection (continued)



47. Leave the Booting and System default selections unchanged (Figure 72).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

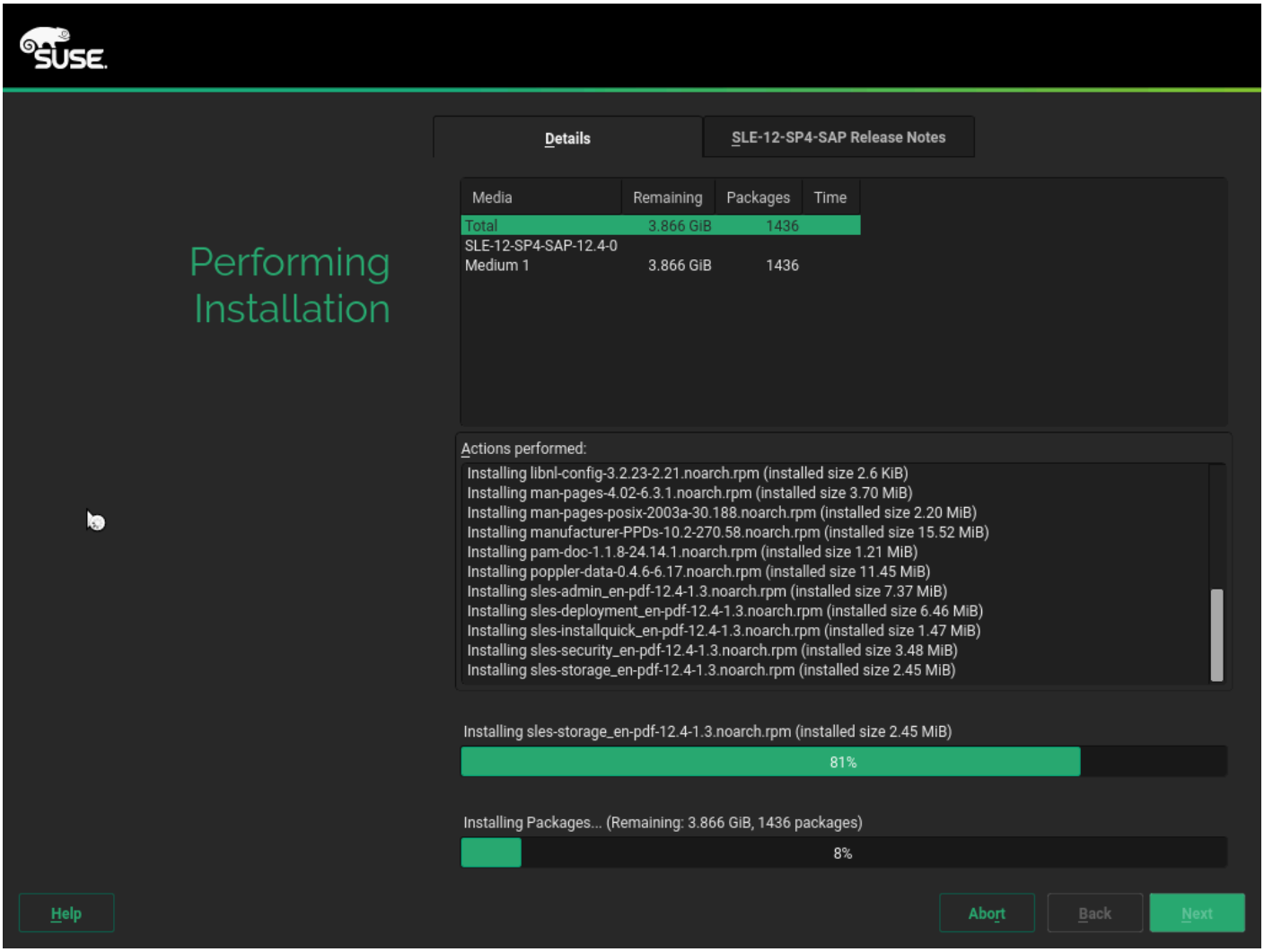
Figure 72. Installation Settings: Final selections



48. Click Install. Also select Install at subsequent Confirm Installation prompts. The installation starts, and you can monitor the status (Figures 73).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 73. Performing the installation



After the installation is complete, a reboot alert appears. The system will reboot and boot from disk on startup (Figure 74).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

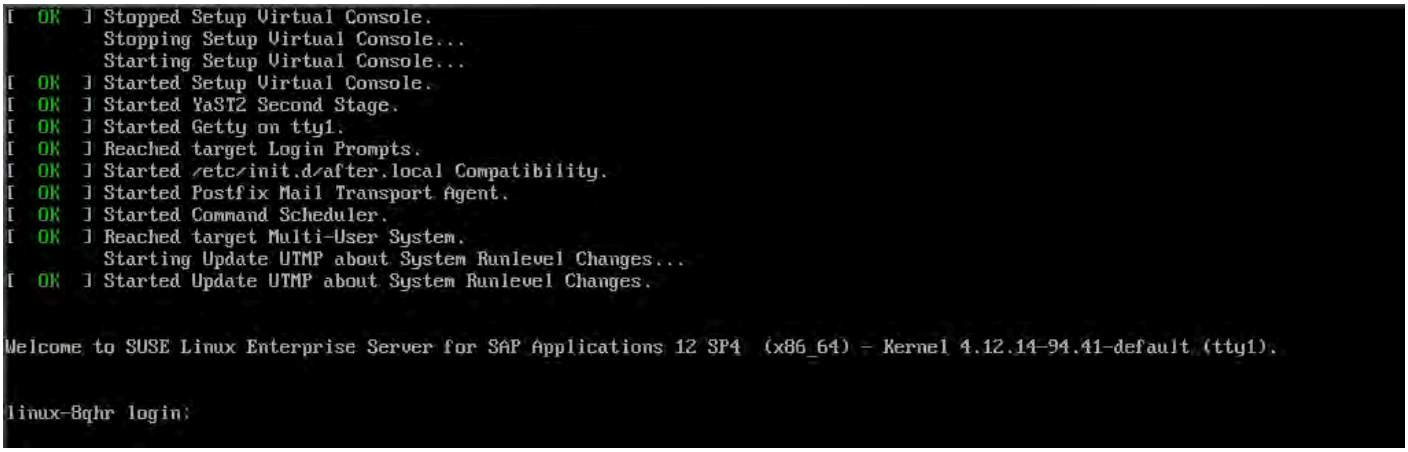
Figure 74. Booting from hard disk



The system then displays the login prompt (Figure 75).

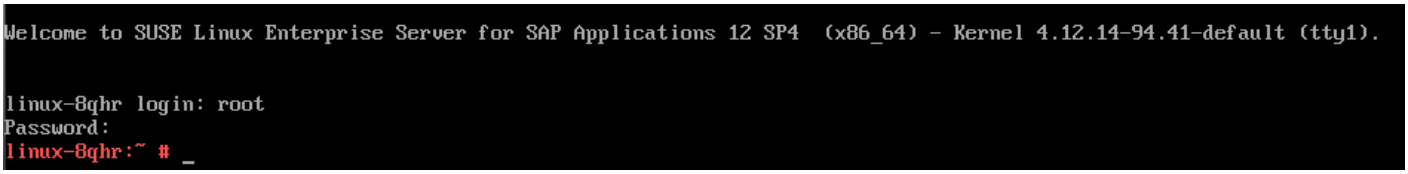
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 75. Login prompt



49. Use the KVM console to log in to the installed system as the user root with the password <<var_sys_root-pw>> (Figure 76).

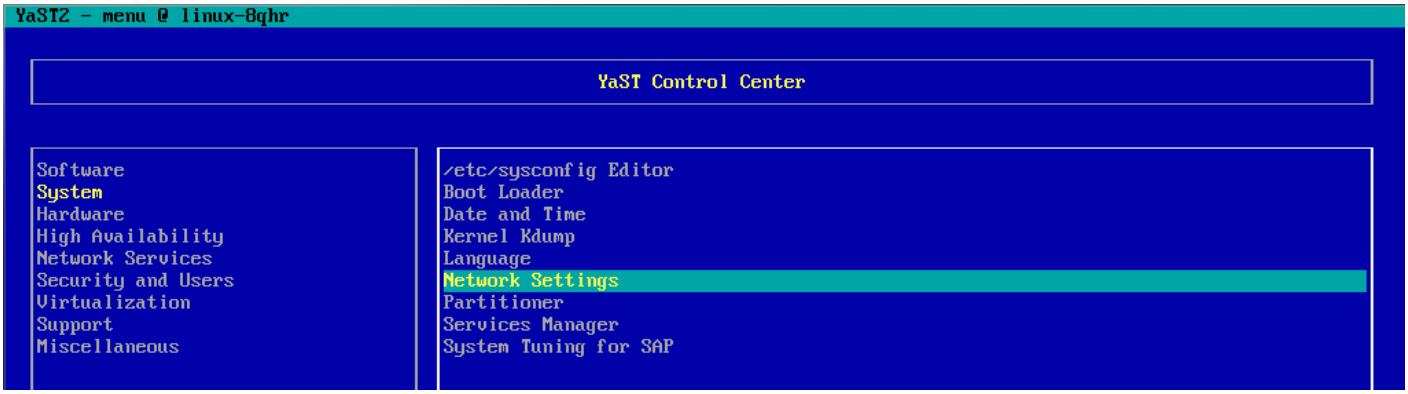
Figure 76. Login using root



50. Configure the host name and disable IPv6 (Figure 77):

```
#yast2
```

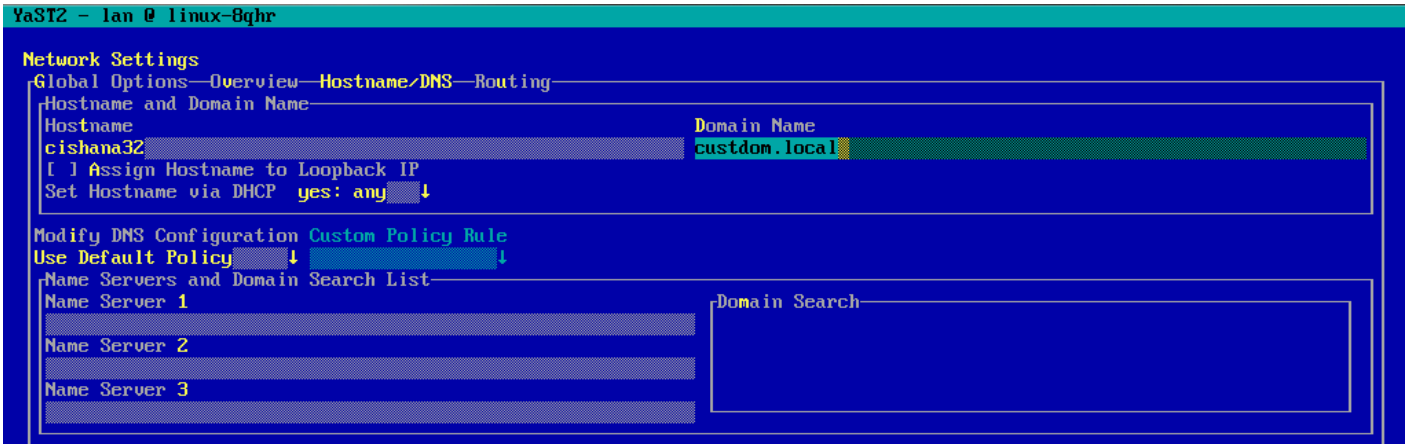
Figure 77. YaST Control Center: Network Settings



51. Choose System > Network Settings and press Alt+S to select the Hostname/DNS tab (Figure 78).

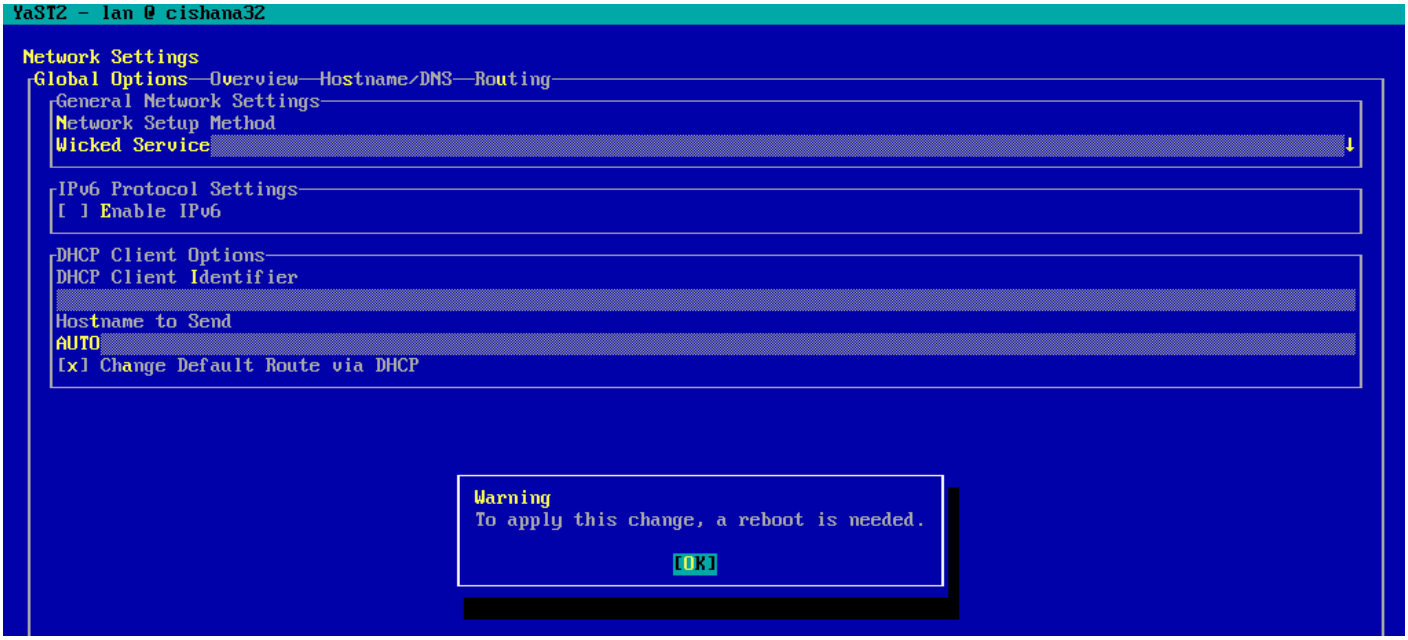
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 78. YaST Control Center: Hostname/DNS



52. Enter <<var_hostname.domain>>. Also enter the Domain Name System (DNS) server address of your network for resolution, if necessary. Then press Alt+O.
53. On the Global Options tab, using Alt+G, disable IPv6 by deselecting the Enable IPv6 option as shown in Figure 79. Note that changing the IPv6 setting requires a reboot to make the change take effect.

Figure 79. YaST: IPv6 setting



54. Press Alt+O to save the network configuration. Press Alt+Q to quit the YaST Control Center.
55. Reboot the server to make the IPv6 selection and the host-name settings take effect:

```
#reboot
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

56. Identify the Ethernet interface port that is connected to the top-of-the-rack (ToR) switch. For now, you can use that port for management connectivity to the host. You can also check the port by using the **ifconfig** command, as shown in the example in Figure 80.

Figure 80. Network interface configuration

```
cishana32:~ # for i in $(seq 0 5); do ifconfig eth$i up; done
cishana32:~ # for i in $(seq 0 5); do cat /sys/class/net/eth$i/operstate; done
down
down
down
down
up
down
cishana32:~ # _
```

57. Assign <<var_mgmt_ip_address>> as the IP address and enter <<var_mgmt_nw_netmask>> as the subnet mask for the available interface (for example, eth5). You can use this configuration temporarily until you port it to a high-availability bond device and create another with the Cisco VIC's 10-Gbps ports.
58. Go to the network configuration directory and create a configuration for eth5:

```
#cd /etc/sysconfig/network
#vi ifcfg-eth5
BOOTROTO='static' IPADDR='<<var_mgmt_ip_address>>' NETMASK='<<var_mgmt_nw_netmask>>' NETWORK=''
MTU='' REMOTE_IPADDR='' STARTMODE='auto' USERCONTROL='no'
```

59. Add the default gateway:

```
#cd /etc/sysconfig/network
#vi routes
default <<var_mgmt_gateway_ip>> - -
```

Note: Be sure that the system has access to the Internet or a SUSE update server to install the patches.

60. Verify /etc/hosts as shown in the example in Figure 81.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 81. Verify /etc/hosts

```
cishana01:~ # more /etc/hosts
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1       localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet

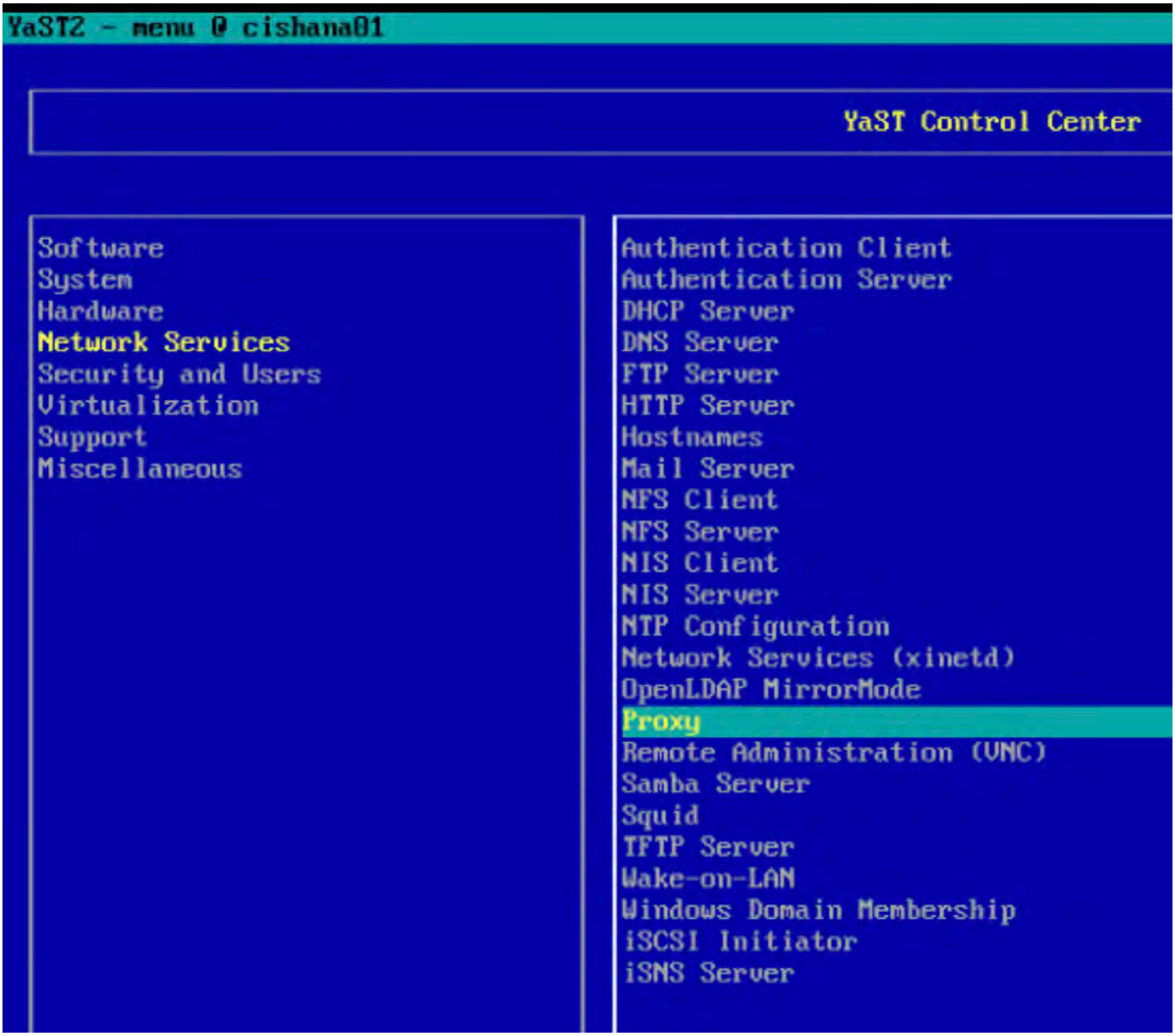
ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
[redacted]      cishana01.custdom.local cishana01
```

61. Set up a proxy service so that the appliance can reach the Internet (Figure 82):

    `#yast2`

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

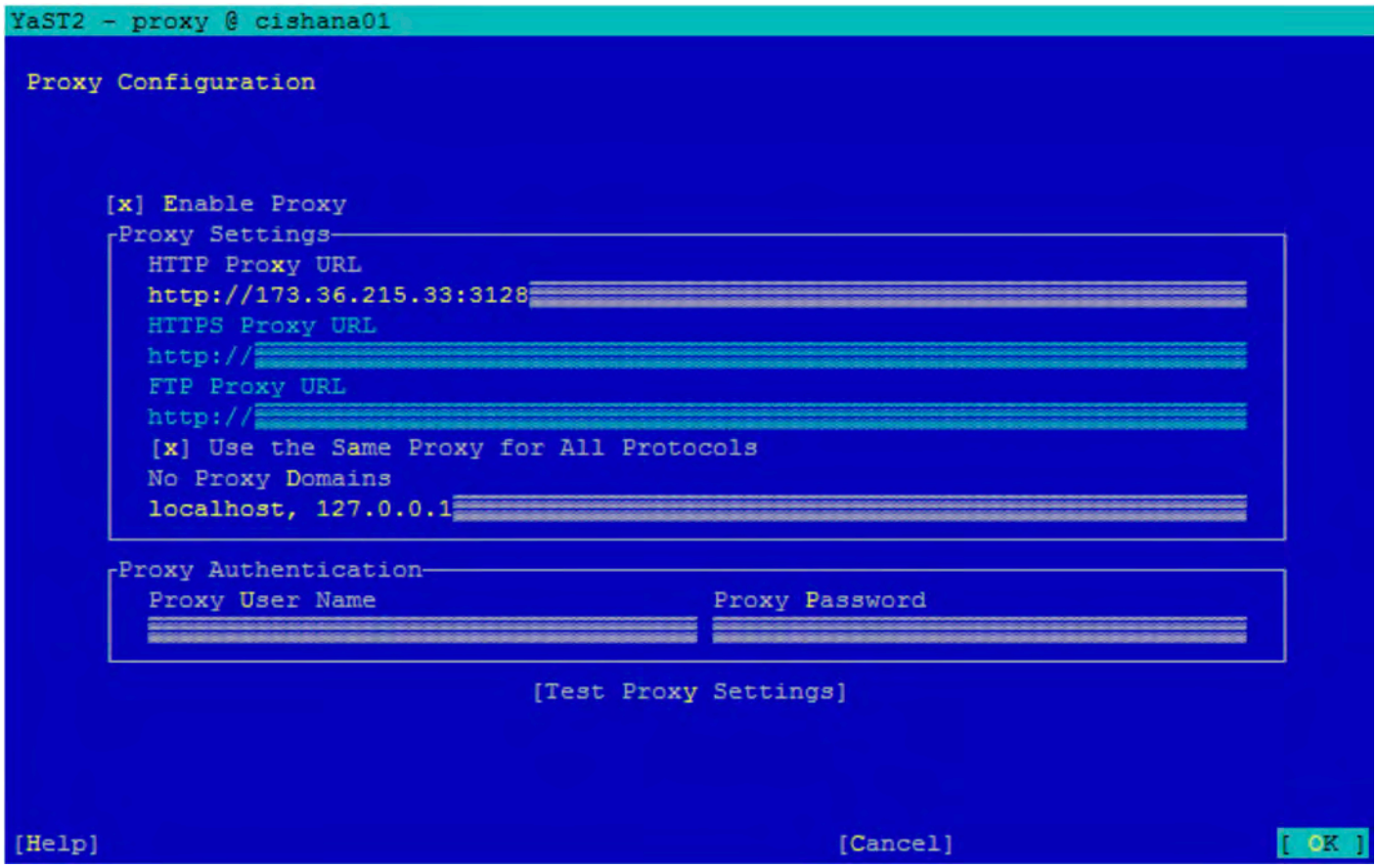
Figure 82. YaST: Proxy configuration



62. Enter the proxy server and port as shown in the sample configuration in Figure 83. Select OK and then quit YaST to save the configuration.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 83. YaST: Proxy configuration (continued)



63. Register the system with SUSE to receive the latest patches. For more information, refer to the SUSE knowledgebase article at https://www.suse.com/de-de/support/kb/doc?id=7016626.

    The system must have access to the Internet to proceed with this step.

    ```
    #SUSEConnect -r <<registration_code>> -e <<email_address>>
    ```

64. Update the system with the following command. Again, the system must have access to the Internet to proceed with this step.

#zypper `update`

65. Follow the on-screen instructions to complete the update process. Reboot the server and log in to the system again.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Post-installation OS configuration

To optimize the use of the SAP HANA database with SLES 12 or SLES for SAP 12 SP1, apply the settings by referring to SAP Note 2205917 - SAP HANA DB: Recommended OS settings for SLES 12 / SLES for SAP Applications 12.

Note: Following is the information from SAP Note 2205917 mentioned above and is current at the time of publishing this whitepapaer. For latest updates please follow the SAP notes.

To customize the SLES 12 SP4 System for HANA Servers, follow these steps:

1. Turn off autoNUMA balancing, disable transparent hugepages and configure C-States for lower latency
2. Edit /etc/default/grub, search for the line starting with "GRUB_CMDLINE_LINUX_DEFAULT" and append the following:
   `numa_balancing=disable transparent_hugepage=never intel_idle.max_cstate=1 processor.max_cstate=1`
3. Save your changes and run:
   `grub2-mkconfig -o /boot/grub2/grub.cfg`

Energy Performance Bias, CPU frequency/Voltage scaling and Kernel samepage merging (KSM).

4. Add the following commands to a script executed on system boot, such as /etc/init.d/boot.local:
   ```
   cpupower set -b 0
   cpupower frequency-set -g performance
   echo 0 > /sys/kernel/mm/ksm/run
   ```
5. Activate tuned and Enable tuned profile
   ```
   saptune daemon start
   saptune solution apply HANA
   ```
6. Reboot the OS issuing reboot command

To optimize the network configuration, apply the settings by referring SAP Note 2382421 – Optimizing the Network Configuration on HANA- and OS-Level.

Configuring bonding for high availability

To configure a bond for high availability, first view the Ethernet interfaces available in the system.

By examining the hardware and MAC addresses of the interfaces using the **ifconfig** command and the properties using **ethtool**, you can clearly differentiate the interfaces for the two dual-port Cisco UCS VIC 1225 adapters installed in the server as well as the onboard 1-Gbps interface.

A bond configured with two 1-Gbps ports can be used for the administration, management, and access networks, and a bond configured with two ports, using one port from each dual-port VIC, can be used for a backup network. Additional interfaces can be configured on the VICs based on needs.

In the example in Figure 85, the **ethtool** output for the interfaces showing Fibre Channel support and 10-Gbps indicates that eth0 through eth4 are VIC ports. In addition, a close observation of their MAC addresses reveals that eth0 and eth1 and that eth2 and eth3 are ports on the same VICs (in both cases, the last octet of the MAC address differs).

Therefore, for high availability, eth0 and eth2 form one possible slave pair for creating a 10-Gbps bond device.

Likewise, 1-Gbps interfaces eth4 and eth5 are potential slave interfaces for a 1-Gbps bond device.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

In this section, you will manually create these two bond interfaces.

Note: In SLES, use of YaST is recommended. It provides an easy wizard-like approach for creating bond devices. For ease of implementation, this section provides steps for manual configuration.

Figure 84. The **ifconfig** output provides an overview of the interfaces

```
cishana01:~ # ifconfig -a | grep HW
eth0      Link encap:Ethernet  HWaddr 84:B8:02:8B:31:40
eth1      Link encap:Ethernet  HWaddr 84:B8:02:8B:31:41
eth2      Link encap:Ethernet  HWaddr 84:B8:02:5B:DE:20
eth3      Link encap:Ethernet  HWaddr 84:B8:02:5B:DE:21
eth4      Link encap:Ethernet  HWaddr 88:1D:FC:39:F2:12
eth5      Link encap:Ethernet  HWaddr 88:1D:FC:39:F2:13
eth6      Link encap:Ethernet  HWaddr 88:1D:FC:39:F2:16
eth7      Link encap:Ethernet  HWaddr 88:1D:FC:39:F2:18
cishana01:~ # for i in `seq -w 0 7`;do ethtool eth$i > /tmp/ethinfo; head -n 5 /tmp/ethinfo;done
Settings for eth0:
        Supported ports: [ FIBRE ]
        Supported link modes:   10000baseT/Full
        Supports auto-negotiation: No
        Advertised link modes:  10000baseT/Full
Settings for eth1:
        Supported ports: [ FIBRE ]
        Supported link modes:   10000baseT/Full
        Supports auto-negotiation: No
        Advertised link modes:  10000baseT/Full
Settings for eth2:
        Supported ports: [ FIBRE ]
        Supported link modes:   10000baseT/Full
        Supports auto-negotiation: No
        Advertised link modes:  10000baseT/Full
Settings for eth3:
        Supported ports: [ FIBRE ]
        Supported link modes:   10000baseT/Full
        Supports auto-negotiation: No
        Advertised link modes:  10000baseT/Full
Settings for eth4:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
Settings for eth5:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
Settings for eth6:
        Supported ports: [ TP ]
        Supported link modes:   100baseT/Full
                                1000baseT/Full
                                10000baseT/Full
Settings for eth7:
        Supported ports: [ TP ]
        Supported link modes:   100baseT/Full
                                1000baseT/Full
                                10000baseT/Full
cishana01:~ #
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

1. Create 1-Gbps bond device ifcfg-bond0 with eth4 and eth5 as slaves.

   a. Create a bond0 configuration file:

```
# vi /etc/sysconfig/network/ifcfg-bond0 BONDING_MASTER='yes' BONDING_MODULE_OPTS='mode=active-backup miimon=100' BOOTPROTO='static'
BROADCAST=''
ETHTOOL_OPTIONS='' IPADDR='<<var_mgmt_ip_address>>/<<var_mgmt_netmask_prefix>>' MTU=''
NAME=''
NETWORK=''
REMOTE_IPADDR=''
STARTMODE='auto'
USERCONTROL='no'
BONDING_SLAVE0='eth4'
BONDING_SLAVE1='eth5'
```

   b. Modify the eth4 and eth5 configuration files:

```
# vi /etc/sysconfig/network/ifcfg-eth4 BOOTPROTO='none'
BROADCAST=''
ETHTOOL_OPTIONS=''
IPADDR=''
MTU=''
NAME='VIC Ethernet NIC' NETMASK=''
NETWORK='' REMOTE_IPADDR='' STARTMODE='hotplug' USERCONTROL='no'
# vi /etc/sysconfig/network/ifcfg-eth5 BOOTPROTO='none'
BROADCAST=''
ETHTOOL_OPTIONS=''
IPADDR=''
MTU=''
NAME='VIC Ethernet NIC' NETMASK=''
NETWORK='' REMOTE_IPADDR=''
STARTMODE='hotplug' USERCONTROL='no'
```

   c. Test the configuration.

      Restart the network service to bring up the bond0 interface. Then enter the following command:

```
# rcnetwork restart
```

   To query the current status of the Linux kernel bounding driver, enter the following command:

```
# cat /proc/net/bonding/bond0
```

Figure 85 shows sample output.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 85. Sample bond0 configuration test output

```
cishana01:/etc/sysconfig/network # cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: eth5
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth4
MII Status: down
Speed: Unknown
Duplex: Unknown
Link Failure Count: 0
Permanent HW addr: 88:1d:fc:39:f2:12
Slave queue ID: 0

Slave Interface: eth5
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 88:1d:fc:39:f2:13
Slave queue ID: 0
cishana01:/etc/sysconfig/network #
```

2. Create 10-Gbps bond device ifcfg-bond1 with eth0 and eth2 as slaves.

   a. Create a bond1 configuration file:

```
# vi /etc/sysconfig/network/ifcfg-bond1 BONDING_MASTER='yes' BONDING_MODULE_OPTS='mode=active-backup miimon=100' BOOTPROTO='static'
BROADCAST='' ETHTOOL_OPTIONS=''
IPADDR='<<ip_address_customer_usecase>>/<<netmask_prefix>>' MTU=''
NAME=''
NETWORK=''
REMOTE_IPADDR='' STARTMODE='auto' USERCONTROL='no' BONDING_SLAVE0='eth0' BONDING_SLAVE1='eth2'
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

b. Modify the eth0 and eth2 configuration files:

```
# vi /etc/sysconfig/network/ifcfg-eth0 BOOTPROTO='none'
BROADCAST=''
ETHTOOL_OPTIONS=''
IPADDR=''
MTU=''
NAME='VIC Ethernet NIC' NETMASK=''
NETWORK='' REMOTE_IPADDR='' STARTMODE='hotplug' USERCONTROL='no'
# vi /etc/sysconfig/network/ifcfg-eth2 BOOTPROTO='none'
BROADCAST=''
ETHTOOL_OPTIONS=''
IPADDR=''
MTU=''
NAME='VIC Ethernet NIC' NETMASK=''
NETWORK='' REMOTE_IPADDR='' STARTMODE='hotplug' USERCONTROL='no'
```

c. Test the configuration.

Restart the networking service to bring up the bond0 interface. Enter the following command:

```
# rcnetwork restart
```

To query the current status of Linux kernel bounding driver, enter the following command:

```
# cat /proc/net/bonding/bond1
```

Figure 86 shows sample output.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 86. Sample bond1 configuration test output

```
cishana01:/etc/sysconfig/network # cat /proc/net/bonding/bond1
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: None
MII Status: down
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: down
Speed: Unknown
Duplex: Unknown
Link Failure Count: 0
Permanent HW addr: 84:b8:02:8b:31:40
Slave queue ID: 0

Slave Interface: eth2
MII Status: down
Speed: Unknown
Duplex: Unknown
Link Failure Count: 0
Permanent HW addr: 84:b8:02:5b:de:20
Slave queue ID: 0
cishana01:/etc/sysconfig/network #
```

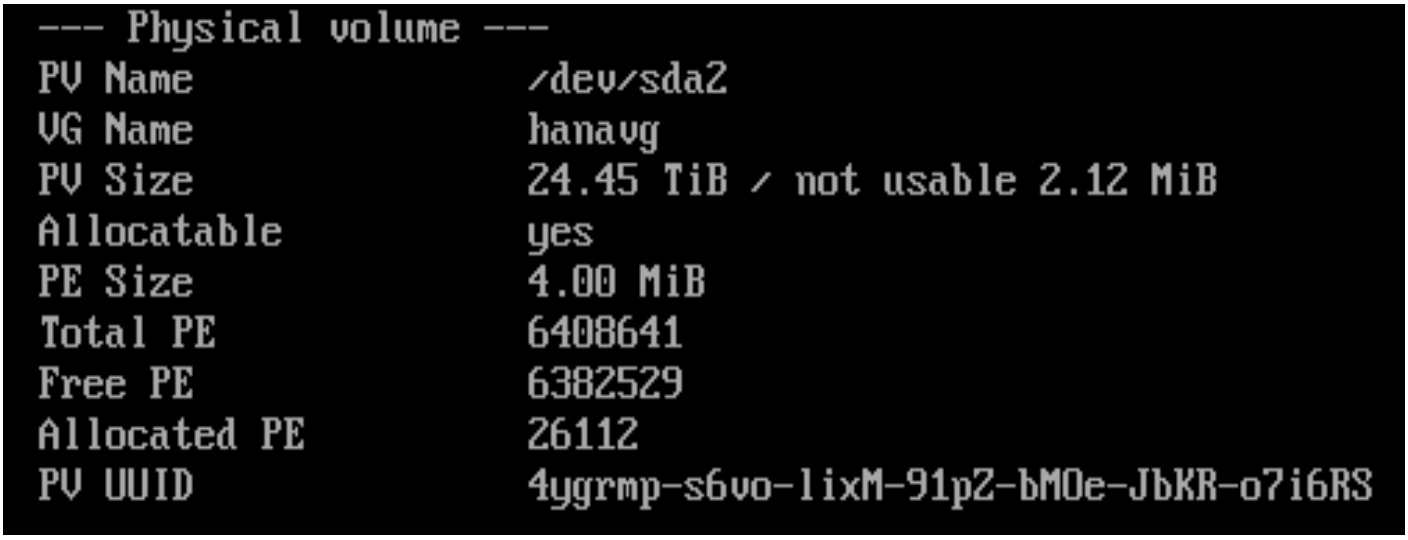
Preparing SAP HANA data, log, and shared file systems

To prepare the file systems, you start by carving out logical volumes for the data, log, and HANA shared files. Then you create the file systems. Then you update /etc/fstab and mount the volumes.

1. Use the following command to check for the available physical volume (PV), as shown in Figure 87:
   `#pvdisplay`

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 87. Checking for the physical volume

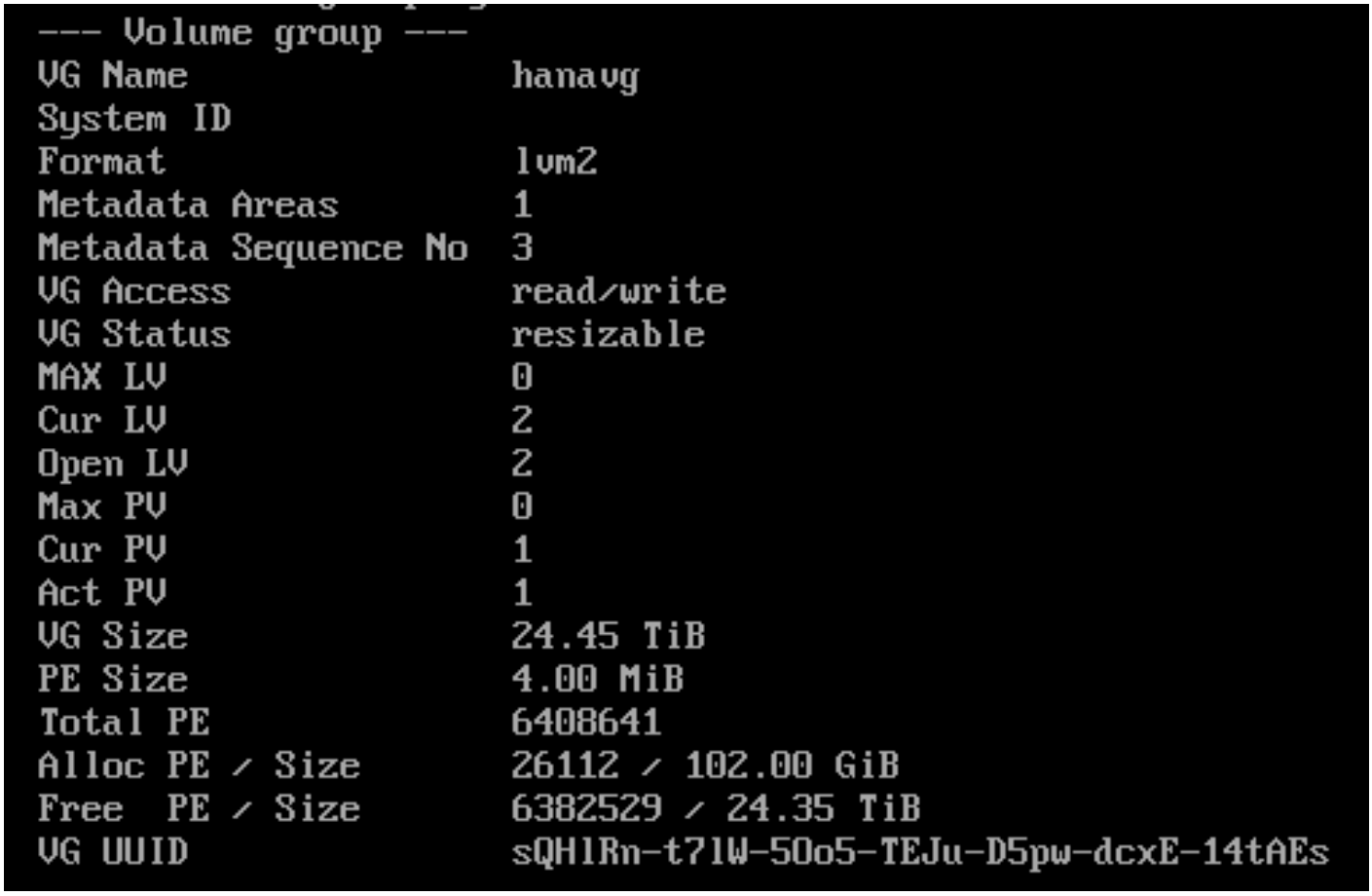


2. 2. Use the following command to check for the available volume group (VG) hanavg (Figure 88):

```
#vgdisplay
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 88. Checking for the volume group



3. Create logical volumes (LVs) for the data, log, and HANA shared file systems (Figure 89):

```
lvcreate –name <<lvname>> -I<<stripesize>> -L<<volume-size>> <<parent-vg-name>> # lvcreate --name datalv -I256 -L9T hanavg
```

Note: The lvcreate command doesn't require you to specify the stripe size when creating volumes on SSDs.

```
# lvcreate --name loglv -I256 -L512G hanavg
# lvcreate --name sharedlv -I256 -L3T hanavg
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 89. Creating logical volumes

```
[root@cishana01 ~]# lvcreate --name datalv -I256 -L9T hanavg
  Ignoring stripesize argument with single stripe.
  Logical volume "datalv" created.
[root@cishana01 ~]# lvcreate --name loglv -I256 -L512G hanavg
  Ignoring stripesize argument with single stripe.
  Logical volume "loglv" created.
[root@cishana01 ~]# lvcreate --name sharedlv -I256 -L3T hanavg
  Ignoring stripesize argument with single stripe.
  Logical volume "sharedlv" created.
```

4. Create file systems in the data, log, and HANA shared volumes (Figure 90):

```
#mkfs.xfs -f /dev/hanavg/datalv
#mkfs.xfs -f /dev/hanavg/loglv
#mkfs.xfs -f /dev/hanavg/sharedlv
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 90. Creating file systems

```
[root@cishana01 ~]# mkfs.xfs -f /dev/hanavg/datalv
meta-data=/dev/hanavg/datalv     isize=256    agcount=9, agsize=268435455 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=2415919095, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=521728, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
[root@cishana01 ~]# mkfs.xfs -f /dev/hanavg/loglv
meta-data=/dev/hanavg/loglv      isize=256    agcount=4, agsize=33554432 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=134217728, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=65536, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
[root@cishana01 ~]# mkfs.xfs -f /dev/hanavg/sharedlv
meta-data=/dev/hanavg/sharedlv   isize=256    agcount=4, agsize=201326592 blks
         =                       sectsz=512   attr=2, projid32bit=0
data     =                       bsize=4096   blocks=805306368, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0
log      =internal log           bsize=4096   blocks=393216, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

5. Create mount directories for the data, log, and HANA shared file systems:

   ```
   #mkdir -p /hana/data
   #mkdir -p /hana/log
   #mkdir -p /hana/shared
   ```

6. Mount options vary from the default Linux settings for XFS for SAP HANA data and log volumes. The following is a sample /etc/fstab entry. Make sure that you use the same mount options for the data and log file systems as shown in the example.

   ```
   /dev/mapper/hanavg-rootlv                                  /                       ext3
   defaults             1           1
   UUID=fc2e52c4-e6f6-4e9a-9ad1-86aeb3369942          /boot             ext3         defaults
   1          2
   /dev/mapper/hanavg-swapvol                           swap                          defaults
   0             0
   /dev/hanavg/datalv  /hana/data   xfs
   nobarrier,noatime,nodiratime,logbufs=8,logbsize=256k,async,swalloc,allocsize=131072k  1    2
   ```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

```
/dev/hanavg/loglv   /hana/log      xfs
nobarrier,noatime,nodiratime,logbufs=8,logbsize=256k,async,swalloc,allocsize=131072k  1    2
/dev/hanavg/sharedlv  /hana/shared  xfs       defaults      1        2
```

This example illustrates the use of default settings for mount options when configuring SSDs.

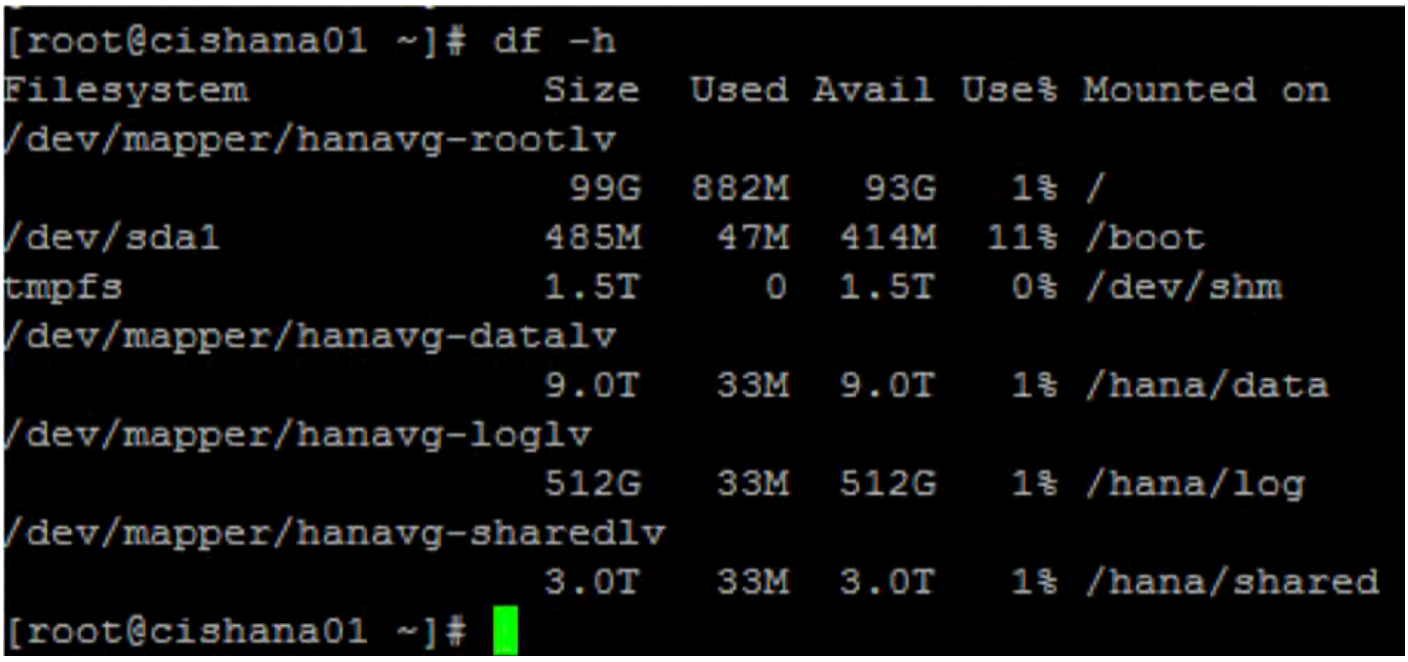
```
/dev/hanavg/swapvol  swap                      defaults              0 0
/dev/hanavg/rootlv   /                  ext3       acl,user_xattr        1 1
UUID=912D-A3CB       /boot/efi          vfat       umask=0002,utf8=true  0 0
/dev/hanavg/datalv      /hana/data      xfs     defaults        1 2
/dev/hanavg/loglv       /hana/log       xfs     defaults        1 2
/dev/hanavg/sharedlv    /hana/log       xfs     defaults        1 2
```

7. Use the following command to mount the file systems:

   ```
   #mount -a
   ```

8. Use the **df –h** command to check the status of all mounted volumes (Figure 91).

Figure 91. Checking the status of mounted volumes



9. Change the directory permissions before you install SAP HANA. Use the **chown** command on each SAP HANA node after the file systems are mounted:

   ```
   #chmod -R 777 /hana/data
   #chmod -R 777 /hana/log
   #chmod -R 777 /hana/shared
   ```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Installing SAP HANA

Use the official SAP documentation, which describes the installation process with and without the SAP unified installer. For the SAP HANA installation documentation, see SAP HANA Server Installation Guide. All other SAP HANA administration documentation is available at SAP HANA Administration Guide.

Important SAP Notes

Read the following SAP Notes before you start the installation. These SAP Notes contain the latest information about the installation, as well as corrections to the installation documentation.

The latest SAP Notes can be found at SAP Notes and Knowledge base.

SAP HANA IMDB notes

- SAP Note 1514967: SAP HANA: Central note
- SAP Note 2298750: SAP HANA Platform SPS 12 Release Note
- SAP Note 1523337: SAP HANA database: Central note
- SAP Note 2000003: FAQ: SAP HANA
- SAP Note 2380257: SAP HANA 2.0 Release Notes
- SAP Note 1780950: Connection problems due to host name resolution
- SAP Note 1755396: Released disaster tolerant (DT) solutions for SAP HANA with disk replication
- SAP Note 2519630: Check whether power save mode is active
- SAP Note 1681092: Support for multiple SAP HANA databases on a single SAP HANA appliance
- SAP Note 1514966: SAP HANA: Sizing the SAP HANA database
- SAP Note 1637145: SAP BW on HANA: Sizing the SAP HANA database
- SAP Note 1793345: Sizing for Suite on HANA
- SAP Note 2399079: Elimination of hdbparam in HANA 2
- SAP Note 2186744: FAQ: SAP HANA Parameters

Linux notes

- SAP Note 2205917: SAP HANA DB: Recommended OS settings for SLES 12 and SLES for SAP Applications 12
- SAP Note 2235581: SAP HANA: Supported operating systems
- SAP Note 1944799: SAP HANA guidelines for the SLES operating system
- SAP Note 1731000: Non-recommended configuration changes
- SAP Note 1557506: Linux paging improvements
- SAP Note 1740136: SAP HANA: Wrong mount option may lead to corrupt persistency
- SAP Note 2382421: Optimizing the Network Configuration on HANA- and OS-Level

Third-party software notes

- SAP Note 1730928: Using external software in an SAP HANA appliance
- SAP Note 1730929: Using external tools in an SAP HANA appliance
- SAP Note 1730930: Using antivirus software in an SAP HANA appliance
- SAP Note 2031547: Using backup tools with Backint for SAP HANA

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

SAP HANA virtualization notes

- SAP Note 1788665: SAP HANA running on VMware vSphere virtual machines

Performing an SAP HANA post-installation checkup

For an SAP HANA system installed with <SID> set to **BWL** and the system number <nr> set to **00**, log in as **<sid>adm ir bwladm** and run the commands presented here.

Commands for checking SAP HANA services

```
bwladm@cishana01:/usr/sap/BWL/HDB00> /usr/sap/hostctrl/exe//sapcontrol -nr 00 -function
GetProcessList
19.02.2019 11:29:27
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2019 02 13 08:51:49, 866:37:38, 41691
hdbcompileserver, HDB Compileserver, GREEN, Running, 2019 02 13 08:51:56, 866:37:31, 41837
hdbindexserver, HDB Indexserver, GREEN, Running, 2019 02 13 08:52:00, 866:37:27, 41863
hdbnameserver, HDB Nameserver, GREEN, Running, 2019 02 13 08:51:50, 866:37:37, 41711
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2019 02 13 08:51:56, 866:37:31, 41839
hdbwebdispatcher, HDB Web Dispatcher, GREEN, Running, 2019 02 13 08:53:11, 866:36:16, 42431
hdbxsengine, HDB XSEngine, GREEN, Running, 2019 02 13 08:52:00, 866:37:27, 41865
bwladm@cishana01-bwl:/usr/sap/BWL/HDB00>
```

Commands for checking SAP HANA database information

```
bwladm@cishana01:/usr/sap/BWL/HDB00> HDB info
USER           PID      PPID    %CPU     VSZ      RSS    COMMAND
bwladm      59578  59577    0.0     108472  1944   -sh
bwladm      59663  59578    0.0     114080  2020   \_ /bin/sh /usr/sap/BWL/HDB00/HDB info
bwladm      59692  59663    0.0     118048  1596   \_ ps fx -U bwladm -o
user,pid,ppid,pcpu,vsz,rss,args
       bwladm      41683          1    0.0     22188    1640   sapstart
pf=/hana/shared/BWL/profile/BWL_HDB00_cishana01-bwl
bwladm      41691  41683    0.0     582888  290988 \_ /usr/sap/BWL/HDB00/cishana01-
bwl/trace/hdb.sapBWL_HDB00 -d -nw -f /usr/sap/BWL/HDB00/cishana01-bwl/daemon.ini
bwladm      41711  41691    0.3     54292416 2058900  \_hdbnameserver
bwladm      41837   41691   0.1     4278472   1243356   \_hdbcompileserver
bwladm      41839   41691   0.2     11773976 8262724    \_hdbpreprocessor
bwladm      41863   41691   6.2     22143172 18184604  \_hdbindexserver
bwladm      41865   41691   0.5     8802064    2446612   \_hdbxsengine
bwladm      42431   41691   0.1     4352988   823220     \_hdbwebdispatcher
bwladm.     41607          1   0.0      497576     23232
/usr/sap/BWL/HDB00/exe/sapstartsrv
pf=/hana/shared/BWL/profile/BWL_HDB00_cishana01-bwl -D -u bwladm
bwladm@cishana01-bwl:/usr/sap/BWL/HDB00>
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Tuning the SAP HANA performance parameters

After SAP HANA is installed, tune the parameters as shown in Table 13 and explained in the following SAP Notes.

Table 13. Tuning parameters

Parameters	Data file system	Log file system
max_parallel_io_requests	256	Default
async_read_submit	On	On
async_write_submit_blocks	All	All
async_write_submit_active	Auto	On

- SAP Note 2399079: Elimination of hdbparam in HANA 2
- SAP Note 2186744: FAQ: SAP HANA Parameters

Performing maintenance operations

This section discusses how to maintain and operate SUSE and SAP HANA.

Maintaining the operating system

The customer is responsible for implementing security updates and patches, adding software components, and changing OS settings that may be requested by SAP for future releases of SAP HANA or that may be required by SUSE to help ensure system security and stability. See the related SAP OSs notes for required OS settings.

This section describes how to update the OS and the implications of updating OS components. It is not meant to replace the Linux administration documentation.

Prerequisites

Whenever you change the OS or parts of the OS such as drivers and kernel parameters, be sure that you have at least a backup copy of your SAP HANA system, preferably not stored on the appliance. You also should check the related OS notes and Cisco support channels for additional information.

Some changes may require a reboot and should be applied when SAP HANA is shut down.

Updating the OS

Not all updates and patches update the OS kernel. But if a kernel update is necessary, you need to take specific precautions. During the entire update process, SAP HANA must be shut down.

These are the general steps for updating the kernel:

- Perform these tasks before updating the kernel:
  - Stop SAP HANA and back up the existing log area (in case the device causes a problem and needs to be re-created).
- Update the kernel using YaST (or zypper).
- Perform these tasks after updating the kernel:
  - Check the GRUB file and boot sector (menu.lst).
  - Reboot

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Updating SUSE online

You can update the operating system and kernel either through YaST or manually.

Using YaST

You can update the OS online using YaST. This method will update all OS components; a kernel update may also be included.

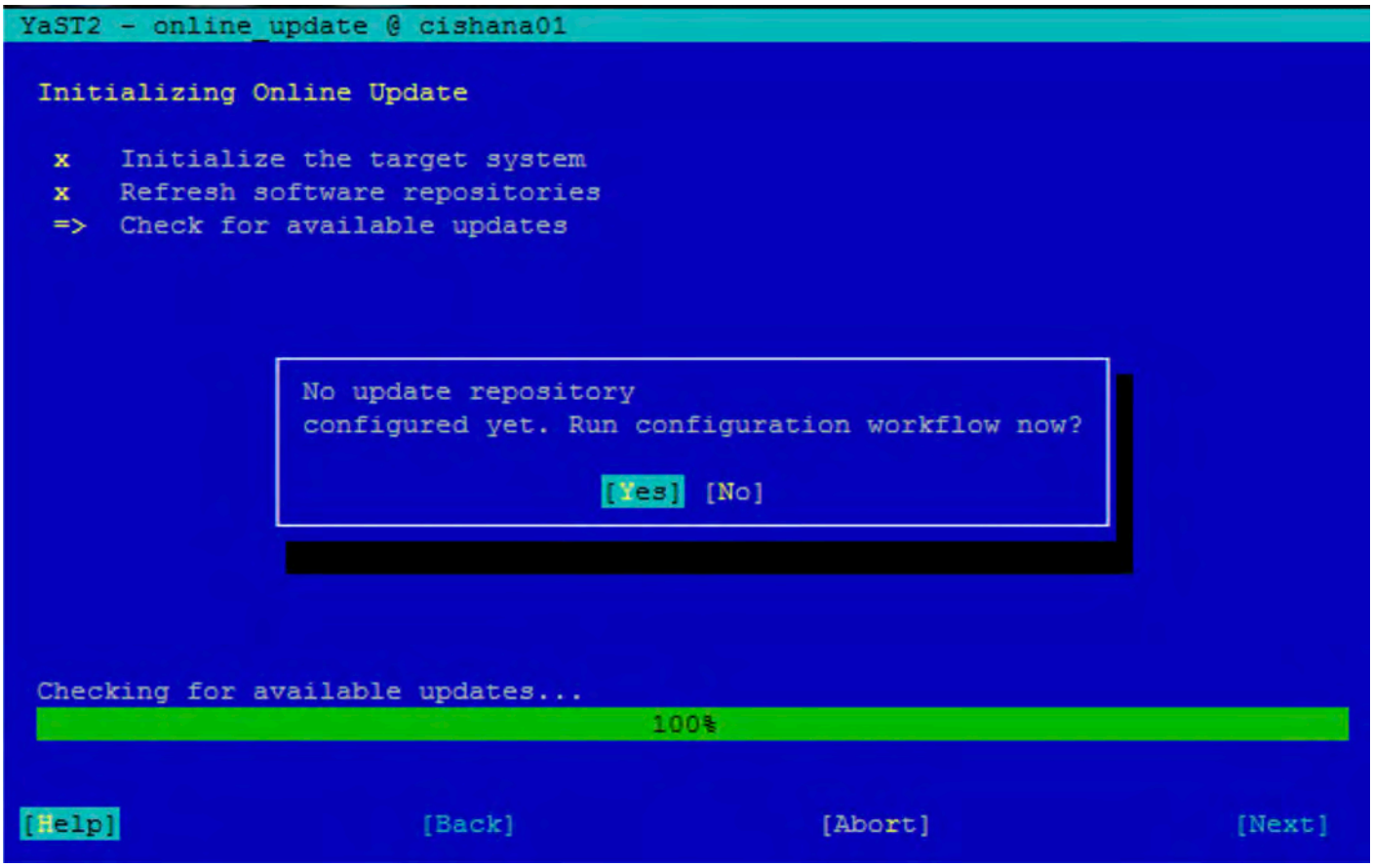
Note: Stop SAP HANA and back up the existing log area (in case the device causes a problem and needs to be re-created).

1. Set up a proxy service, if necessary, so that the appliance can reach the Internet. Make sure that PROXY_ENABLED is set to "yes" and that the appropriate proxy server host, IP address, and port are configured and used.

```
cishana01:~ # cd /etc/sysconfig/
cishana01:/etc/sysconfig # vi proxy
PROXY_ENABLED="yes" HTTP_PROXY="http://<Proxy_server_IP>:<Proxy_Service_port>"
HTTPS_PROXY="http://<Proxy_server_IP>:<Proxy_service_port>"
FTP_PROXY="http://<Proxy_server_IP>:<Proxy_service_port>"
```

2. Start YaST and choose Software > Online Update.
   i. Select Yes to configure the update repository (Figure 92).

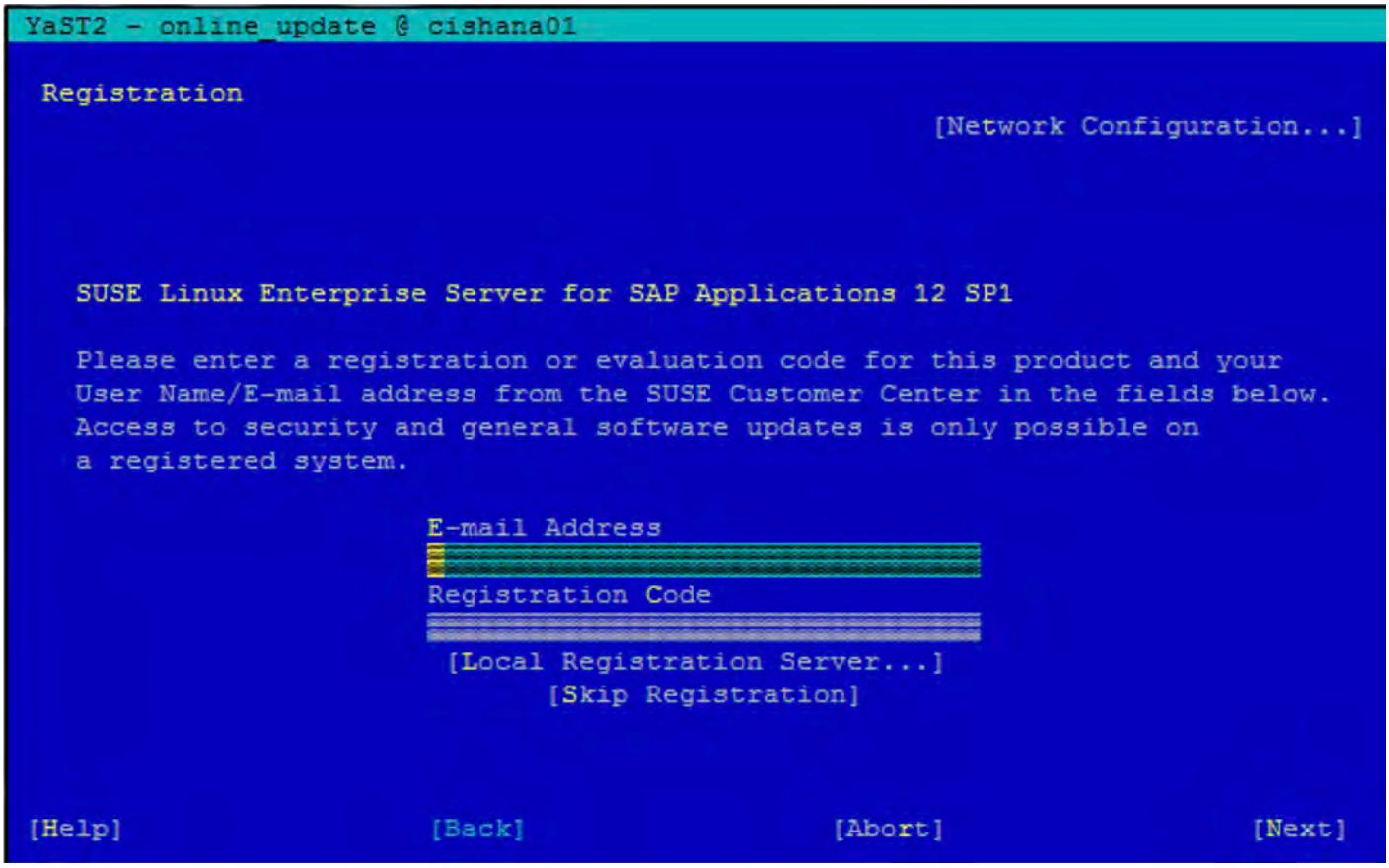
Figure 92. YaST: Online update



   ii. Log in with the account you used for licensing to register the server (Figure 93). Then click Next.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

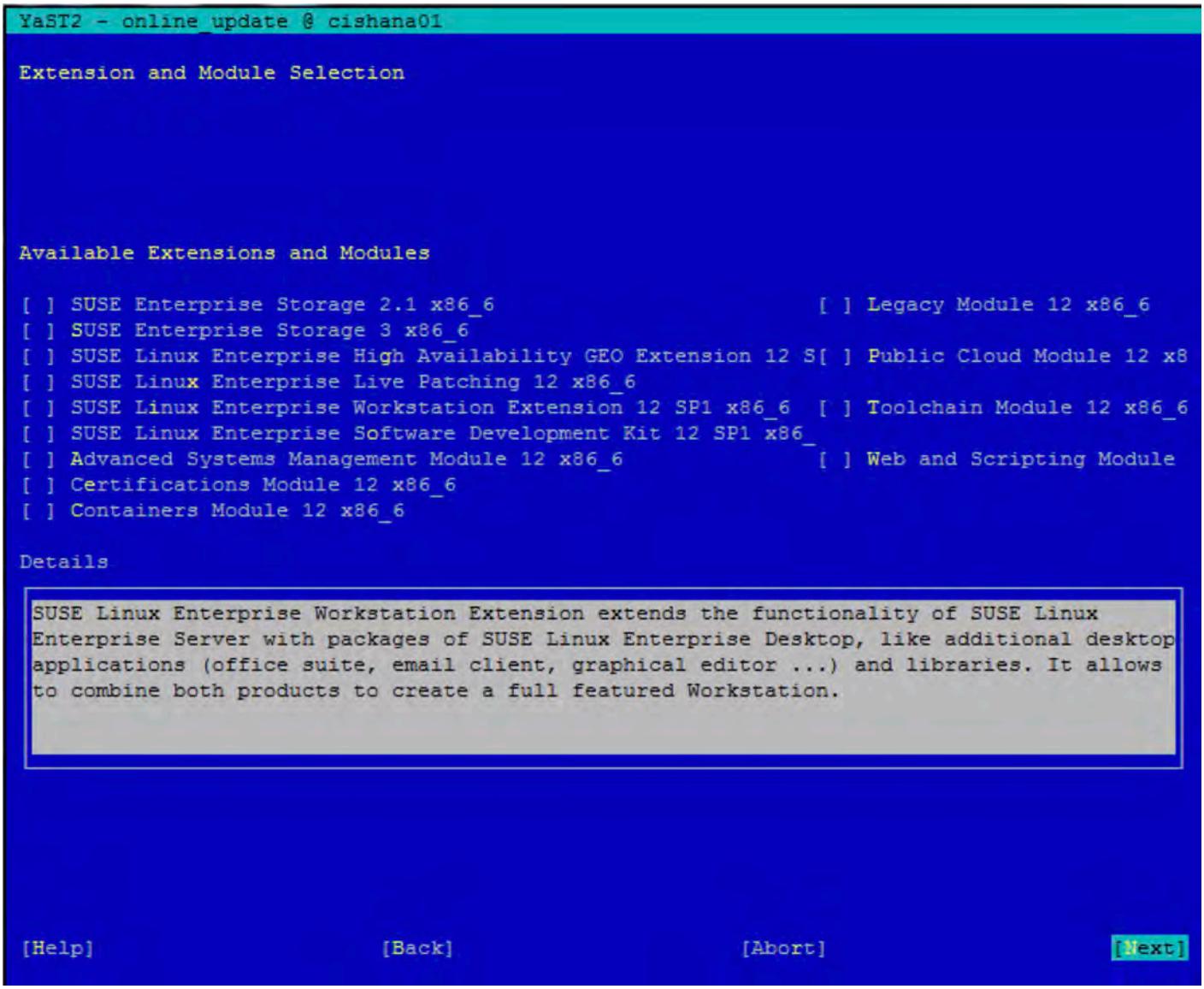
Figure 93. YaST online update: Registration



iii. An overview of the available extension and modules is displayed (Figure 94). Click Next.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

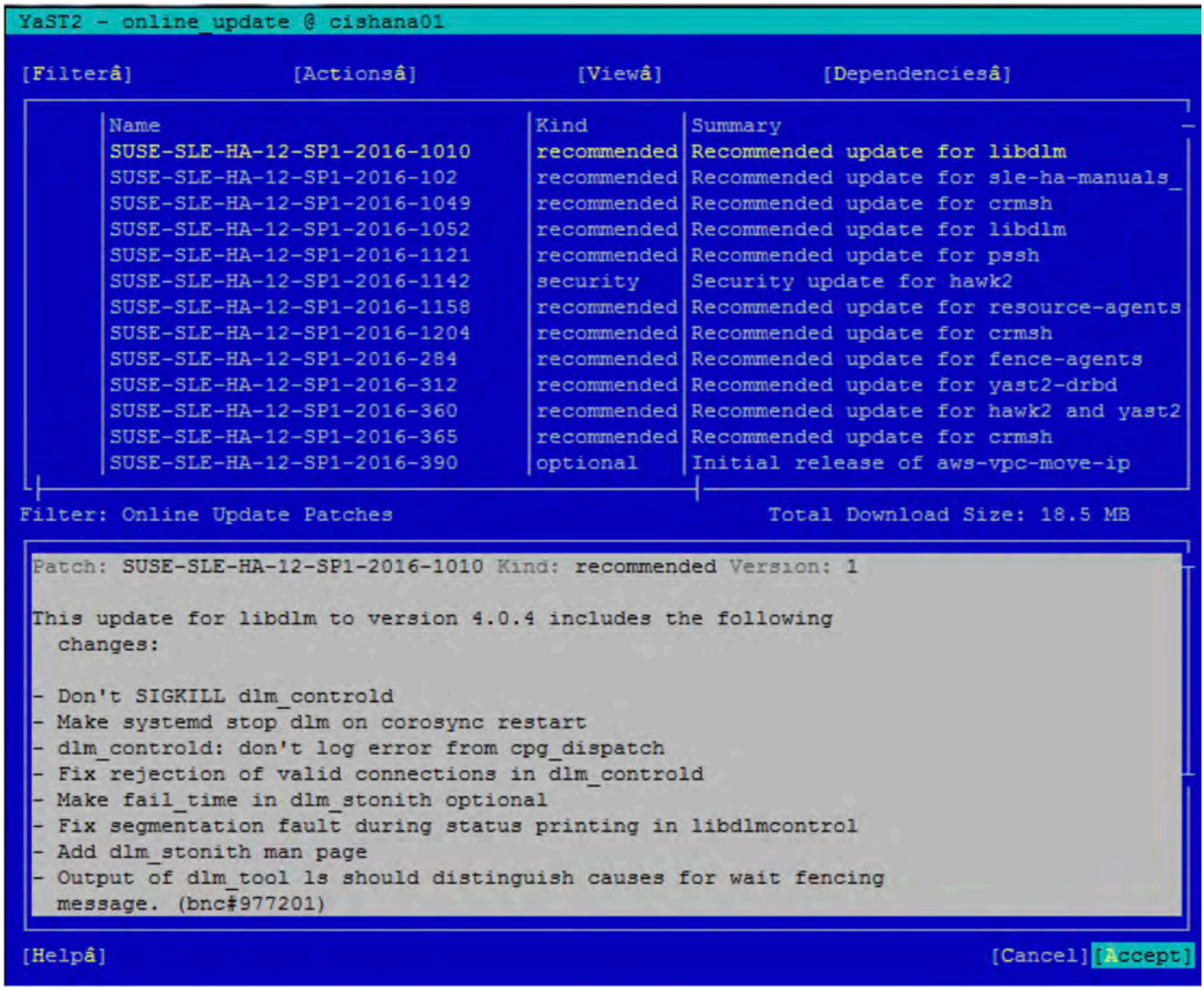
Figure 94. YaST online update: Extension and Module Selection



iv. A list of the available patches form the online repository is displayed (Figure 95). Click Accept.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

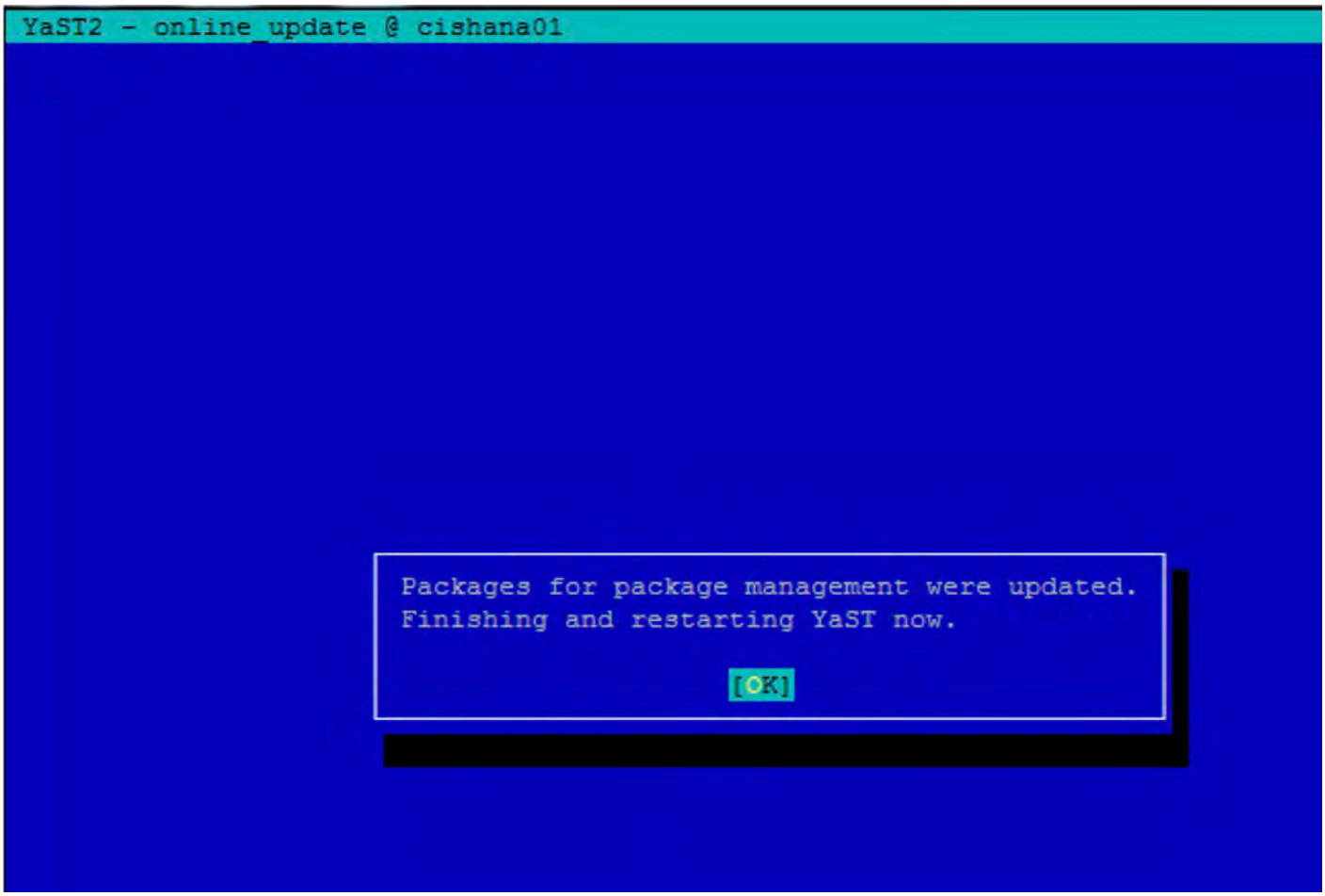
Figure 95. YaST online update: Patches list



The system will download all available patches (Figures 96 and 97).

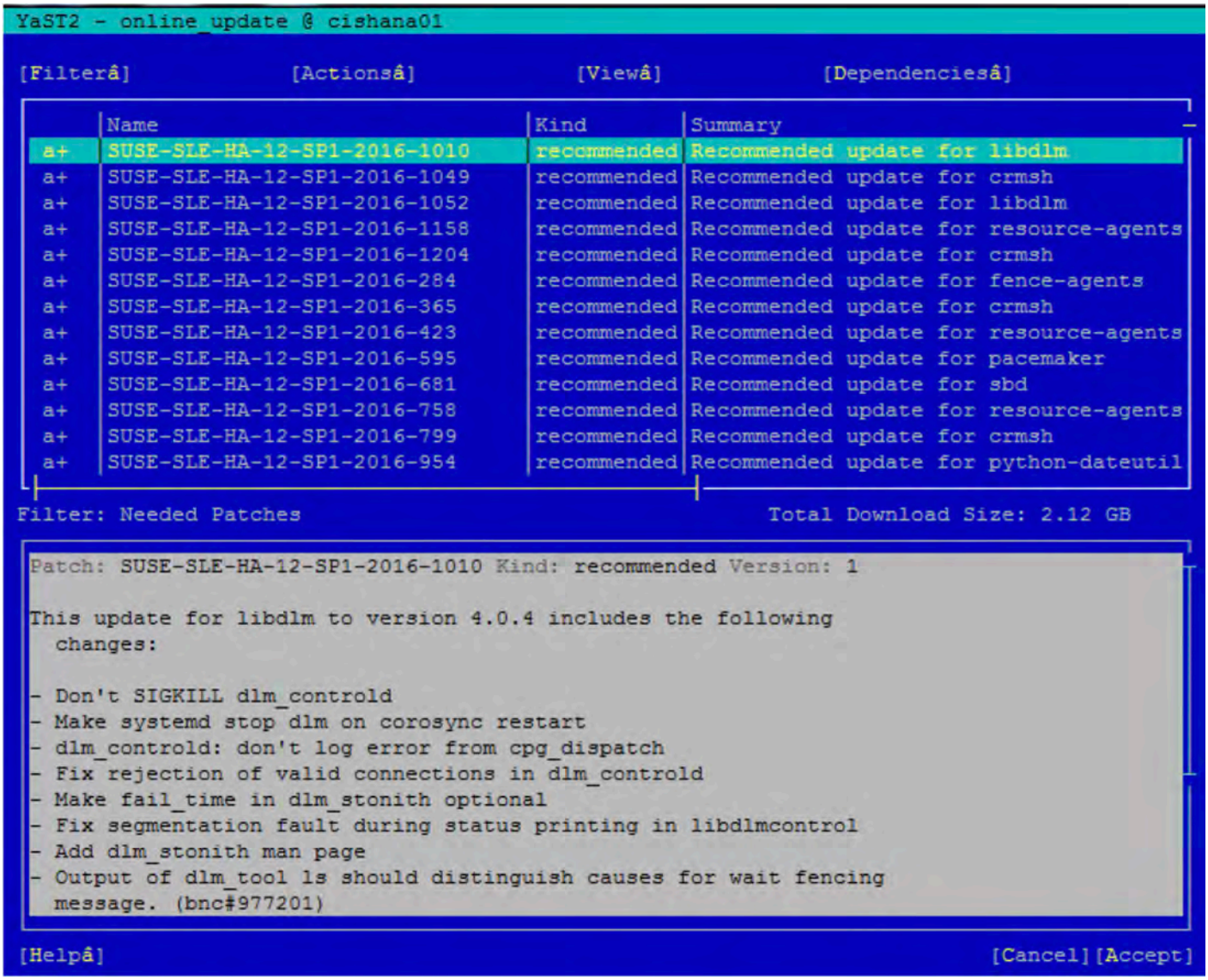
© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 96. YaST online update: Package update



© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

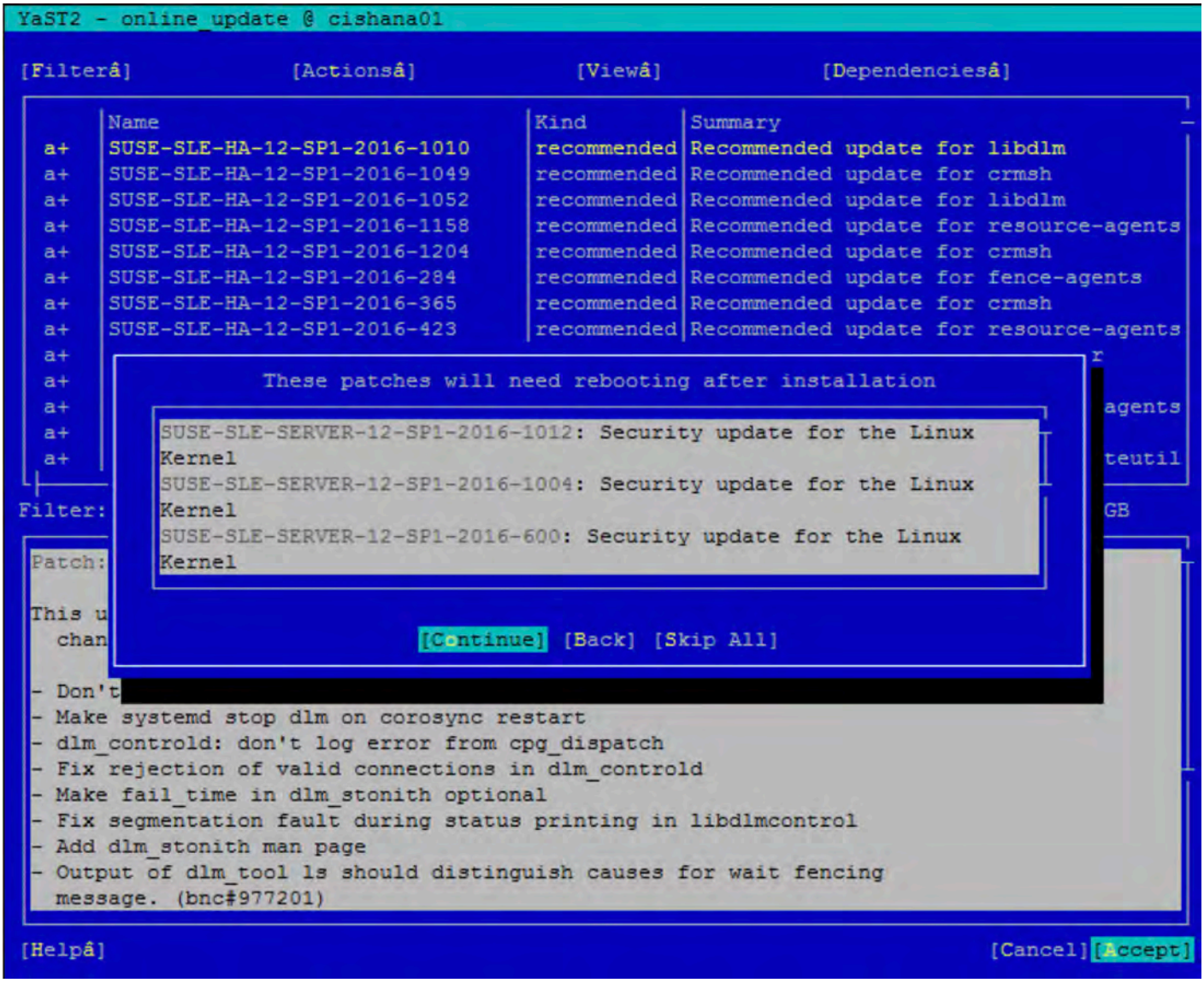
Figure 97. YaST online update: List of packages updated



v. Some patches may require reboot after installation. Select Continue (Figure 98).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

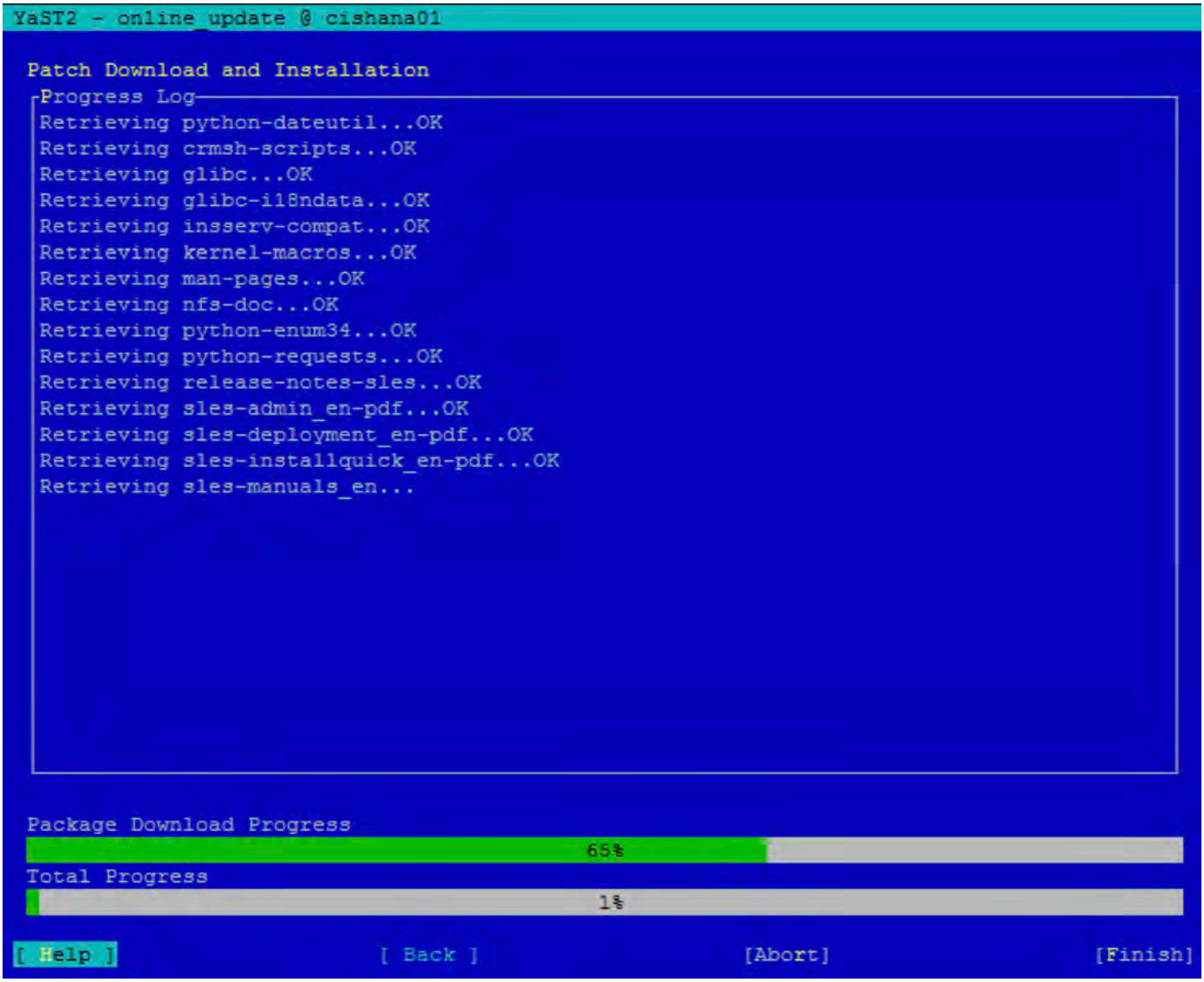
Figure 98. YaST online update: Package update



Patches are downloaded and installed at this time (Figure 99).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

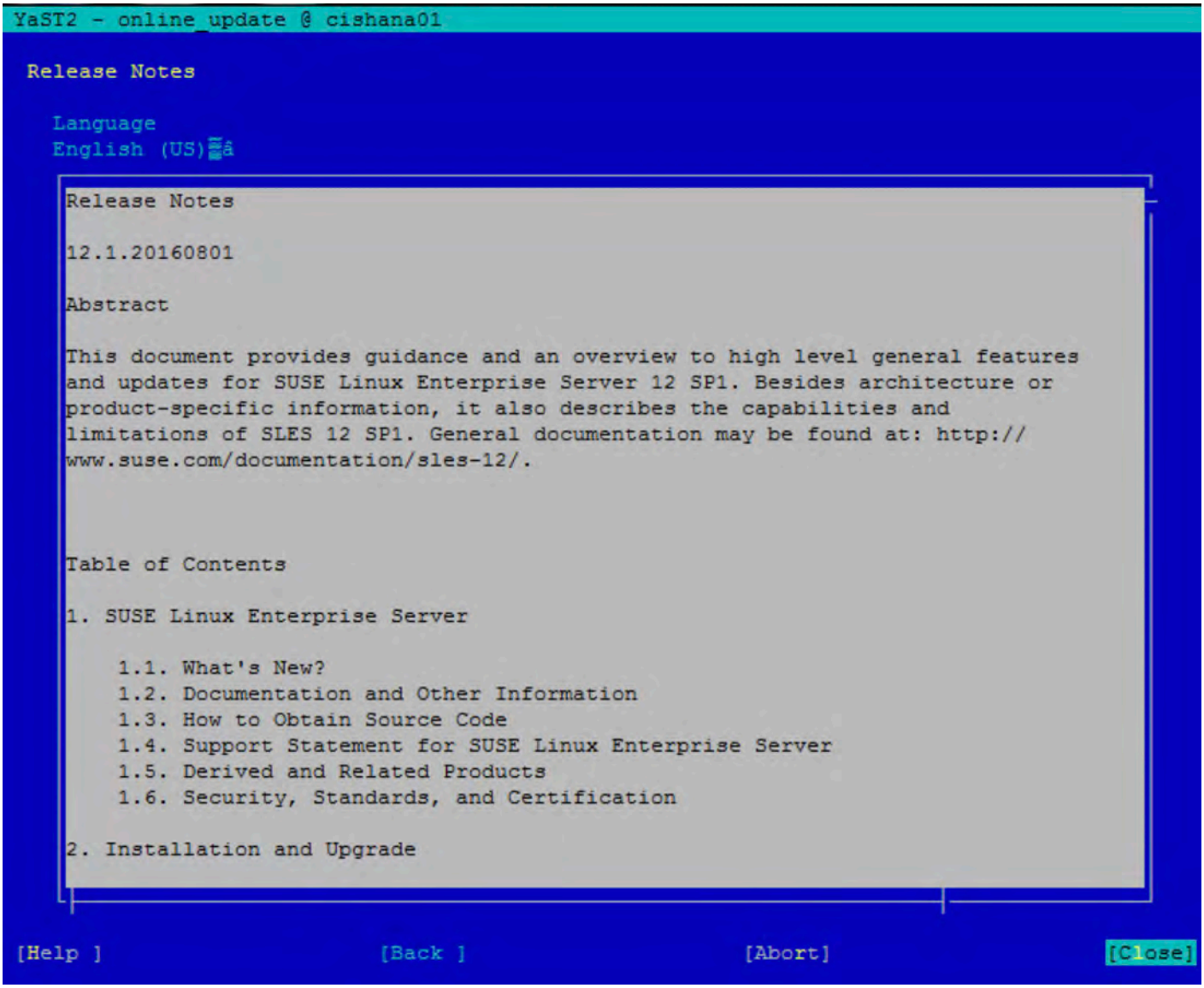
Figure 99. YaST online update: Package update progress



vi. When the packages have been updated, the release notes are displayed (Figure 100). Select Close.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

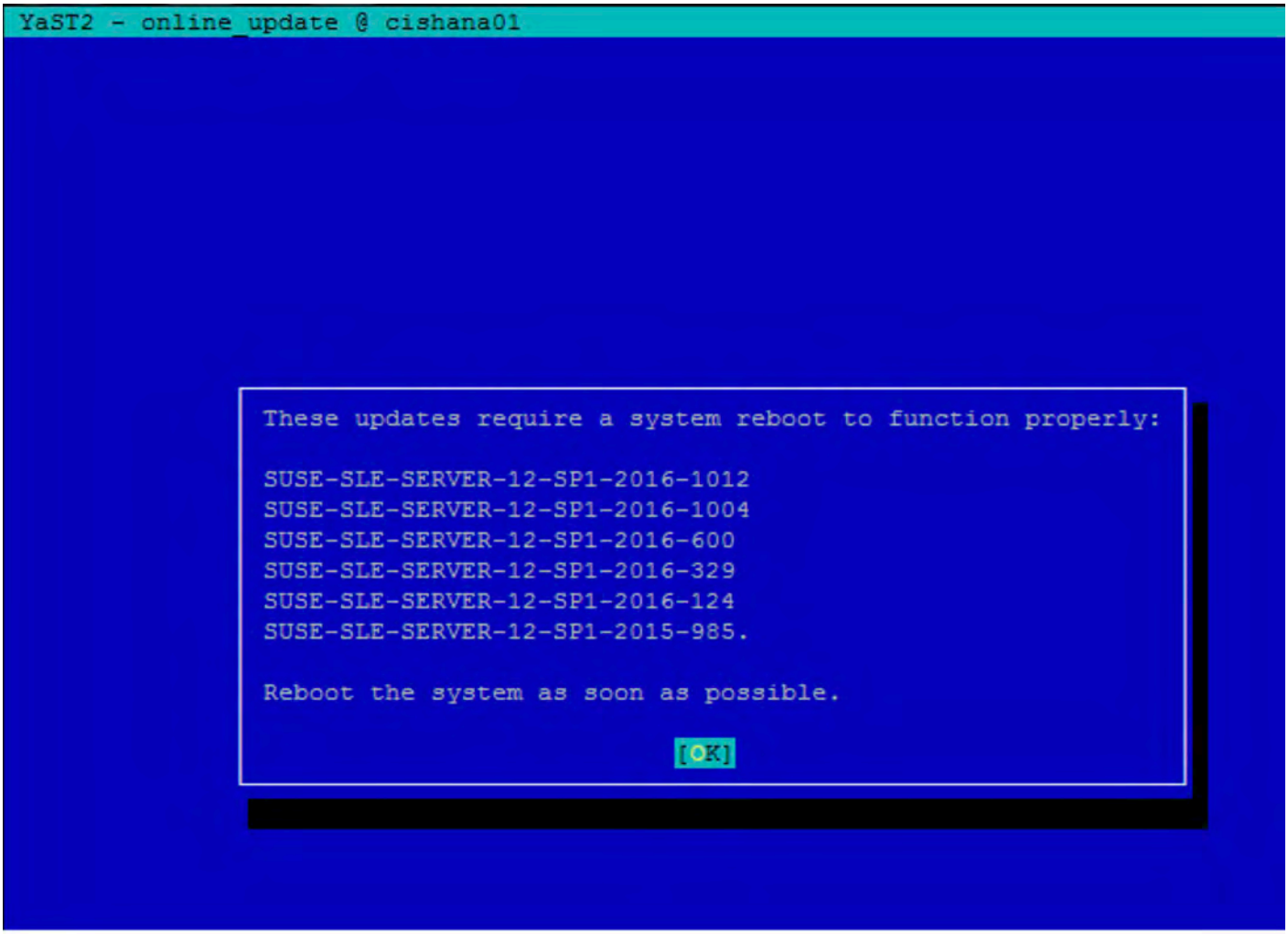
Figure 100. YaST online update: Release Notes



vii. Click OK to acknowledge the reboot prompt (Figure 101).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 101. YaST online update: Reboot message



viii. Quit YaST.

ix. Reboot the system to make the patch installation to take effect.

Operating and maintaining SAP HANA

SAP HANA operation and maintenance are described in detail in many related SAP documents. For a complete list of the documentation, see http://help.sap.com/hana.

This document summarizes only a few important operation and maintenance procedures. Most of the procedures described in this document are command-line interface (CLI) procedures and are independent of any GUI requiring an X terminal or other GUI front end (Microsoft Windows PC, Linux desktop, etc.). CLI procedures can be started using the KVM or any SSH tool such as PuTTY (for Windows) or Terminal (for Mac OS), or any Linux terminal window to connect to the SAP HANA database system (the appliance).

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Monitoring SAP HANA

Three easy CLI methods are available to check the running SAP HANA database.

```
saphostagent
```

Start a shell and connect to the SAP HANA system as the root user:

```
cishana01:~ # /usr/sap/hostctrl/exe/saphostctrl -function ListDatabases
Instance name: HDB00, Hostname: cishana01, Vendor: HDB, Type: hdb, Release: 1.00.60.0379371
Database name: HAN, Status: Error
cishana01:~ #
```

Get a list of installed SAP HANA instances or databases:

```
cishana01:~ # /usr/sap/hostctrl/exe/saphostctrl -function ListInstances Inst Info : HAN - 00 -
cishana01 - 740, patch 17, changelist 1413428
cishana01:~ #
```

Using this information (system ID [SID] and system number), you can use **sapcontrol** to gather more information about the running SAP HANA database.

```
sapcontrol
```

In a shell, use the **sapcontrol** function **GetProcessList** to display a list of running SAP HANA OS processes:

```
cishana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 00 -function GetProcessList 19.02.2019
14:54:45
GetProcessList
OK
name, description, dispstatus, textstatus, starttime, elapsedtime, pid
hdbdaemon, HDB Daemon, GREEN, Running, 2019 02 15 11:57:45, 98:57:00, 8545
hdbnameserver, HDB Nameserver, GREEN, Running, 2019 02 15 12:05:27, 98:49:18, 11579
hdbpreprocessor, HDB Preprocessor, GREEN, Running, 2019 02 15 12:05:27, 98:49:18, 11580
hdbindexserver, HDB Indexserver, GREEN, Running, 2019 02 15 12:05:27, 98:49:18, 11581
hdbstatisticsserver, HDB Statisticsserver, GREEN, Running, 2019 02 15 12:05:27, 98:49:18, 11582
hdbxsengine, HDB XSEngine, GREEN, Running, 2019 02 15 12:05:27, 98:49:18, 11583
sapwebdisp_hdb, SAP WebDispatcher, GREEN, Running, 2019 02 15 12:05:27, 98:49:18, 11584
hdbcompileserver, HDB Compileserver, GREEN, Running, 2019 02 15 12:05:27, 98:49:18, 11585
```

You see processes such as **hdbdaemon, hdbnameserver**, and **hdbindexserver** that belong to a running SAP HANA database. You can also get a system instance list, which is more useful for a scale-out appliance:

```
cishana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 00 -function GetSystemInstanceList 19.02.2019
15:03:12
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus cishana01, 0,
50013, 0, 0.3, HDB, GREEN
```

HDB info

Another important tool is the **HDB** info command, which needs to be issued by the <SID>adm user: the OS user who owns the SAP HANA database.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

As the root user on the SAP HANA appliance, enter the command shown here:

```
cishana01:~ # su - hanadm

cishana01:/usr/sap/HAN/HDB00> HDB info
USER          PID        PPID     %CPU    VSZ        RSS    COMMAND
hanadm     61208   61207     1.6      13840    2696    -sh
hanadm     61293   61208     0.0       11484  1632     \_ /bin/sh /usr/sap/HAN/HDB00/HDB info
hanadm     61316   61293     0.0      4904      872      \_ ps fx -U hanadm -o
user,pid,ppid,pcpu,vsz,rss,args
hanadm     8532            1      0.0      20048  1468    sapstart
pf=/hana/shared/HAN/profile/HAN_HDB00_cishana01
      hanadm     8545     8532      1.5      811036 290140 \_
/usr/sap/HAN/HDB00/cishana01/trace/hdb.sapHAN_HDB00 -d -nw -f /usr/sap/HAN/HDB00/cis
hanadm     11579   8545      6.6     16616748 1789920  \_ hdbnameserver
hanadm     11580   8545     1.5      5675392   371984    \_ hdbpreprocessor
hanadm     11581   8545     10.9    18908436 6632128   \_ hdbindexserver
hanadm     11582   8545     8.7      17928872 3833184  \_ hdbstatisticsserver
hanadm     11583   8545     7.4      17946280 1872380  \_ hdbxsengine
hanadm     11584   8545     0.0      203396     16000      \_ sapwebdisp_hdb
pf=/usr/sap/HAN/HDB00/cishana01/wdisp/sapwebdisp.pfl -f /usr/sap/H
hanadm     11585   8545     1.5     15941688  475708 \_ hdbcompileserver
hanadm      8368          1     0.0      216268     75072 /usr/sap/HAN/HDB00/exe/sapstartsrv
pf=/hana/shared/HAN/profile/HAN_HDB00_cishana01 -D -u
```

This command produces output similar to that from the **sapcontrol GetProcessList** function, with a bit more information about the process hierarchy.

Starting and stopping SAP HANA

Before you stop the SAP HANA appliance, you must be able to stop and start the SAP HANA database. You can use the commands shown here.

```
sapcontrol
```

You can use the sapcontrol functions **StartSystem** and **StopSystem** to start and stop a SAP HANA database.

Stop the system with the **StopSystem** function:

```
cishana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 00 -function StopSystem HDB 19.02.2019
15:05:35
StopSystem
OK
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Use the following command to check that the database has stopped:

```
cishana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 00 -function GetSystemInstanceList 19.02.2019
15:05:58
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus cishana01, 0,
50013, 0, 0.3, HDB, YELLOW
Wait for the status to be GRAY.
cishana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 00 -function GetSystemInstanceList 19.02.2019
15:07:52
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus cishana01, 0,
50013, 0, 0.3, HDB, GRAY
```

Alternatively, use the **HDB info** command:

```
cishana01:~ # su -l hanadm
cishana01:/usr/sap/HAN/HDB00> HDB info
USER PID PPID %CPU VSZ RSS COMMAND
hanadm 61477 61476 2.0 13840 2692 -sh
hanadm 61562 61477 0.0 11484 1632 \_ /bin/sh /usr/sap/HAN/HDB00/HDB info
hanadm 61585 61562 0.0 4904 872 \_ ps fx -U hanadm -o user,pid,ppid,pcpu,vsz,rss,args
hanadm 8368 1 0.0 216784 75220 /usr/sap/HAN/HDB00/exe/sapstartsrv
pf=/hana/shared/HAN/profile/HAN_HDB00_cishana01 -D -u
cishana01:/usr/sap/HAN/HDB00>
```

You can start the database again with the **sapcontrol** command **StartSystem** function:

```
cishana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 00 -function StartSystem HDB 19.02.2019
15:08:48
StartSystem
OK
```

To check the system status, use the **sapcontrol** command **GetSystemInstanceList** function. Wait for the status to be **GREEN**.

```
cishana01:~ # /usr/sap/hostctrl/exe/sapcontrol -nr 00 -function GetSystemInstanceList 19.02.2019
15:10:19
GetSystemInstanceList
OK
hostname, instanceNr, httpPort, httpsPort, startPriority, features, dispstatus cishana01, 0,
50013, 0, 0.3, HDB, GREEN
```

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

HDB

You can use the **HDB start** and **stop** commands to stop and start the SAP HANA database.

Use **HDB stop** to stop the database:

```
cishana01:~ # su - hanadm
cishana01:/usr/sap/HAN/HDB00> HDB stop
hdbdaemon will wait maximal 300 seconds for NewDB services finishing.
Stopping instance using: /usr/sap/HAN/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function
19.07.2019 19:10:37
Stop
OK
StopWait 400 2
```

In contrast to **sapcontrol**, this command waits until the database is stopped or started:

```
cishana01:/usr/sap/HAN/HDB00> HDB start
StartService
Impromptu CCC initialization by 'rscpCInit'.
     See SAP note 1266393.
OK
OK
Starting instance using: /usr/sap/HAN/SYS/exe/hdb/sapcontrol -prot NI_HTTP -nr 00 -function
StartWait 2700 2
19.02.2019 19:11:20
Start
OK
```

Downloading revisions

To download revisions, you need to connect to the service marketplace and select the software download area to search for available patches.

Refer to SAP HANA master guide for update procedures for SAP HANA.

For more information

For information about SAP HANA, see https://hana.sap.com/abouthana.html.

For information about certified and supported SAP HANA hardware, see https://global.sap.com/community/ebook/2014-09-02-hana-hardware/enEN/index.html.

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Appendix: Solution variables used in this document

Before starting the configuration process, you need to collect some specific configuration information. Table 14 provides information to help you assemble the required network and host address, numbering, and naming information. This worksheet can also be used as a “leave behind” document for future reference.

Table 14. Solution variables used in this document

Variable	Description	Value used in the lab for this document
<<var_cimc_ip_address>>	Cisco UCS C480 M5 server’s IMC IP address	<IP address>
<<var_cimc_ip_netmask>>	Cisco UCS C480 M5 server’s IMC network netmask	255.255.255.0
<<var_cimc_gateway_ip>>	Cisco UCS C480 M5 server’s IMC network gateway IP address	<Gateway IP>
<<var_raid50_vd_name>>	Name for virtual drive VD0 during RAID configuration	ucs_hana
<<var_hostname.domain>>	SAP HANA node FQDN	cishana01.custdom.local
<<var_sys_root-pw>>	SAP HANA node’s root password	
<<var_lvm_vg_name>>	SAP HANA node’s OS LVM volume group name	hanavg
<<var_mgmt_ip_address>>	SAP HANA node’s management and administration IP address	<Management IP>
<<var_mgmt_nw_netmask>>	SAP HANA node’s management network netmask	255.255.255.0
<<var_mgmt_gateway_ip>>	Cisco UCS C480 M5 server’s management and administration network gateway IP address	<Management GW IP>
<<var_mgmt_netmask_prefix>>	Netmask prefix in CIDR notation	24

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C11-742178-00 5/19

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.