UNIS 综合日志审计平台

软件安装指导

紫光恒越技术有限公司
www.unisyue.com

资料版本：5W100-20200907

前 言

本指导主要介绍紫光恒越综合日志审计平台的软件安装注意事项及安装步骤。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | … }	表示从多个选项中仅选取一个。
[x | y | …]	表示从多个选项中选取一个或者不选。
{ x | y | … }*	表示从多个选项中至少选取一个。
[x | y | …]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@unisyue.com

感谢您的反馈，让我们做得更好！

目　录

1 安装环境准备

1.1 注意事项

- 紫光恒越综合日志审计平台（以下简称平台）一般部署在安全管理区。
- 必须严格按照本手册进行安装部署，否则可能会导致安装失败。

1.2 安装环境及组网接线要求

1.2.1 安装环境硬件配置要求

平台支持安装在物理服务器或虚拟机上，对安装环境的要求如下。

1. 服务器配置要求

在物理服务器上部署平台时，服务器的最低配置要求如下表所示。

单台服务器存储要求	单台服务器内存要求
4TB硬盘*2	内存要求32GB

2. 虚拟机配置要求

在虚拟机中部署平台时，虚拟机的最低配置要求如下表所示。

虚拟机 CPU 要求	虚拟机存储要求	虚拟机内存要求
8核，底层最低要求E5-2620V4	8TB	32GB

1.2.2 服务器网络接入规划

注意

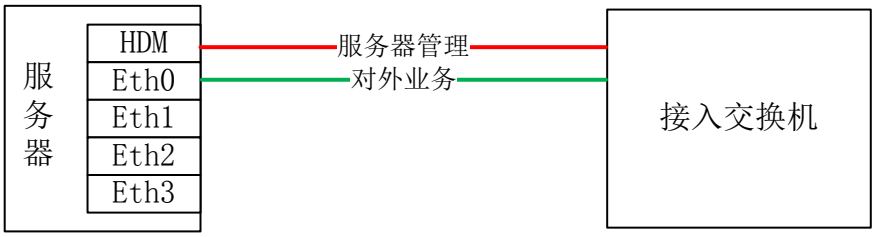
- 服务器的通信网口和管理口必须都与接入设备连接，否则，可能会导致安装失败。
- 不能将通信网口与其他接口做接口备份或接口聚合配置，否则，可能会导致安装失败。

1.2.3 组网连线

1. 服务器组网要求

将服务器 HDM、Eth0 端口都连接到接入设备（本手册以交换机为例）。组网连线示意图如下图所示。其中，HDM 端口为服务器管理口，Eth0 端口为平台对外业务通信口，即用户通过 Eth0 端口 IP 地址登录平台。

图1-1 服务器网络接入连线



2. 虚拟机组网要求

在虚拟机上部署平台时，其所在硬件组网要求同物理服务器。

1.2.4 网路接入要求

1. 服务器网络接入要求

需要客户分配以下 2 个 IP 地址：

- HDM 端口 IP 地址：根据实际组网重新配置 HDM 端口 IP（出厂配置为 192.168.1.2/24），方便对服务器进行管理。
- Eth0 端口 IP 地址：可以被网络管理员及普通用户访问的有效 IP，同时与组网中其他设备网络互通。

2. 虚拟机网络接入要求

在虚拟机上部署平台时，其所在硬件网络接入需求同物理服务器，且虚拟机要求配置 1 个虚拟网卡并分配独立 IP 地址。

1.3 安装主机（PC机）要求

安装主机（PC机）用于运行一键部署安装程序，通过一键部署安装程序可实现远程一键式安装，简化安装过程。对于运行一键部署工具的要求如 表 1-1所示。

表1-1 安装主机（PC 机）配置需求

配置项	配置要求
操作系统	Windows 7 64位操作系统
浏览器版本	Chrome Version 55.0.2883.87 m及以上版本

1.4 安装文件确认

平台安装文件包含三个部分：

- 操作系统：CentOS-7-x86_64-Minimal-1708.iso
- 安装包：UNIS-SDOP-SA-XXXX-install.tar.gz，XXXX 为版本号
- 一键部署安装程序：UNIS-SDOP-SA.zip

1.5 获取安装文件

用户可在官网获取安装文件，并将所有安装文件拷贝到 PC 上。

2 系统安装

本手册以紫光恒越服务器为例介绍平台的安装部署方法。

2.1 服务器操作系统安装

服务器出厂前，已配置 HDM 接口的缺省 IP 地址，并设置了默认的 HDM 登录信息，用户可以直接使用该默认信息登录 HDM Web 界面。

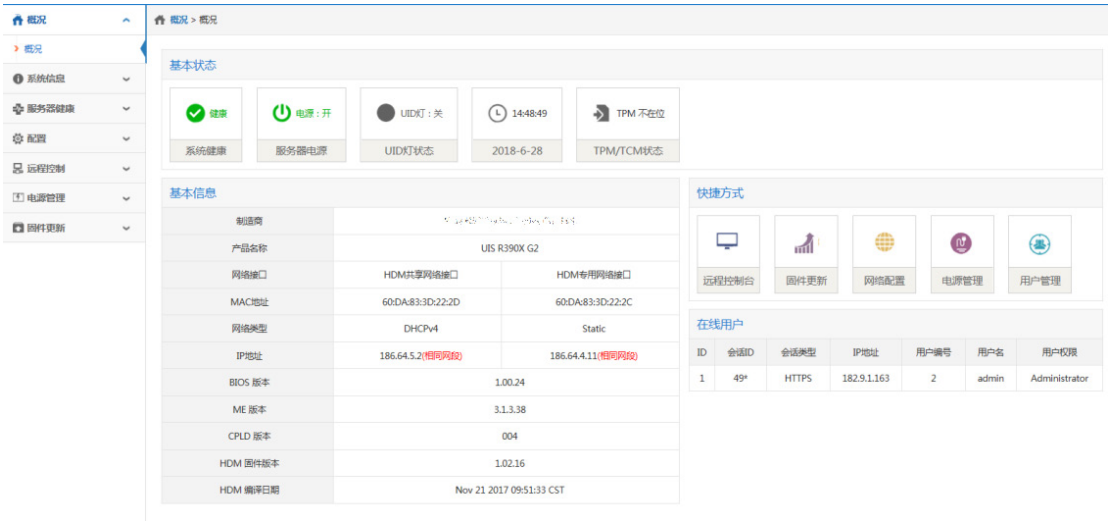
HDM的缺省管理IP地址和用户信息如 表 2-1所示。

表2-1 HDM 缺省数据

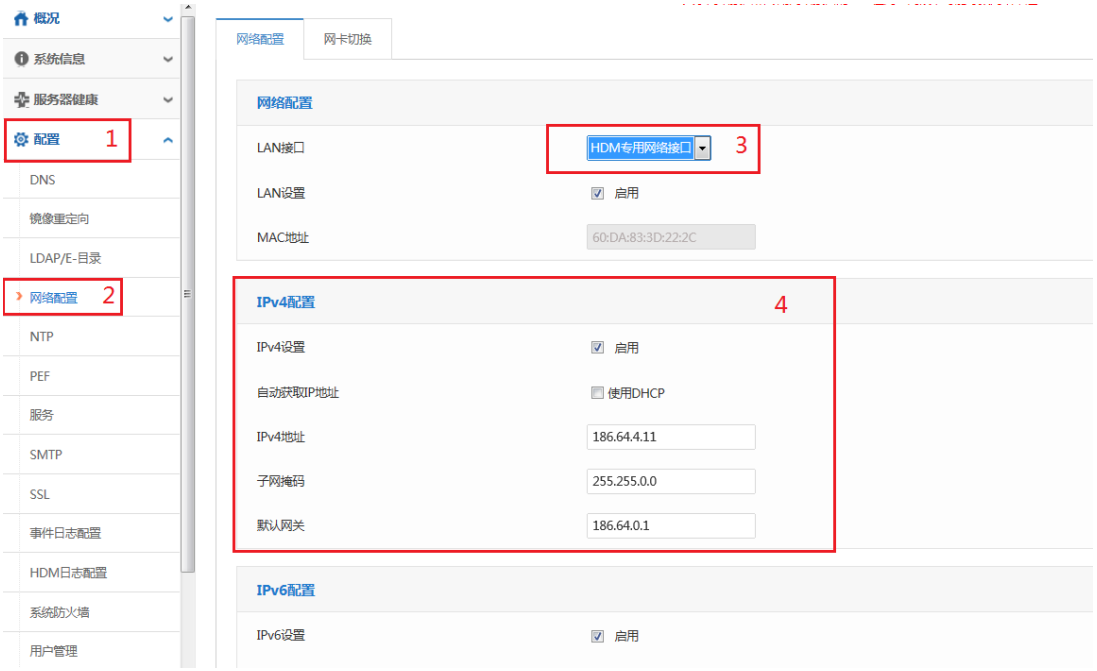
项目	缺省值
管理IP地址	HDM专用网络接口的IP地址：192.168.1.2/24
用户名、密码	• 用户名：admin • 密码：Password@_

(1) 修改 PC 的 IP 地址为 192.168.1.0/24 网段内任意主机地址（除 192.168.1.2 外），例如 192.168.1.3，然后用网线连接 PC 和服务器 HDM 专用网口，确保 PC 与服务器之间网络互通。

(2) 在 PC 上打开 IE 浏览器，在浏览器地址栏输入 192.168.1.2 进入设备 Web 登录界面，输入用户名/密码，登录成功后进入到如下界面。



(3) 单击左侧菜单中“配置 > 网络配置”进入到如下界面，选择 HDM 专用网络接口，根据实际情况修改其 IPv4 地址、子网掩码和默认网关，然后单击<保存>按钮。

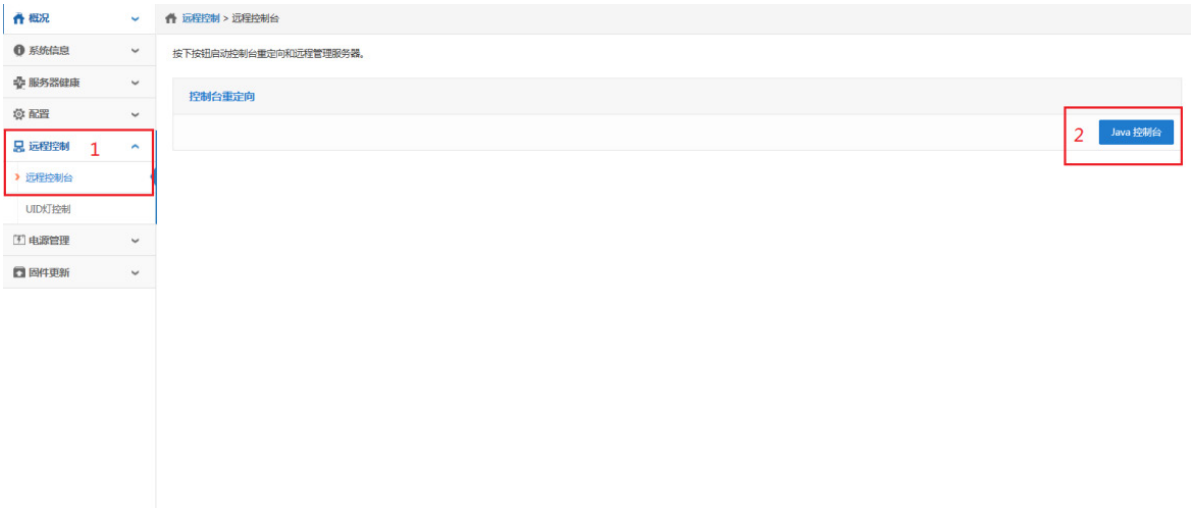


(4) 重新修改 PC 的 IP 地址，确保 PC 与服务器之间网络互通，然后使用新的管理口 IP 地址登录 HDM Web 界面。

2.1.2 登录使用远程控制台

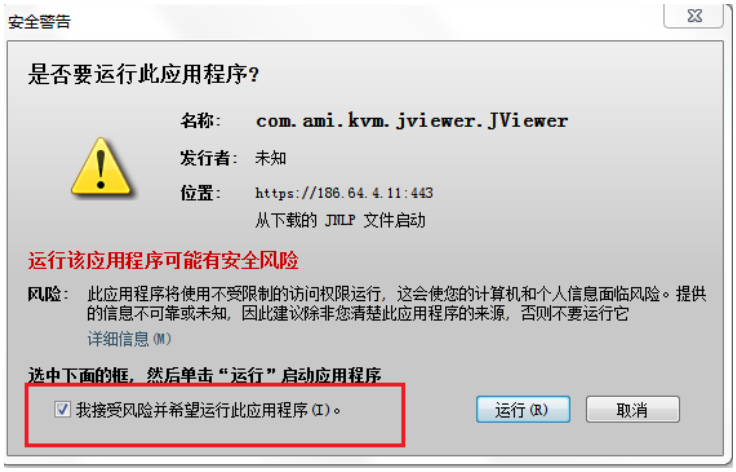
(1) 在 PC 上将新配置的管理口 IP 地址添加到 java 安全例外列表中。添加方法为：单击“计算机开始菜单 > 控制面板 > 程序 > java > 安全 > 编辑站点列表 > 添加”将管理口 IP 地址添加到“例外站点”列表中。

(2) 重新登录 HDM Web 界面，单击左侧菜单中的“远程控制 > 远程控制台 > Java 控制台”。

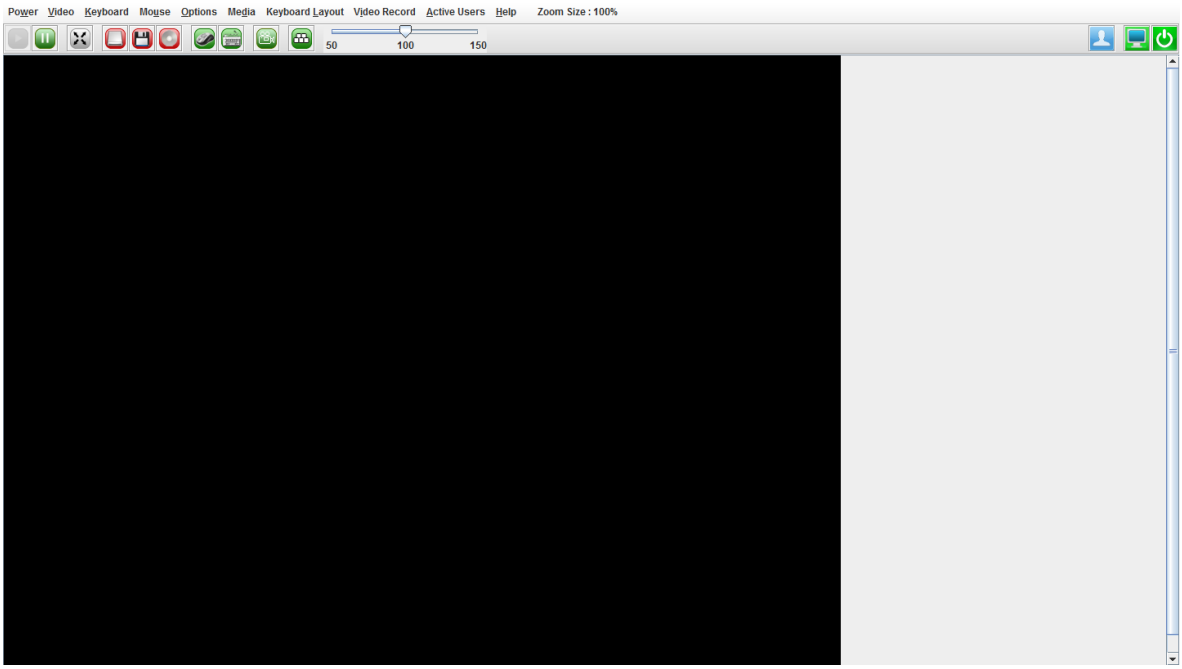


(3) 出现如下图警告时，单击<继续>按钮。

(4) 勾选“我接受风险并希望运行此应用程序”，单击<运行>按钮。

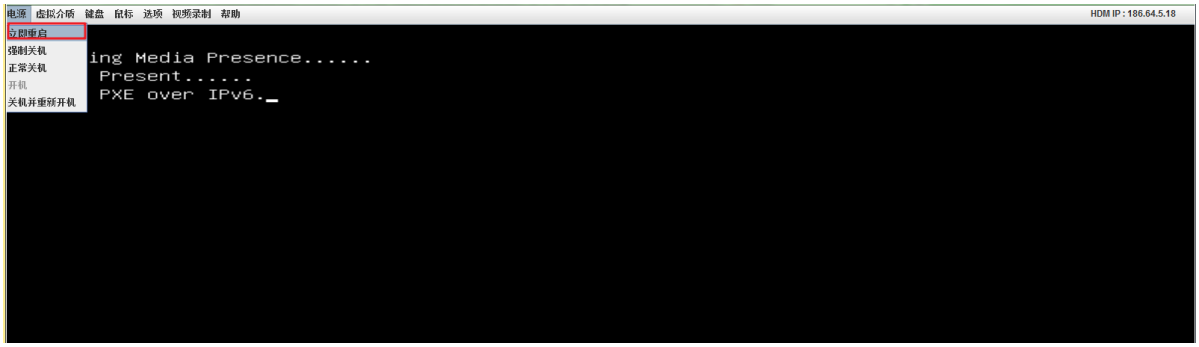


(5) 然后出现下图中的 JViewer 界面。

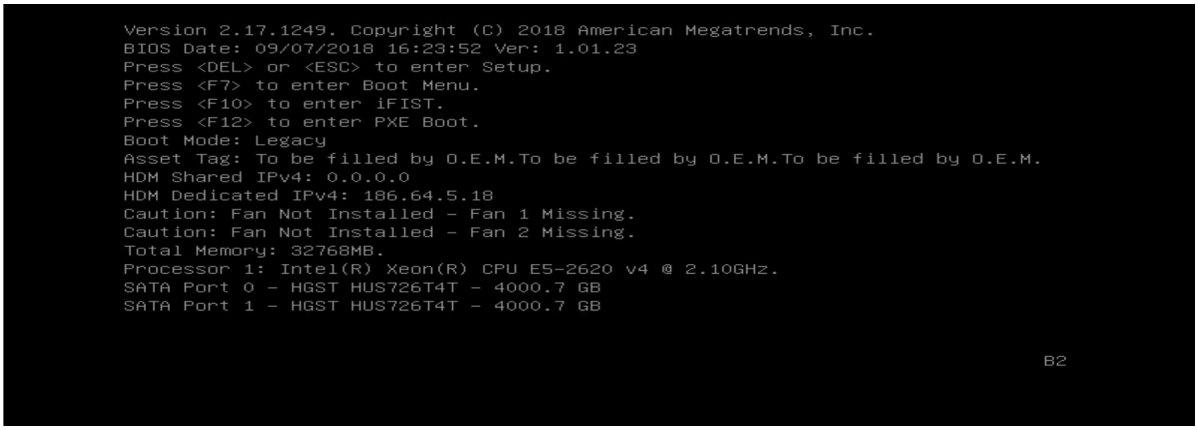


2.1.3 配置BIOS设置

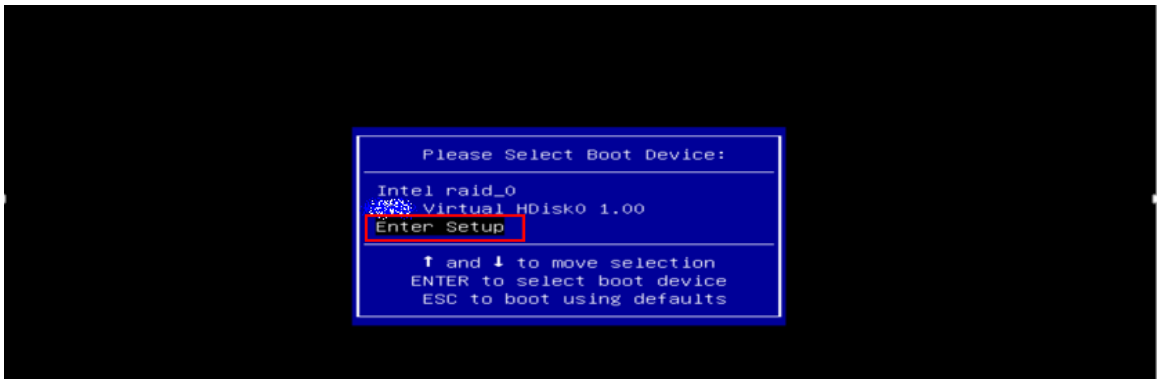
(1) 在 JViewer 界面，单击“电源 > 立即重启”重启服务器。



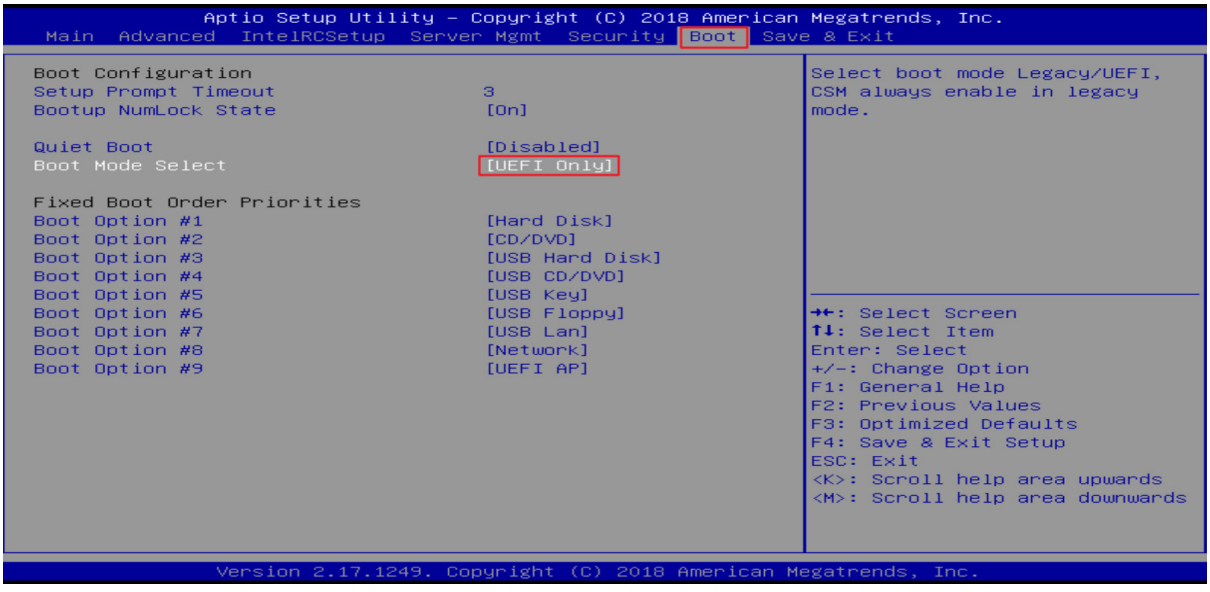
(2) 服务器启动过程中，当出现如下界面时，立即按下<F7>键进入 Boot 菜单页面，如下所示。



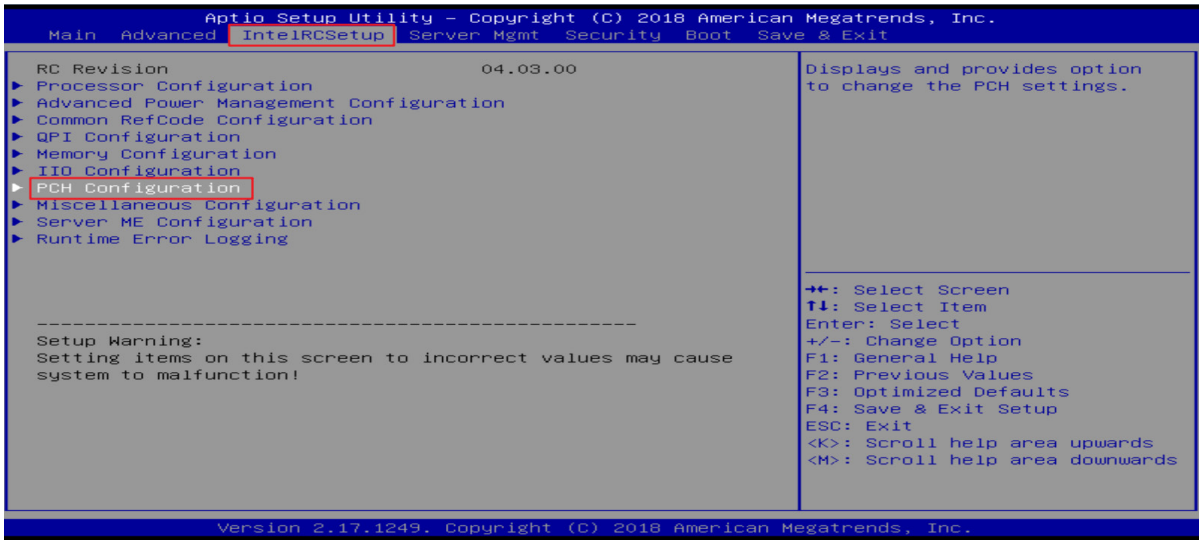
(3) 进入下面界面，选中“Enter Setup”，按<回车>键进入 BIOS 页面。



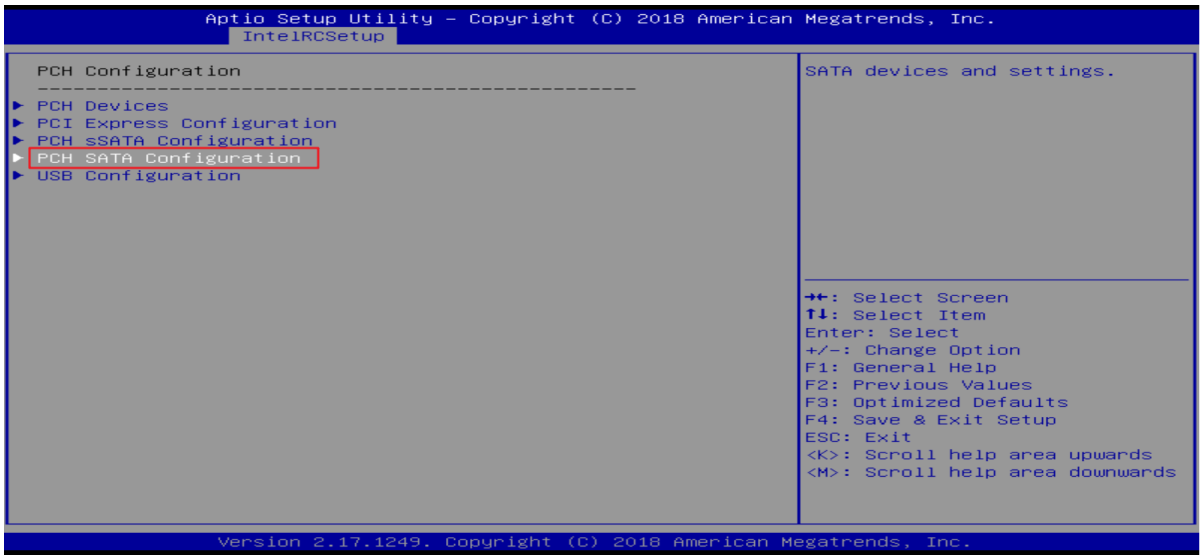
(4) 选择“Boot”页签，修改“Boot Mode Select”为“UEFI Only”。



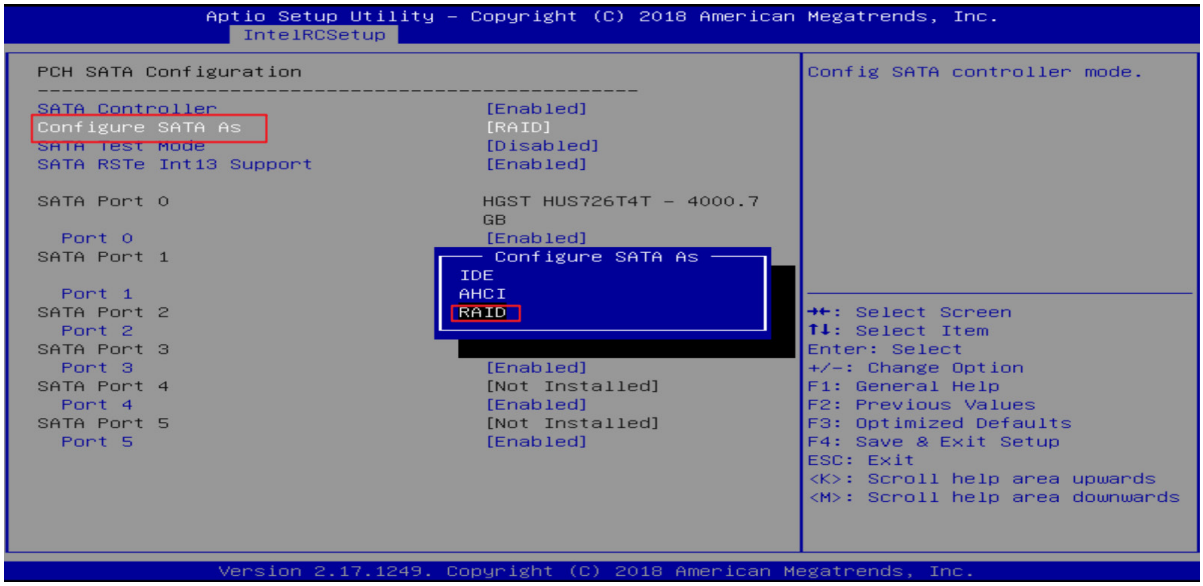
(5) 选择“IntelRCSetup”页签，选中“PCH Configuration”，按<回车>键进入 PCH 配置页面。



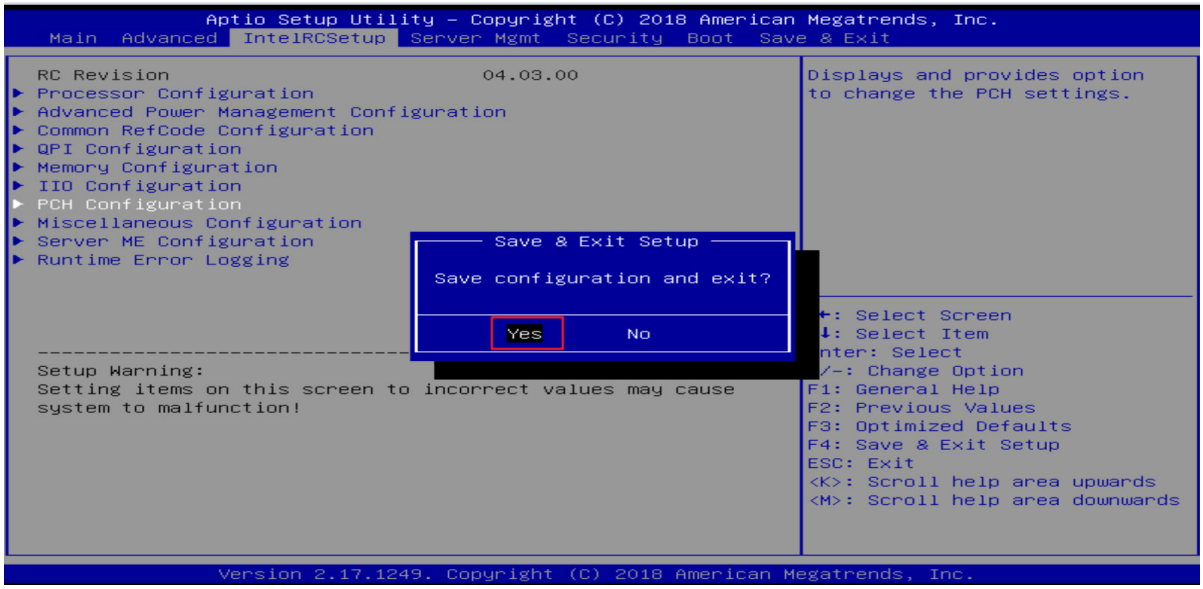
(6) 选中“PCH SATA Configuration”，按<回车>键进入 PCH SATA 配置页面。



(7) 设置“Configure SATA As”为“RAID”。

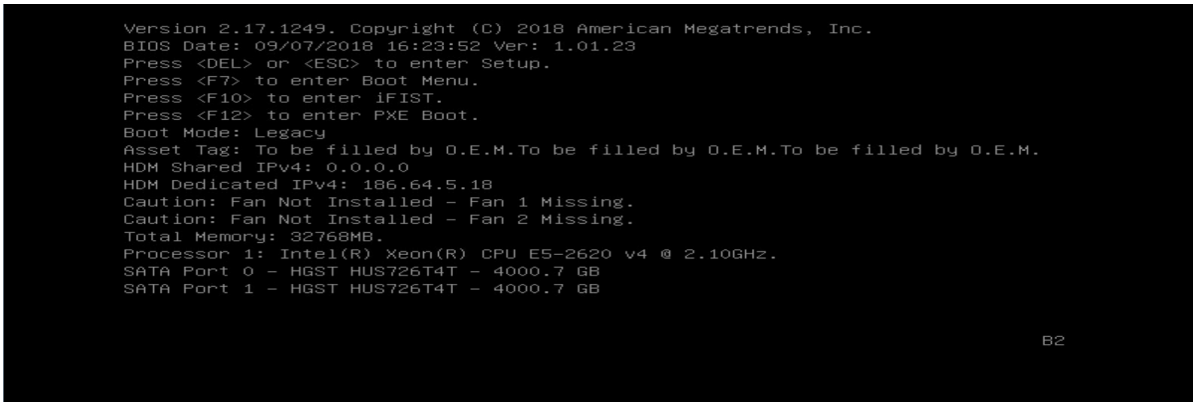


(8) 按<F4>键保存配置并退出，Boot 设置完成。

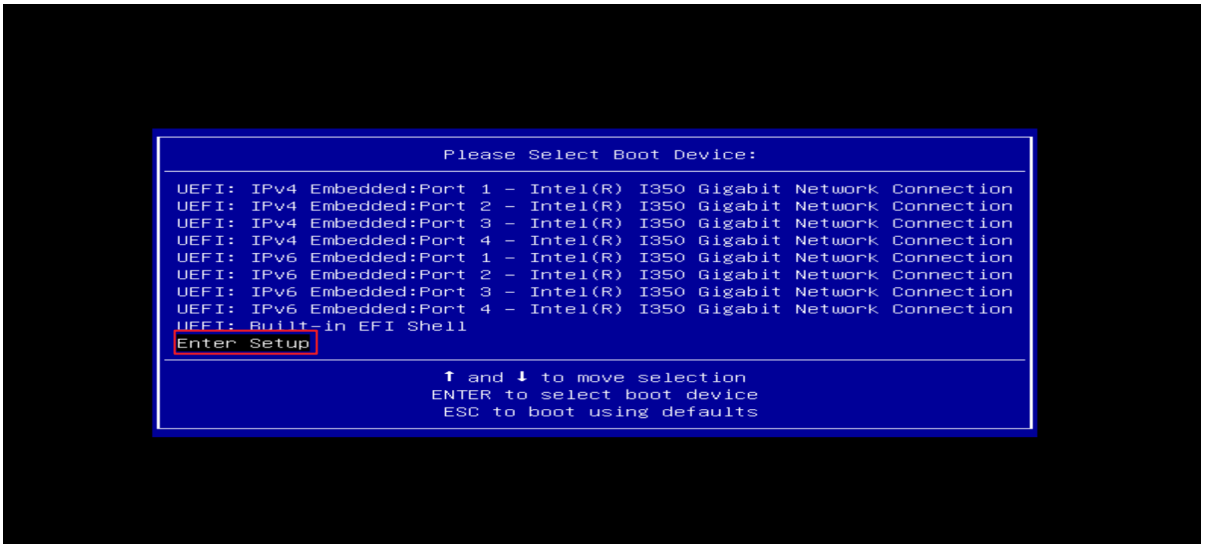


2.1.4 配置服务器RAID

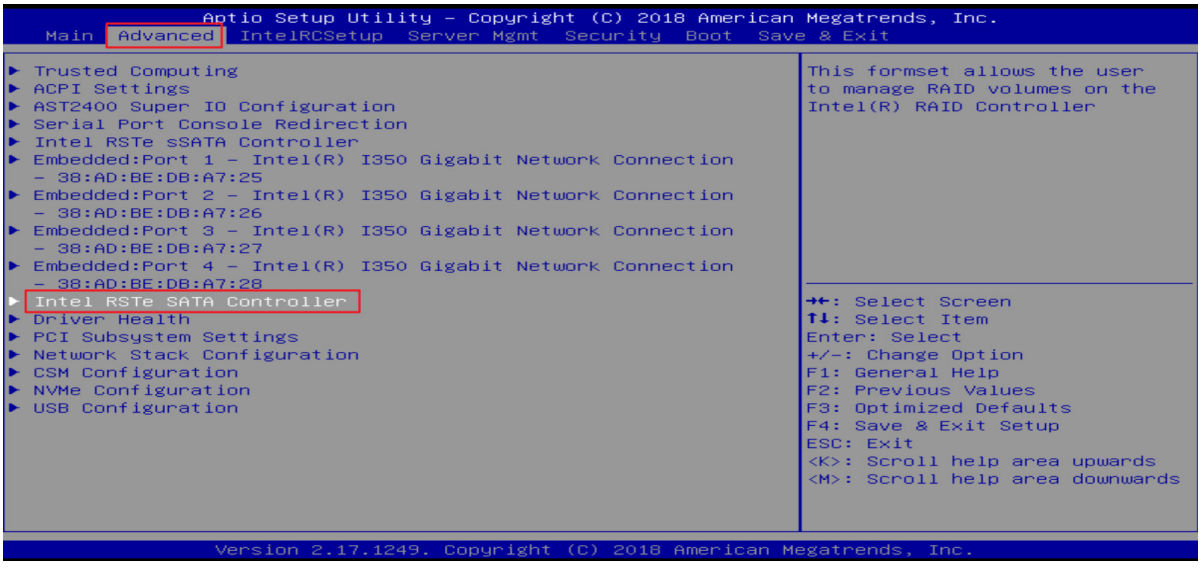
(1) BIOS 配置完成后，保存并退出，然后重启服务器。服务器启动过程中，进入以下页面时按<F7>键重新进入 Boot 菜单页面。



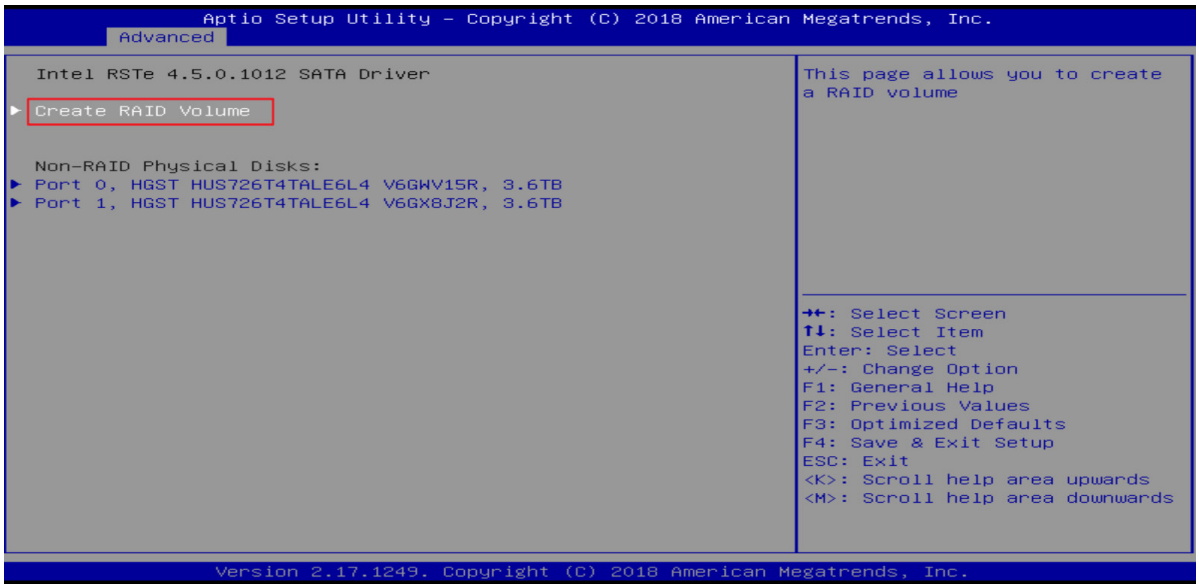
(2) 当出现下图界面后，选择“Enter Setup”，按<回车>键进入下一级菜单页面。



(3) 选择“Advanced”页签，选中“Intel RSTe SATA Controller”，按<回车>键进入下一级菜单页面。



(4) 选中“Create RAID Volume”，按<回车>键，开始创建 RAID。



(5) 进入 RAID 创建页面后，按下图所示配置各项参数。

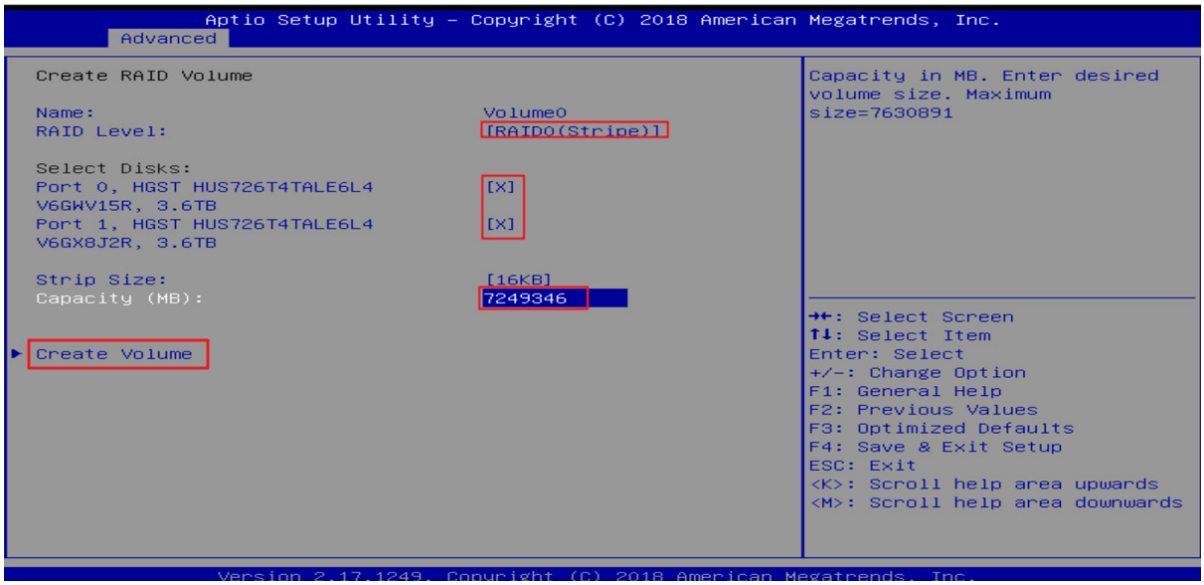
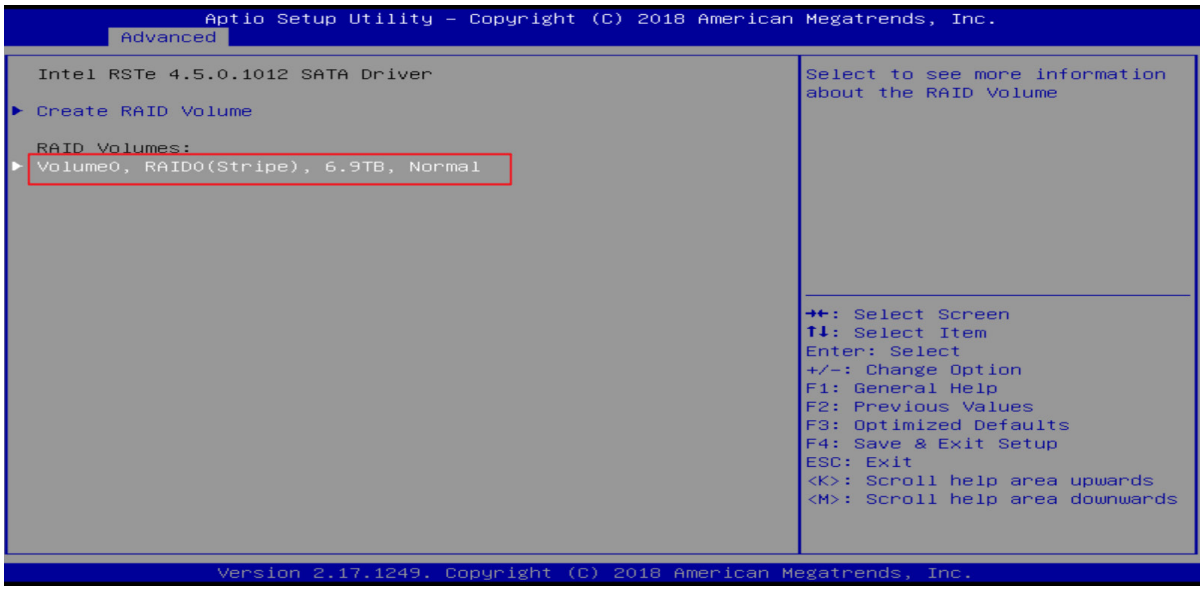


表2-2 参数说明

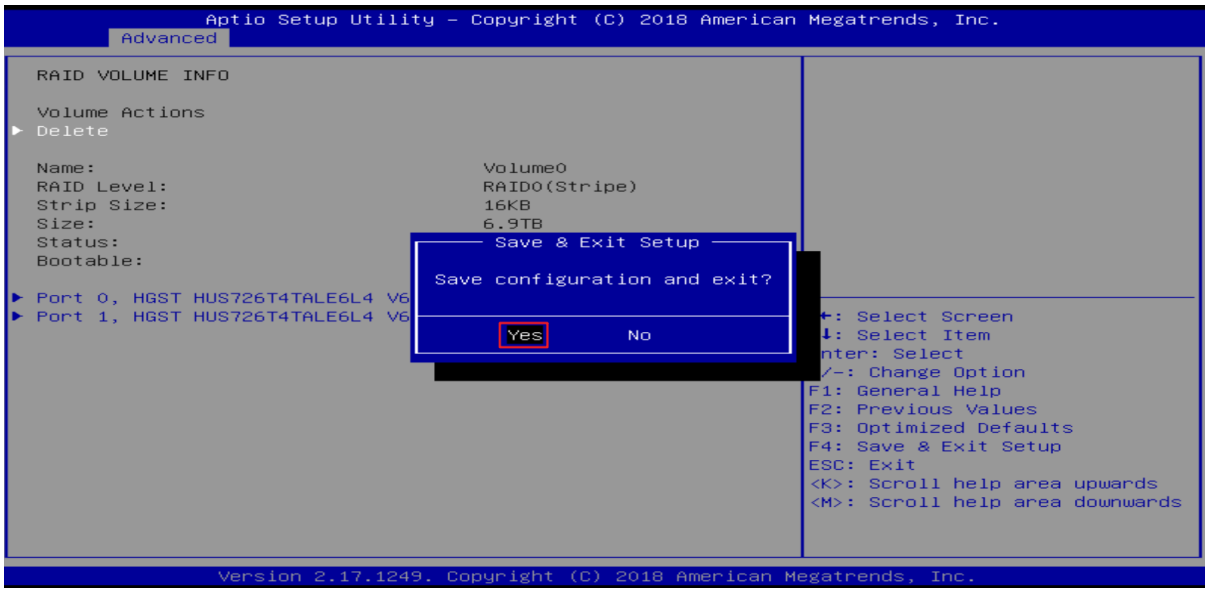
配置项	说明
Name	RAID的名称
RAID Level	RAID级别，决定逻辑磁盘的性能、容量及容错能力。此处配置为RAID0，若发生单个磁盘故障会导致整机不可用、数据丢失等情况
Select Disks	选择组成RAID的成员磁盘。Select Disks参数下方显示的是可用的磁盘，按Enter键可选择成员磁盘。[X]表示该磁盘已被选中

配置项	说明
Strip Size	条带大小，写在磁盘上的的条带数据块的容量大小
Capacity	逻辑磁盘的容量

(6) 配置完成后，选中“Create Volume”，按<回车>键确认创建 RAID 阵列，创建后页面如下图所示。

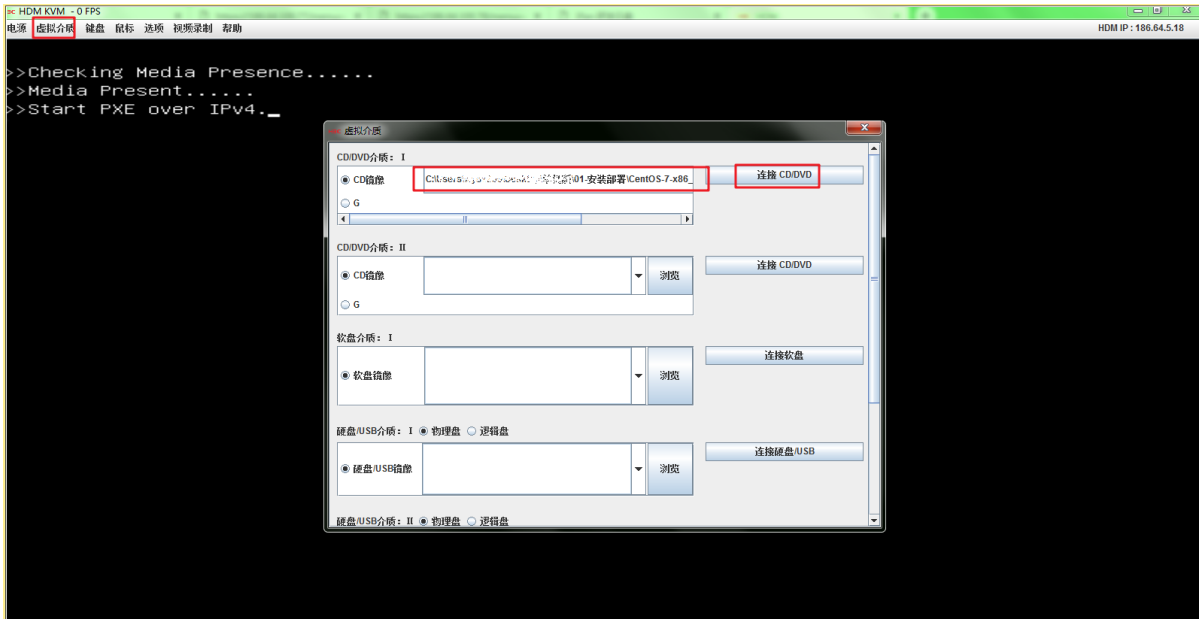


(7) 按<F4>按键保存配置并退出，RAID 设置完成。

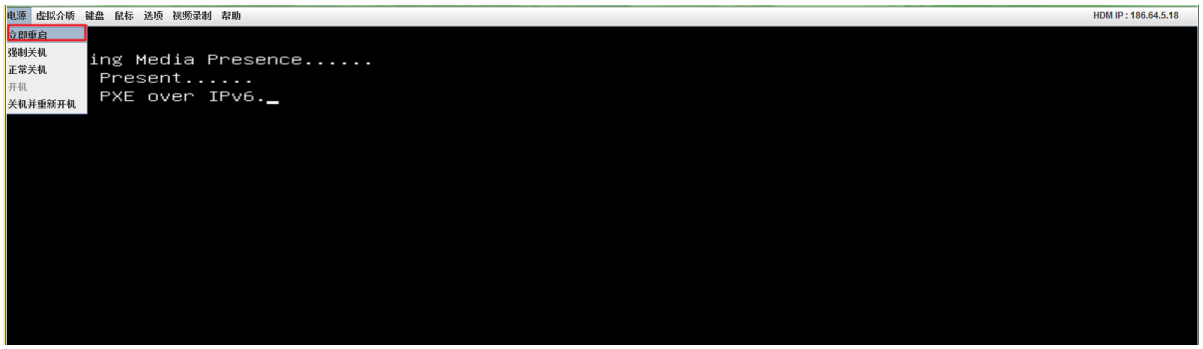


2.1.5 安装操作系统

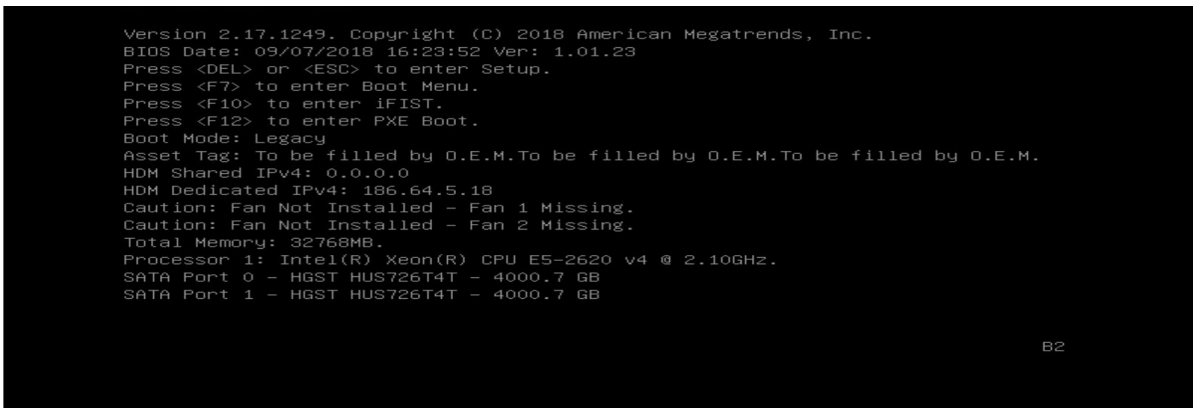
(1) 在 JViewer 界面，单击菜单栏中的“虚拟介质”，弹出导入镜像对话框。单击<浏览>，在弹出的界面中，选择 ISO 镜像文件（镜像文件名称以实际情况为准），单击<打开>，然后单击<连接 CD/DVD>。



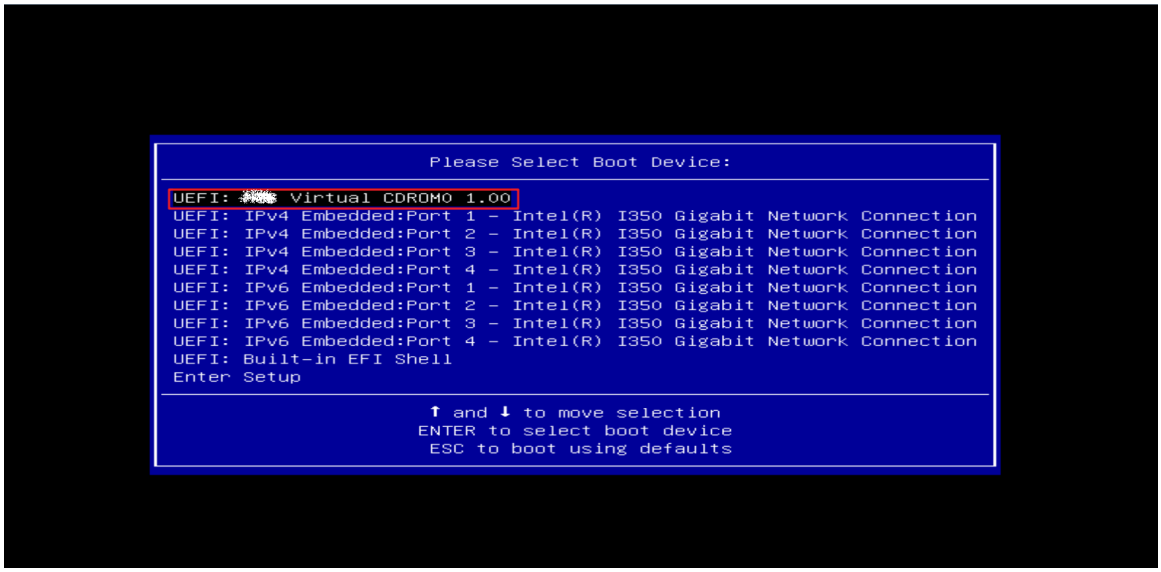
(2) 导入完成后，单击菜单栏中的电源菜单，选择“立即重启”重启服务器。



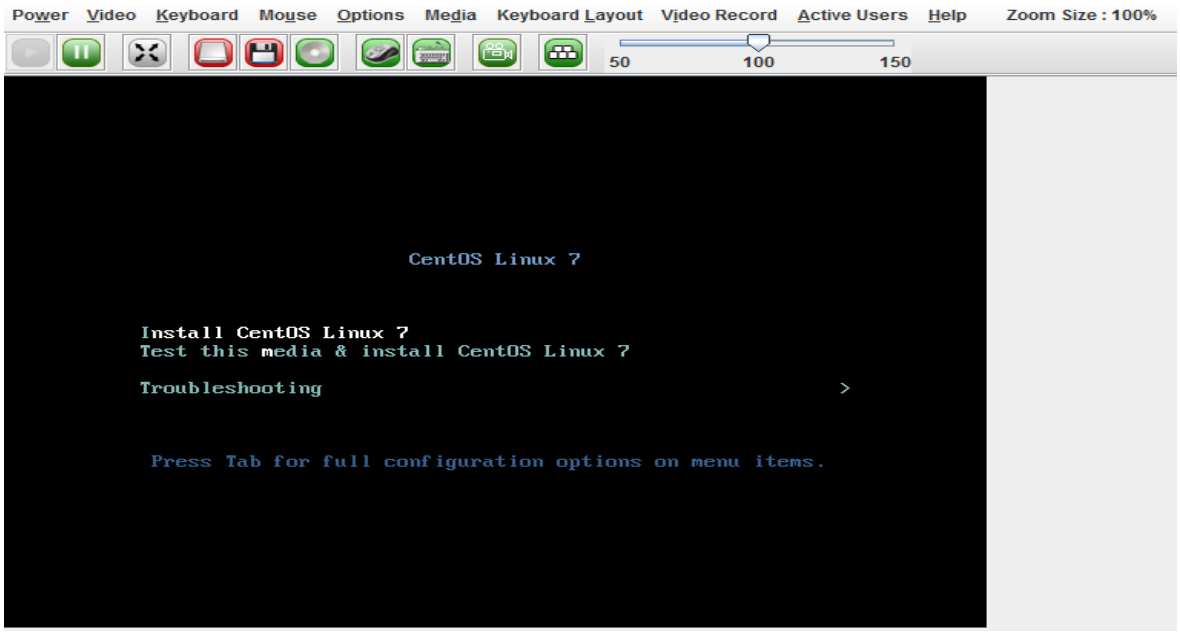
(3) 重启过程中，进入如下页面时，立即按下<F7>进入启动设置界面。



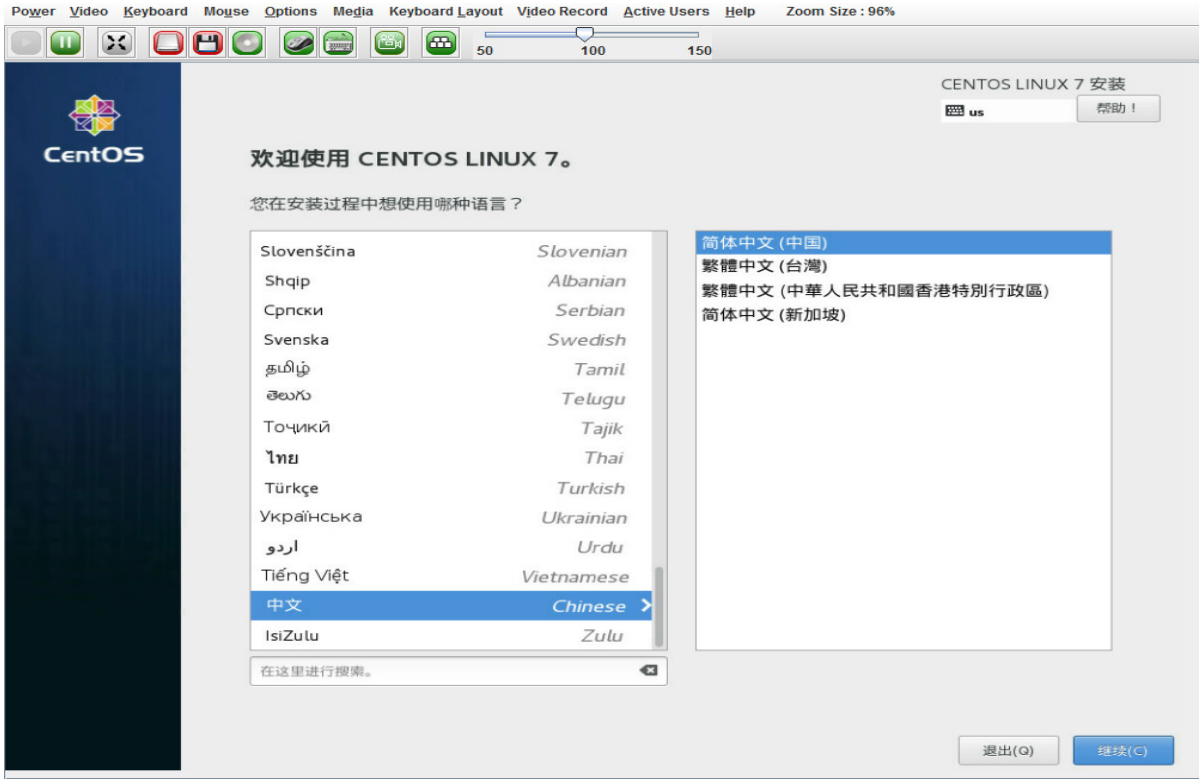
(4) 当出现如下图所示界面时，选择“Virtual CDROMO 1.00”选项，按<Enter>键进入安装页面。



(5) 选中“Install CentOS linux 7”，按<Enter>键进入下一步安装界面。



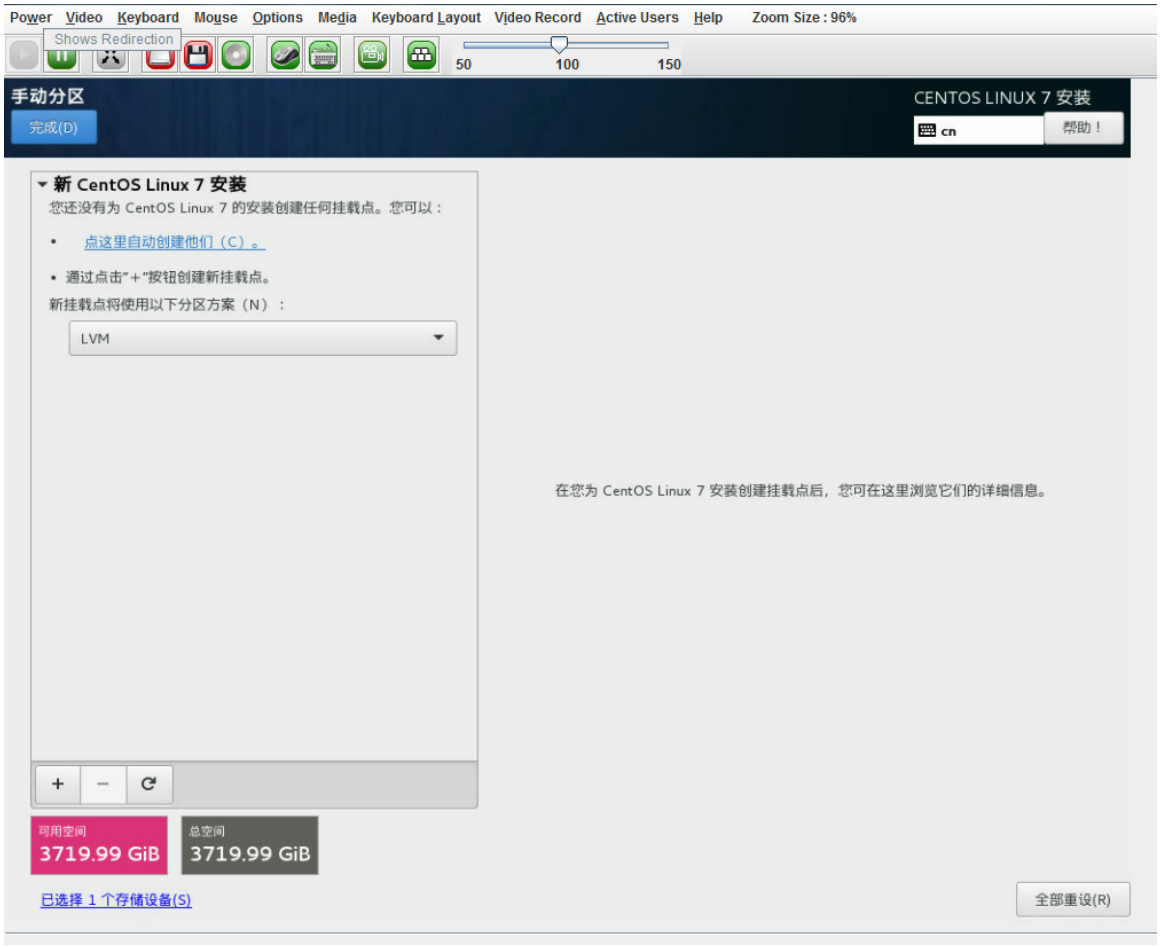
(6) 当出现如下图所示界面时，选择安装语言“中文 > 简体中文（中国）”，单击<继续>。



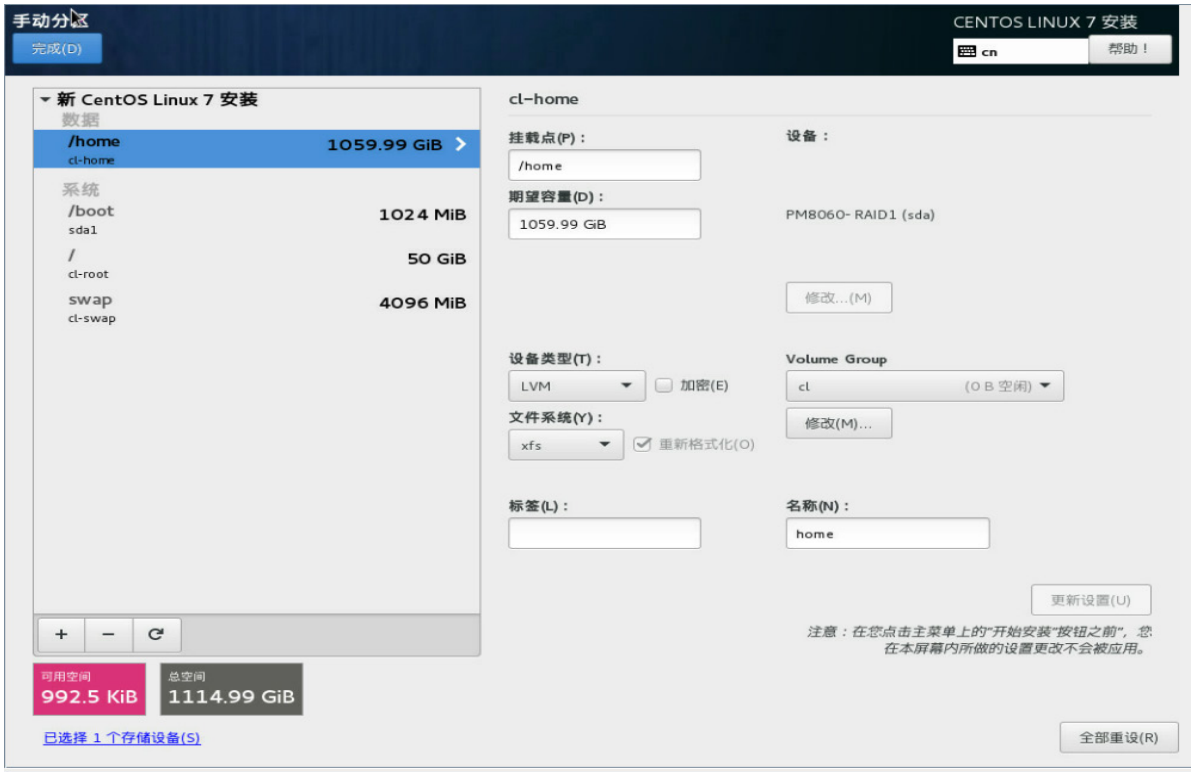
(7) 出现如下图所示界面时，单击“安装位置”。

(8)　选择 RAID0 盘进行分区设置，选择“我要配置分区”选项，单击<完成>按钮进入下一界面。

(9)　当出现如下图所示界面时，单击“点这里自动创建他们”进入下一级安装界面。



(10) 使用默认配置进行安装，不需要调整。单击<完成>按钮。



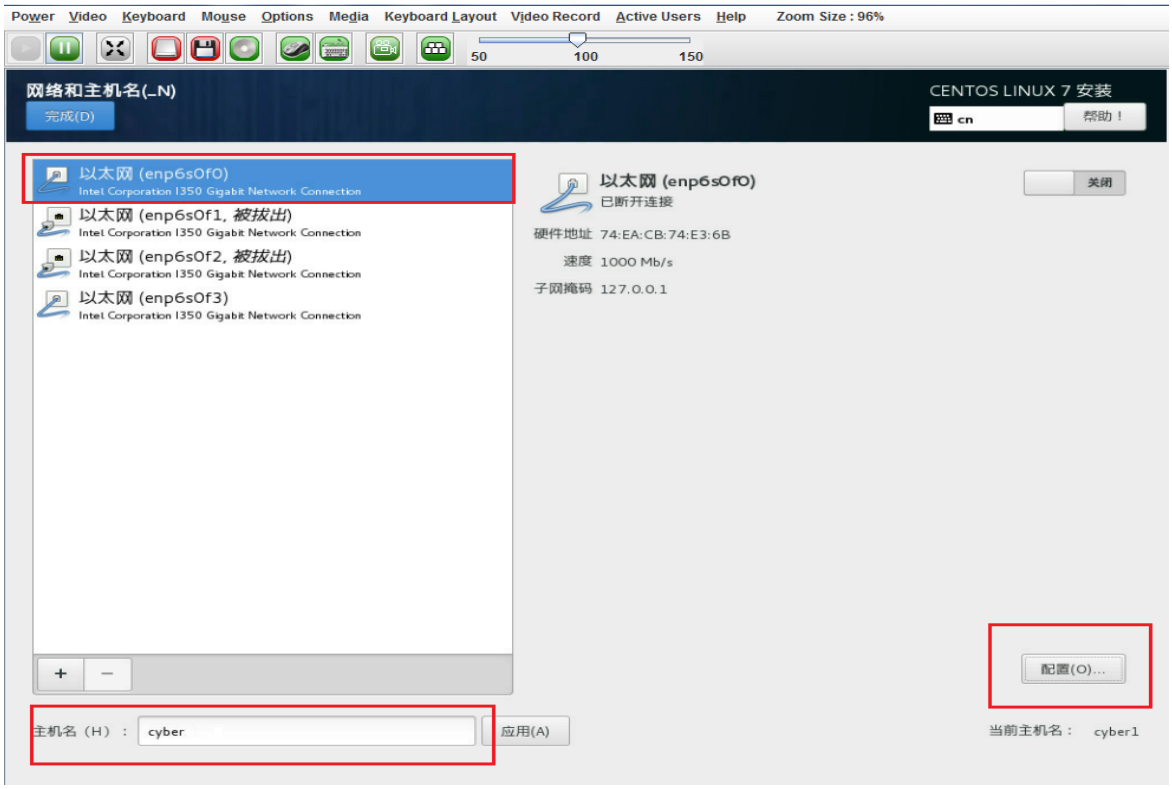
(11) 在弹出确认更改配置的对话框中，单击<接受更改>返回安装主界面。

(12) 系统盘分区完成后，在安装主界面上选择“网络和主机名”，进入网络和主机名配置页面。

注意

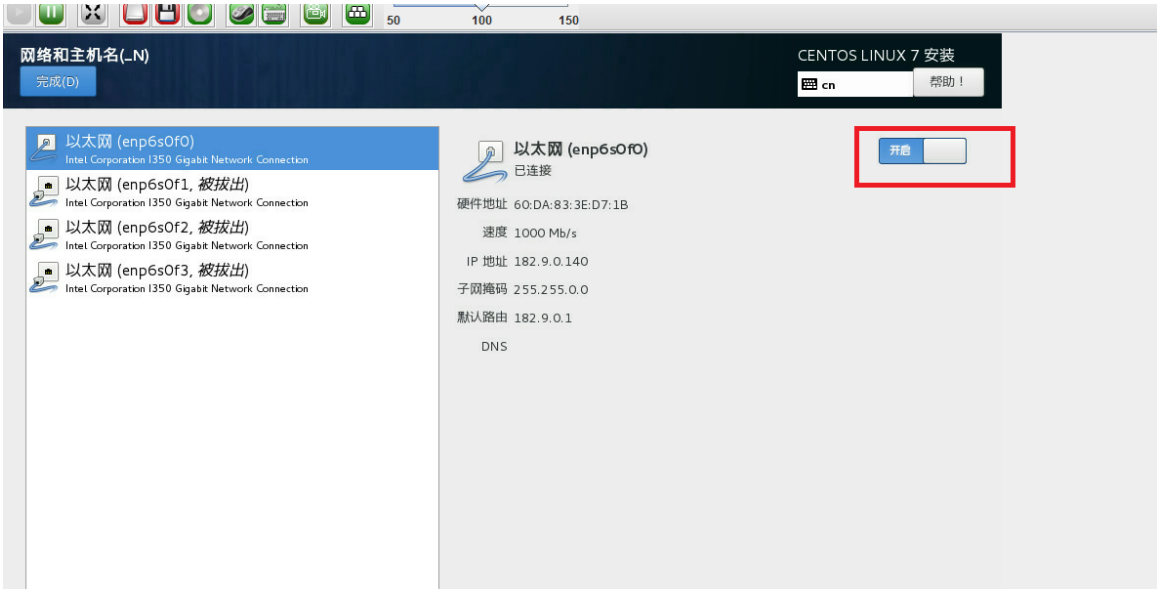
- 主机名必须配置为 cyber，否则将会导致平台软件安装失败。
- 配置网络时，必须选择第一块网卡，并为其配置有效 IP 地址，保证其他设备可访问该 IP，否则平台软件无法成功安装。

(13) 进入如下界面时，先在页面右下角配置主机名为 cyber，单击<应用>，然后选择第一个以太网选项（一般网卡的编号顺序是 XXX0-XXX3，末位数字 0 代表第一块网卡，数字 3 代表第四块网卡），单击右下角<配置>按钮，弹出配置 IP 界面。



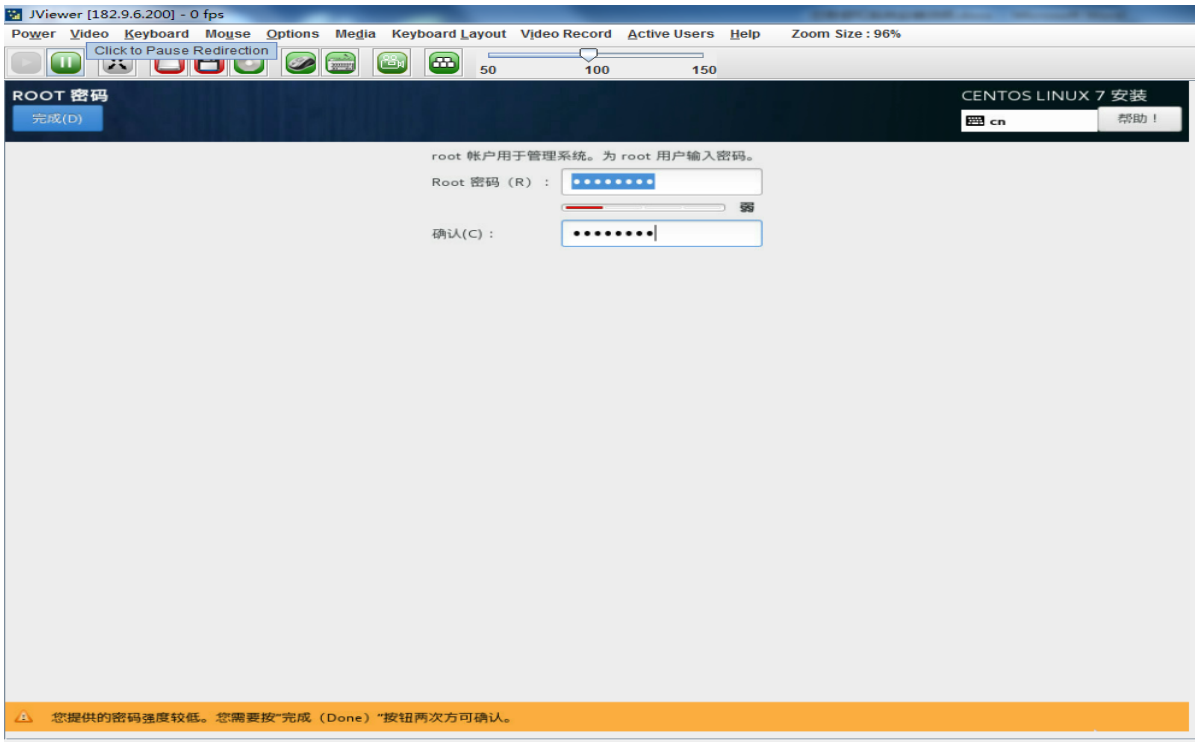
(14) 当出现如下图所示的界面时，先选择 IPv4 设置，设置方法改为手动，然后单击<Add>按钮，输入 IP 地址和子网掩码，确认无误后，单击<保存>。

(15) 配置完成后，开启网卡，否则无法连接服务器。



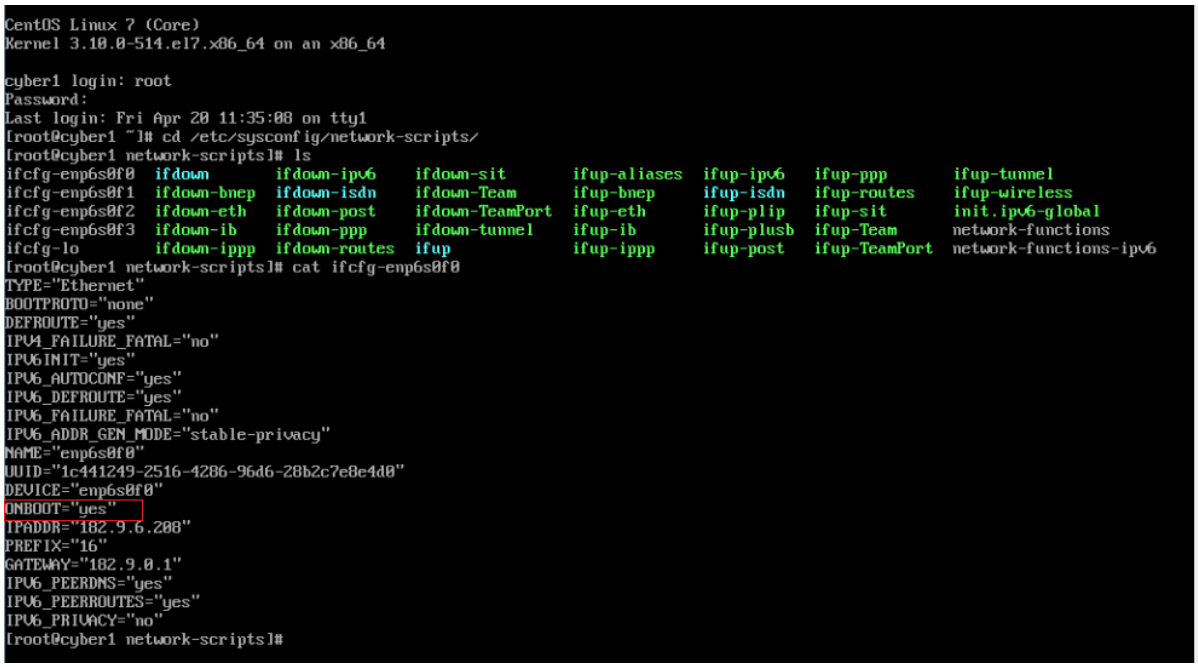
(16) 配置完网络和主机名后，单击右上角<完成>按钮返回安装主界面，单击<开始安装>按钮安装操作系统。

(17) 当出现下图所示界面时，将系统的 ROOT 密码设置为 unis_csap，设置完后不可以更改。



(18) 最后等待系统安装完成，然后单击<reboot now>重启服务器，重启完成后通过jview进入系统登录界面，输入root，密码unis_csap进入系统，执行 **cd /etc/sysconfig/network-script/**命令进入相应目录，然后通过cat打开ifconfig-xxx0

文件，然后确认onboot配置后面是否为yes，如果不是则修改为yes，保存修改后，然后执行 **service network restart**命令完成系统安装。



(19) 系统安装完成后，需要通过远程连接工具进行连接，如果连接失败请检查网络问题。

2.2 虚拟机操作系统安装

在虚拟机上部署平台时，不需要配置 BIOS 和 RAID，操作系统安装方法与服务器安装操作系统相同。

2.3 服务器安装部署平台软件

在进行平台软件安装之前，确保服务器与 PC 之间网络互通，否则无法进行平台软件安装。

2.3.1 安装环境准备

(1) 在 PC 上通过 SSH 登录服务器，登录地址为系统安装时设置为 cyber 的服务器 IP 地址。

(2) 在 PC 解压 UNIS-SDOP-SA.zip，并运行一键安装部署程序 UNIS-SDOP-SA.exe，不要关闭弹出的窗口。

2.3.2 安装平台软件

(1) 在 PC 上打开 Chrome 浏览器，访问 http://127.0.0.1:8080/login，进入下图所示页面，输入 cyber 主机的 IP 地址，用户名为 root，密码为 unis_csap。

(2) 登录成功后，在部署包路径中输入平台软件包 UNIS-SDOP-SA-XXXX-install.tar.gz 全路径（例如，存放在 C 盘根目录下时，其全路径为 C:\UNIS-SDOP-SA-XXXX-install.tar.gz），单击<开始部署>，当部署进度显示为 100%时表示安装成功

2.3.3 登录平台页面

安装完成后需进行 License 激活才能登录到平台。有关 License 激活文件申请的详细介绍请参见紫光恒越 License 手册。

获取基础平台软件授权后，其安装步骤如下：

(1) 在浏览器上输入主机名为“cyber”的设备的 IP 地址后，按 Enter 键进入平台 Web 登录页面，（首次登录可能会提示建立不安全的连接提示，单击继续即可），然后单击<产品注册>进入产品注册页面。

说明

如果没有进入登录页面表示安装失败，需要重新安装系统。

(2) 在“选择基本操作”页签选择“使用 License 文件对产品进行注册”后单击<下一步>，导入已申请的 License 文件即可。

(3) License 激活后，在登录页面输入用户名 admin，密码 admin@admin，单击<登录>即可进入平台主界面。