UNIS 服务器 HDM

用户指南

紫光恒越技术有限公司
http://www.unisyue.com

资料版本：6W102-20220525

前 言

本手册介绍了 HDM 的登录方法，以及如何通过 HDM 查看设备信息，进行设备健康诊断、网络配置、安全管理、远程控制、电源功耗管理与设备维护等内容。

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
- 负责服务器配置和维护的管理员

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. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

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

说明

- 本文中硬件图片仅供参考，具体请以硬件实物为准。
- 本文中软件页面可能会不定期更新，请以产品实际显示页面为准。
- 本文中部分数据为举例数据，操作步骤中以举例数据进行说明。用户操作时，请以现场的真实数据为准。

1 HDM 概述

1.1 简介

硬件设备管理系统（Hardware Device Management，以下简称 HDM）是 UNIS 自主研发的服务器远程管理系统。HDM 提供了丰富的特性：

- 丰富的管理接口
  - 提供 IPMI/HTTPS/SNMP/Redfish 管理接口，满足多种方式的系统集成需求。
  - 兼容 IPMI1.5/IPMI2.0，提供标准的管理接口，可被标准管理系统集成。
- 远程维护手段
  - 提供虚拟 KVM（Keyboard、Video、and Mouse，键盘、视频和鼠标）、虚拟媒体等远程管理工具，使管理员能够方便地对服务器进行远程监控和管理。
  - 支持 RAID 的带外监控和配置，提升了 RAID 配置效率，简化了配置操作。
  - 支持 HDM\BIOS\RAID 配置导入导出，提升了服务器远程管理效率。
- 故障监控与诊断
  - 通过截屏和录像可以快速分析系统崩溃的原因。
  - 支持 Syslog 报文、Trap 报文和电子邮件上报告警，方便搜集服务器故障信息。
  - HDM 能对服务器进行全面精细的监控，并且提供丰富的告警和详细的日志，如 CPU 的内核温度、内存故障、硬盘故障、电压、风扇转速、电源故障等。
  - 支持 SHD（Smart Hardware Diagnosis，智能硬件诊断系统），SHD 支持基于部件的精准故障诊断，方便部件故障定位和更换。
- 网络功能
  - HDM 支持最新的边带网络技术以及 VLAN 网络功能，通过边带网络可以支持更加灵活的管理组网。
  - 支持 NTP，帮助服务器同步网络时间，提高设备时间精度。
  - 支持域服务器和目录服务器，简化服务器用户管理，并提高了用户管理的安全性。
- 安全管理
  - 双镜像备份，提高系统的安全性，即使当前运行的软件完全崩溃，也可以从备份镜像启动。
  - 多样化的用户安全接口，保证用户登录安全性。
  - 支持多种证书的上传和替换，保证数据传输的安全性。
  - 支持 PFR 固件保护功能，保护 HDM 系统免受攻击。

- 智能电源管理
  - 功率封顶功能有利于精确部署设备数量，合理分配资源。
  - 节能设置和电源性能支持用户根据应用需求设置节能模式，降低能耗。
- 联合管理
  - 支持服务器的批量管理，提高运维效率。
  - 支持单台或批量添加服务器，满足多种需求。
- LCD 液晶显示屏
  - 部分服务器可选配 3.5 英寸可触摸 LCD 液晶显示屏，方便了服务器的临场巡检或维护。
  - LCD 显示屏直接从 HDM 获取服务器状态信息，方便快速了解服务器的健康状态。

1.2 常用操作接口

HDM 支持多种操作接口，包括 Web 端、Redfish 接口、IPMI 接口和 SNMP 接口。

1.2.1 HDM Web 端

HDM Web 端为服务器提供直观便捷的配置查询接口，并将操作按照功能实现划分到不同的模块。HDM Web 端主要包括首页、系统管理、HDM 设置、远程服务、远程运维、用户&安全和联合管理几大模块。

HDM Web 端目前支持简体中文和英文双语环境，单击页面上的语言按钮  或可以切换语言环境。

在使用 Web 端功能时，可以单击页面右上方的  按钮，查看联机帮助获取操作指导。

1.2.2 Redfish 接口

HDM 支持标准的 Redfish 接口。Redfish 客户端（Redfish 接口工具，如 Postman）把 HTTPS 操作发送到服务器，通过 GET、PATCH、POST 和 DELETE 命令对服务器进行查询、配置和监控。关于服务器支持的 Redfish 接口说明，请联系技术支持。

1.2.3 IPMI 接口

HDM 支持标准的 IPMI1.5/IPMI2.0 接口。IPMI（Intelligent Platform Management Interface，智能平台管理接口）是一项应用于服务器管理系统设计的标准，有助于在不同类服务器系统硬件上实施系统管理，使不同平台的集中管理成为可能。

在 IPMI 管理平台中，BMC（Baseboard Management Controller，基板管理控制器）是核心控制器，系统管理软件主要是通过和 BMC 通信来实现管理功能。

IPMI 提供了一组应用于带外管理和监视功能的功能，这些功能包括：

- 资产管理
- 故障监视
- 日志记录
- 恢复控制

关于服务器支持的 IPMI 命令说明，请参考《HDM IPMI 基础命令参考手册》。

1.2.4 SNMP 接口

SNMP（Simple Network Management Protocol，简单网络管理协议）广泛用于网络设备的远程管理和操作。它规定了在网络环境中对设备进行监视和管理的标准化管理框架、通信的公共语言、相应的安全和访问控制机制。

- HDM 提供了基于 SNMP 的编程接口，支持 SNMP Get/Set/Trap 操作，第三方管理软件通过调用 SNMP 接口可以方便地对服务器集成管理。SNMP 代理支持 V1/V2C/V3 版本。

- SNMP 代理提供接口查询系统健康状态、硬件状态、内存和 CPU 型号、告警上报配置、功率统计数据、资产信息、散热管理、固件版本信息、网络管理等。

2 用户须知

2.1 HDM使用准则

- 优先使用专用网口对 HDM 进行管理配置。
- HDM 不接入 Internet。
- 避免使用不安全的协议和端口。
- 定期审计操作日志。

2.2 缺省参数

HDM 部分功能提供的缺省参数如表 2-1 所示，方便用户首次操作。为了保证系统的安全性，建议在首次操作时修改缺省值，并定期更新。

表2-1 缺省参数

类型	缺省值
登录用户名	admin
登录密码	Password@_
专用网口IPv4地址	192.168.1.2/24
SNMP只读团体名	rocommstr
SNMP读写团体名	空
Trap团体名	public

2.3 用户类型

HDM 登录用户包括本地用户和域用户（LDAP 用户和 AD 用户）。

HDM 最多支持 16 个本地用户，本地用户适用于小型环境，如实验室和中小型企业。

域用户是通过域服务器侧管理，数量和权限不受 HDM 限制，此功能适用于用户数量较多的环境。

2.4 常见问题解答

2.4.1 故障诊断和定位

HDM 提供 BSOD（Blue Screen of Death，蓝屏死机）和系统崩溃前视频录制功能。当操作系统发生故障并重启后，可以在 BSOD 屏幕中查看故障发生时的蓝屏快照，还可以在录制视频界面查看操作系统在崩溃或重置前录制的视频，从而帮助技术人员快速定位故障原因。

2.4.2 登录 HDM Web 界面失败

登录 HDM Web 界面失败的可能原因以及相应解决方法如表 2-2 所示：

表2-2 原因及解决方法

原因分类	具体原因	处理方法
网络错误	HDM管理接口断开连接	请检查HDM管理接口的网线连接是否正常
	HDM管理IP地址错误	请确保您访问的IP地址与当前连接的HDM管理接口的IP地址一致
	本地PC和HDM管理接口的IP地址不在同一个网段内	请确保本地PC和HDM管理接口的IP地址位于同一网段内
	访问HDM时提示未获授权	请确保本地PC和HDM管理接口的IP地址位于同一网段内
未清除浏览器缓存	近期HDM升级了固件，但未清除浏览器缓存	请清除浏览器缓存后再次登录HDM
登录信息不正确	使用的用户名不存在	请确认您输入的用户名已经创建；如果您是首次登录HDM，请使用缺省用户名和密码
	密码不正确	请确保您输入的密码正确。需要注意的是，HDM用户的密码区分大小写
无法登录	修改默认用户名或密码，但是忘记用户名或密码	使用系统维护开关，关于系统维护开关的详细信息请参见服务器用户指南
	HDM 登录时提示会话超出限制	请长按UID按钮重启HDM以初始化HDM配置

3 登录 HDM Web

HDM 提供了 Web 界面，通过可视化、友好的界面来帮助用户完成服务器的管理。

3.1 机架服务器

3.1.1 环境准备

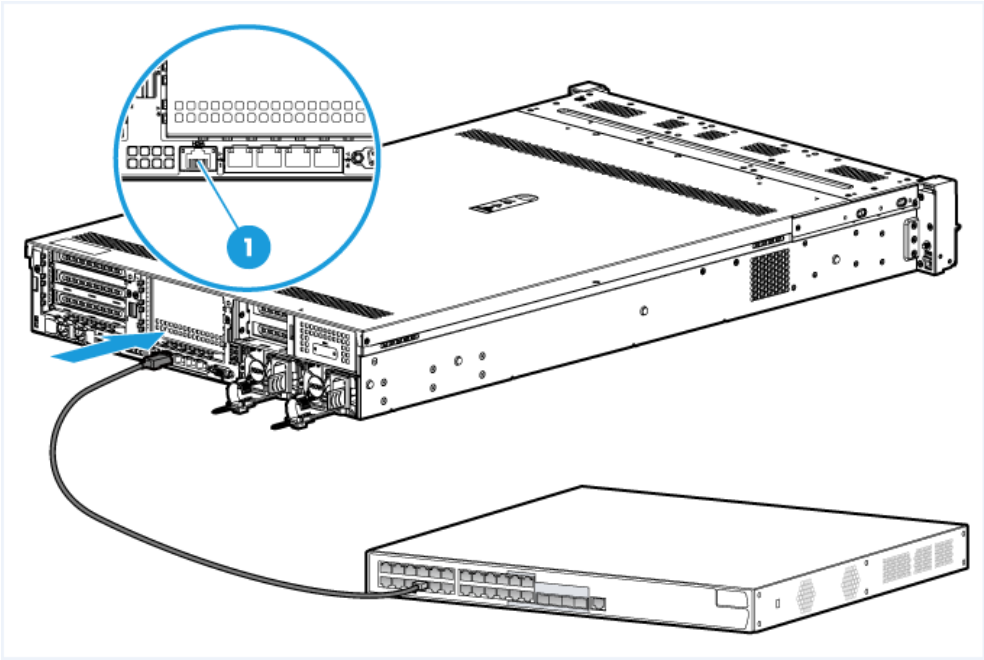
1. 将服务器连接到网络

登录 HDM 前，请先将 HDM 管理接口连接到网络，确保本地 PC 和服务器路由可达。

服务器支持以下两种 HDM 管理接口，详情请参考网络设置，您可以根据业务需求，选择合适的 HDM 管理接口。

- HDM 共享网口：可以同时处理 HDM 管理流量和服务器业务数据流量的网络接口。
- HDM 专用网口：专门用于处理 HDM 管理流量的网络接口，如图 3-1 所示。

图3-1 网络连接（以 R3800 G3 的 HDM 专用网口为例）

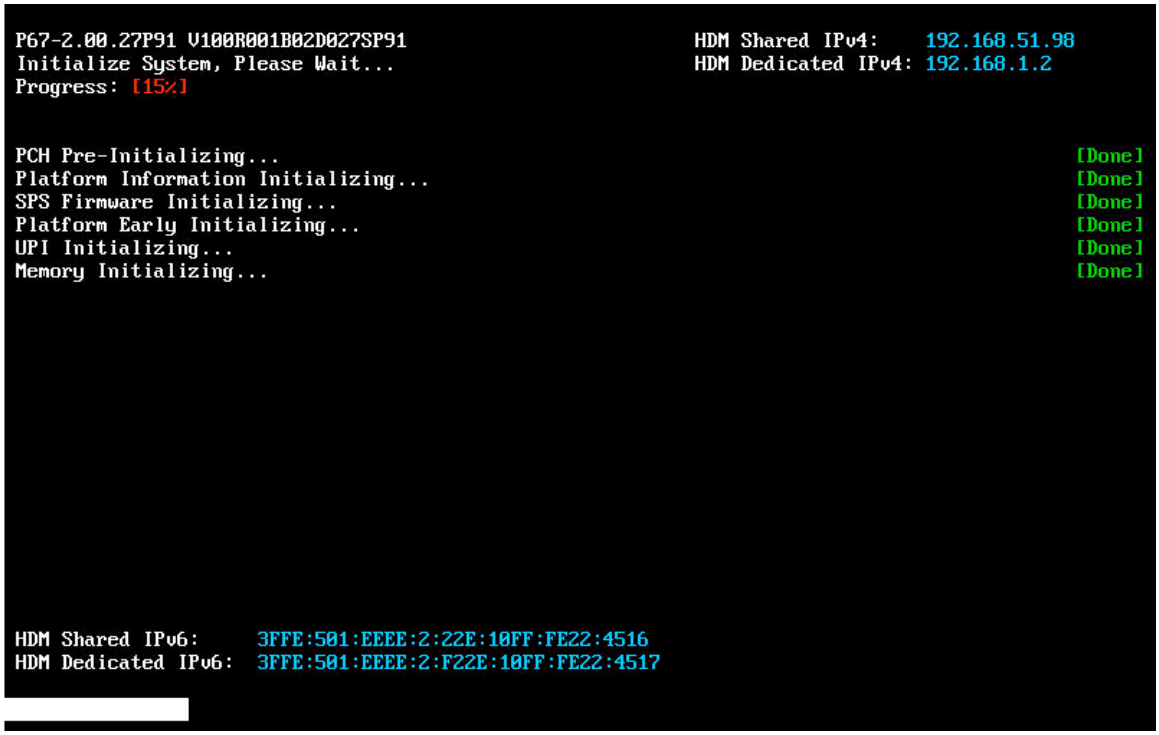


2. 获取 HDM 管理 IP 地址

登录 HDM 前，需要先获取 HDM 管理 IP 地址（HDM 专用网口/共享网口的 IP 地址）可以通过查看 POST 界面来获取 HDM 管理 IP 地址，如图 3-2 所示：

- HDM Shared IPv4：表示 HDM 共享网口的 IPv4 地址。
- HDM Dedicated IPv4：表示 HDM 专用网口的 IPv4 地址。
- HDM Shared IPv6：表示 HDM 共享网口的 IPv6 地址。
- HDM Dedicated IPv6：表示 HDM 专用网口的 IPv6 地址。

图3-2 HDM 管理 IP 地址（以 2.00.27 版本 BIOS 为例）



缺省 HDM 管理 IP 地址如表 3-1 所示，登录后可参考网络设置修改 HDM 管理 IP 地址。

表3-1 缺省 HDM 管理 IP 地址

接口	缺省 IP 地址
HDM共享网口	通过网络中的DHCP服务器分配IP地址
HDM专用网口	192.168.1.2/24

3. 访问 HDM

通过 Web 浏览器即可访问 HDM。HDM 支持的浏览器版本及客户端分辨率如表 3-2 所示。

表3-2 客户端配置需求

浏览器版本	分辨率
Google Chrome 48.0及以上	要求不低于1366*768，推荐设置为1600*900或更高
Mozilla Firefox 50.0及以上	
Internet Explorer 11及以上	

3.1.2 登录 HDM Web 界面

本指南以 IE 11.0 浏览器为例介绍登录 HDM Web 界面的操作步骤。

说明

- 默认情况下，系统超时时间为 30 分钟，如果您未在 Web 界面执行任何操作，系统将自动退出登录。
- 连续 5 次输入错误的密码后，系统将对此用户进行锁定，等待 5 分钟后，方可重新登录。
- 为保证系统的安全性，初次登录后，请及时修改缺省用户名和密码，并定期更新。

(1) 打开 IE 浏览器，在地址栏中输入 HDM 管理 IP 地址，弹出告警窗口，如图 3-3 所示。

图3-3 安全告警

(2) 单击“继续浏览此网站（不推荐）”，进入 HDM Web 登录界面，如图 3-4 所示。

图3-4 HDM Web 登录界面

(3) （可选）单击“Chinese”或“English”切换 HDM 界面语言。HDM 支持简体中文和英语两种界面语言。

(4) 在登录框中输入用户名和密码（包括本地用户和域用户）后，单击<登录>按钮，进入 HDM Web 界面首页。缺省用户名和密码如表 3-3 所示，登录后可参考用户访问设置修改用户名和密码。

表3-3 HDM 本地用户缺省用户名和密码

类型	缺省值
用户名	admin
密码	Password@_

3.2 刀片服务器和AE模块

说明

刀片服务器和 AE 模块的登录方法一致，本文以刀片服务器为例进行介绍。

3.2.1 登录 HDM 流程

用户可通过 OM Web 页面登录到刀片服务器的 HDM Web 页面，支持的方式包括：

- 方式一：免认证登录功能。
- 方式二：系统管理网络 HDM 地址链接。

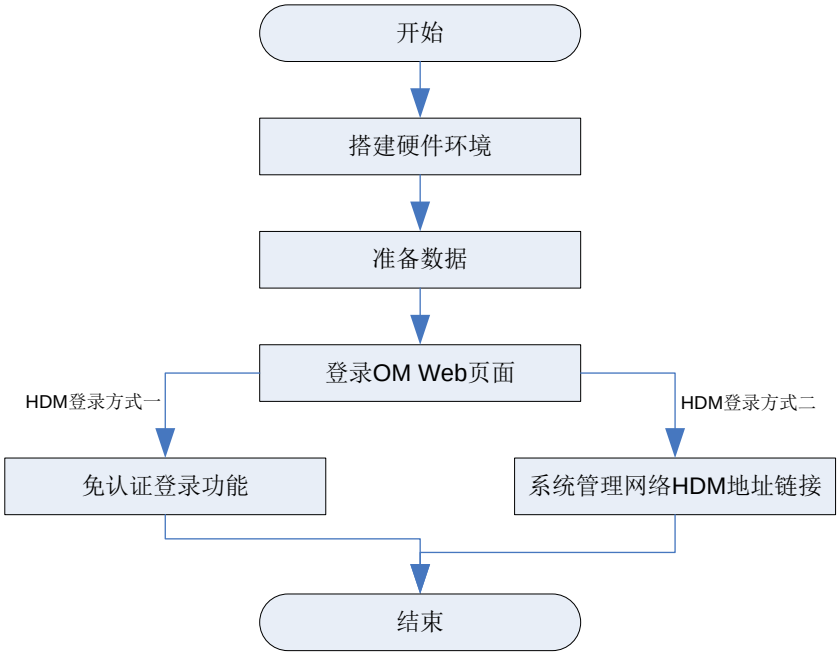
具体流程如图 3-5 所示。

说明

仅具有如下权限的用户才能使用 OM Web 页面的免认证登录功能和系统管理网络 HDM 地址链接。

- 具有 OM 管理员权限的用户。
- 具有待登录刀片服务器操作权限的操作员用户。

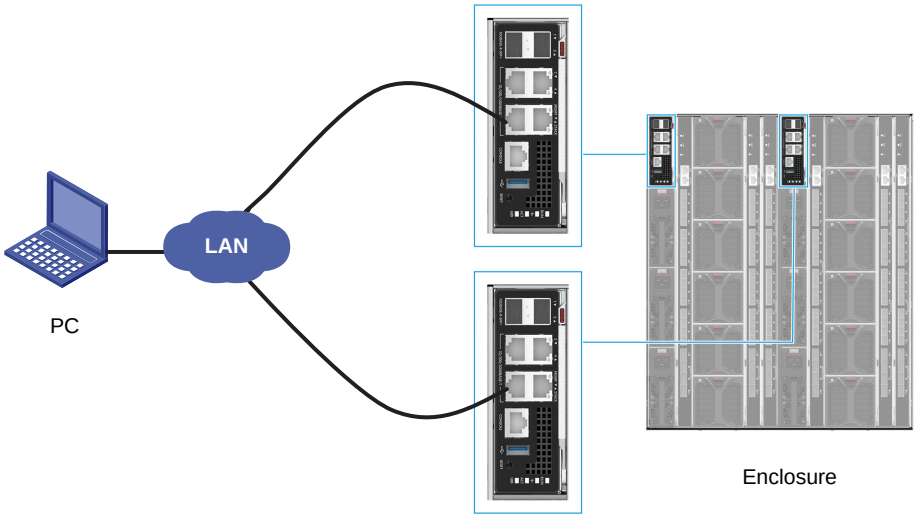
图3-5 登录 HDM 流程图



3.2.2 搭建硬件环境

本地 PC 通过局域网与主备 OM 模块的管理端口（MGMT）相连，如图 3-6 所示，管理端口（MGMT）具体位置参见 OM 模块前面板丝印。

图3-6 硬件环境搭建



3.2.3 准备数据

登录刀片服务器 HDM Web 页面前，用户需获取如下数据，具体如表 3-4 所示。

表3-4 缺省 OM 信息

数据类别	缺省信息
OM管理IP地址	192.168.100.100/24
OM登录信息	用户名：admin 密码：Password@_

3.2.4 客户端要求

本地 PC 作为客户端需要满足的浏览器及版本，如表 3-5 所示。

表3-5 客户端要求

浏览器版本	分辨率
Google Chrome 58.0及以上	推荐设置为1600*900或更高

说明

为了正常登录 OM Web 和 HDM Web，需确保客户端已分别配置了与 OM 管理 IP 地址及 HDM 管理 IP 地址相同网段的地址。用户可通过登录 OM Web 页面后查看刀片服务器 HDM 管理 IP 地址，具体方法参见 OM Web 联机帮助。

3.2.5 登录 OM Web 页面

(1) 打开客户端浏览器，输入 OM 管理 IP 地址（格式为 https://*OM_ip_address*），如图 3-7 所示，进入 OM 登录页面。输入用户名和密码，单击<登录>按钮，完成操作。

图3-7 登录 OM Web 页面

3.2.6 登录 HDM Web 页面

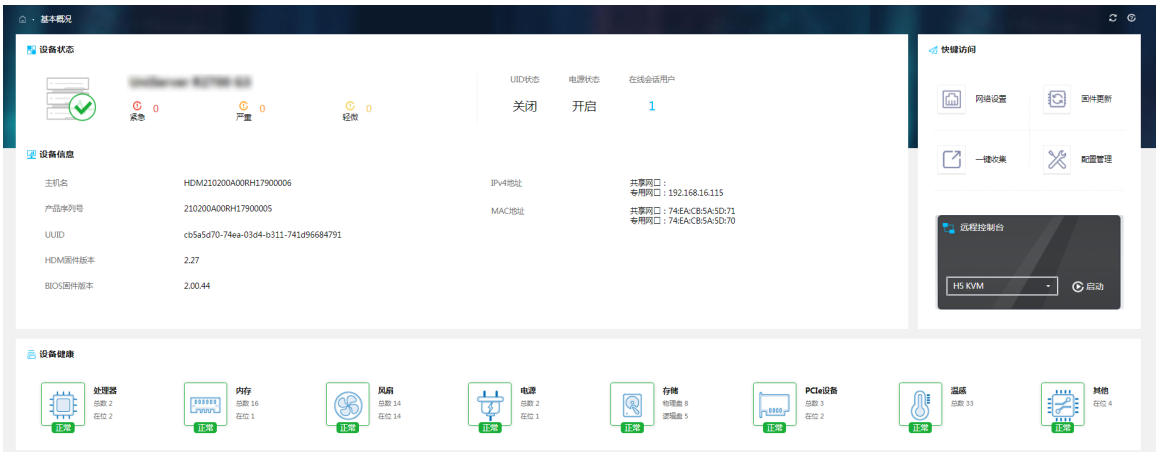
1. 方式一：通过免认证登录 HDM Web 页面

(1) 在 OM Web 首页，单击左树[计算节点管理]，在列表中选择目标刀片服务器，然后单击[远程控制台/远程控制台]，进入远程控制台页面。如图 3-8 所示，单击<免认证登录>按钮，页面跳转至 HDM Web 页面。需要注意的是，首次通过该方式登录时，需要在浏览器设置允许弹出式窗口且需信任该网页，具体步骤参见 3.2.7 常用操作。

图3-8 通过免认证登录 HDM Web 页面

(2) 如图 3-9 所示，进入 HDM Web 页面。

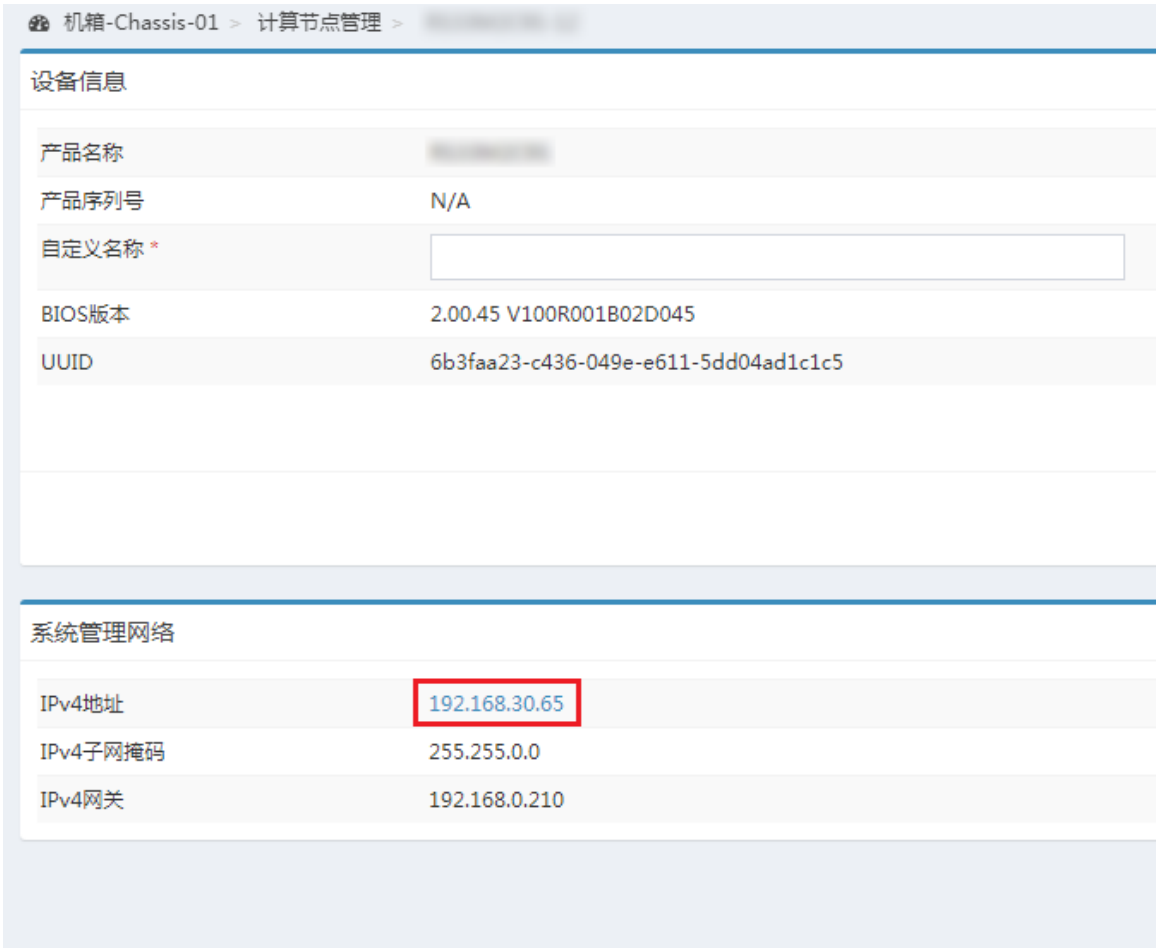
图3-9 HDM Web 页面



2. 方式二：通过系统管理网络 HDM 地址链接登录 HDM Web 页面

(1) 在 OM Web 首页，单击左树[计算节点管理]，在列表中选择目标刀片服务器。如图 3-10 所示，在系统管理网络页面下，单击红框中地址链接，页面跳转至 HDM Web 页面。需要注意的是，首次通过该方式登录时，需要在浏览器设置允许弹出式窗口且需信任该网页，具体步骤参见 3.2.7 常用操作。

图3-10 通过系统管理网络 HDM 地址链接登录 HDM Web 页面



(2) 如图 3-11 所示，进入 HDM Web 页面。

图3-11 HDM Web 页面

3.2.7 常用操作

首次通过 OM Web 页面登录 HDM Web 页面时，需要信任该网页，如图 3-12 所示，单击红框链接，浏览器将自动跳转至目的页面。

图3-12 信任该网页

4 查看设备信息

4.1 查看基本概况信息

本功能用于查看服务器的基本概况，包括产品型号、整机图片、设备状态、UID 灯状态、电源状态、在线会话、用户数量、告警信息和基本信息、健康状态和快捷访问入口。

说明

G3 系列服务器和 G5 系列服务器的首页略有差异，请以实际界面显示为准。

1. 操作步骤

(1) 单击[首页]菜单项，进入首页页面，G3 系列服务器首页如图 4-1 所示，G5 系列服务器首页如图 4-2 所示。

图4-1 整体概况（G3 系列服务器）

图4-2 整体概况（G5 系列服务器）

(2) 查看服务器的基本概况信息。

- 在功能区域 1，可以查看以下信息。
  - 设备状态：服务器整体的健康状态。
    - 正常：HDM 监测的服务器所有组件均正常运行。
    - 紧急、严重：HDM 监测的服务器部分组件发生故障。
  - UID 状态：服务器 UID 灯的状态。
    - 开启：服务器 UID 灯蓝色常亮，表示服务器被选中。
    - 闪烁：服务器 UID 灯蓝色闪烁，表示服务器正在进行固件更新，或者远程控制台被打开。
    - 关闭：服务器 UID 灯熄灭，表示服务器未被选中。
  - 电源状态：包括开启和关闭两种状态
  - 告警信息
    - 严重：表示对系统产生较大的影响，有可能中断部分系统的正常运行，导致业务中断。
    - 紧急：表示可能会使服务器下电，系统中断。需要马上采取相应的措施进行处理。
  - 设备信息
    - 主机名：设备的主机名称，设置主机名请参见网络设置。
    - 产品序列号：服务器的产品唯一编码。
    - UUID：服务器的通用唯一识别码（Universally Unique Identifier）。
    - HDM 固件版本：当前 HDM 固件版本，固件版本更新请参见固件更新。
    - BIOS 固件版本：当前 BIOS 固件版本，固件版本更新请参见固件更新。
    - 服务器名称：服务器的名称，缺省为空。仅刀片服务器和 AE 模块支持显示此参数。
    - IPv4 地址：用户访问 HDM 的网络接口的 IPv4 地址，更改网络配置请参见网络设置。
    - 网口模式为 Bonding 模式时，表示 HDM Bond0 网络接口。
    - 网口模式为正常模式或网口自适应模式时，表示 HDM 共享网络接口和 HDM 专用网络接口。
    - MAC 地址：HDM 网络接口的 MAC 地址。
- 在功能区域 2，可以查看当前服务器各组件的健康状态。

- 正常：组件运行正常。
- 严重：组件性能显著下降。
- 紧急：服务器可能会自动关机以防止组件被损坏。

各组件健康状态如表 4-1 所示：

表4-1 各组件健康状态

组件	状态	状态含义
处理器	正常	处理器正常
	严重	• CPU 产生过温告警 CPU 配置错误
	紧急	• CPU 产生极限温度告警 • CPU 发生不可恢复错误 • 主 CPU 不在位 • CPU 错误导致 BIOS 卡在 POST 阶段
内存	正常	内存正常
	严重	• 全部内存不在位或全部内存被隔离 • 内存发生不可恢复错误 • 内存插法错误或发生兼容性错误
	紧急	内存错误导致BIOS卡在POST阶段
风扇	正常	风扇冗余正常（非关键位置风扇异常）
	严重	风扇冗余异常（2个及以上关键位置风扇异常）
电源	正常	电源工作正常
	严重	电源发生严重错误
存储	正常	逻辑盘、物理盘和存储控制卡都处于正常状态
	严重	• 逻辑盘出现错误 • 物理盘出现严重错误 • 存储控制卡出现错误
PCIe设备	正常	PCIe设备（网卡、GPU、FC HBA、QAT卡或FPGA卡）处于正常状态
	严重	PCIe设备（网卡、GPU、FC HBA、QAT卡或FPGA卡）出现bus uncorrectable error、bus fatal error或PCIe err错误
温度	正常	组件温度未超过轻微阈值
	严重	组件温度达到严重阈值，未超过紧急阈值
	紧急	组件温度达到紧急阈值
其他	正常	所有部件处于正常状态

组件	状态	状态含义
	严重	部件出现严重错误
	紧急	部件出现紧急故障

(3) 在功能区域 3，可以查看当前 HDM 的快捷访问入口。启动远程控制台之前，请先选择 KVM 或 H5 KVM，再单击<启动>按钮。启动的 KVM 或 H5 KVM 模式以启动 KVM/H5 KVM 远程控制台章节的设置为准。

4.2 查看虚拟按钮

表4-2 虚拟按钮

功能	图标	含义
服务器UID灯		UID灯蓝色常亮，表示服务器被选中
		UID灯蓝色闪烁，表示服务器正在进行固件更新，或者远程控制台被打开
		UID灯熄灭，表示服务器未被选中
服务器电源		服务器电源处于开启状态，单击可以切换服务器电源状态 • 立即重启：强制重启服务器。此过程不会断开服务器的电源 • 强制关机：立即强制关闭服务器，此操作与长按服务器前面板上的电源按钮 5 秒以上效果相同。此过程中会断开服务器电源 • 正常关机：正常关闭服务器，即先关闭操作系统，再关闭电源 • 开机：正常启动服务器 • 关机并重新开机：立即强制重启服务器。此过程中会断开服务器电源
		服务器电源处于关闭状态，单击可以切换服务器电源状态
语言		单击可以切换界面语言为中文
		单击可以切换界面语言为英文
告警信息		单击可以查看告警信息详情
用户		• 当前登录用户信息，包括用户名、登录时间和所有在线用户信息 • 单击<查看详情>可以查看所有在线用户信息 • 单击<退出登录>可以退出登录
刷新		单击可以刷新界面
联机帮助		单击可以打开联机帮助

5 系统管理

5.1 查看系统信息

通过本功能可以查看服务器的产品信息、处理器、内存、PCIe 设备、传感器曲线图和其他信息。不同产品支持的配置不完全一样，具体差异请以实际界面显示为准。

注意

- 服务器关机状态时，处理器、内存和 PCIe 设备页签显示的是上次 POST 阶段得到的信息。
- 服务器 POST 完成时，处理器、内存和 PCIe 设备信息才会更新完成。即在 POST 过程中，处理器、内存和 PCIe 设备信息可能不正确或者显示不完整，请在 POST 完成后刷新页面查看相关正确信息。

5.1.1 产品信息

通过本功能可以查看服务器的产品信息和固件信息。

1. 操作步骤

(1) 单击[系统管理/系统信息]菜单项，进入系统信息页面。

(2) 单击“产品信息”页签，如图 5-1 所示，查看服务器的产品信息和固件信息。

图5-1 产品信息

2. 参数说明

- 产品名称：服务器的型号。

- 整机类型：服务器的整机类型。
- 产品部件号：服务器的产品部件号，和型号相对应，无法获取时显示 N/A。
- 产品序列号：服务器的产品唯一编码。
- 资产标签：服务器的固定资产号。
  - 输入长度为 1～48 个字符，仅支持字母、数字、空格和特殊字符 `~!@#$%^&*()_+-=[]{}|;':\",./<>?。
  - 可以为空。
- 主分区 HDM 版本：主分区 HDM 的固件版本号。
- 主分区 HDM 版本编译时间：主分区 HDM 的编译时间。
- 备分区 HDM 版本：备分区 HDM 的固件版本号。
- 备分区 HDM 版本编译时间：备分区 HDM 的编译时间。
- BIOS 版本：BIOS（Basic Input Output System，基本输入输出系统）的版本号。
- ME 版本：Intel ME（Intel Management Engine，英特尔管理引擎）的版本号，仅安装 Intel 处理器的服务器支持显示此参数。
- 主板 CPLD 版本：主板 CPLD（Complex Programmable Logical Device，复杂可编程逻辑器件）的版本号。
- STBCPLD 版本：主板 STBCPLD 的版本号，仅 R6700 G3 服务器型号支持显示此参数。
- iFIST 版本：当前 iFIST（integrated Fast Intelligent Scalable Toolkit，集成化的快速智能可扩展工具集）的版本，无法获取时显示“N/A”。

 说明

产品是否支持 iFIST，请以产品实际交付情况为准。

- PFR 版本：当前 PFRCPLD 固件的版本，仅 G5 系列服务器支持显示此参数。

5.1.2 处理器

本功能用于查看处理器的汇总信息、详细信息和故障信息。

1. 操作步骤

(1) 单击[系统管理/系统信息]菜单项，进入系统信息页面。

(2) 单击“处理器”页签，如图 5-2 所示，界面上将显示对应的处理器信息。

图5-2 处理器信息

2. 参数说明

- 状态：处理器的健康状态，如果处于异常状态，请查看故障描述确认原因。
- 型号：处理器的型号。
- PPIN：制造商分配的产品唯一编码，无法获取时显示 N/A。
- 主频：处理器的主频。
- 核心数：处理器实际包含的核心数。
- 线程数：处理器支持的最高线程数。
- 支持 64 位：是否支持 64 位处理器。
- 一级缓存：处理器支持的最大一级缓存容量。
- 二级缓存：处理器支持的最大二级缓存容量。
- 三级缓存：处理器支持的最大三级缓存容量。
- 故障描述：处理器出现故障时的告警日志信息。

5.1.3 内存

本功能用于查看内存的汇总信息、视图、详细信息和故障信息。

1. 操作步骤

(1) 单击[系统管理/系统信息]菜单项，进入系统信息页面。

(2) 单击“内存”页签，进入内存页面，如图 5-3 所示，界面上将显示对应的内存信息。

(3) （可选）如果服务器有多个计算模块，可以先选择计算模块，再查看对应的内存信息。

图5-3 内存信息

2. 参数说明

- 内存 RAS 配置
  - ECC：内存是否支持错误检查和纠正技术。
  - Mirror Mode：镜像模式，包括未开启、Full Mirror Mode 和 Partial Mirror Mode 三种状态。
    - Full Mirror Mode：完全镜像模式，设置系统中所有 1LM 内存被镜像。
    - Partial Mirror Mode：部分镜像模式，设置系统中部分 1LM 内存被镜像。
  - Memory RANK Sparing：内存 Rank 备用模式，使用通道中的一部分 Rank 作为该通道中其他 Rank（非备用 Rank）的备用 Rank。
  - SDDC：SDDC（DRAM Single Device Data Correction，单内存颗粒数据错误纠正功能），能够纠正一个 x4 或者 x8 内存颗粒上的多个 bit 错误。
  - ADDDC：ADDDC（Adaptive Double Device Data Correction Sparing，自适应双设备数据校正备用设置功能），可纠正两个内存颗粒上的数据错误。
  - Patrol Scrub：内存巡检设置，CPU 主动对内存的数据进行周期性的巡检并纠正可纠正的内存错误。
- 详情
  - 位置：内存对应的处理器编号、通道编号和插槽丝印编号。
  - 状态：内存在位时显示健康状态和认证状态，内存不在位时仅显示不在位，如果内存处于异常状态，请查看故障描述确认原因。
    - 已认证：内存经过厂商认证。
    - 普通：内存未经过厂商认证。
  - 容量：内存的容量。
  - 最大频率：内存的主频。
  - 标准：内存的规范标准。
  - 厂商：内存的制造商。

- 类型：内存的技术类型。
- Rank：内存的 Rank 数量。
- ECC 状态：内存是否支持错误检查和纠正技术。
- 厂家序列号：制造商分配的产品唯一编码，无法获取时显示 N/A。
- 厂家部件号：内存的部件号，无法获取时显示 N/A。
- 工作频率：内存的工作频率。
- 工作电压：内存的工作电压。
- 故障描述：内存出现故障时的告警日志信息。

3. 注意事项

- 内存视图中，绿色代表内存在位且状态正常，灰色代表内存不在位，灰色条纹代表内存被禁用，黄色、橙色和红色分别代表内存发生轻微、严重和紧急等级的错误。
- 当内存不在位时，对应的状态栏显示为“不在位”，其他栏目显示为“~”。
- 当 Channel 中有内存发生 Training 错误导致 Channel 被禁用时，Channel 中其他在位内存对应的状态栏显示为“禁用”。

5.1.4 PCIe 设备

通过本功能可以查看 PCIe 设备的相关信息。

说明

- 当服务器未插入 PCIe 设备或 PCIe 设备不支持信息获取时，则无法获取并显示 PCIe 设备信息。
- 如果无法获取当前功率，请先检查是否安装 GPU 驱动。
- 支持 MCTP（Management Component Transport Protocol，管理组件传输协议）功能的 PCIe 设备，需要先把固件升级到支持 MCTP 功能的版本，再开启 MCTP 功能。然后进入 BIOS Setup，选择 Advanced>Platform Configuration>Server ME Configuration 菜单，启用 Enable MCTP Proxy 选项，最后重启服务器。

1. 操作步骤

(1) 单击[系统管理/系统信息]菜单项，进入系统信息页面。

(2) 单击“PCIe 设备”页签，界面上将显示 PCIe 设备汇总信息，如图 5-4 所示。

(3) 选择 PCIe 设备类型，查看对应的设备信息。

图5-4 PCIe 设备信息

2. 参数说明

- 设备列表
  - 槽位号：关于插槽的具体位置，请参见服务器用户指南。
  - 状态：PCIe 设备的状态，包括正常和异常两种。
  - 产品名称：PCIe 设备的型号。
  - 设备厂商：PCIe 设备的制造商。
  - 芯片厂商：PCIe 设备芯片的制造商。
  - 序列号：制造商分配的产品唯一编码，无法获取时显示 N/A。
  - 部件号：PCIe 设备的部件号，和型号相对应，无法获取时显示 N/A。
  - 最大速率：PCIe 设备链路的最大速率。
  - 协商速率：自协商的 PCIe 链路速率。
  - 最高协议：PCIe 设备支持的最高协议等级。
  - 协商协议：自协商的 PCIe 协议等级。
  - 最大带宽：PCIe 槽位支持的最大带宽。
  - 设备最大带宽：PCIe 设备支持的最大带宽。
  - 协商带宽：自协商的 PCIe 链路宽度。
  - Mezz 槽位：PCIe 设备的 Mezz 槽位，仅刀片服务器支持显示 Mezz 槽位。
  - 所属 CPU：PCIe 设备所属的 CPU，此参数是否显示和服务器型号有关。
  - Riser 编号：PCIe 设备所在的 Riser 编号。
- 网卡
  - 产品名称：网卡的名称。
  - 接口：网卡端口的类型。
  - 设备厂商：网卡的制造商。
  - 芯片厂商：网卡芯片的制造商。
  - Mezz 槽位：网卡的 Mezz 槽位，仅刀片服务器支持显示 Mezz 槽位。
  - 固件版本：网卡的固件版本。
  - 健康状态：网卡的健康状态，如果处于异常状态，请查看事件日志确认原因。
  - 位置：网卡的物理位置。

- 序列号：制造商分配的产品唯一编码，无法获取时显示 N/A。
- 部件号：网卡的部件号，和型号相对应，无法获取时显示 N/A。
- 端口：网卡的物理端口。
- 状态：端口的状态，包括连接和断开两种状态。
- MAC 地址：网卡端口的 MAC 地址。
- PCIe 地址：网卡的 PCIe 地址，即 BDF（Bus：Device：Function）信息。
  - Bus：网卡的设备总线号。
  - Device：网卡的设备号。
  - Function：网卡的功能号。
- 协商速率：网卡端口的协商速率，无法获取时显示 N/A。
- 接口类型：网卡端口的介质类型，包括光口和电口两种类型。
- 连接状态：网卡端口的连接状态，包括连接和断开两种状态，无法获取时显示 N/A。
- LLDP：可以开启或关闭网络端口的 LLDP 功能，如果状态置灰不可设置，说明该端口不支持 LLDP 功能。开启或关闭 LLDP 功能后，需要重启服务器才能使配置生效。

- GPU
  - 产品名称：GPU 的型号。
  - 设备厂商：GPU 的制造商。
  - 固件版本：GPU 的固件版本。
  - 健康状态：GPU 的健康状态，如果处于异常状态，请查看事件日志确认原因。
  - 位置：GPU 所在的 PCIe 槽位号。关于插槽的具体位置，请参见服务器用户指南。
  - 厂家部件号：GPU 的部件号，和型号相对应，无法获取时显示 N/A。
  - 厂家序列号：制造商分配的产品唯一编码，无法获取时显示 N/A。
  - 功率：GPU 的当前功率。
- FC HBA
  - 产品名称：FC HBA 卡的名称。
  - 设备厂商：FC HBA 卡的制造商。
  - 固件版本：FC HBA 卡的固件版本。
  - 健康状态：FC HBA 卡的健康状态，如果处于异常状态，请查看事件日志确认原因。
  - 位置：FC HBA 卡的物理位置。
  - 端口：FC HBA 卡的网络端口号。
  - WWNN：网络端口的 WWNN（全球节点名称）。
  - WWPN：网络端口的 WWPN（全球端口名称）。
  - 连接状态：网络端口的连接状态，包括连接和断开两种状态，无法获取时显示 N/A。
  - 速率：网络端口的速率，无法获取时显示 N/A。
- QAT（Quick Assist Technology，硬件加速卡）
  - 产品名称：QAT 卡的名称。
  - 设备厂商：QAT 卡的制造商。
  - 芯片厂商：QAT 卡芯片的制造商。
  - 健康状态：QAT 卡的健康状态，如果处于异常状态，请查看事件日志确认原因。

- 位置：QAT 卡所在的 PCIe 槽位号。关于插槽的具体位置，请参见服务器用户指南。
- 厂家部件号：QAT 卡的部件号，和型号相对应，无法获取时显示 N/A。
- 厂家序列号：制造商分配的产品唯一编码，无法获取时显示 N/A。

- FPGA（Field Programmable Gate Array，现场可编程逻辑门阵列）
  - 产品名称：FPGA 卡的型号。
  - 设备厂商：FPGA 卡的制造商。
  - 健康状态：FPGA 卡的健康状态，如果处于异常状态，请查看事件日志确认原因。
  - 位置：FPGA 卡所在的 PCIe 槽位号。关于插槽的具体位置，请参见服务器用户指南。
  - 厂家部件号：FPGA 卡的部件号，和型号相对应，无法获取时显示 N/A。
  - 厂家序列号：制造商分配的产品唯一编码，无法获取时显示 N/A。
- 故障描述：PCIe 设备出现故障时的告警日志信息。

5.1.5 其他

通过本功能可以查看主板及其他部件的信息。不同产品支持的部件类型有差异，具体请以界面显示为准。

1. 操作步骤

(1) 单击[系统管理/系统信息]菜单项，选择其他页签，进入其他页面。

(2) 选择“部件”类型，如图 5-5 所示，查看对应的部件信息。

图5-5 其他

2. 参数说明

- 状态：部件的健康状态，如果处于异常状态，请查看事件日志确认原因。
- 制造商：部件的制造商。
- 产品部件号：部件的部件号，和型号相对应，无法获取时显示 N/A。

- 产品序列号：制造商分配的产品唯一编码，无法获取时显示 N/A。
- CPLD 版本号：CPLD 的固件版本号。
- STBCPLD 版本号：主板 STBCPLD 的版本号，仅 R6700 G3 服务器型号支持显示此参数。
- AUXCPLD 版本号：AUXCPLD 的固件版本号，此参数仅适用于部分刀片服务器。
- PCB 版本号：PCB（Printed Circuit Board，印制电路板）的固件版本号。
- 单板型号：硬盘背板扩展板的型号。
- 当前固件版本：硬盘背板扩展板的固件版本号。
- 当前配置文件：硬盘背板扩展板的配置文件版本号。
- Bootloader 版本：硬盘背板扩展板的 Bootloader 版本号。
- EEPROM 版本（固件使用）：硬盘背板扩展板的 EEPROM (Electrically erasable programmable read only memory，带电可擦可编程只读存储器)版本号。
- 故障描述：部件出现故障时的告警日志信息。

3. 注意事项

如果服务器未安装某个部件，则不显示该部件及相关的参数信息。

5.1.6 传感器曲线图

本功能可以查看服务器在网运行每个监控周期（5 分钟）的传感器信息和曲线图。

说明

R3830 G3 和 R4950 G5 仅支持显示平均曲线信息。

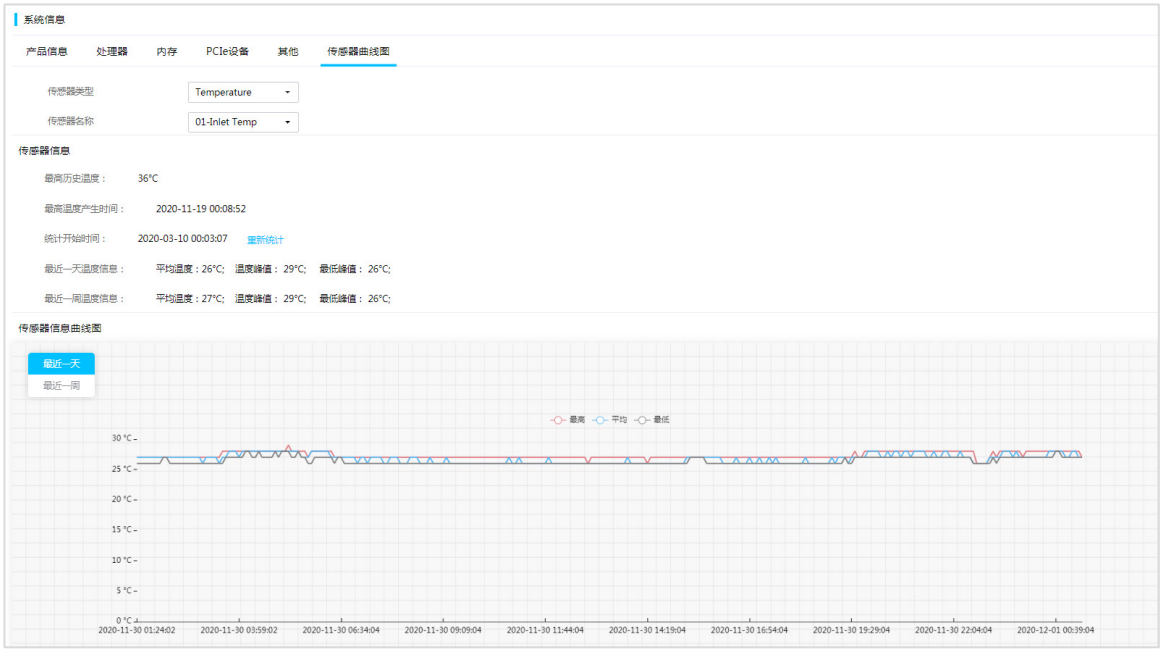
1. 操作步骤

(1) 单击[系统管理/系统信息]菜单项，选择“传感器曲线图”页签，进入传感器曲线图页面，如图 5-6 所示。

(2) 选择传感器类型和名称，查看对应的传感器信息和曲线图。

- （可选）单击<重新统计>按钮重新开始统计传感器信息。
- （可选）单击最近一天或最近一周按钮，选择曲线图的时间周期，将鼠标移到曲线上，可查看该监控周期内传感器信息的最高值、平均值和最低值。
- （可选）单击 最低、 平均或 最高，系统仅显示对应的传感器信息曲线。

图5-6 传感器曲线图



2. 注意事项

- 重启 HDM 期间，系统无法记录曲线数据。
- 如果恢复 HDM 配置，所有的曲线信息都会清除。
- 传感器信息曲线图只支持线性传感器。

5.2 存储管理

通过本功能可以执行以下操作：

- 查看存储控制卡、逻辑盘和物理盘的汇总信息、详细信息和故障信息。
- 通过指定存储控制卡设置物理盘状态、创建或删除逻辑盘。
  - 目前仅以下存储控制卡支持带外配置 RAID 功能，不同产品支持的卡类型不一样，具体支持情况请参见《服务器支持的操作系统列表》。
    - RAID-LSI-9361-8i(1G)-A1-X
    - RAID-LSI-9361-8i(2G)-1-X
    - RAID-LSI-9361-8i(2G)
    - RAID-LSI-9460-8i(2G)
    - RAID-LSI-9460-8i(4G)
    - RAID-LSI-9460-16i(4G)
    - HBA-LSI-9440-8i
    - RAID-L460-M4
    - RAID-P5408-Mf-8i-4GB
    - RAID-P5408-Ma-8i-4GB
    - HBA-H5408-Mf-8i

- RAID-LSI-9560-LP-16i-8GB
- RAID-LSI-9560-LP-8i-4GB

5.2.1 查看存储汇总信息

通过本功能可以查看存储汇总信息，包括存储系统的健康状态、存储控制卡数量、逻辑盘数量和物理盘数量及故障描述信息。

1. 操作步骤

(1) 单击[系统管理/存储管理]菜单项，进入存储管理页面，如图 5-7 所示。

(2) 查看存储汇总信息，包括存储系统的健康状态、存储控制卡数量、逻辑盘数量和物理盘数量及故障描述信息。

(3) 如果健康状态处于异常状态，请查看故障描述和事件日志确认原因。

图5-7 存储管理

5.2.2 查看存储控制卡信息

1. 操作步骤

(1) 单击[系统管理/存储管理]菜单项，进入存储管理页面。

(2) 选择逻辑视图，进入逻辑视图页面。

(3) 选择目标存储控制卡，查看相关信息，如图 5-8 所示。

图5-8 存储控制卡信息

2. 参数说明

- 型号：存储控制卡的型号。
- 厂商：存储控制卡的制造商。
- 固件版本：存储控制卡的固件版本。
- Package 版本：存储控制卡的软件包版本，仅部分 LSI 存储控制卡支持显示此参数。
- 配置版本：存储控制卡的配置版本。
- 序列号：制造商分配的产品唯一编码。
- WWN：存储控制卡的 SAS 地址。
- 模式：存储控制卡的模式。

- LSI 存储控制卡包括 RAID 和 JBOD 两种模式。
- PMC 存储控制卡包括 RAID、HBA、Mixed、Simple volume 和 Auto volume 五种模式。

- JBOD 状态：BIOS 下的 JBOD mode 选项的状态。
- 接口类型：存储控制卡支持的接口类型。
- 接口速率：存储控制卡的接口速率。
- 缓存容量：RAID 卡上内置的读写高速缓存的容量。
- Flash 卡：Flash 卡用于在系统意外掉电时，通过超级电容供电，备份读写高速缓存中的数据，以防止数据丢失。
  - PMC RAID 卡上的 Flash 卡的状态包括：“正常”、“异常”、“警告”和“不在位”。如果未安装 Flash 卡，状态显示为“不在位”；如果 Flash 卡状态显示为“异常”+“状态码”或“警告”+“状态码”，异常或警告的原因需要通过解析状态码来获取。以 0x500 的状态码为例，需要先把状态码 0x500 从十六进制转换为二进制的 0000 0101 0000 0000，最右端的数字对应 Bit0，最左端的数字对应 Bit15，其中 Bit8 和 Bit10 对应的数字为 1，说明异常的原因就是 Bit8 和 Bit10。具体原因见表 5-1。

表5-1 GB 状态表

Bit #	Bit 状态	状态描述
0	1	GB子系统正在初始化
1	1	GB子系统处于就绪状态
2	1	GB子系统正在执行学习周期，学习周期不会影响正常运行和数据保护功能
3	1	GB子系统故障
4	1	超级电容模块温度超过了最大温度阈值
5	1	超级电容模块温度超过了警告温度阈值
6	1	超级电容模块出现过压状态
7	1	超级电容模块超过了最大充电电流
8	1	成功通过GB子系统学习周期
9	1	GB子系统学习周期失败
10	1	超级电容模块故障
11	1	超级电容模块生命周期即将结束，建议更换
12	1	超级电容模块生命周期已经结束，需要更换
13	1	超级电容模块丢失一个电容器
14	N/A	保留
15	N/A	保留

  - LSI RAID 卡上 Flash 卡的状态包括：“正常”、“异常”和“不在位”。如果 Flash 卡未连接超级电容，状态显示为“不在位”。

- 超级电容：超级电容的状态，包括“不在位”、“充电中”、“充电完毕”、“致命”、“过温”、“校准失败”和“异常”状态。当超级电容处于“致命”、“过温”、“校准失败”或“异常”状态时，表示超级电容故障。
- 充电状态：超级电容当前可用的电量。
- 支持 RAID 级别：存储控制卡支持的 RAID 级别。PMC 存储控制卡支持的 RAID1(Triple)和 RAID10(Triple)的级别在 HDM Web 端显示为 RAID1(ADM)和 RAID10(ADM) 。

3. 注意事项

- 若存储控制卡不包含 Flash 卡和超级电容，则不显示相关参数。
- 请在服务器操作系统成功启动后，刷新存储页面获取存储信息。
- 不支持 RAID 功能的存储控制卡无逻辑视图。
- 不支持带外管理功能的 LSI HBA 卡无法获取对应的存储信息及温感信息。

5.2.3 逻辑盘管理

通过本功能可以查看已有的逻辑盘信息，并创建新的逻辑盘。

创建逻辑盘时，请注意以下事项：

- 创建或删除逻辑盘有短暂延时，如果立即刷新页面，逻辑盘及相关物理盘属性可能呈现为动作执行过程中的状态，请稍候几分钟再刷新页面查看配置生效情况。
- 如果硬盘部分容量已用来组建 RAID，本页面不支持使用剩余容量继续组建逻辑盘。
- 使用默认最大容量组 RAID 时与手动所组最大 RAID 容量存在偏差，因为容量、条带大小和 RAID 级别三者之间不是整除的关系，获取存储信息的接口反馈给前端的容量是有误差的。
- 每张存储控制卡通过 HDM 最多可以管理 64 个逻辑盘。

1. 操作步骤

(1) 单击[系统管理/存储管理]菜单项，进入存储管理页面。

(2) 选择逻辑视图，进入逻辑视图页面。

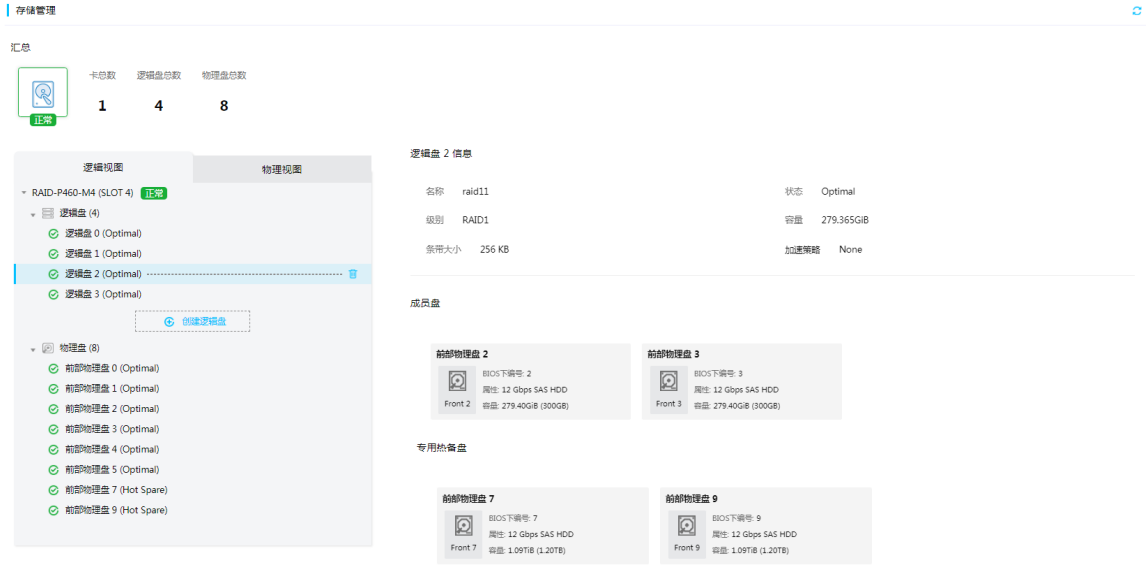
(3) 选择目标存储控制卡下的目标逻辑盘，查看相关信息，如图 5-9所示。

(4) （可选）单击  图标，可以删除逻辑盘。

(5) 单击<创建逻辑盘>按钮，进入创建逻辑盘页面。

(6) 输入或选择相应的参数，选择要组成逻辑盘的物理盘，单击<保存>按钮。

图5-9 逻辑盘信息



2. 参数说明

- 名称：逻辑盘名称，长度为 0～15 个字符，建议输入英文字符或数字，尽量避免使用特殊字符。如果是 PMC 存储控制卡，为必填项。
- 组个数：创建 Mixed 模式 RAID（RAID00、RAID10、RAID50 和 RAID 60）时的磁盘组个数。
  - LSI 存储控制卡：Span 个数。
  - PMC 存储控制卡：parity group 个数。
- 初始化类型：
  - No：不进行初始化。
  - Fast：快速初始化。
  - Full：完全初始化。
- 容量：逻辑盘的容量（最小容量为 100M），如果不填写该参数，则默认使用当前配置的最大容量。
- 专用热备盘：专用热备盘为具有冗余功能的特定逻辑盘提供热备份。
- 状态：逻辑盘的状态，包括：Optimal、Degraded、Rebuilding、Offline、Zeroing、Scrubbing、Suboptimal、Morphing、Copying。
  - Optimal：表示逻辑盘处于正常状态。
  - Degraded：表示组成 RAID 的部分成员盘出现异常，请及时更换故障硬盘。
  - Rebuilding：RAID 重建是在 RAID 降级后的一个恢复动作。
  - Offline：表示逻辑盘完全损坏，无法存取数据。
  - Zeroing：表示逻辑盘正处于格式化进程，格式化完成会删除逻辑盘上的所有数据。
  - Scrubbing：组建 RAID 5、RAID 6 等带校验位的逻辑盘时会有这个扫描状态，用于使逻辑盘内的数据保持连续。
  - Suboptimal：RAID 6 或 RAID 60 级别逻辑盘损坏一个成员盘时的状态为局部性能下降，损坏两个成员盘的状态为降级。

  - Morphing：将 RAID 中的数据迁移到其他的硬盘上或者将当前的 RAID 级别转换成其它的 RAID 级别。
  - Copying：热备盘替代 RAID 中的故障硬盘后，故障硬盘中的数据被重建到热备盘中。当 RAID 卡检测到故障硬盘被新硬盘替换后，数据从热备盘回拷到新硬盘，拷贝完成后，热备盘重新回到热备状态。回拷功能常用于阵列创建以及阵列修复的情形。
- 级别：RAID 级别。

  以下参数是否显示和存储控制卡的型号有关。
- 启动盘：当前逻辑盘是否为启动盘。
- 条带大小：每个物理盘上的数据条带的大小。
- 读策略：逻辑盘的读缓存策略。
  - No read ahead：关闭预读取缓存。
  - Read ahead：开启预读取缓存。
- 写策略：逻辑盘的写缓存策略。
  - Write through：当物理盘子系统接收到所有传输数据后，存储控制卡将向主机返回数据传输完成信号。
  - Write back：当存储控制卡没有安装超级电容时，存储控制卡将自动切换到 Write through 模式。
  - Always write back：当存储控制卡缓存收到所有的传输数据后，将向主机返回数据传输信号。
- IO 策略：逻辑盘的 Input/Output 策略。
  - Direct：所有读和写不需要经过 RAID 控制器缓存模块处理。
  - Cached：所有读和写均经过 RAID 控制器缓存模块处理。
- 物理盘缓存策略：逻辑盘下物理盘的缓存设置。
  - Unchanged：保持默认的缓存策略。
  - Enable：读写过程中数据经过物理盘写 Cache，使写性能提升，但当系统意外掉电时，如果没有保护机制，数据会丢失。
  - Disable：读写过程中数据不经过物理盘写 Cache，当系统意外掉电时，数据不会丢失。
- 访问策略：逻辑盘的访问策略。
  - Read/Write：可读可写。
  - Read only：只读访问。
  - Blocked：禁止访问。
- 加速策略：存储控制卡读写缓存策略。
  - Controller Cache：开启存储控制卡读写缓存。
  - None：关闭存储控制卡读写缓存。
  - IO Bypass：针对 SSD 硬盘，存储控制卡通过 IO Bypass 路径提高读写性能。

3. 注意事项

仅部分 LSI 存储控制卡处于 RAID 模式时，支持在 BIOS 下查看并设置 JBOD mode 选项。

5.2.4 物理盘管理

通过本功能可以查看所有物理盘的信息，并切换物理盘状态、设置热备盘和开启硬盘定位灯功能。

说明

- 仅空闲物理盘可设置为热备盘，逻辑盘的成员盘不能设置为热备盘。
- 热备盘必须是 SATA 硬盘或 SAS 硬盘，容量不小于逻辑盘成员盘的最小容量，且属性要和逻辑盘成员盘的属性一致。
- 除 RAID 0 外其他级别的逻辑盘都支持设置热备盘。
- 仅当 LSI 存储控制卡下的物理盘处于 Unconfigured Good 状态，PMC 存储控制卡下的物理盘处于 Ready 或 Hot Spare 状态时，才能设置为热备盘。

1. 操作步骤

(1) 单击[系统管理/存储管理]菜单项，进入存储管理页面。

(2) 选择目标物理盘，查看逻辑视图下的物理盘信息，如图 5-10 所示。

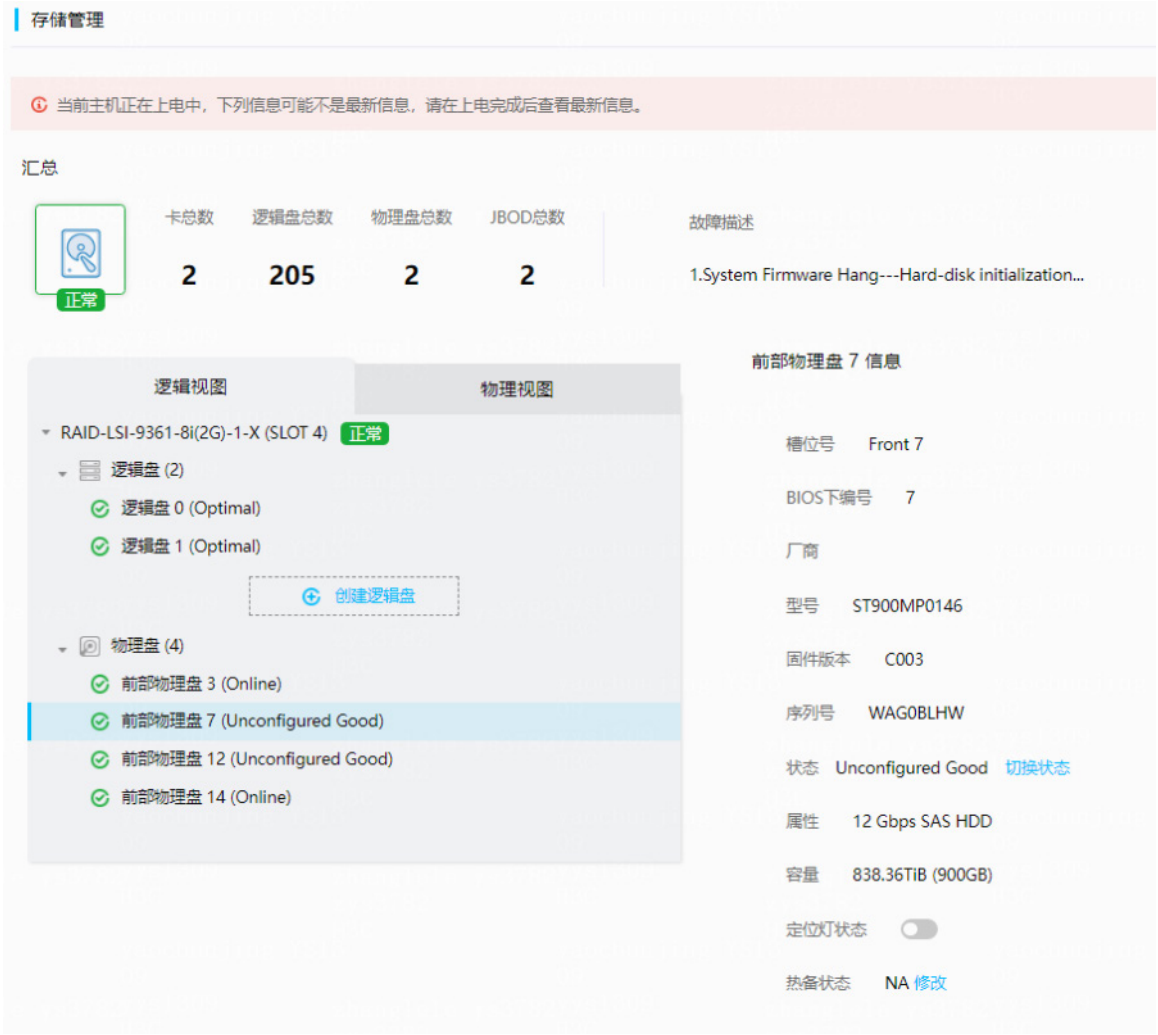
a. （可选）如果是 LSI 存储控制卡下的物理盘，单击<切换状态>按钮可以改变物理盘的状态。

b. （可选）单击<修改>按钮，设置物理盘的热备状态。

- LSI 存储控制卡下的物理盘支持全局热备和专属热备两种热备状态。设置专属热备盘时，可以选择多个目标逻辑盘。
- PMC 存储控制卡下的物理盘仅支持专属热备一种热备状态。设置专属热备盘时，只能选择一个目标逻辑盘。用户需要设置多次才能为专属热备盘设置多个目标逻辑盘。

c. （可选）部分物理盘支持开启硬盘定位灯功能。

图5-10 物理盘信息（逻辑视图）



(3) 查看所有物理盘的信息，如图 5-11 所示。

a. 选择物理视图，进入物理视图页面，可以查看所有物理盘信息。

b. （可选）部分物理盘支持单击<切换状态>按钮，改变物理盘的状态。

c. （可选）部分物理盘支持开启硬盘定位灯功能。

图5-11 物理盘信息（物理视图）

2. 参数说明

- Disk：
  - 槽位号：物理盘所在位置的丝印编号。
  - BIOS 下编号：物理盘在 BIOS 中查看到的硬盘编号。
  - 厂商：物理盘的制造商。
  - 型号：物理盘的型号。
  - 固件版本：物理盘的固件版本。
  - 厂商序列号：物理盘的产品序列号。
  - 状态：物理盘的状态。
    - 如果物理盘属于 LSI 存储控制卡，单击“切换状态”可以切换物理盘的状态。
    - Ready/Unconfigured Good：表示该物理盘已初始化，或该硬盘未进行任何配置，可用于创建 RAID 和设置热备盘。不同型号的存储控制卡显示的状态不一样。

- Unconfigured Bad：表示该物理盘处于异常状态，需要切换物理盘状态为 Unconfigured Good 后才能使用，如果不能切换成功，说明物理盘发生故障，需要更换物理盘。
- Unconfigured Good（Foreign）：表示物理盘存在残留的 RAID 信息，手动删除残留的 RAID 信息后，该物理盘会切换为 Unconfigured Good 状态。
- Unconfigured Bad（Foreign）：表示物理盘存在残留的 RAID 信息，手动删除残留的 RAID 信息后，该物理盘会切换为 Unconfigured Bad 状态。
- Optimal/Online：表示已使用该物理盘创建了 RAID，不同型号的存储控制卡显示的状态不一样。
- Offline：表示已禁用该物理盘。
- Rebuilding：表示该物理盘正用于 RAID 重建。
- Hot spare：表示该物理盘已为 RAID 提供热备。
- JBOD：表示该物理盘是直通盘，不组 RAID 仍可以在 OS 下使用。
- Failed：表示物理盘已损坏。
- Predict Fail/PFA：表示正在进行硬盘故障预分析。不同型号的存储控制卡显示的状态不一样。
- Raw：表示新接的硬盘或者未配置状态的硬盘进行 Uninitialize 操作后。
- Normal：表示该物理盘作为普通硬盘使用，不具有其他功能。
- Copyback：热备盘替代 RAID 中的故障硬盘后，故障硬盘中的数据被重建到热备盘中。当 RAID 卡检测到故障硬盘被新硬盘替换后，数据从热备盘回拷到新硬盘，拷贝完成后，热备盘重新回到热备状态。回拷功能常用于阵列创建以及阵列修复的情形。此状态仅适用于 LSI 存储控制卡下的物理盘。

o 重建进度：物理盘的重建进度。（此参数只有当物理盘处于 Rebuilding 状态时才会显示）

o 属性：物理盘的接口速率、接口类型和硬盘类型，部分存储控制卡无法获取硬盘的接口速率，仅显示硬盘的协商速率。

o 容量：物理盘的容量。

o SSD 剩余寿命：硬盘的剩余寿命百分比，仅当硬盘处于支持带外配置 RAID 的 LSI 存储控制卡（卡列表详见“查看存储汇总信息”章节）下，且硬盘型号满足以下要求时，此参数才会显示。

- 英特尔 SSD S4610 系列硬盘
- 英特尔 SSD S4600 系列硬盘
- 英特尔 SSD S4510 系列硬盘
- 英特尔 SSD S4500 系列硬盘
- 英特尔 SSD S3520 系列硬盘
- 美光 SSD 5200 系列硬盘
- 三星 SSD 硬盘

o 定位灯状态：可以查看并切换硬盘定位灯的状态，此参数是否显示和硬盘是否直接连接到硬盘背板有关。

o 热备状态：物理盘的热备状态，热备盘是用于替代目标逻辑盘故障成员盘的物理盘，用于承载故障盘的数据。不同类型存储控制卡下的物理盘支持的热备状态不一样。

  - 全局热备：热备盘为 LSI 存储控制卡下所有符合要求的逻辑盘所共有，当任一逻辑盘的成员盘发生故障时，全局热备盘均可自动替代该故障盘，用户更换故障盘后，热备盘中的数据会回拷至新的物理盘，全局热备盘会恢复热备状态。
  - 专属热备：热备盘为当前存储控制卡下多个逻辑盘所共有。当存储控制卡下的逻辑盘的成员盘发生故障时，专属热备盘会自动替代该故障盘，用户更换故障盘后，热备盘中的数据会回拷至新的物理盘，专属热备盘会恢复热备状态。
- NVMe：
  - 产品名称：NVMe 硬盘的型号。
  - 制造商：NVMe 硬盘的生产厂商。
  - 状态：
    - 正常：NVMe 硬盘状态正常。
    - 异常：NVMe 硬盘出现 bus uncorrectable error、bus fatal error 或 PCIe err 错误。
    - 备用空间低于阈值：NVMe 硬盘可用的备用空间不足。
    - 温度异常：NVMe 硬盘温度过高或过低。
    - 子系统降级：存储介质故障，出现硬盘子系统降级。
    - 只读模式：NVMe 硬盘处于只读模式。
    - 缓存模块故障：易失性存储备份设备故障。
  - 固件版本：NVMe 硬盘固件的版本，不支持则显示 N/A。
  - 序列号：制造商分配的硬盘序列号。
  - 硬盘编码：制造商分配的硬盘编码。
  - 接口类型：NVMe 硬盘的总线接口类型。
  - 容量：NVMe 硬盘的存储空间大小。
  - 物理槽位：NVMe 硬盘所在位置的丝印号。
  - PCIe 槽位：系统下 PCIe Slot 号。
  - 最大速率：NVMe 硬盘支持的最大速率。
  - 已使用寿命：评估 NVMe 硬盘已使用寿命的百分比，根据 NVMe 产品手册，该值可以大于 100。
  - 定位灯状态：可以查看并切换硬盘定位灯的状态，此参数是否显示和硬盘是否直接连接到硬盘背板有关。

3. 注意事项

- 如果存储控制卡和背板没有按规格安装，则物理盘各个编号可能显示不正确。
- 当硬盘状态显示为故障（Failed）时，该硬盘的相关信息（包括但不局限于容量、接口类型、连接速率等）均存在获取不准确的情况，仅作为参考。
- 无法对处于 Unconfigured Good（Foreign）、Unconfigured Bad（Foreign）或 Online 状态下的物理盘进行设置修改。

5.3 电源管理

5.3.1 设备上下电

电源控制实现了远程控制服务器电源状态的功能。通过本功能可以查看当前服务器的电源状态，并执行电源控制和是否屏蔽挂耳上电源按钮的操作。

注意

- 下列参数中，除“正常关机”外的其他关机方式可能会损坏用户的程序或者未保存的数据，请根据实际情况谨慎选择操作方式。
- 仅 G5 系列服务器（刀片服务器除外）支持屏蔽挂耳上电源按钮的功能，开启此功能后，挂耳上的电源按钮将会失效，无法控制服务器电源。

1. 操作步骤

(1) 单击[系统管理/电源管理]菜单项，进入电源管理页面，如图 5-12 所示。

(2) “目前主机状态”后的字样即为当前服务器电源的状态。

(3) 单击虚拟电源按钮，完成操作。

(4) 选择是否开启“屏蔽挂耳上电源按钮的功能”。

图5-12 电源管理

2. 参数说明

- 立即重启：强制重启服务器。此过程不会断开服务器的电源。
- 强制关机：立即强制关闭服务器，此操作与长按服务器前面板上的电源按钮 5 秒以上效果相同。此过程中会断开服务器电源。
- 正常关机：正常关闭服务器，即先关闭操作系统，再关闭电源。此过程中会断开服务器电源。
- 开机：正常启动服务器。
- 关机并重新开机：立即强制重启服务器。此过程中会断开服务器电源。

5.3.2 查看电源信息

通过本功能可以查看电源的汇总信息和详情。

说明

刀片服务器和 AE 模块不支持查看电源信息。

1. 操作步骤

(1) 单击[系统管理/电源管理]菜单项，选择“电源信息”页签，进入电源信息页面。

(2) 查看电源汇总信息和详情，如图 5-13 所示。

(3) （可选）单击输入电压栏的图标，可以查看输入电压历史曲线图，如图 5-14 所示。

图5-13 电源信息

图5-14 输入电压历史曲线图

2. 参数说明

- 主电源模式：电源模块按需求输出功率。
- 备用电源模式：电源模块处于备份状态，低功率输出。
- 输入功率：电源的输入功率。
- 当前状态：电源的健康状态，如果处于异常状态，请查看事件日志确认原因。
- 槽位号：电源所在的槽位号。
- 厂商：电源的制造商。
- 型号：电源的型号。
- 序列号：制造商分配的产品唯一编码。
- 固件版本：电源固件 PSU 的版本信息。
- 额定功率：电源的额定功率。
- 输入电压：电源的输入电压。
- 输出电压：电源的输出电压。
- 电源输入模式：
  - No input：未接入电源。
  - AC：交流电源输入。
  - HVDC：高压直流电源输入，电压范围是 192V～400V。
  - LVDC：低压直流电源输入，电压范围是 12V～72V。
- 电源供电类型：电源模块支持的电源输入模式，包括 AC、AC or DC、DC 和 unknown 几种类型。
  - AC：电源模块仅支持交流输入模式。
  - AC or DC：电源模块支持交流输入和直流输入两种模式。
  - DC：电源模块仅支持直流输入模式。
  - unknown：无法获取电源模块的信息。

5.3.3 设置电源工作模式

通过本功能可以设置服务器电源的工作模式，包括主备模式和负载分担模式。

- 主备模式：包括至少 1 个主电源，至少 1 个备用电源。当主电源发生故障，备用电源会自动切换为主电源，以保证电源的可靠性。当主电源实际功率超过主电源额定功率（主电源最大功率）的 62%时，备用电源将自动切换为主电源，实际功率下降后，不会切换回主备模式。
- 负载均衡：所有在位电源均处于主电源模式，实现负载分担。

说明

- 刀片服务器和 AE 模块不支持设置电源工作模式。
- 请在服务器成功进入系统启动项后，再设置电源工作模式，否则可能会设置失败。

1. 操作步骤

(1) 单击[系统管理/电源管理]菜单项，选择“电源信息”页签，进入电源信息页面，如图 5-13 所示。

(2) 单击<电源设置>按钮，跳出对话框，如图 5-15 所示。

(3) 设置电源工作模式，如果选择主备模式，还需要设置主电源。

(4) 单击<确定>按钮，完成操作。

图5-15 电源设置

2. 注意事项

如果同时设置多个电源的工作模式失败，HDM 只会记录最小槽位号的电源的操作日志。

5.3.4 设置 AC 恢复配置

通过本功能可以设置服务器通电后系统的启动策略。

说明

刀片服务器和 AE 模块不支持设置 AC 恢复配置。

1. 操作步骤

(1) 单击[系统管理/电源管理]菜单项，选择“电源信息”页签，进入电源信息页面，如图 5-13 所示。

(2) 单击<AC 恢复配置>按钮，跳出对话框，如图 5-16 所示。

(3) 设置自动开机电源状态和开机延迟时间。

(4) 单击<确定>按钮，完成操作。

图5-16 AC 恢复配置

2. 参数说明

- 自动开机电源状态：
  - 总是开启：通电后，服务器系统会自动启动。
  - 总是关闭：通电后，服务器系统保持关闭状态。
  - 上一次电源状态：通电后，服务器系统会恢复到上次断电前的状态。服务器缺省处于此模式。
- 开机延迟设置：设置开机延迟时间，如果选择“随机”，可以自定义延迟时间范围。

5.3.5 查看电源功率信息

通过本功能可以查看服务器的功率汇总信息、功率信息和最近一周或一天的历史功率信息。

说明

- R3830 G3、R3630 G5、R4950 G5 和 R5500 G5 仅支持显示平均曲线信息。
- 刀片服务器和 AE 模块仅支持查看电源汇总信息和功率封顶信息。

1. 操作步骤

(1) 单击[系统管理/电源管理]菜单项，选择“功率信息”页签，进入功率信息页面。

(2) 查看功率汇总信息、总功率告警信息、主板功率封顶信息、GPU 功率封顶信息和历史功率信息，如图 5-17 所示。

(3) （可选）单击<重新统计>按钮重新开始统计最大功率信息，如图 5-18 所示。

(4) （可选）选择时间区间，单击<确定>按钮，可以查看指定时间段内的功率信息，如图 5-18 所示。

(5) （可选）单击 最低、 平均或 最高，仅显示对应的历史功率曲线。

图5-17 电源功率信息

图5-18 历史功率

5.3.6 设置总功率告警阈值

通过本功能可以设置服务器总功率告警阈值，当总功率超过告警阈值时，HDM 会触发一条事件日志提醒用户。

说明

刀片服务器和 AE 模块不支持设置总功率告警阈值。

1. 操作步骤

(1) 单击[系统管理/电源管理]菜单项，选择“功率信息”页签，进入功率信息页面。

(2) 单击功率信息栏的按钮，跳出对话框。

(3) 选择开启总功率配置的告警应用，输入总功率告警阈值，如图 5-19 所示。

图5-19 总功率告警设置

(4) 单击<确定>按钮，完成操作。

5.3.7 设置功率封顶信息

通过功率封顶功能，可以实现对服务器 CPU 等组件运行功率的限制。

说明

- 刀片服务器和 AE 模块不支持设置主板功率封顶信息。
- 仅 R5500 G5 服务器支持 GPU 功率封顶功能。

当电源功率超过设置的功率封顶值时，服务器会自动降低 CPU 或 GPU 等组件的运行频率，以降低 CPU 的运行功率。

功率封顶值失效指的是如果服务器的电源功率超过功率封顶值，并在连续 30 秒内无法降低到功率封顶值以下，则功率封顶失效。功率封顶失效时，可以设置服务器自动关机功能或服务器继续以实际功率运行。

注意

- 请合理设置功率封顶值，如果封顶功率过低，系统性能和业务会受到影响。
- 为避免对正常业务造成影响，请谨慎设置封顶失效后的关机操作。
- 设置 GPU 功率封顶信息前，请确保操作系统侧已安装 GPU 驱动，否则会导致设置无法生效。

1. 操作步骤

(1) 单击[系统管理/电源管理]菜单项，选择“功率信息”页签，进入功率信息页面。

(2) 单击主板功率/GPU 功率栏的按钮，跳出对话框。

(3) 选择开启功率封顶功能，输入功率封顶值，如图 5-20 所示。

(4) 并根据实际需求设置功率封顶失效是否关机。

(5) 单击<确定>按钮，完成操作。

图5-20 功率配置

2. 参数说明

- 功率封顶值：开启功率封顶功能后，当服务器的电源功率达到功率封顶值时，服务器会采取自动降低对应组件的运行频率等措施，以降低电源功耗。
- 功率封顶失效是否关机：如果服务器的电源功率超过功率封顶值，并在连续 30 秒内无法降低到功率封顶值以下，则功率封顶失效。若选择“是”则服务器会在功率封顶失效后强制关机；若选择“否”，则服务器会在功率封顶失效后继续运行。

3. 注意事项

- 请合理设置功率封顶值，如果功率封顶值过小，功率封顶值可能失效。
- 重启 HDM 以及服务器关机期间，系统无法记录历史功率信息。
- 如果恢复 HDM 配置，所有的历史功率信息都会清除。

5.3.8 节能设置

HDM 支持通过配置电源性能模式实现降低服务器能耗。

说明

R3830 G3、E3200 G3、B5700 G3、B5800 G3、B7800 G3、R3630 G5、R3830 G5、R4950 G5、R5500 G5 AMD、B5700 G5 和 AE100 不支持节能设置。

1. 操作步骤

说明

配置电源性能模式前，请先进入 BIOS 界面，选择 Socket Configuration>Advanced Power Management Configuration 菜单，执行以下操作：

- 进入 CPU P State Control 界面，将 EIST (P-States)选项设置成 Enabled。
- 进入 CPU Thermal Management>CPU T State Control 界面，将 Software Controlled T-States 选项设置成 Enabled，部分服务器还需要开启并选择 T-State Throttle Level 的节流等级。
- 进入 Hardware PM State Control 界面，将 Hardware P-States 选项设置成 Disabled。
- 进入 CPU Advanced PM Tuning>Energy Perf BIAS 界面，将 Power Performance Tuning 设置为 BIOS Controls EPB。

(1) 单击[系统管理/电源管理]菜单项，选择“节能设置”页签，进入节能设置页面，如图 5-21 所示。

(2) 单击<高级设置>按钮，弹出对话框。

(3) 设置 P-state 和 T-state 的调节等级。

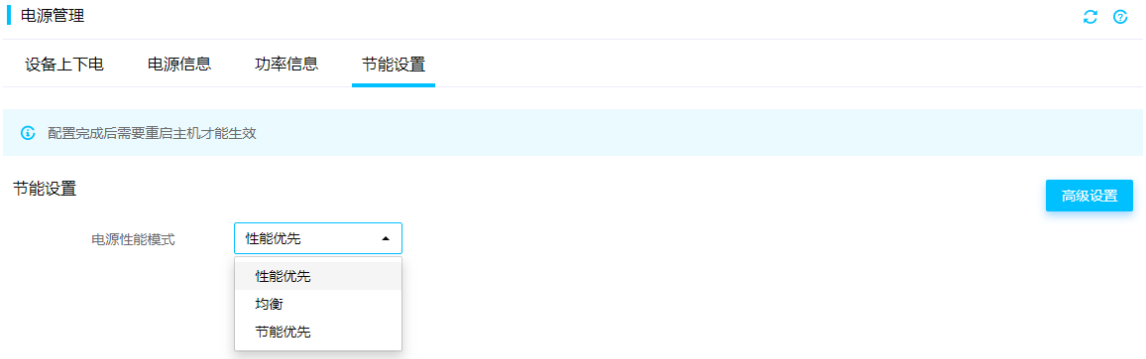
(4) 单击<确定>按钮，关闭对话框。

(5) 选择电源性能模式。

(6) 单击<保存>按钮，完成操作。

(7) 重启服务器使配置生效。

图5-21 节能设置



2. 参数说明

- 性能优先：处理器以性能优先运行。
- 均衡：处理器以性能和节能的均衡模式运行。
- 节能优先：根据处理器利用率自动更改处理器的速度和能耗。该选项可以降低总体能耗，而对性能的影响很小或没有影响。
- P-state：CPU 的最高工作频率。
  - 设置为 P0 状态时，CPU 最高频率为当前支持的最大值。
  - 设置为 P1、P2……状态时，CPU 最高工作频率依次递减，功耗和性能也随之递减。
- T-state：CPU 的空闲工作时间占空比。
  - 设置为 T0 状态时，CPU 工作时间占空比为当前支持的最大值。
  - 设置为 T1、T2……状态时，CPU 工作时间占空比依次递减，功耗和性能也随之递减。

3. 注意事项

不同 CPU 支持的 P-state 和 T-state 的节能策略不同，可调节等级也不同。

5.4 散热管理

5.4.1 温度海洋

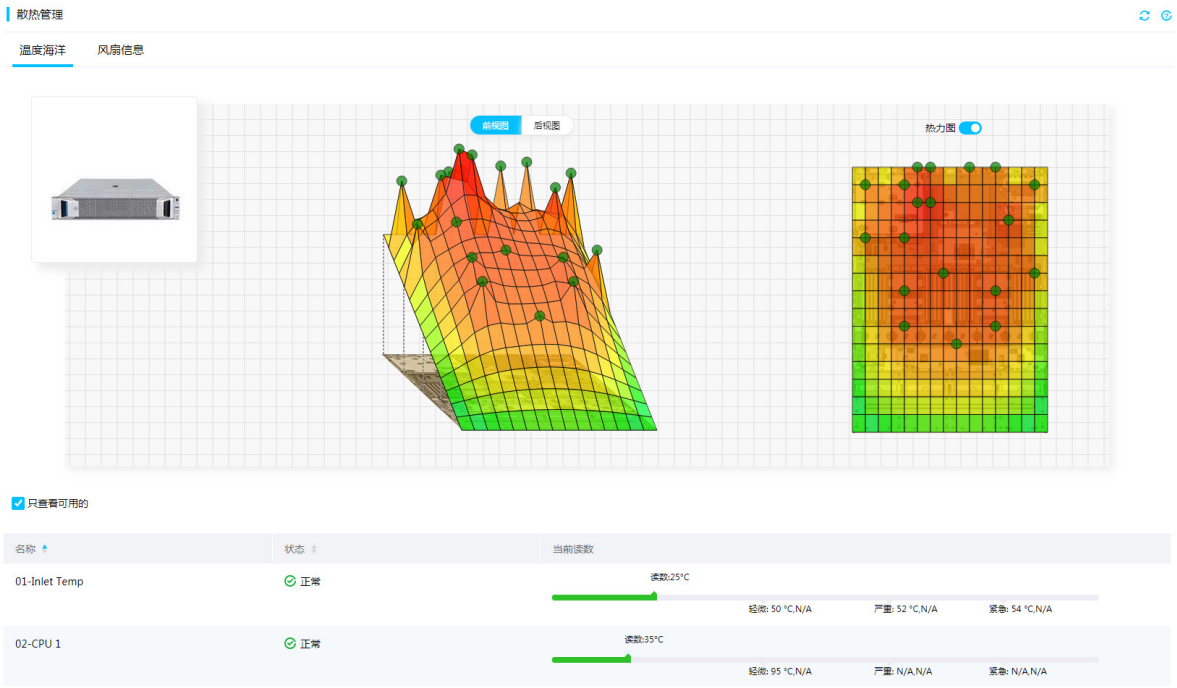
通过本功能可以查看服务器温度海洋及各组件的温度信息。

1. 操作步骤

(1) 单击[系统管理/散热管理]菜单项，进入散热管理页面，如图 5-22 所示。

(2) 查看温度海洋图、热力图和传感器信息表。

图5-22 温度海洋



2. 参数说明

- 温度海洋：显示服务器机箱中各组件温度传感器的分布图及数值。
  - 温度海洋上的圆圈与表中可用的传感器相对应，将鼠标移到温度海洋上的圆圈上可查看传感器名称、状态、温度读数和阈值。
  - 温度海洋的颜色从绿色逐渐变为红色。绿色表示温度为 0°C，红色表示温度较高。
- 热力图：显示服务器中各组件温度传感器的分布图及数值。
  - 热力图上的圆圈与表中可用的传感器相对应，将鼠标移到圆圈上可查看传感器名称、状态、温度读数和阈值。
  - 热力图的颜色从绿色逐渐变为红色。绿色表示温度为 0°C，红色表示温度较高。
- 状态：各组件的温度状态。
  - 正常：表示该组件温度数值处于轻微下限阈值（不含）和轻微上限阈值（不含）之间。
  - 轻微：表示该组件温度数值在轻微下限阈值（含）和严重下限阈值（不含）之间或者该组件温度数值在轻微上限阈值（含）和严重上限阈值（不含）之间。
  - 严重：表示该组件温度数值在严重下限阈值（含）和紧急下限阈值（不含）之间或者该组件温度数值在严重上限阈值（含）和紧急上限阈值（不含）之间。
  - 紧急：表示该组件温度数值小于紧急下限阈值（含）或者大于紧急上限阈值（含）。
  - 不可用：表示没有安装该组件或者温度数值无法被读取。
- 当前读数：该组件当前的温度。如果温度数值无法被读取，则当前读数显示“N/A”。
- 阈值：组件温度的门限值。
  - 紧急：包括紧急上限阈值和紧急下限阈值。如果组件温度超过上限紧急阈值或低于下限紧急阈值，服务器可能会自动关闭系统防止组件被损坏。

- 严重：包括严重上限阈值和严重下限阈值。如果组件温度超过上限严重阈值或低于下限严重阈值，服务器运行性能会显著下降。
- 轻微：包括轻微上限阈值和轻微下限阈值。服务器正常运行时，组件温度在下限轻微阈值和上限轻微阈值之间。如果组件温度超过上限轻微阈值或低于下限轻微阈值，会导致服务器运行性能下降。

3. 注意事项

当传感器读数为负数时，温度海洋和热力图暂不显示该传感器信息。

5.4.2 风扇信息

通过本功能可以查看风扇的汇总信息、详细信息和故障信息，结合用户对散热、噪声以及功耗的需求，设置风扇调速模式。

说明

刀片服务器和 AE 模块不支持查看和设置风扇信息。

1. 操作步骤

(1) 单击[系统管理/散热管理]菜单项，选择“风扇信息”页签，进入风扇信息页面，如图 5-23 所示。

(2) 查看风扇信息。

(3) 单击<风扇配置>按钮，弹出对话框，如图 5-24 所示。

(4) 选择风扇调速模式或自定义模式。

(5) 单击<确定>按钮，完成操作。

图5-23 风扇信息

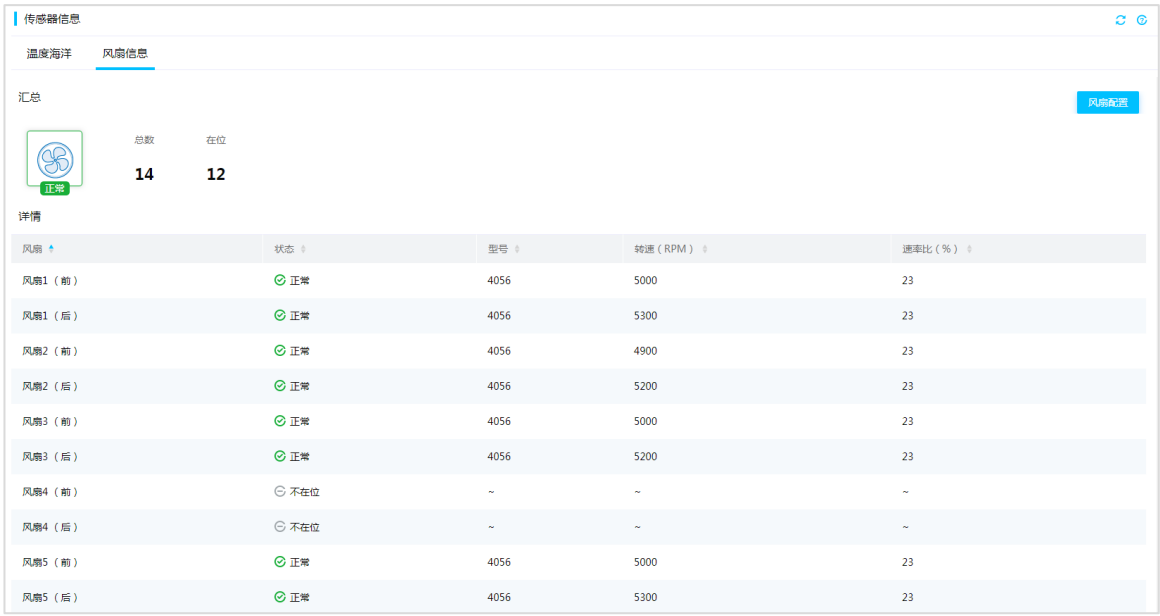
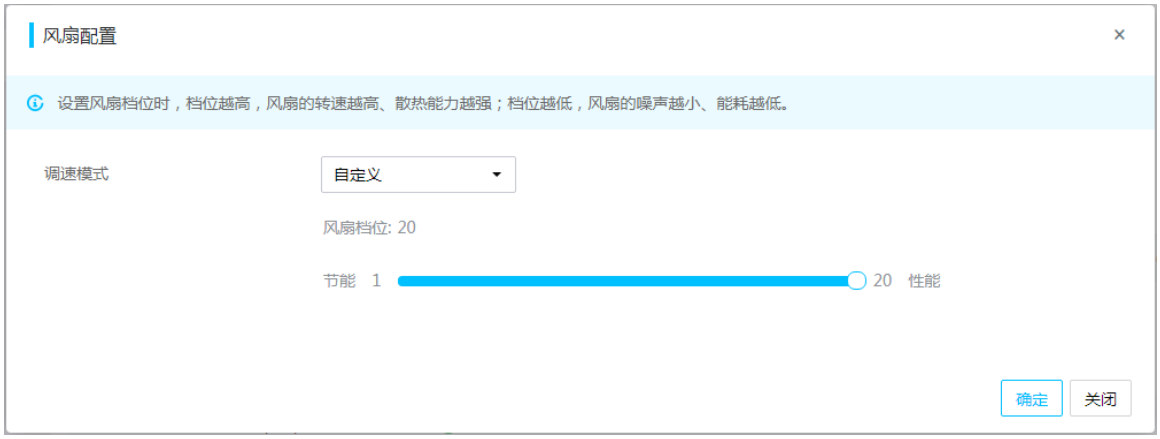


图5-24 风扇配置



2. 参数说明

- 状态：风扇的健康状态和在位状态，如果处于异常状态，请查看故障描述和事件日志确认原因。
- 型号：风扇型号。
- 转速（RPM）：当前的实际转速。
- 速率比（%）：实际转速/满转速。
- 故障描述：风扇发生故障时产生的告警日志信息。
- 静音模式：风扇调速模式为静音模式时，在确保服务器正常散热的前提下，风扇以最低转速运转，此时噪音最小。该模式适用于对噪音要求比较高的场景。
- 均衡模式：风扇调速模式为均衡模式时，风扇会加快转速，此时的噪音和散热能力介于静音模式和强劲模式之间。该模式适用于对噪音和散热能力有平衡要求的场景。
- 强劲模式：风扇调速模式为强劲模式时，风扇以当前条件下的最高转速运转，此时噪音最大，但风扇的散热能力最强，能有效降低 CPU 等关键组件的温度。该模式适用于对服务器散热要求比较高的场景，如业务繁忙导致 CPU 等关键组件负载较大、工作环境温度变化频繁。
- 自定义：设置风扇模式时，档位越高，风扇的转速越高、散热能力越强，噪声也越大；档位越低，风扇的转速越低、噪声越小、功耗越低。

5.5 系统资源监控

5.5.1 系统资源

本功能可以设置 CPU、内存、磁盘、网络带宽的占用率告警阈值，并查看对应的资源使用信息。当资源占用率超过告警阈值时，系统会产生告警；恢复正常时，系统会解除告警。告警日志和解除告警日志都可以在事件日志中查看。

说明

- 网络带宽占用率告警阈值在 HDM Web 不可配置，需要通过 IPMI 命令设置，具体操作请联系技术支持。
- 使用本功能时需要在操作系统侧安装并运行 FIST SMS，具体操作请联系技术支持。

1. 操作步骤

(1) 单击[系统管理/系统资源监控]菜单项，进入系统资源页面。

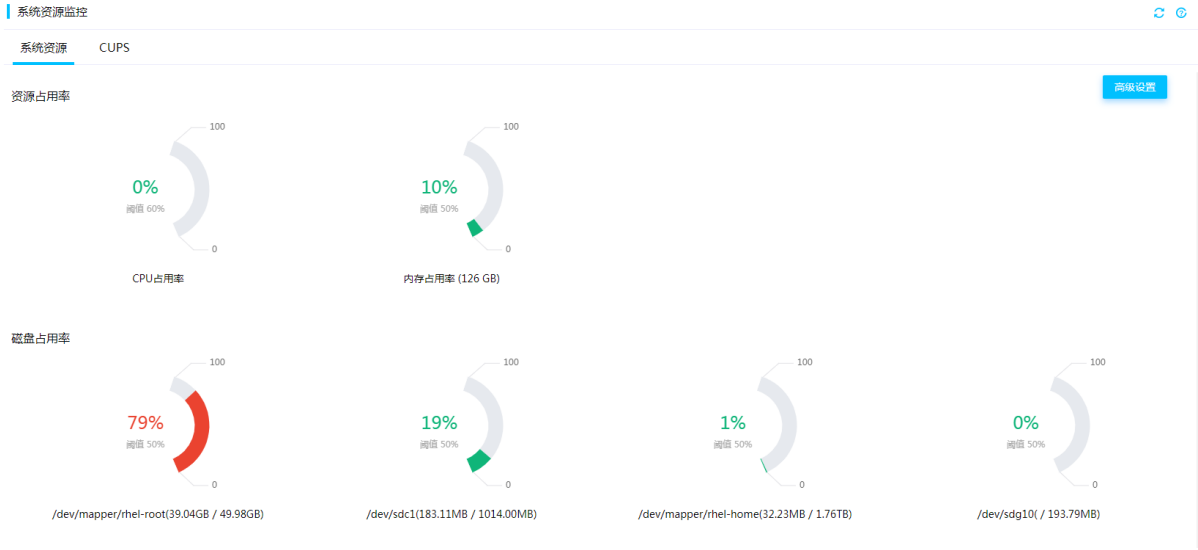
(2) 单击<高级设置>按钮，设置 CPU、内存、磁盘的占用率告警阈值，如图 5-25 所示。

图5-25 系统资源监控

(3) 单击<确定>按钮，保存设置。

(4) 查看资源使用信息，如图 5-26 所示。

图5-26 资源使用信息



2. 参数说明

- CPU 占用率：运行程序消耗的 CPU 资源比例。
- 内存占用率：所有进程占用的内存比例。
- 磁盘占用率：磁盘分区中已使用的空间占整个分区空间的比例、磁盘分区路径、已使用容量及磁盘分区总容量。
- CPU 占用率告警阈值(%)：CPU 占用率告警触发的阈值。
- 内存占用率告警阈值(%)：内存占用率告警触发的阈值。
- 磁盘占用率告警阈值(%)：磁盘分区占用率告警触发的阈值。

5.5.2 CUPS

CUPS（Compute Usage Per Second，每秒计算使用量）将 CPU、Memory、IO 三者作为一个整体资源，从硬件带宽维度来描述三种计算资源的总利用率。通过 CUPS 动态负载率可判断当前主机所运行业务类型比例，动态负载率高说明该业务为当前主机主要运行业务。CUPS 下的动态负载率和 OS 下的利用率算法不同，两者的数值没有直接的关系。

通过本功能可以查看服务器的 CUPS 信息和历史曲线图。

说明

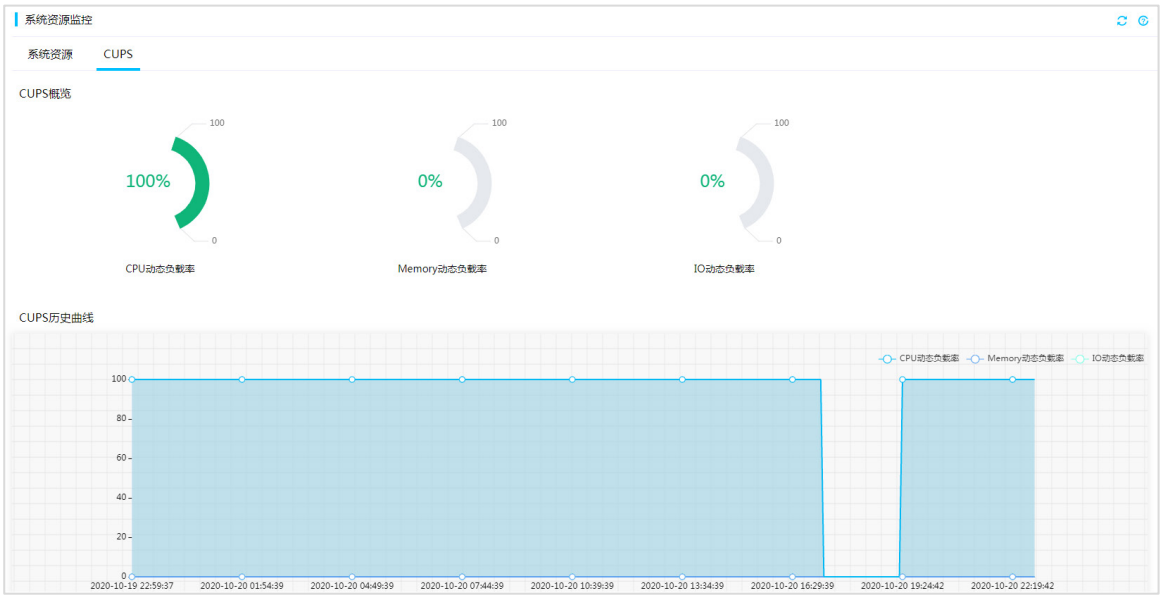
R3830 G3、R3630 G5、R3830 G5、R4950 G5、R5500 G5 AMD 不支持 CUPS 功能。

1. 操作步骤

(1) 单击[系统管理/系统资源监控]菜单项，选择“CUPS”页签，进入 CUPS 页面，如图 5-27 所示。

(2) 查看 CUPS 信息和历史曲线图。

图5-27 CUPS



2. 参数说明

- CPU CUPS 动态负载率：当前 CPU 核心数据的累计利用率，CPU 值较高说明当前主要运行了计算密集型业务。
- Memory CUPS 动态负载率：当前内存总线的累计传输率，Memory 值较高说明内存总线访问频率高，跟使用的内存容量大小无直接关系。而 OS 下的内存使用率=已使用内存容量/内存总容量，如使用了 8GB 内存中的 2GB 内存，内存使用率为 25%。
- IO CUPS 动态负载率：当前 PCIe 总线的 IO 带宽利用率，IO 值较高说明 PCIe 总线访问频率高，当前主要运行了 IO 密集型业务。

3. 注意事项

- 当 CPU、Memory 和 IO 的动态负载率之和不为 0 时，曲线图上的值是动态负载率的累加值，鼠标光标弹窗显示的才是动态负载率的具体值。
- 服务器关机状态下或 OS 下不运行任何业务时，CPU CUPS 动态负载率、Memory CUPS 动态负载率和 IO CUPS 动态负载率均为 0。
- CUPS 功能属于带外监控，不消耗 CPU 资源。
- 如果恢复 HDM 配置，所有的曲线信息都会清除。
- CPU/ Memory 动态负载率的算法与系统资源监控的 CPU/内存的占用率算法不一致，两者的数值没有相关性。

5.6 系统设置

5.6.1 系统启动项

本功能可以通过以下两种方式配置服务器的启动模式和启动设备。

- 设置系统启动项，包括启动模式和启动设备，支持选择有效期（一次性和永久性）。

- 设置系统启动顺序，包括启动模式和启动顺序，且设置永久生效。

说明

- 仅 G5 系列服务器支持设置系统启动顺序。
- 仅 HDM-2.11 及以后的版本支持设置系统启动顺序功能。
- B5700 G3、B5800 G3、B7800 G3、AE100 和 B5700 G5 不支持永久性启动设置。
- 如果系统启动项的永久性设置和系统启动顺序的设置不一样，服务器启动时会以系统启动项的永久性设置为准。
- 如果系统启动项的一次性设置和系统启动顺序的设置不一样，服务器下一次启动时会以一次性设置为准，启动完成后系统启动顺序的设置才会生效。

---

1. 设置系统启动项操作步骤

(1) 单击[系统管理/系统设置]菜单项，选择“系统启动项”页签，进入系统启动项页面，如图 5-28 所示。

(2) 在“系统启动项”栏选择设置有效期。

(3) 设置启动模式和启动设备。

(4) 查看当前启动模式和当前第一启动设备。

(5) 单击<保存>按钮，完成操作。

2. 设置系统启动顺序操作步骤

(1) 单击[系统管理/系统设置]菜单项，选择“系统启动项”页签，进入系统启动项页面，如图 5-28 所示。

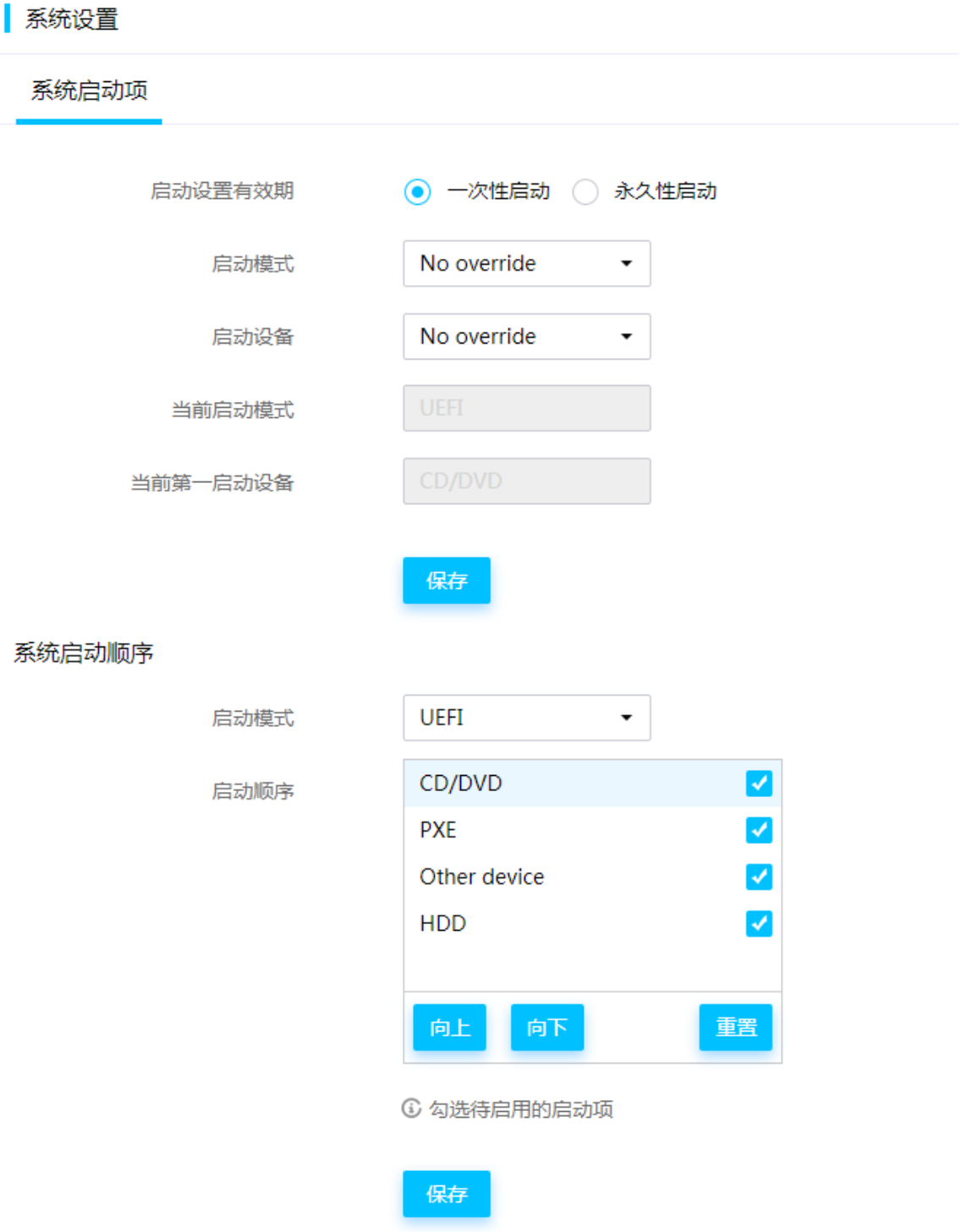
(2) 在“系统启动顺序”栏设置启动模式。

(3) 勾选待启用的启动项并调整启动顺序。

- 单击<向上>按钮，可以提高选中的启动设备的优先级。
- 单击<向下>按钮，可以降低选中的启动设备的优先级。
- 单击<重置>按钮，可以撤销对启动设备顺序的调整。

(4) 单击<保存>按钮，完成操作。

图5-28 系统启动项



3. 参数说明

- 一次性启动：启动模式和启动设备只在下一次启动时生效，然后恢复为默认值。
- 永久性启动：启动模式和启动设备将永久生效。
- 启动模式：设置服务器的启动模式，包括 Legacy 和 UEFI。

- AE100 不支持 Legacy 模式。
- No override 表示未对服务器的启动模式进行修改，服务器按 BIOS 设置的启动模式进行启动。

- 启动设备：设置服务器的启动设备，No override 表示未对服务器的启动设备进行修改，服务器按 BIOS 设置的启动顺序进行启动。
- 当前启动模式：显示服务器的当前启动模式。
- 当前第一启动设备：显示服务器的当前第一启动设备。
- 启动顺序：设置服务器的系统启动设备的顺序，下一次启动时会优先从第一启动设备启动。
  - Other device 表示其它启动设备，包含以下几种启动设备。
    - 进入内置的 UEFI Shell 的启动项，当 BIOS 下的 EFI Shell Boot 选项设置为“Enabled”时显示。
    - 其它未识别类型的启动设备。

4. 注意事项

- 如果选择从硬盘以 Legacy 模式启动，请确保硬盘支持 Legacy 模式。
- 配置系统启动模式、启动设备和启动顺序时，如果 BIOS 还处于启动阶段，则系统启动配置可能不生效

5.6.2 硬分区配置

通过本功能可以配置服务器硬分区，切换成单系统模式或独立双系统模式运行。服务器处于单系统或双系统时，电源都是统一供电模式。

- 当服务器处于单系统模式时，只有管理模块 1 处于运行状态，通过管理模块 1 的 HDM、BIOS 和操作系统可以管理整机。此时服务器做为一个整体对外提供服务。
- 当服务器处于双系统模式时，管理模块 1 和 2 处于独立运行状态，通过管理模块 1 和 2 对应的 HDM、BIOS 和操作系统可以管理对应的分区。此时可以把整机看成两个独立的服务器，两个服务器独立运行，互不影响，工作效率更高。
- 关于管理模块 1 和 2 的详细信息，请参见服务器用户指南。


说明

- 仅 R8900 G3 支持硬分区功能。
- 仅 HDM-2.18.01、BIOS-2.00.47 及以后的版本支持硬分区功能，两者需同时满足。
- 仅 CPLD-V006、PDBCPLD-V005 及以后的版本支持硬分区功能，两者需同时满足。
- 当服务器处于双系统时，请确保首个分区开机或重启成功后，再对另一个分区执行开机或重启操作。
- 请在技术支持的指导下配置硬分区功能。

---

1. 从单系统切换到双系统

配置限制和指导

模式切换前，应确保满足如下几个条件：

- 服务器已正常关机且 HDM 未处于固件更新状态。

- HDM、BIOS 和所有 CPLD 版本都支持硬分区配置功能，且不同软件的版本符合配套关系。
- 若服务器的固件版本不符合硬分区配置功能要求，请按照如下步骤进行固件更新。

  a. 更新服务器的 HDM、BIOS 和所有 CPLD 固件到支持硬分区功能的版本。

  b. 将服务器下电，并将管理模块 1 和管理模块 2 的物理位置互换。
- 上电启动后，再次更新服务器的 HDM、BIOS 和所有 CPLD 固件到支持硬分区功能的版本。

操作步骤

(1) 登录 HDM，单击[系统管理/系统设置]菜单项，选择“硬分区”页签，进入硬分区页面，如图 5-29所示。

图5-29 切换为双系统

(2) 选择<双系统>模式。

(3) 输入 Administrator、Operator 或拥有远程控制权限的用户名和密码。

(4) 单击<保存>按钮。

(5) 对服务器进行断电重启，使配置生效。

登录分区的 HDM

(1) 切换为双系统模式后，管理模块 1 和 2 均处于运行状态，对应分区的 HDM 也会恢复默认配置，需要重新获取分区对应的专用网口和共享网口的 IP 地址才能访问 HDM。为了方便区分两个分区，根据分区的物理位置差异，两个分区命名为上分区和下分区。

- 如果分区的专用网口处于连接状态，可以通过缺省地址 192.168.1.2/24 登录对应分区的 HDM。
- 如果分区的共享网口处于连接状态，下分区的共享网口地址缺省通过 DHCP 获取，需要通过查看 POST 界面获取 IP 地址，上分区的共享网口地址获取方式有两种。
  - 如果切换模式前的共享网口是 DHCP 分配的地址，切换后的上分区会继承之前的 IP 地址。
  - 如果切换模式前的共享网口是静态地址，切换后的上分区会通过 DHCP 重新获取一个 IP 地址，需要查看 BIOS POST 界面获取 IP 地址。

(2) 成功获取上下分区对应的专用网口或共享网口的 IP 地址后，通过 HDM 的缺省用户 admin，密码：Password@_，可以访问分区的 HDM。

2. 从双系统切换到单系统

配置限制和指导

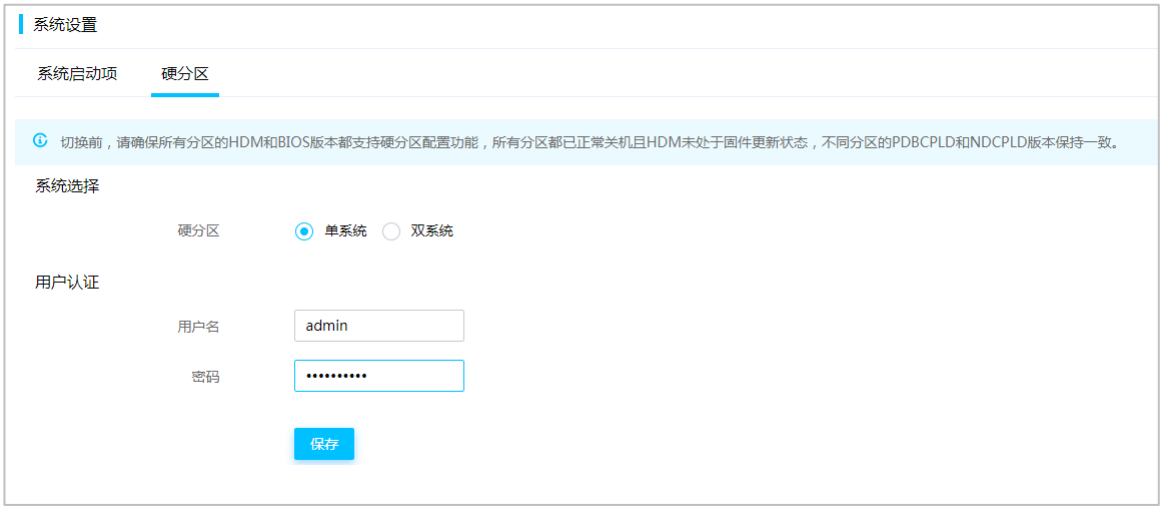
模式切换前，应确保满足如下几点条件：

- 所有分区已正常关机且 HDM 未处于固件更新状态。
- 所有分区的 PDBCPLD 和 NDCPLD 版本保持一致。
- 所有分区的 HDM 和 BIOS 版本都支持硬分区配置功能。
- 仅管理模块 1（即上分区）的 HDM 支持切换为单系统模式。

切换模式操作步骤

(1) 登录管理模块 1（即上分区）的 HDM，单击[系统管理/系统设置]菜单项，选择“硬分区”页签，进入硬分区页面，如图 5-30 所示。

图5-30 切换为单系统



(2) 选择<单系统>模式。

(3) 输入 Administrator、Operator 或拥有远程控制权限的用户名和密码。

(4) 单击<保存>按钮。

(5) 对服务器进行断电重启，使配置生效。

登录 HDM

(1) 切换为单系统后，仅管理模块 1 处于运行状态，对应的 HDM 和 BIOS 也会恢复默认配置。需要重新获取管理模块 1 对应的 HDM 的专用网口和共享网口的 IP 地址才能访问 HDM。

- 如果专用网口处于连接状态，可以通过缺省地址 192.168.1.2/24 登录 HDM。
- 如果共享网口处于连接状态，IP 地址获取方式有两种。
  - 如果切换模式前，上分区的共享网口是 DHCP 分配的地址，切换后的共享网口会继承之前的 IP 地址。

- 如果切换模式前，上分区的共享网口是静态地址，切换后的共享网口会通过 DHCP 重新获取一个 IP 地址，需要查看 BIOS POST 界面获取 IP 地址。

(2) 成功获取专用网口或共享网口的 IP 地址后，通过 HDM 的缺省用户 admin，密码：Password@_，可以访问 HDM。

6 HDM 设置

6.1 网络设置

HDM 专用网口是专门用于处理 HDM 管理流量的网络接口，缺省 IPv4 地址为 192.168.1.2/24，IPv6 地址缺省通过 DHCP 自动获取。

说明

刀片服务器和 AE 模块不支持专用网口。

HDM 共享网口是可以同时处理 HDM 管理流量和服务器业务流量的网络接口，HDM 共享网口缺省通过 DHCP 自动获取 IP 地址。

配置网络可能会影响 HDM 的正常访问，配置前请注意以下事项：

- 网口模式为正常模式时，请将 HDM 共享网口、专用网口和无线网络的 IP 地址配置在三个不同的网段，且 IP 地址不能相同，否则可能会引起网络故障。
- 请勿同时停用所有 HDM 网络接口，否则会导致用户无法访问 HDM Web 界面。
- 修改 HDM 网络配置后，浏览器会话将断开连接，可能需要等待数分钟后，才能重新连接 HDM Web 界面。
- 修改 HDM 网络配置后，请等待配置生效后再对服务器进行断电重启操作。

6.1.1 查看专用网口信息

通过本功能可以查看当前 HDM 专用网口信息，包括接口名称、MAC 地址、IP 概况、VLAN 概况等。

1. 操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“专用网口”页签，进入专用网口页面，如图 6-1 所示。

(2) 查看 HDM 专用网口信息。

图6-1 专用网口信息

2. 参数说明

- 网口状态：包括主用和断开两种状态。此参数只有在网口自适应模式开启后才会显示。
  - 主用：当前网口处于启用状态。
  - 断开：当前网口处于断开状态。
- 连接状态：每个端口的连接状态。
  - 未连接：当前端口未连接网线。
  - 使用中：当前端口已连接网线并启用。

6.1.2 配置专用网口

1. 配置限制和指导

- 配置前请确认已将 HDM 专用网口连接到网络。
- 通过 DHCPv6 方式或无状态自动配置方式配置 IPv6 地址，只支持 64 位子网前缀长度。
- 如果使用 IPv6 地址无法正常访问 HDM Web，请先关闭代理服务器。
- 网口自适应模式开启后，只有当网口状态处于主用时，才能进行 IPv4 配置和 IPv6 配置，配置生效后，会自动同步到其它网口。

2. IPv4 配置操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“专用网口”页签，进入专用网口页面，如图 6-1 所示。

(2) 单击<配置>按钮，进入专用网口配置页面。

(3) 在 IPv4 配置栏，配置以下参数，如图 6-2 所示。

(4) 选择启用 IPv4 配置。

(5) 开启“自动获取 IP 地址”功能以启用 DHCPv4 功能；如果要配置静态 IPv4 地址，则关闭该功能，并在后续的地址栏中输入相关信息。

(6) 单击<保存>按钮，完成操作。

图6-2 IPv4 配置

3. IPv6 配置操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“专用网口”页签，进入专用网口页面，如图 6-1 所示。

(2) 单击<配置>按钮，进入专用网口配置页面。

(3) 在 IPv6 配置栏，配置下列参数，如图 6-3 所示。

(4) 选择启用 IPv6 配置。

(5) 开启“自动获取 IP 地址”功能以启用 DHCPv6 功能；如果要配置静态 IPv6 地址，则关闭该功能，并在后续的地址栏中输入相关信息。

(6) 单击<保存>按钮，完成操作。

图6-3 IPv6 配置

4. VLAN 设置操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“专用网口”页签，进入专用网口页面，如图 6-1 所示。

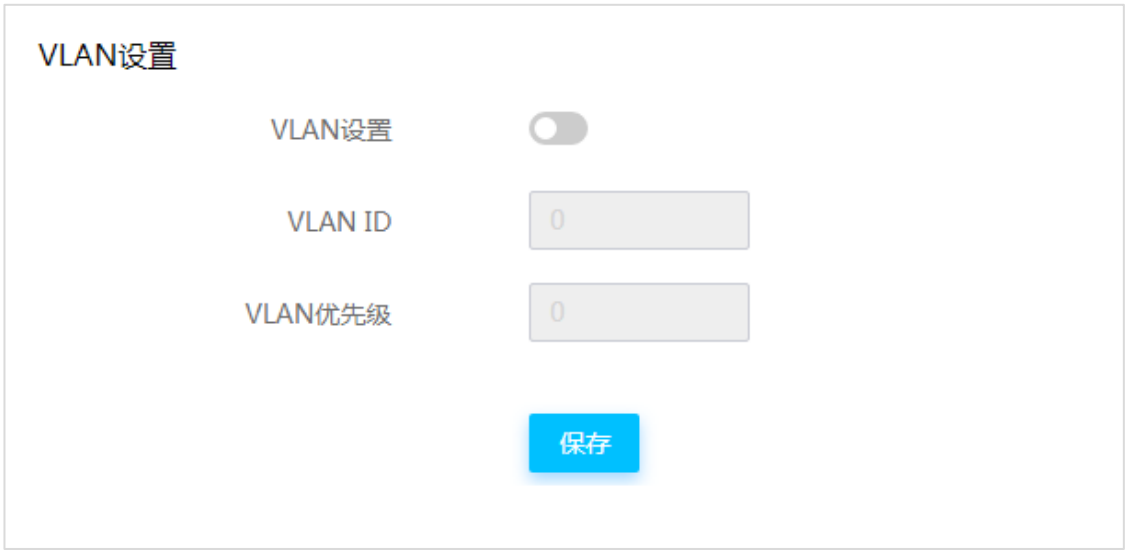
(2) 单击<配置>按钮，进入专用网口配置页面。

(3) 在 VLAN 设置栏，配置下列参数，如图 6-4 所示。

(4) 选择启用 VLAN 设置，并输入相关信息；如果要停用，则关闭该功能。

(5) 单击<保存>按钮，完成操作。

图6-4 VLAN 设置



5. 参数说明

- 默认网关：服务器的默认网关地址。
  - 对于 IPv4 地址，0.0.0.0 表示未配置默认网关。
  - 对于 IPv6 地址，fe80::9628:2eff:fe9c:ffda 表示默认网关。
- 子网前缀长度：IPv6 地址的子网前缀长度，子网前缀长度的范围为 1～127。
- VLAN ID：指定 VLAN 的标签值。VLAN ID 的范围为 2～4094。
- VLAN 优先级：指定 VLAN 的优先级别。VLAN 优先级的范围为 0～7，其中 7 为最高优先级。主要用于当交换机端口发生拥塞时，交换机通过识别 VLAN 优先级，优先发送优先级高的数据包。

6.1.3 查看共享网口信息

通过本功能可以开启或关闭共享网口的 NCSI（Network Controller Sideband Interface，网络控制器边带接口）设置。

- 如果 NCSI 设置处于开启状态，共享网口将处于启用状态，可以查看当前共享网口的情况，包括接口名称、MAC 地址、IP 概况、VLAN 概况和端口的连接状态。
- 如果 NCSI 设置处于关闭状态，共享网口将处于禁用状态，用户无法通过共享网口访问 HDM。

1. 操作步骤

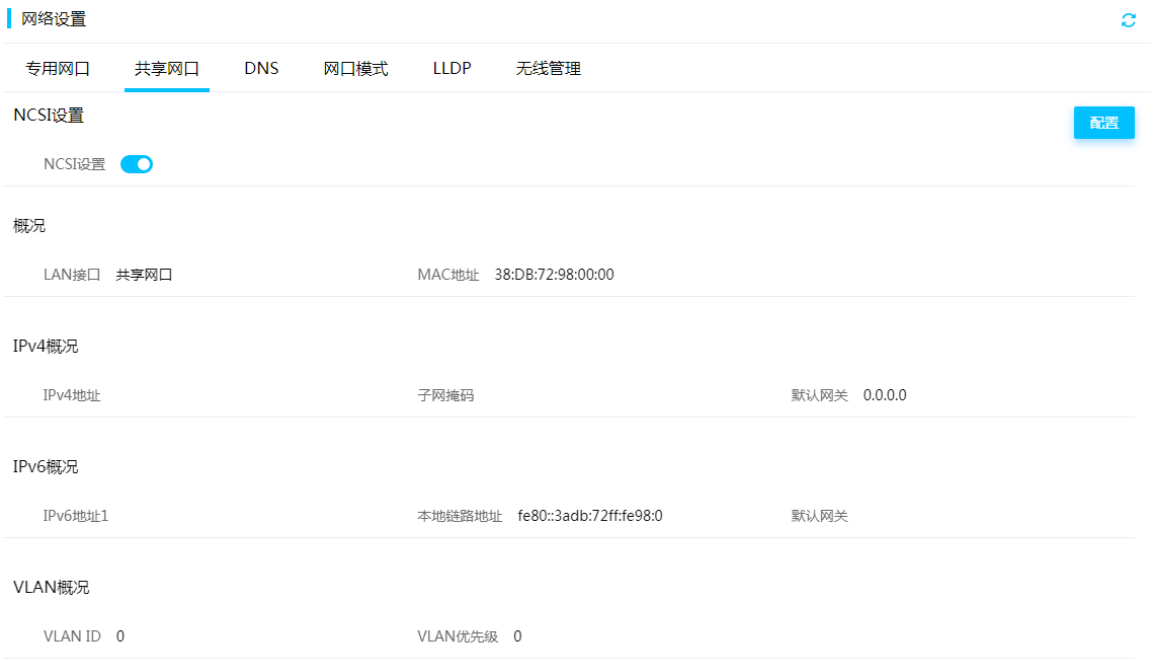
(1) 单击[HDM 设置/网络设置]菜单项，选择“共享网口”页签，进入共享网口页面，如图 6-5 所示。

(2) 开启或关闭 NCSI 设置，在对话框中单击<确定>按钮，保存设置。

(3) 当前页面会断开连接，网络会自动重启使配置生效。

- 开启 NCSI 设置后，重新登录 HDM，可以查看或配置 HDM 共享网口信息。
- 关闭 NCSI 设置后，HDM 共享网口无法访问。

图6-5 共享网口信息



2. 参数说明

- 网口状态：包括主用、断开和备用三种状态。此参数只在网口自适应模式开启后才会显示。
  - 主用：当前网口处于启用状态。
  - 断开：当前网口处于断开状态。
  - 备用：当前网口已连接，但并未启用。
- 连接信息：共享网口启用的网卡信息，包括端口自适应模式的状态、网卡类型和网卡上每个端口的连接状态。当服务器未插入网卡或网卡不支持 NCSI 功能时，端口连接信息不显示。
  - 未连接：当前端口未连接网线。
  - 已连接：当前端口已连接网线但未启用。
  - 使用中：当前端口已连接网线并启用。

6.1.4 配置共享网口

开启 NCSI 设置后，通过本功能可以配置 HDM 共享网口的 IPv4 地址、IPv6 地址、VLAN 设置和网卡选择。

网卡选择是指切换 HDM 共享网口的物理端口后，用户只要重新接入切换后的共享网口即可访问 HDM，该功能具有以下优点：

- 不用更改服务器在整网中的网络信息。
- 不需要重新配置切换后共享网口的网络信息（包括 IP 地址、VLAN 等）。
- 共享网口支持自动切换（即端口自适应模式）和手动切换两种方式。
- sLOM、mLOM、FLOM、OCP 网卡、支持 NCSI 功能的 PCIe 网卡均支持端口自适应模式。

1. 配置限制和指导

- 配置前请确认已将 HDM 共享网口连接到网络。
- 通过 DHCPv6 方式或无状态自动配置方式配置 IPv6 地址，只支持 64 位子网前缀长度。
- 如果使用 IPv6 地址无法正常访问 HDM Web，请先关闭代理服务器。
- 网口自适应模式开启后，只有当网口状态处于主用时，才能进行 IPv4 配置和 IPv6 配置，配置生效后，会自动同步到其它网口。

2. LAN 设置操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“共享网口”页签，进入共享网口页面，如图 6-5 所示。

(2) 单击<配置>按钮，进入共享网口配置页面。

(3) 选择启用 LAN 设置。

(4) 单击<保存>按钮，完成操作。

图6-6 LAN 配置

3. IPv4 配置操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“共享网口”页签，进入共享网口页面，如图 6-5 所示。

(2) 单击<配置>按钮，进入共享网口配置页面。

(3) 在 IPv4 配置栏，配置下列参数，如图 6-7 所示。

(4) 选择启用 IPv4 配置。

(5) 开启“自动获取 IP 地址”功能以启用 DHCPv4 功能；如果要配置静态 IPv4 地址，则关闭该功能，并在后续的地址栏中输入相关信息。

(6) 单击<保存>按钮，完成操作。

图6-7 IPv4 配置

4. IPv6 配置操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“共享网口”页签，进入共享网口页面，如图 6-5 所示。

(2) 单击<配置>按钮，进入共享网口配置页面。

(3) 在 IPv6 配置栏，配置下列参数，如图 6-8 所示。

(4) 选择启用 IPv6 配置。

(5) 开启“自动获取 IP 地址”功能以启用 DHCPv6 功能；如果要配置静态 IPv6 地址，则关闭该功能，并在后续的地址栏中输入相关信息。

(6) 单击<保存>按钮，完成操作。

图6-8 IPv6 配置

5. VLAN 设置操作步骤

说明

刀片服务器和 AE 模块不支持 VLAN 设置。

(1) 单击[HDM 设置/网络设置]菜单项，选择“共享网口”页签，进入共享网口页面，如图 6-5 所示。

(2) 单击<配置>按钮，进入共享网口配置页面。

(3) 在 VLAN 设置栏，配置下列参数，如图 6-9 所示。

(4) 选择启用 VLAN 设置，并输入相关信息；如果要停用，则关闭该功能。

(5) 单击<保存>按钮，完成操作。

图6-9 VLAN 设置

6. 网卡切换操作步骤

说明

- 刀片服务器和 AE 模块不支持网卡选择。
- 网卡切换前，请检查目标端口是否处于连接状态。
- 网卡切换后的端口会继承原共享端口的静态 IP 地址及 VLAN 等信息。如果切换前共享网口使用的是 DHCP 分配的 IP 地址，切换后，端口会重新获取 IP 地址。
- 关闭端口自适应模式后，如未手动切换，系统会将网口恢复到开启该功能前的端口，请确保上次配置的网卡端口处于连接状态。
- 端口自适应模式和网口自适应模式不能同时开启，否则可能会导致网络故障。
- 通过导入配置文件修改网卡选择的端口和网口模式时，请保证配置文件信息的完整性和正确性。

(1) 单击[HDM 设置/网络设置]菜单项，选择“共享网口”页签，进入共享网口页面，如图 6-5 所示。

(2) 单击<配置>按钮，进入共享网口配置页面，如图 6-10 所示。

(3) （可选）在网卡选择栏，选择启用端口自适应模式。

(4) 选择在位网卡中的任一端口。

(5) 单击<保存>按钮，完成操作。

图6-10 网卡切换

7. 参数说明

- LAN 设置：启用 LAN 设置后，才可配置共享网口的所有参数。关闭 LAN 设置后，所有共享网口的配置都被禁用。关闭 LAN 设置前，请确保专用网口 IP 地址可达。
- 默认网关：服务器的默认网关地址。
  - 对于 IPv4 地址，0.0.0.0 表示未配置默认网关。
  - 对应 IPv6 地址，fe80::9628:2eff:fe9c:ffda 表示默认网关。
- 子网前缀长度：IPv6 地址的子网前缀长度，子网前缀长度的范围为 1～127。
- VLAN ID：指定 VLAN 的标签值。VLAN ID 的范围为 2～4094。
- VLAN 优先级：指定 VLAN 的优先级别。VLAN 优先级的范围为 0～7，其中 7 为最高优先级。主要用于当交换机端口发生拥塞时，交换机通过识别 VLAN 优先级，优先发送优先级高的数据包。

6.1.5 配置 DNS

通过本功能对 HDM 的域名服务系统进行配置后，用户可以使用便于记忆的、有意义的域名直接访问 HDM，DNS 服务器会将该域名解析为 HDM 的管理 IP 地址。

配置 DNS 功能时，需要分别配置以下两个参数：

- 主机名配置：配置服务器主机名。
- DNS 配置：配置上级域名信息和域名服务器。网络中的其他设备可以通过该域名服务器解析到 HDM 的管理 IP 地址。

1. 配置主机名操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“DNS”页签，进入 DNS 页面。

(2) 在主机名配置栏目中，选择<手动>或<自动>选项，如图 6-11 所示。

(3) 如果选择<手动>选项，在主机名的文本框中输入主机名称。

(4) 如果选择<自动>选项，此时主机名缺省将被设置为“HDM+产品序列号”。

(5) 单击<保存>按钮，完成操作。

图6-11 DNS 主机名

2. 配置 DNS 操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“DNS”页签，进入 DNS 页面。

(2) 在 DNS 配置栏目中，选择启用域名服务配置，如图 6-11 所示。

(3) 勾选 DNS 服务器地址获取方式，“手动”或“自动获取 IPv4 DNS 地址”或“自动获取 IPv6 DNS 地址”。

a. 如果 DNS 服务器设置为“手动”，即静态注册 DNS 地址，则需要输入上级域名（选填）和 DNS 服务器地址。

b. 如果 DNS 服务器设置为“自动获取 IPv4 DNS 地址”或“自动获取 IPv6 DNS 地址”。

– 需要先选择动态注册选项，“主机名”或者“DHCP Client FQDN”。

- 再选择 DNS 注册信息获取网口，“专用网口”或“共享网口”。只有当专用网口和共享网口都处于 DHCP 状态时，此选项才会显示。
- 然后系统会自动获取上级域名和 DNS 服务器地址，在完成 DNS 配置后，DNS 服务器栏会显示 DNS 服务器地址。

(4) 完成所有栏目的配置后，单击<保存>按钮，完成操作。

3. 参数说明

- 主机名：设备的主机名称。
  - 主机名称的长度为 1～48 个字符。
  - 允许使用特殊字符连接符（-），但不能以连接符（-）开头或结束。
- 上级域名：注册到 DNS 服务器相应区域的域名后缀，“主机名+上级域名”组成公网下唯一标识主机的域名，用户可通过此域名访问 HDM。
- 动态注册选项：选择 DHCP Client FQDN 或主机名，都是通过 DHCP 服务器分配给主机 IP 地址，同时将此地址动态注册到 DNS。
- DNS 服务器 1～3：HDM 指定的 DNS 服务器，数字表示使用 DNS 服务器的优先级，数字越小，优先级越高。

4. 注意事项

- 当所有网口都配置静态 IP 地址时，只能选择手动方式配置 DNS 服务器。
- 如果选择“手动”为 DNS 服务器配置 IPv6 地址，请输入全局 IPv6 地址。

6.1.6 选择网口模式

通过本功能可以配置 HDM 的网口模式。缺省情况下，网口模式为正常模式。

说明

刀片服务器和 AE 模块不支持网口模式。

Bonding 模式下，专用网口和共享网口绑定成一个通信端口，只能配置一个 VLAN。网口自适应模式开启后，专用网口和共享网口都可以配置 VLAN。对于需要在不同 VLAN 下灵活切换通信端口的情况，网口自适应模式相较于 Bonding 模式更有优势。

1. 配置限制与指导

在配置网口模式前，请检查以下配置：

- 切换为 Bonding 模式前，请确保 HDM 专用网口已存在 IP 地址，且和共享网口的 IP 地址连接在不同网段。切换后，Bonding 接口将继承 HDM 专用网口的 IP 地址和 MAC 地址。
  - 如果切换前 HDM 专用网口的 IP 地址是通过 DHCP 方式获取，切换后的 Bonding 接口会重新获取 IP 地址。
  - 如果切换前 HDM 专用网口的 IP 地址是静态地址，切换后的 Bonding 接口会继承原来的 IP 地址。
- 网口模式为正常模式且 HDM 网口（包括 HDM 共享网口和 HDM 专用网口）已启用 VLAN 设置时，系统不支持将网口模式切换为 Bonding 模式。
- 网口自适应模式和端口自适应模式不能同时开启，否则可能会导致网络故障。

- 通过导入配置文件修改网卡选择的端口或网口模式时，请保证配置文件信息的完整性和正确性。

2. 操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“网口模式”页签，进入网口模式页面，如图 6-12 所示。

(2) 选择网口模式。

(3) 单击<保存>按钮，完成操作。

图6-12 网口模式

3. 参数说明

- 网口模式：包括 Bonding 模式、网口自适应模式和正常模式。
  - Bonding 模式：该模式下 HDM 共享网口和 HDM 专用网口将作为一个逻辑上的网络接口使用。切换后，Bonding 接口将继承 HDM 专用网口的 IP 地址和 MAC 地址。只要 HDM 共享网口和 HDM 专用网口中的任意一个接口处于连接状态，用户就可以通过 HDM Bonding 网口的 IP 地址访问 HDM。
  - 网口自适应模式：指的是 HDM 管理流量优先选择专用网口作为通信端口。
    - 当专用网口连接网线时，无论共享网口是否连接网线，选择专用网口作为通信端口。
    - 当共享网口连接网线，专用网口未连接网线时，选择共享网口作为通信端口。
  - 正常模式：该模式下可通过 HDM 共享网口或 HDM 专用网口访问 HDM。

6.1.7 配置 LLDP

LLDP（Link Layer Discovery Protocol，链路层发现协议）提供了一种标准的链路层发现方式，使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息。

通过本功能可以设置服务器发送 LLDP 信息，并查看已接收到的 LLDP 信息。

1. 操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“LLDP”页签，进入 LLDP 页面，如图 6-13 所示。

(2) （可选）选择是否发送 LLDP 信息。

(3) 查看接收到的 LLDP 信息。

图6-13 LLDP 配置

2. 参数说明

- 网络接口：服务器接收 LLDP 信息的网络接口。
- 交换机 MAC 地址：上联交换机端口的 MAC 地址。
- 交换机系统名：上联交换机系统名。
- 连接端口号：上联交换机端口号。
- 端口信息：上联交换机端口的信息。
- VLAN ID：服务器网络接口的 VLAN ID。

3. 注意事项

当网络连接断开或交换机不支持发送 LLDP 信息时，对应的信息将显示 N/A。

6.1.8 无线管理

说明

- 仅 G5 系列服务器支持无线管理功能，B5700 G5 服务器不支持无线管理功能。
- 仅 HDM-2.14 及以后的版本支持无线管理功能。

服务器接入 USB 无线模块后，可以通过本功能开启并配置无线网络。配置完成后，用户可以通过客户端接入无线网络，访问服务器，并查看已接入无线网络的客户端信息。

1. 操作步骤

(1) 单击[HDM 设置/网络设置]菜单项，选择“无线管理”页签，进入无线管理页面。

(2) 选择启用无线网络，根据需要，配置以下参数，如图 6-14 所示。

a. 输入无线网络名称。

b. 选择加密方式；如果选择“加密”，需要输入无线网络密码。

c. （可选）输入定时关闭无线网络的时间。

d. 输入无线网络 IPv4 地址。

e. 输入可分配给客户端的 IPv4 地址范围。

图6-14 无线管理

(3) 单击<保存>按钮，完成操作。

(4) 查看客户端接入信息，如图 6-15 所示。

图6-15 客户端信息

2. 参数说明

- 设备状态：USB 无线模块的在位状态。

- 无线名称：无线网络的名称，必填项。
  - 缺省名称为：产品名称_产品序列号后 10 位。
  - 长度 1～31 个字符，仅支持字母、数字、句点（.）、连接符（-）和下划线（_），区分大小写。
- 加密方式：无线网络的加密方式，支持“加密”和“不加密”两种方式，缺省不加密。
- 无线密码：加密方式为“加密”时，需要设置密码。长度支持 8～63 个字符，仅支持字母、数字、空格和特殊字符`~!@#$%^&*()_+-=[]\{}|;':,./<>?，区分大小写。
- 无线定时关闭：无线网络的定时关闭时间，范围为 0～200 小时， 缺省为 1，0 表示无线网络不会自动关闭。
- 无线 IP 地址：无线网络的 IPv4 地址，缺省为 192.168.199.1，子网掩码固定为 255.255.255.0，不能和 HDM 的专用网口、共享网口在同一网段。
- 地址段：客户端接入无线网络时，HDM 为客户端分配 IPv4 地址的范围，需要和无线 IP 地址保持在同一网段，子网掩码固定为 255.255.255.0。
- 序号：接入无线网络的客户端序号，最多支持同时接入两个客户端。
- 客户端 MAC 地址：接入无线网络的客户端 MAC 地址。
- 客户端 IP 地址：接入无线网络的客户端 IPv4 地址。
- 主机名：接入无线网络的客户端主机名。

3. 注意事项

当无线网络无客户端接入的时间超过定时关闭时间时，无线网络会自动关闭。可以拔插 USB 无线模块或登录 HDM Web 端开启无线网络，使网络恢复正常。

6.2 NTP

NTP(Network Time Protocol)是网络时间协议，可以用来在分布式时间服务器和 HDM 客户端之间进行时间同步，使网络内所有 HDM 客户端的时间保持一致，并提供较高的时间同步精度。通过本功能可以配置 HDM 所在的时区，并配置连接的 NTP 服务器地址。

1. 操作步骤

(1) 单击[HDM 设置/NTP]菜单项，进入“NTP”页面，如图 6-16 所示。

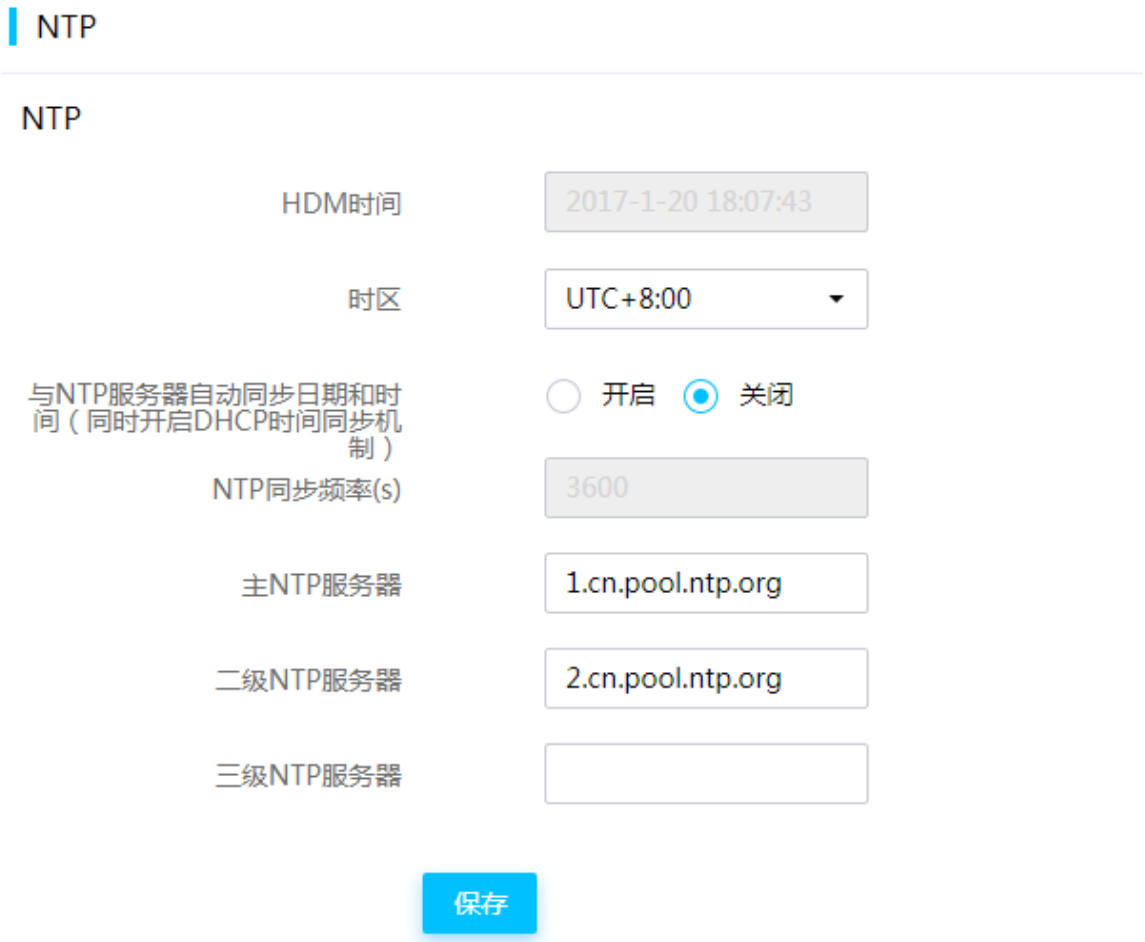
(2) 在时区一栏选择 HDM 所在的时区。

(3) 选择是否开启“与 NTP 服务器自动同步日期和时间”功能。

(4) 选择开启后，设置 NTP 同步频率，在主 NTP 服务器、二级 NTP 服务器和三级 NTP 服务器三栏填写服务器的 NTP 服务器地址。

(5) 单击<保存>按钮，完成操作。

图6-16 NTP



2. 参数说明

- 时区：选择 HDM 所在的时区。
- 与 NTP 服务器自动同步日期和时间：
  - 选择开启，HDM 会自动同步 NTP 服务器的日期和时间。
  - 选择关闭，HDM 会与 ME 周期性同步时间。如果 BIOS 重启，HDM 会以 BIOS 时间（UTC 时间）为基准，根据 HDM 时区设置来同步时间，若 HDM 时区设置为 UTC+8，则 HDM 时间比 BIOS 时间早 8 小时。
- NTP 同步频率：开启 NTP 功能后，HDM 与 NTP 服务器同步时间的时间间隔，缺省为 3600 秒，取值范围为 600 秒～2592000 秒。
- 主 NTP 服务器、二级 NTP 服务器和三级 NTP 服务器：配置 NTP 服务器地址。
  - 支持 IPv4 地址、IPv6 地址和域名地址。

    - 二级 NTP 服务器和三级 NTP 服务器为可选项。如果主 NTP 服务器不能正常工作，会使用二级 NTP 服务器和三级 NTP 服务器。如果主 NTP 服务器和二级 NTP 服务器不能正常工作，会使用三级 NTP 服务器。
- 缺省情况下，开启 NTP 服务。主 NTP 服务器地址为 1.cn.pool.ntp.org，二级 NTP 服务器地址为 2.cn.pool.ntp.org，三级 NTP 服务器地址为空。

3. 注意事项

- 当启用 NTP 服务时，若 HDM 从主、二级和三级 NTP 服务器同步时间失败，且能获取到 DHCP 服务器分配的 NTP 服务器 IP 时，在重启 HDM 后尝试从 DHCP 服务器分配的 NTP 服务器中获取时间。如果组网中没有 DHCP 服务器，HDM 会以上一次同步 NTP 服务器或原有的时间继续运行。
- 如果由于 NTP 服务器地址不可达等原因导致同步时间失败，界面上会显示“与 NTP 服务器同步时间失败”，如果 NTP 服务器恢复连通或管理员需要再次触发同步时间操作，请手动点击<保存>按钮。

7 远程服务

7.1 服务设置

7.1.1 查看服务

通过本功能可以查看 HDM 所提供服务的详细信息。

说明

- R2700 G3、R2900 G3、R4300 G3、R4400 G3、R4700 G3、R3800 G3、R5300 G3、R6700 G3、R4300 G5、R4700 G5、R3800 G5、R5300 G5、B5700 G5 支持 Remote-XDP 服务。
- 仅 R4950 G5 和 R5500 G5 AMD 支持 iHDT 服务。

1. 操作步骤

(1) 单击[远程服务/服务设置]菜单项，进入“服务设置”页面，如图 7-1 所示。

(2) 在列表可查看服务名称等信息。

在列表中选择一个服务，单击操作栏的查看按钮，在弹出的页面中可以查看服务的详细信息，如图 7-2 所示。

图7-1 服务信息

图7-2 会话信息

(3) 在服务会话页面可进行以下两种操作：

- 返回服务页面：单击<关闭>按钮，返回服务页面。
- 结束指定会话：选择一个会话，单击<删除>按钮，结束该会话。

2. 参数说明

- 名称：HDM 所提供服务的名称，包括：
  - CD-Media：支持通过 HDM 访问虚拟媒体 CD/DVD。
  - FD-Media：支持通过 HDM 访问虚拟媒体软盘。
  - HD-Media：支持通过 HDM 访问虚拟媒体硬盘/USB 存储设备。
  - iHDT：支持使用 HDT（Hardware Debug Tool，硬件调试工具）客户端进行调试功能。
  - IPMI：支持使用 RMCP/RMCP+方式连接 HDM。
  - KVM：支持使用远程控制台。
  - Remote_XDP：支持远程连接 XDP 接口进行调试功能。
  - SNMP：支持使用简单网络管理协议连接 HDM。
  - SSH：支持使用 SSH 连接 HDM。
  - Telnet：支持使用远程登录服务连接 HDM。
  - VNC：支持使用 VNC 客户端远程控制台。
  - Web：支持访问 HDM Web 界面。
- 状态：该服务运行的状态，包括“开启”和“禁用”。“开启”表示该服务已启用，“禁用”表示该服务未启用。
- 接口：该服务所使用的 HDM 网络接口，仅 G3 服务器支持显示此参数。
  - eth0 表示 HDM 共享网络接口。
  - eth1 表示 HDM 专用网络接口。
  - both 表示 HDM 共享网络接口和专用网络接口，如果是 Bonding 模式，该接口为 Bond0，Bond0 表示 HDM Bonding 网络接口。
- 非安全端口：该服务所使用的未加密的通信端口。
- 安全端口：该服务所使用的经加密的端口号。

- 超时：服务会话的超时时间，单位为分钟。超时后，使用该服务的会话会自动断开。
- 最大会话：该服务所允许的最大会话数。
- 会话 ID：表示该会话在所有 HDM 服务的编号。如果标*，表示该会话为访问当前 Web 端的客户端 IP 建立的会话。
- 会话类型：表示该会话所采用的协议类型或服务类型。
- 用户编号：当前用户在[用户&安全/用户访问设置]用户列表的编号，非“本地用户”或“域用户”的用户编号为 0。
- 用户名：当前用户的名字。
- IP 地址：当前用户的 IP 地址。
- 用户权限：当前用户所拥有的访问权限。

3. 注意事项

- SSH 和 Telnet 服务使用相同的超时时间。如果用户设置 SSH 的超时时间，此值将会被 Telnet 服务采用，反之亦然。
- ipmitool 工具发送 IPMI 命令使用 623 端口，若修改 IPMI 默认非安全端口号，发送 IPMI 命令时需加-p 参数指定端口号。
- 不同机型支持的服务类型不完全一样，具体差异请以界面显示为准。

7.1.2 修改服务

通过本功能可以修改 HDM 所提供服务的配置参数。

1. 操作步骤

(1) 单击[远程服务/服务设置]菜单项，进入“服务设置”页面，如图 7-1 所示。

(2) 在服务列表中选择一个服务，单击操作栏的修改按钮，弹出“修改服务”对话框，如图 7-3 所示。

图7-3 修改服务

(3) 在对话框中根据需要修改服务的当前状态、端口号和超时时间等参数。

(4) （仅适用于 iHDT 服务）单击<重启>按钮会重启 iHDT 服务。

(5) 单击<确定>按钮，完成操作。

2. 参数说明

- 非安全端口：该服务所使用的未加密的通信端口，取值范围为 1～65535，VNC 的取值范围为 100～65535，缺省情况如表 7-1 所示。
- 安全端口：该服务所使用的经加密的端口号，取值范围为 1～65535，缺省情况如表 7-1 所示。

表7-1 缺省端口号

服务名称	缺省的非安全端口号	缺省的安全端口号
CD-Media	5120	5124
FD-Media	5122	5126
HD-Media	5123	5127
iHDT	6123	N/A
IPMI	623	N/A
KVM	7578	7582

服务名称	缺省的非安全端口号	缺省的安全端口号
Remote_XDP	6868	N/A
SNMP	161	N/A
SSH	N/A	22
Telnet	23	N/A
VNC	5900	N/A
Web	80	443

- 超时：服务会话的超时时间，单位为分钟。可以对 Web、KVM、SSH、Telnet 和 VNC 服务配置超时时间，取值范围和缺省情况如表 7-2 所示。

表7-2 超时时间取值范围和缺省情况

服务	超时时间取值范围	缺省超时时间
Web	5～120分钟	30分钟
KVM	5～30分钟	30分钟
SSH	1～30分钟	10分钟
Telnet	1～30分钟	10分钟
VNC	5～30分钟	10分钟

3. 注意事项

- 如果用户修改了 Web 服务的端口号，请使用 http://ip_address:port 或 https://ip_address:*secure*-port 地址格式进入 HDM Web 登录界面，如：https://192.168.50.81:8080。
- HDM 支持单独关闭 Web 服务的非安全端口，如果关闭 Web 服务的非安全端口，会导致非加密模式的 H5 KVM 无法访问。
- 如果用户修改了 Remote_XDP 服务的端口号，同时需要修改 OpenIPC 客户端的端口号设置，修改位置：安装目录\OpenIPC\Config\SKX\ SKX_ASD_JTAG.xml。
- 修改服务配置后，该服务会自动重启。这个过程中，已活动的服务会话会断开，该服务在自动重启期间将短暂不可用。
- 开启iHDT服务前请先确认服务器处于开机状态。
- 不同机型支持的服务类型不完全一样，具体差异请以界面显示为准。

7.2 远程控制台

该功能用于登录远程控制台，通过远程控制台，可以远程连接到服务器完成配置管理服务器、安装操作系统等操作。

HDM 目前支持 KVM、H5 KVM 和 VNC 三种类型的远程控制台。本章节主要介绍如何使用 KVM、H5 KVM 远程控制台，以及如何修改 VNC 登录密码。

- 启动 KVM 远程控制台之前需要先配置环境，针对不同的操作系统，配置方法不完全一样。
- 启动 VNC 远程控制台之前需要先安装 VNC 客户端。
- H5 KVM 不需要配置环境，也不需要安装客户端。

7.2.1 Windows 系统下配置 KVM 环境

本章节主要介绍如何在 Windows 系统下配置 KVM 环境。

对于 Windows 系统，建议使用 Zulu OpenJDK 8 +IcedTea-Web 1.7.1 来运行 HDM KVM，您可以通过下列链接，选择对应版本及平台进行下载：

Zulu OpenJDK：https://www.azul.com/downloads/zulu/

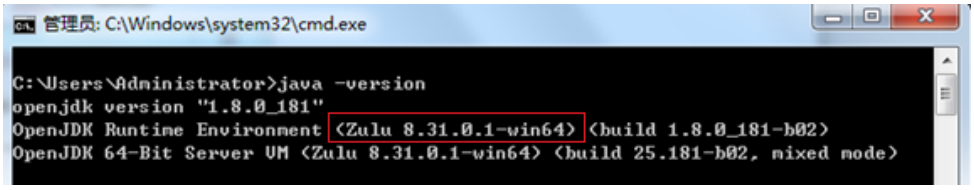
IcedTea-Web：http://icedtea.wildebeest.org/download/icedtea-web-binaries/

1. 安装 OpenJDK，配置 Java 环境

(1) 下载对应系统的 Zulu OpenJDK 版本的 msi 安装文件，使用默认设置直至安装完成。

(2) 验证已安装 OpenJDK 的版本，如图 7-4 所示。

图7-4 验证版本



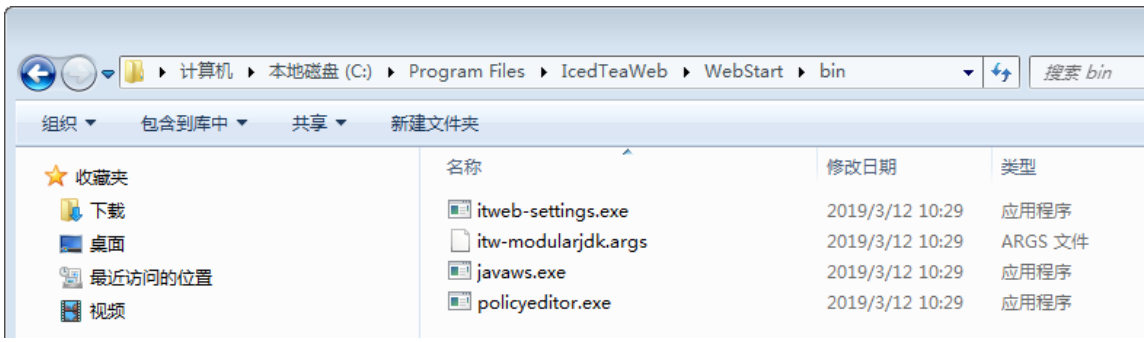
2. 安装 IcedTea-Web 插件

选择对应版本的 msi 安装文件，使用默认设置直至安装完成即可。

3. 运行 HDM KVM

(1) 进入 IcedTea-Web 的安装目录，例如：C:\Program Files\IcedTeaWeb\WebStart\bin，如图 7-5 所示。

图7-5 安装目录

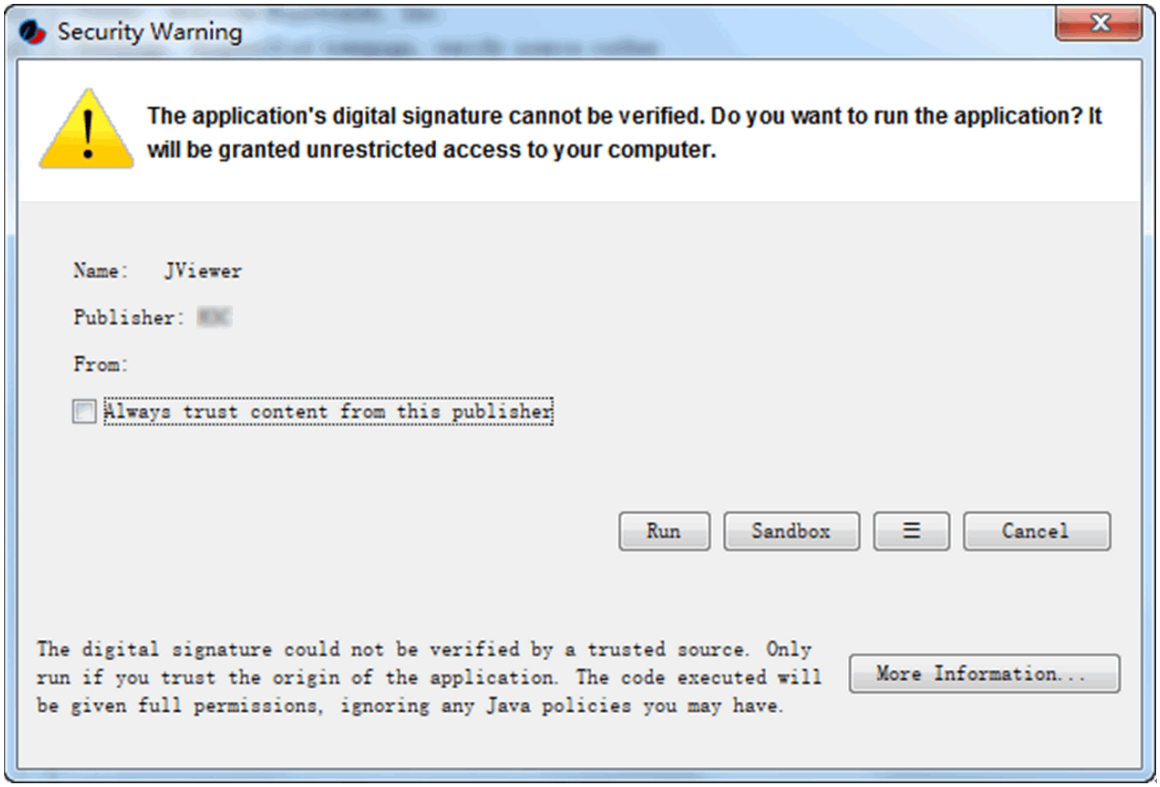


(2) 在此目录下，打开命令行窗口，并输入 javaws 命令和已下载的.jnlp 文件路径，如图 7-6 所示。

图7-6 命令窗口

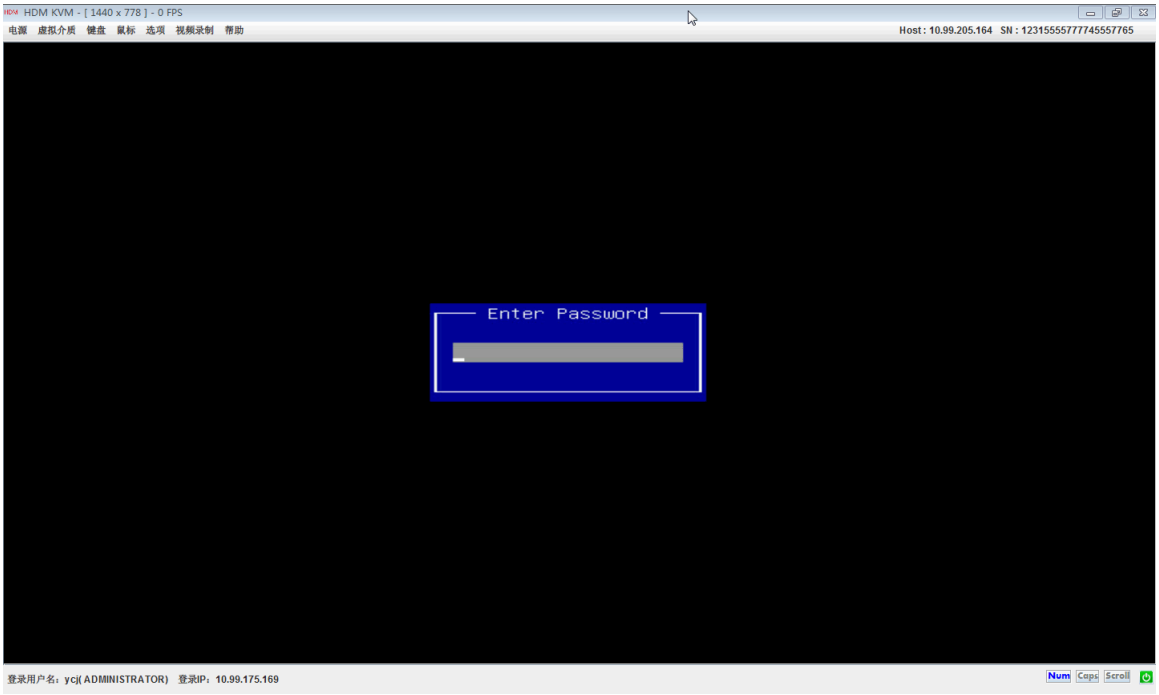
(3) 运行该命令后，在弹出窗口中单击<Run>按钮，如图 7-7 所示。

图7-7 Security Warning



(4) 连接 KVM 远程控制台成功，如图 7-8 所示。

图7-8 KVM



7.2.2 Linux 系统下配置 KVM 环境

本章节主要介绍如何在 Linux 系统下配置 KVM 环境。

对于 Linux 系统，建议使用 Zulu OpenJDK 8 +IcedTea-Web 来运行 HDM KVM，您可以通过下列链接，选择对应版本及平台进行下载：

Zulu OpenJDK：https://www.azul.com/downloads/zulu/

IcedTea-Web：http://icedtea.wildebeest.org/download/source/

1. 安装 IcedTea-Web 插件

可使用 yum install 命令进行安装，如图 7-9 所示。

图7-9 yum install 命令

```
[root@jys1235 ~]# yum install icedtea-web.x86_64
```

2. 安装 OpenJDK，配置 Java 环境

(1) 安装 Zulu OpenJDK：

直接下载对应平台以及对应版本的 rpm 安装包，使用 rpm –ivh xxx.rpm 命令进行安装或下载对应平台以及对应版本的 tar.gz 压缩包，解压至/usr/lib/jvm 目录，然后在/etc/profile 文件末尾追加以下命令，如图 7-10 所示。

图7-10 追加命令

```
export JAVA_HOME=/usr/lib/jvm/zulu8.31.0.1-jdk8.0.181-linux_x64
export PATH=$JAVA_HOME/bin:$PATH
export CLASSPATH=.:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib/tools.jar
```

(2) 验证是否安装成功，如图 7-11 所示。

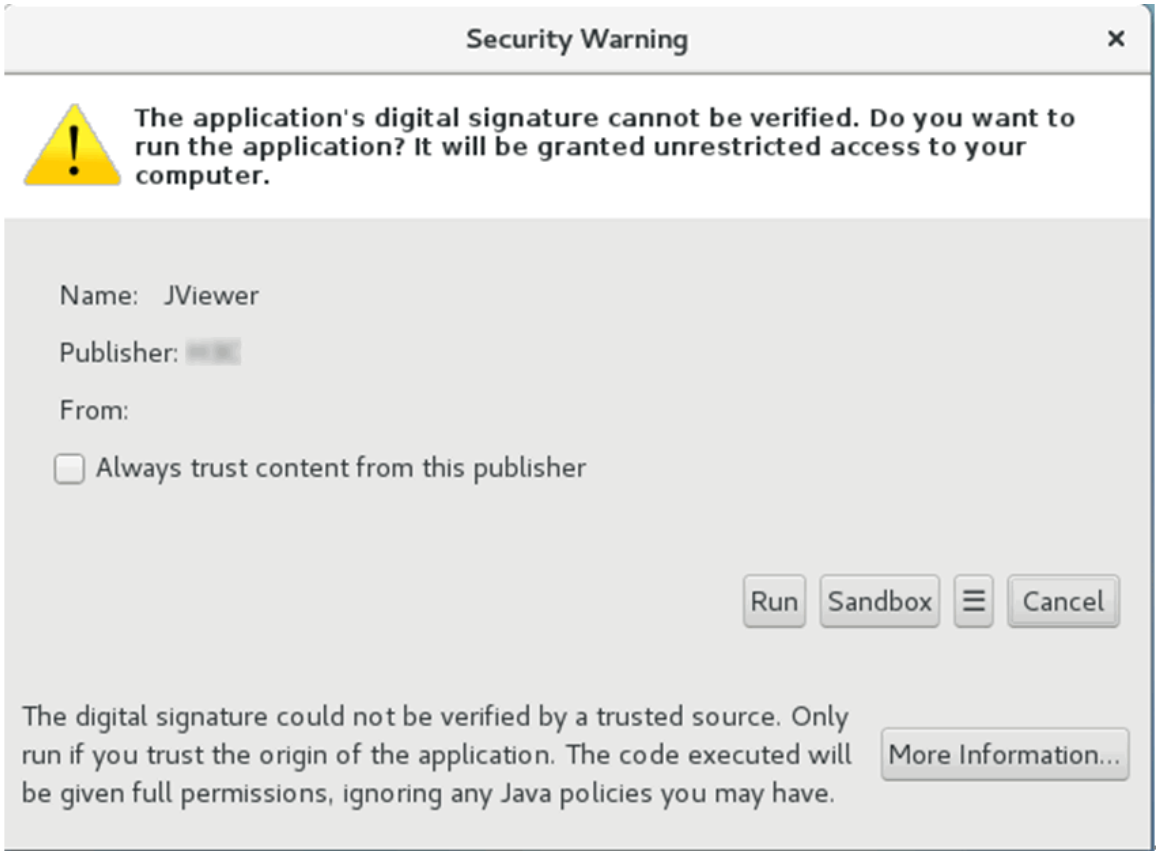
图7-11 安装成功

```
[root@jys1235 jvm]# java -version
openjdk version "1.8.0_181"
OpenJDK Runtime Environment (Zulu 8.31.0.1-linux64) (build 1.8.0_181-b02)
OpenJDK 64-Bit Server VM (Zulu 8.31.0.1-linux64) (build 25.181-b02, mixed mode)
[root@jys1235 jvm]#
```

3. 运行 HDM KVM

(1) 可直接双击下载下来的 KVM.jnlp 文件，并在弹出框中单击<Run>按钮，如图 7-12 所示。

图7-12 Security Warning



(2) 连接 KVM 远程控制台成功，如图 7-8 所示。

7.2.3 启动 KVM/H5 KVM 远程控制台

说明

- 本地 PC 访问服务器时，建议不要同时使用多个浏览器打开该服务器的远程控制台。
- 本地 PC 访问服务器时，建议不要同时使用 KVM 和 H5 KVM 打开服务器的远程控制台。

启动远程控制台前，请检查以下配置：

- 确认用户是否拥有远程控制权限，可通过[用户&安全/用户访问设置]菜单项修改用户权限。
- 必须先开启 KVM 服务才能使用 KVM 功能，H5 KVM 需同时开启 WEB 和 KVM 服务。可通过[远程服务/服务设置]菜单项开启 KVM 和 WEB 服务。

1. 操作步骤

(1) 单击[远程服务/远程控制台]菜单项，进入远程控制台页面，如图 7-13 所示。

图7-13 远程控制台

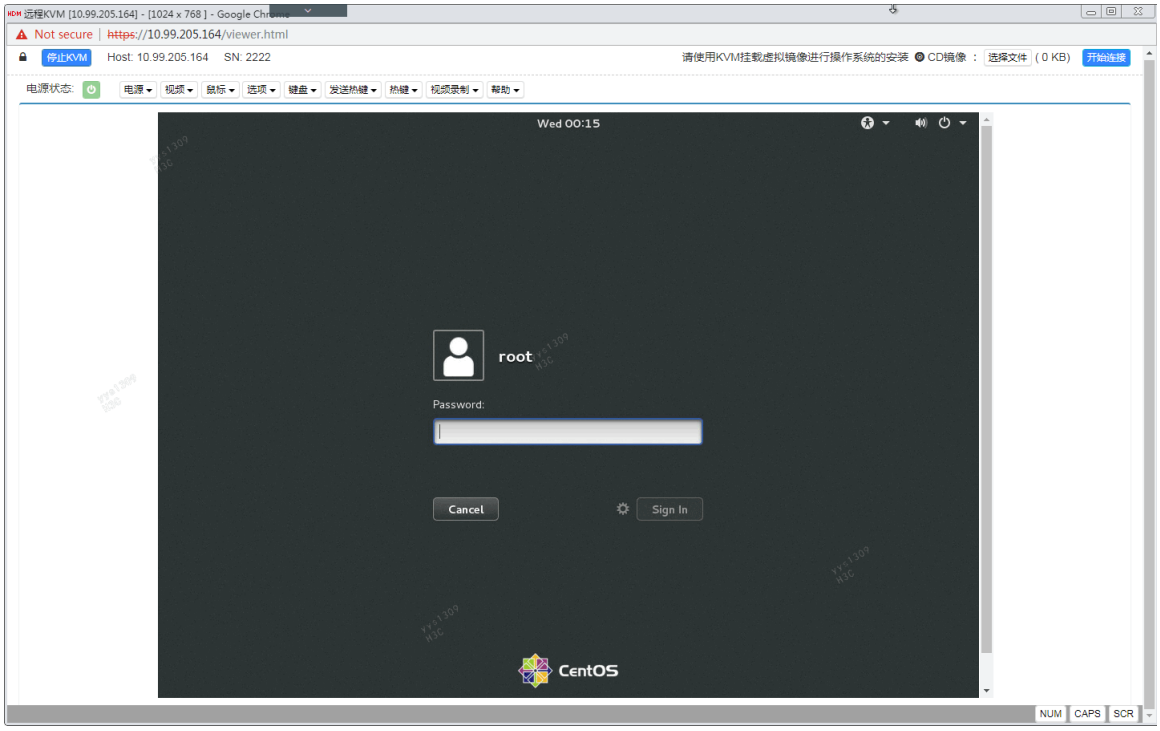
(2) （可选）单击<配置>按钮，在对话框中选择 KVM 和 H5 KVM 的启动模式。

(3) （可选）单击<确定>按钮，完成操作。

(4) 单击<启动 KVM>或<启动 H5 KVM>按钮，弹出远程控制台窗口，本文以 H5 KVM 为例。

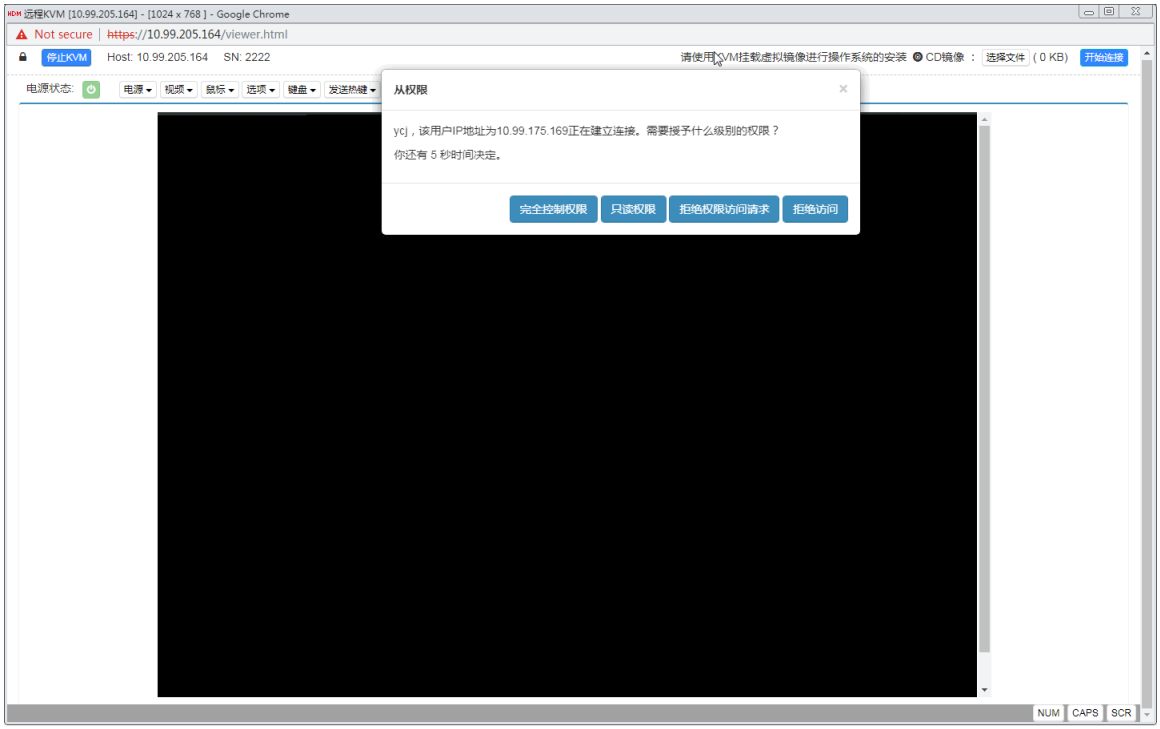
- H5 KVM 支持加密模式和非加密模式，两种模式在操作上没有任何差别，差别仅体现在数据安全性和传输速度上。
- 独占模式：
  - 若您直接启动了远程控制台，如图 7-14 所示。则说明您是当前唯一一个启动远程控制台的用户，您具有完全控制权限。
  - 如果其他用户已启动远程控制台，则您无法启动该远程控制台。

图7-14 主用户权限



- 共享模式：
  - 若您直接启动了远程控制台，如图 7-14 所示。则说明您是当前唯一一个启动远程控制台的用户（即主用户），您具有完全控制权限。当从用户向您申请权限时，您可能涉及以下操作，如图 7-15 所示：

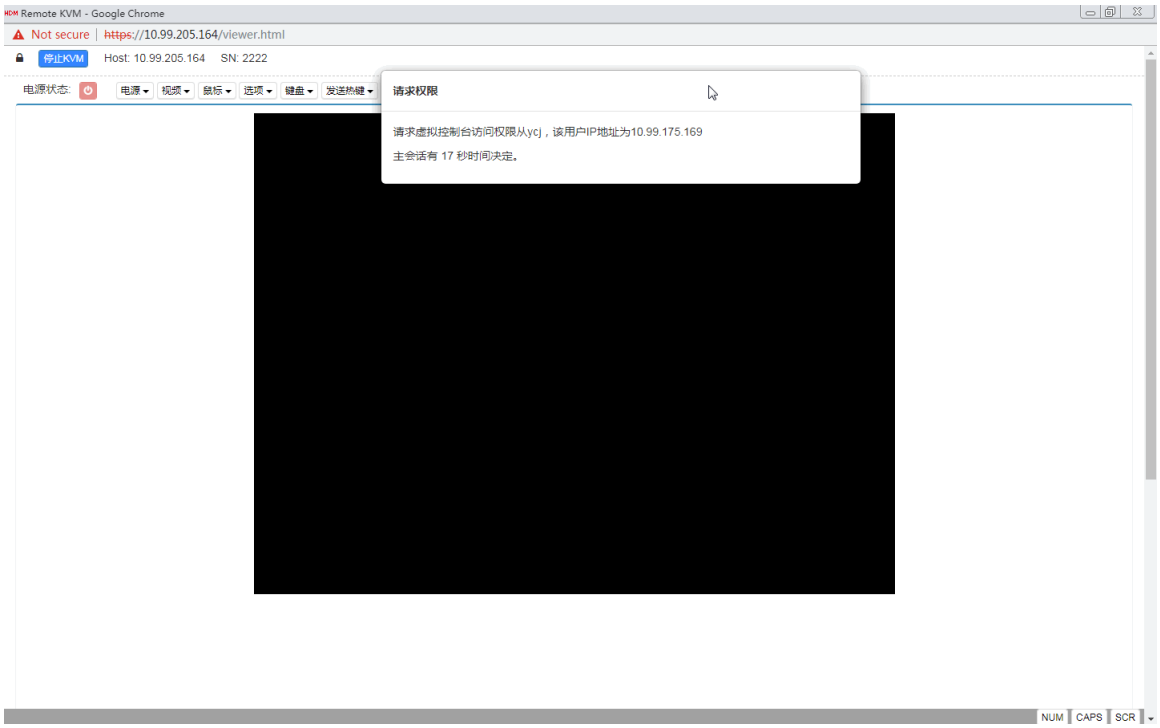
图7-15 从用户权限



- 从用户向您申请访问权限时，您可以在 30s 内授予或拒绝授予访问权限。如果您授予了从用户完全控制权限，则您拥有的访问权限变为只读权限。如果您在 30s 之内未进行授予权限操作，则默认授予从用户只读权限。
- 您在关闭远程控制台窗口时，可以把完全控制权限授予其他用户。如果您在 10s 内未将访问权限授予其他用户，其他用户拥有的访问权限保持不变。

○ 若您收到系统信息，提示您等待主用户授予您访问权限，则说明当前有其他用户在使用远程控制台，此时您是从用户，需要主用户授予您权限后才能使用远程控制台。您可能涉及以下操作，如图 7-16 所示：

图7-16 从用户请求权限



- 如果主用户授予您完全控制权限，此时，您既能查看远程控制台，又能操作远程控制台。
- 如果主用户授予您只读权限，此时，您只能查看远程控制台视频、截屏和视频录制操作，但不能进行任何控制操作。
- 如果主用户拒绝了您的访问权限，系统会关闭 KVM 窗口，您需要重新启动远程控制台，申请访问权限。
- 如果主用户在 30s 内未选择授予您的访问权限，您将被授予只读权限。

2. 参数说明

- 独占模式：仅支持 1 个远程控制台会话，且拥有完全控制权限。
- 共享模式：支持多个（1 主 N 从）远程控制台会话，只有主用户拥有完全控制权限。
- 加密模式：信息在客户端和服务器之间加密传输，以使他人无法查看或修改在网络上传送的数据。优点是数据传输安全性高。
- 非加密模式：信息在客户端和服务器之间不加密传输。优点是数据传输速度较快。KVM 当前仅支持非加密模式。
- 完全控制权限：具有该权限的用户，既能查看远程控制台界面，又能操作远程控制台。
- 只读权限：具有该权限的用户，只能查看远程控制台视频、进行截屏和视频录制操作，但不能进行任何控制操作。

3. 注意事项

- 远程控制台最多支持 4 个会话。
- 远程控制台处于活动状态时，UID 灯将闪烁。

7.2.4 使用 KVM 远程控制台

启动 KVM 远程控制台后，您可以通过远程控制台进行如下常用操作：

- 访问服务器：通过本功能，可以使用本地 PC 的键盘、鼠标和显示器访问服务器的 BIOS 和操作系统，实现对服务器的远程控制。
- 电源控制：通过本功能，可以在远程控制台界面开启或关闭服务器电源。
- 捕获画面：通过本功能，可以快速捕获远程控制台的当前画面。
- 录制视频：通过本功能，可以对远程控制台界面进行录像，并将录制的视频保存到本地。
- 使用虚拟媒体：通过本功能，可以在远程控制台上挂载虚拟介质，用于安装操作系统或传输文件。安装操作系统过程中请勿执行重启 HDM、更新 HDM 或电源管理操作。

1. 电源控制操作步骤

单击电源菜单，执行电源操作，各菜单项和电源图标的含义请参见下表所示。

表7-3 电源菜单项介绍

菜单项	含义
立即重启	强制重启服务器。此过程不会断开服务器的电源
强制关机	立即强制关闭服务器，此操作与长按服务器前面板上的电源按钮5秒以上效果相同。此过程中会断开服务器电源
正常关机	正常关闭服务器，即先关闭操作系统，再关闭电源。此过程中会断开服务器电源
开机	正常启动服务器
关机并重新开机	关机并重新开机，此过程中会断开服务器电源

表7-4 电源图标

菜单项	含义
	表示服务器电源开启
	表示服务器电源关闭

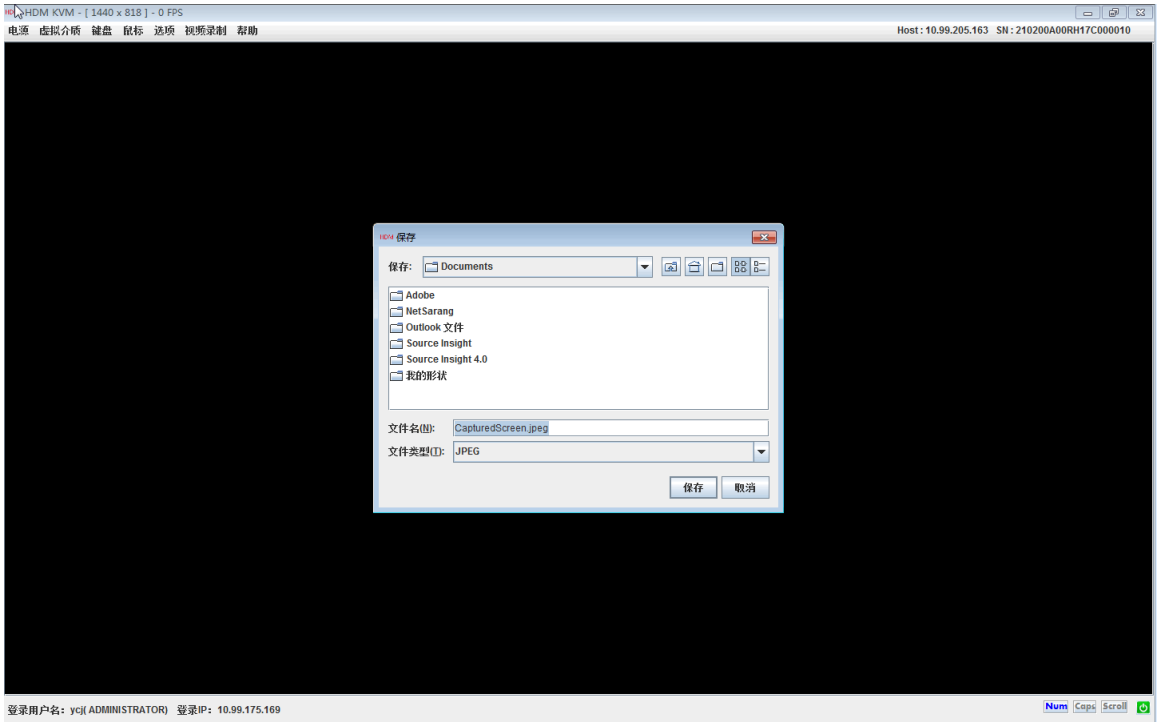
2. 捕获画面操作步骤

(1) 单击远程控制台[选项/截屏]菜单项，弹出保存对话框，如图 7-17 所示。

(2) 选择文件保存路径，输入文件名。

(3) 单击<保存>按钮，完成操作。

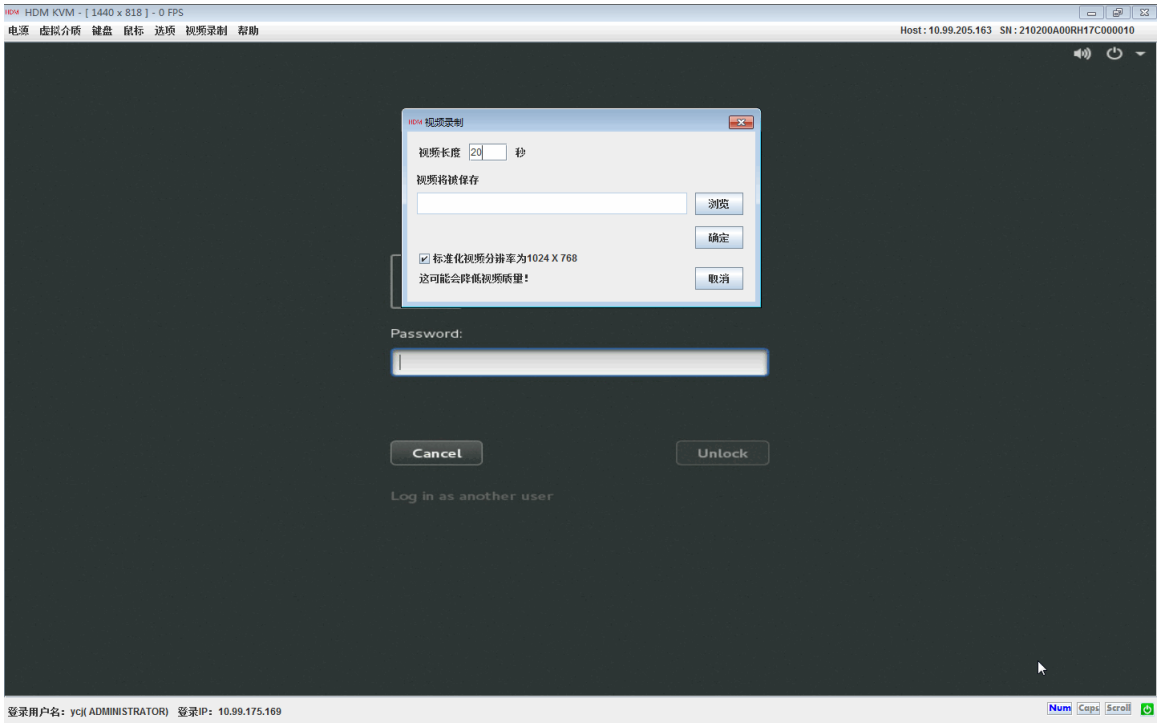
图7-17 截屏



3. 录制视频操作步骤

(1) 单击远程控制台[视频录制/设置]菜单项，在弹出的录像设置对话框中设置参数，如图 7-18 所示，完成录制视频设置。

图7-18 视频录制/设置



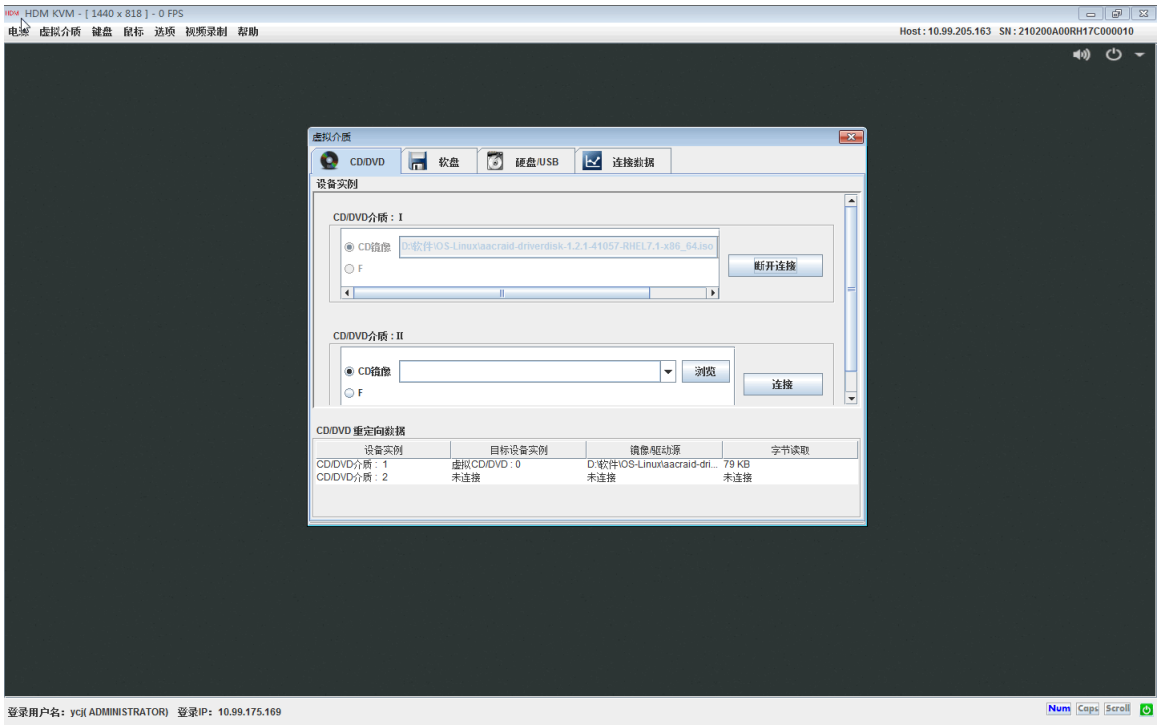
(2) 单击[视频录制/开始录制]菜单项，开始录制视频。

(3) 单击[视频录制/停止录制]菜单项，结束录制视频。

4. 挂载虚拟媒体操作步骤

(1) 单击远程控制台[虚拟介质/虚拟介质向导]菜单项，弹出对话框，如图 7-19 所示。

图7-19 虚拟介质向导



(2) HDM 支持软盘、CD/DVD、硬盘/USB 设备三种虚拟媒体，执行以下操作完成虚拟介质挂载。

- 在 CD 栏单击<浏览>按钮，选择客户端计算机上的 CD/DVD 文件或本地光驱，单击<连接>按钮完成虚拟 CD/DVD 挂载。
- 在软盘栏单击<浏览>按钮选择客户端计算机上的软盘文件，单击<连接>按钮完成虚拟软盘挂载。
- 在硬盘/USB 栏单击<浏览>按钮，选择客户端计算机上的磁盘文件或本地 USB 设备，单击<连接>按钮完成虚拟硬盘/USB 设备挂载。
- 在文件夹路径栏单击<浏览>按钮，选择客户端计算机上的需要挂载的文件夹(不要超过600M)，在镜像路径栏单击<浏览>按钮，选择<浏览>按钮，选择客户端计算机上的需要制作成镜像文件的存放路径，点击<连接>按钮完成文件夹的挂载。注意文件夹路径与镜像的路径不能相同。

(3) 挂载成功后，如果要取消挂载，选中要取消挂载的文件所在的栏，单击<断开连接>按钮。

5. 退出 KVM 操作步骤

单击右上角的  按钮，关闭远程控制台。

- 如果在 HDM 界面点击“退出登录”按钮确认登出，KVM 也将会退出。
- 如果通过远程控制台挂载了虚拟介质，则在[远程服务/服务设置]中配置的 KVM 超时时间不会生效。

6. 参数说明

远程控制台包括以下菜单项。各菜单项的功能如下表所示。

表7-5 虚拟介质菜单项介绍

菜单项	含义
虚拟介质向导	选中此菜单项，可在弹出的对话框中配置虚拟媒体。支持CD/DVD、软盘、硬盘/USB设备三种虚拟媒体

表7-6 键盘菜单项介绍

菜单项	含义
Ctrl+Alt+Del	选中此菜单项，等同于同时按键盘的<Ctrl>键、<Alt>键和<Delete>键
热键	您可在此菜单项定义热键，并使用热键。最多可支持20个热键，且每个热键最多支持6个键的组合
软键盘	打开软键盘，仅支持英语（美式）软键盘

表7-7 鼠标菜单项介绍

菜单项	含义
显示光标	• 选中此菜单项，远程控制台显示客户端中的鼠标轨迹 • 取消选中此菜单项，远程控制台隐藏客户端中的鼠标轨迹
鼠标校准	选择此菜单项用于校准相对模式下鼠标的位置
鼠标模式	• 鼠标模式用于计算鼠标的当前位置，包括： o 绝对鼠标模式：绝对模式，根据桌面的绝对坐标来计算鼠标位置 o 相对鼠标模式：相对模式，根据鼠标移动的偏移量来计算鼠标的位置 o 其他鼠标模式：其他模式，根据离桌面中心的距离来计算鼠标的位置 • 以下为常见操作系统推荐的鼠标模式，其他操作系统推荐使用绝对鼠标模式： o 绝对鼠标模式：Windows 2008、Windows 2012、Redhat 6.5、Redhat 7.0、CentOS 6.5、CentOS 7.1、Ubuntu 12.04、Ubuntu 15.04、SLES 11、SLES 13 o 相对鼠标模式：低于 Redhat 6、CentOS 6、Fedora 14 版本的操作系统 o 其他鼠标模式：SLES 11 操作系统的安装界面 注意： • 不建议频繁变更鼠标模式 • 从其他鼠标模式或相对鼠标模式切换到绝对鼠标模式后，会自动启用显示光标功能

表7-8 选项菜单项介绍

菜单项	含义
截屏	捕获画面
界面语言	设置远程控制台的语言
拒绝权限访问请求	拒绝权限访问请求。仅主用户可以选择此选项，选中后，从用户无法提出权限申请

菜单项	含义
CD/DVD加速	• 当网络中只有千兆以上交换机或路由器时，通过共享网口挂载 CD 虚拟镜像并安装操作系统时，勾选此选项可以启用加速安装操作系统功能 • 其他类型的网络环境不推荐使用此功能 • 此选项是否显示和服务器配置有关
BIOS启动项设置	配置服务器的下一次启动模式以及启动设备，具体步骤请参见系统启动项。
BIOS启动顺序设置	配置服务器的启动模式和启动顺序，具体步骤请参见系统启动项，仅G5系列服务器支持本功能。

表7-9 视频录制菜单项介绍

菜单项	含义
开始录制	开始录制视频
停止录制	停止录制视频
设置	录像设置，可设置视频最长的可录制时间、录制视频的保存路径和分辨率

表7-10 帮助菜单项介绍

菜单项	含义
关于 HDM KVM	选中此菜单项，显示HDM KVM的版本和版权信息

表7-11 其它

菜单项	含义
Num	等同于启用了键盘的<NUM>键
Caps	等同于启用了键盘的<CAPS>键
Scroll	等同于启用了键盘的<Scroll>键

7.2.5 使用 H5 KVM 远程控制台

启动 H5 KVM 远程控制台后，您可以通过远程控制台进行如下常用操作：

- 访问服务器：通过本功能，可以使用本地 PC 的键盘、鼠标和显示器访问服务器的 BIOS 和操作系统，实现对服务器的远程控制。
- 电源控制：通过本功能，可以在远程控制台界面开启或关闭服务器电源。
- 捕获画面：通过本功能，可以快速捕获远程控制台的当前画面。
- 录制视频：通过本功能，可以对远程控制台界面进行录像，并将录制的视频保存到本地。
- 使用虚拟媒体：通过本功能，可以在远程控制台上挂载虚拟介质（仅支持挂载.iso 镜像），用于安装操作系统或传输文件。安装操作系统过程中请勿执行重启 HDM、更新 HDM 或电源管理操作。

1. 电源控制操作步骤

单击电源菜单，执行电源操作，各菜单项和电源图标的含义请参见下表所示。

表7-12 电源菜单项介绍

菜单项	含义
立即重启	强制重启服务器。此过程不会断开服务器的电源
强制关机	立即强制关闭服务器，此操作与长按服务器前面板上的开机/待机按钮5秒以上效果相同。此过程中会断开服务器电源
正常关机	正常关闭服务器，即先关闭操作系统，再关闭电源。此过程中会断开服务器电源
开机	正常启动服务器
关机并重新开机	关机并重新开机，此过程中会断开服务器电源

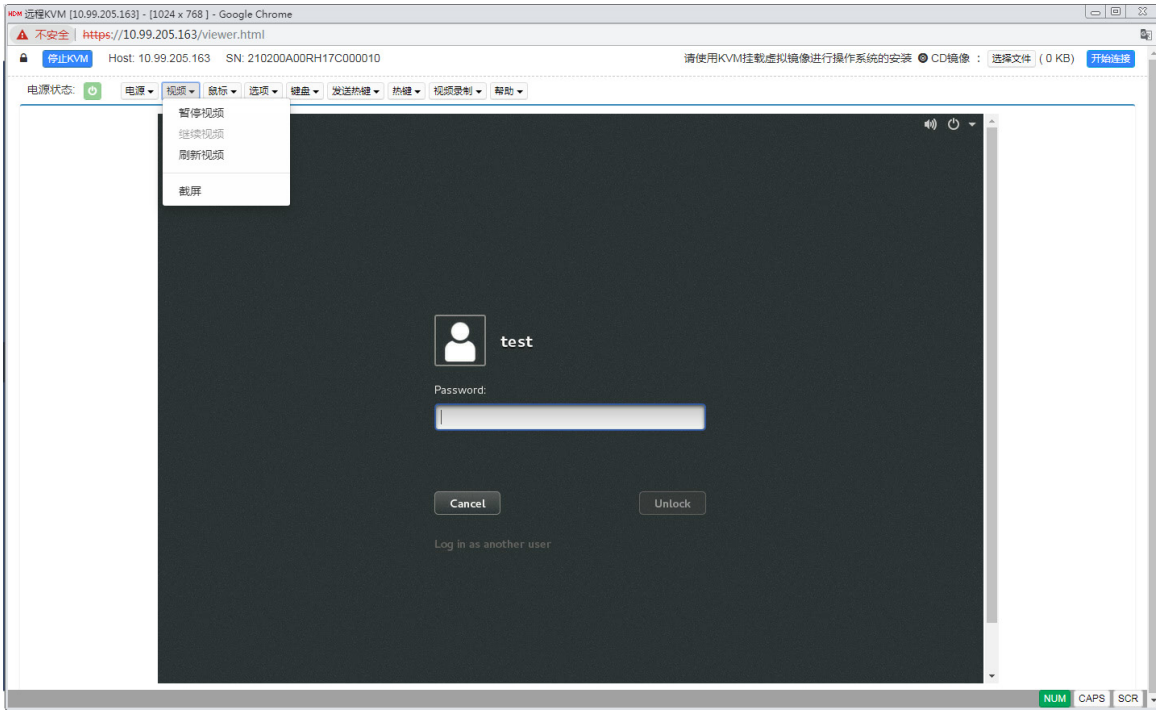
表7-13 电源图标

菜单项	含义
	表示服务器电源开启
	表示服务器电源关闭

2. 捕获画面操作步骤

单击远程控制台[视频/截屏]菜单项，完成使用远程控制台捕获画面操作，如图 7-20 所示。

图7-20 截屏



3. 录制视频操作步骤

单击远程控制台[视频录制/录制设置]菜单项，如图 7-21 所示，在弹出的录像设置对话框中设置参数，完成录制视频设置，如图 7-22 所示。

图7-21 录制视频

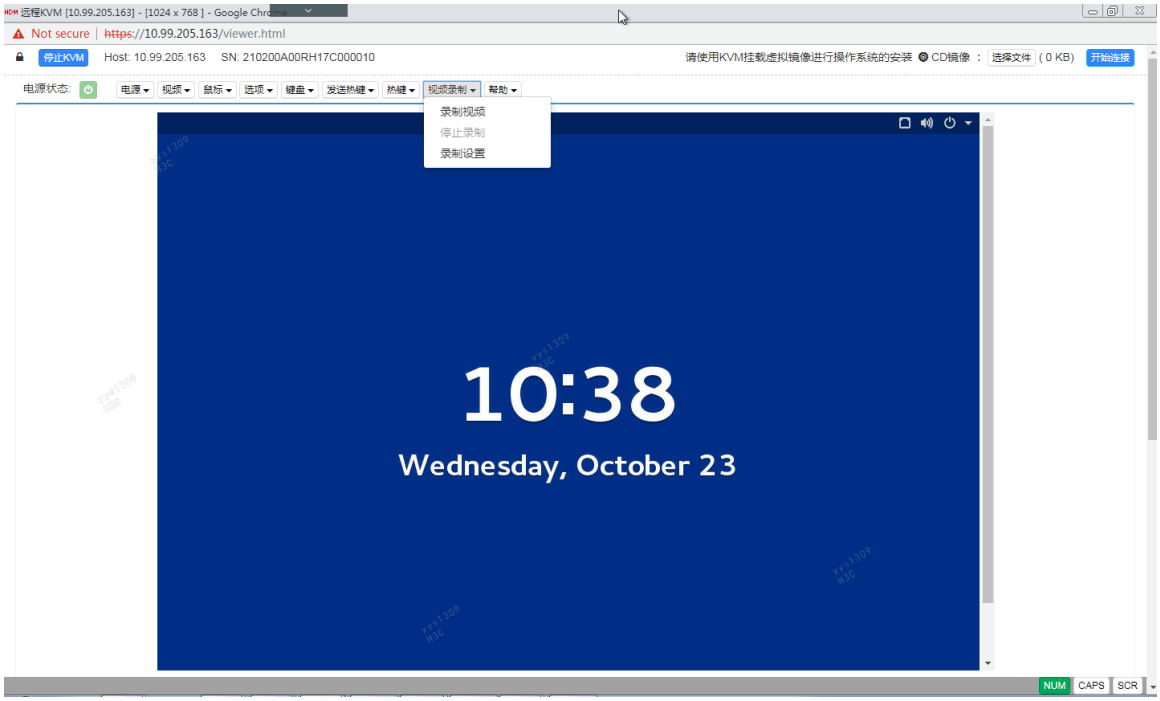
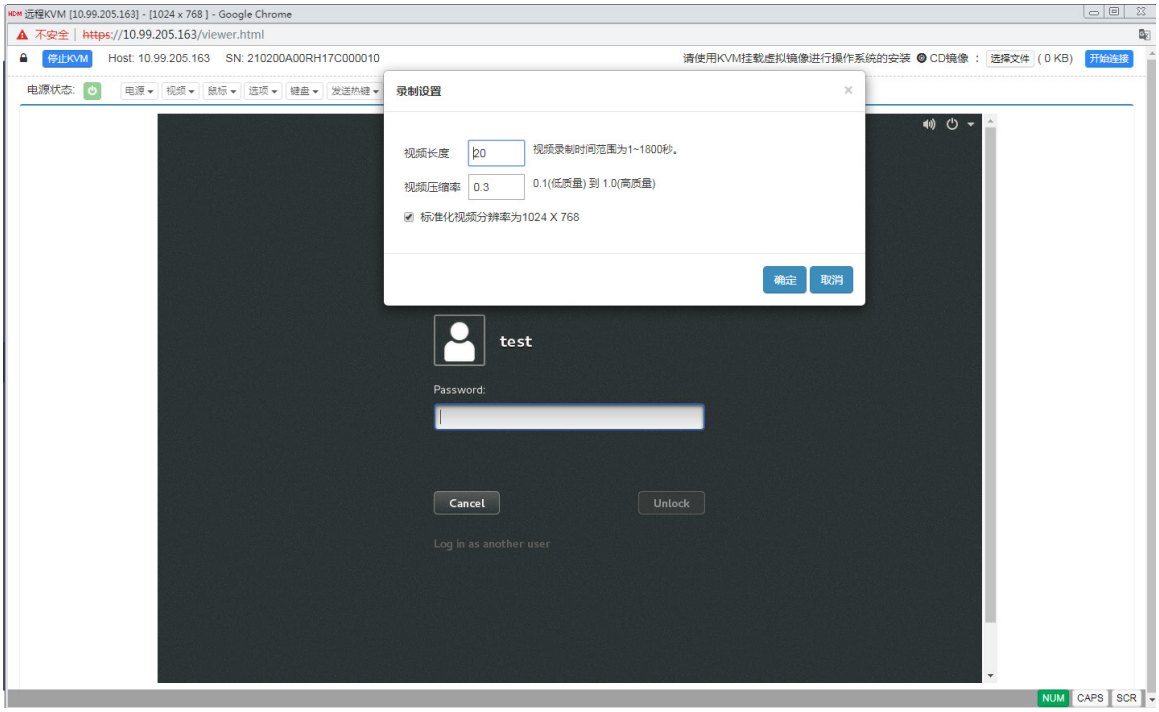


图7-22 录制设置



(2) 单击[视频录制/录制视频]菜单项，开始录制视频。

(3) 单击[视频录制/停止录制]菜单项，结束录制视频。

4. 挂载虚拟媒体操作步骤

(1) 单击远程控制台右上方<选择文件>按钮，弹出虚拟媒体对话框。H5 KVM 仅支持挂载.iso 镜像。

(2) （可选）挂载成功后，自动开始连接。如果要取消挂载，选中要取消挂载的文件所在的栏，单击<断开连接>按钮。

5. 退出 H5 KVM 操作步骤

退出 H5 KVM 远程控制台时，建议单击控制台左上角<停止 KVM>按钮。

- 如果在 HDM 界面点击“退出登录”按钮确认登出，H5 KVM 也将会退出。
- 如果通过远程控制台挂载了虚拟介质，则在[远程服务/服务设置]中配置的 KVM 超时时间不会生效。

6. 参数说明

远程控制台包括以下菜单项。各菜单项的功能如下表所示。

表7-14 视频菜单项介绍

菜单项	含义
暂停视频	暂停视频播放
继续视频	恢复视频播放
刷新视频	刷新远程控制台中的视频显示
截屏	捕获视频画面

表7-15 鼠标菜单项介绍

菜单项	含义
显示客户端光标	• 选中此菜单项，远程控制台显示客户端的鼠标轨迹 • 取消选中此菜单项，远程控制台隐藏客户端的鼠标轨迹
鼠标模式	• 鼠标模式用于计算鼠标的当前位置，H5 KVM 包括： o 绝对鼠标模式：绝对模式，根据桌面的绝对坐标来计算鼠标位置 o 其他鼠标模式：其他模式，根据离桌面中心的距离来计算鼠标的位置 • 以下为常见操作系统推荐的鼠标模式，其他操作系统推荐使用绝对鼠标模式： o Windows 2008、Windows 2012、Redhat 6.5、Redhat 7.0、CentOS 6.5、CentOS 7.1、Ubuntu 12.04、Ubuntu 15.04、SLES 11、SLES 13 等操作系统，推荐使用绝对鼠标模式 o 低于 Redhat 6、CentOS 6、Fedora 14 版本的操作系统，推荐使用 KVM，并使用其中的相对鼠标模式 o SLES 11 操作系统的安装界面，推荐使用 KVM，并使用其中的其他鼠标模式 注意： • 不建议频繁变更鼠标模式 • 从其他鼠标模式切换到绝对鼠标模式后，会自动启用显示客户端光标功能

表7-16 选项菜单项介绍

菜单项	含义
拒绝权限访问申请	拒绝从用户权限申请
中文	设置远程控制台的语言为中文
English	设置远程控制台的语言为英文
CD/DVD加速	• 当网络中只有千兆以上交换机或路由器时，通过共享网口挂载 CD 虚拟镜像并安装操作系统时，勾选此选项可以启用加速安装操作系统功能。 • 其他类型的网络环境不推荐使用此功能。 • 此选项是否显示和服务器配置有关。
BIOS启动项设置	配置服务器的下一次启动模式以及启动设备，具体步骤请参见系统启动项。
BIOS启动顺序设置	配置服务器的启动模式和启动顺序，具体步骤请参见系统启动项，仅G5系列服务器支持本功能。

表7-17 键盘菜单项介绍

菜单项	含义
美式英语	使用英语语言的键盘布局

表7-18 发送热键菜单项介绍

菜单项	含义
按住栏	
右Ctrl键	选中此菜单项，等同于按住键盘右侧的<Ctrl>键
右Alt键	选中此菜单项，等同于按住键盘右侧的<Alt>键
右Windows键	选中此菜单项，等同于按住键盘右侧的<WIN>键
左Ctrl键	选中此菜单项，等同于按住键盘左侧的<Ctrl>键
左Alt键	选中此菜单项，等同于按住键盘左侧的<Alt>键
左Windows键	选中此菜单项，等同于按住键盘左侧的<WIN>键
按下并松开栏	
Ctrl+Alt+Del	选中此菜单项，等同于同时按键盘的<Ctrl>键、<Alt>键和<Delete>键
左 Windows 键	选中此菜单项，等同于按下后释放键盘左侧的<WIN>键
右 Windows 键	选中此菜单项，等同于按下后释放键盘右侧的<WIN>键
上下文菜单键	选中此菜单项，等同于按下后释放键盘上下文键
Print Screen 键	选中此菜单项，等同于按下后释放截屏键

表7-19 热键菜单项介绍

菜单项	含义
添加热键	您可在此菜单项定义热键，并使用热键

表7-20 视频录制菜单项介绍

菜单项	含义
录制视频	开始录制视频
停止录制	停止录制视频
录制设置	录像设置，可设置视频最长的可录制时间和视频压缩率 • 视频长度：范围为 1～1800 秒 • 视频压缩率：视频压缩率：压缩后的视频大小和原视频大小的比值，范围为 0.1～1

表7-21 其它

菜单项	含义
Num	等同于启用了键盘的<NUM>键
Caps	等同于启用了键盘的<CAPS>键
Scroll	等同于启用了键盘的<Scroll>键

表7-22 帮助菜单项介绍

菜单项	含义
关于 H5 Viewer	选中此菜单项，显示H5 Viewer的版权和版本信息

7.2.6 启动 VNC 远程控制台

VNC（Virtual Network Console，虚拟网络控制台）用于传送服务端的原始图像到客户端，该协议提供一种不用登录 HDM 即可访问控制服务器的方法，即用本地主机的显示器和输入设备远程控制服务器。HDM 支持 IPv4、IPv6 VNC 会话，丰富了远程控制操作接口，为用户提供更为灵活的远程控制方式。

VNC 系统由客户端，服务端和 RFB 协议组成：

- VNC 服务端即 VNC Server：服务端在 HDM 端运行，用于接受客户端连接，然后向客户端发送屏幕图像，响应客户端的输入操作。
- VNC 客户端即 VNC Viewer（PC 端本地应用程序）：客户端用于远程连接服务器，然后通过本地的显示器和输入设备与服务器交互。

- RFB 协议：RFB（Remote Frame Buffer 远程帧缓冲）协议是一个用于远程访问图形用户界面的简单协议。由于 RFB 协议工作在帧缓冲层，因此它适用于所有的窗口系统和应用程序，如 Windows 和 Mac 等。

HDM 同时最多支持 2 个 VNC 会话，且支持两种会话模式，会话模式是由客户端选项决定。

- 共享模式：支持打开 2 个 VNC 会话，2 个 VNC 会话均有权限控制鼠标和键盘，可控制 OS。
- 独占模式：支持打开 1 个 VNC 会话。

启动 VNC 远程控制台前，请检查以下配置：

- 必须先开启 VNC 服务才能使用 VNC 功能。可通过[远程服务/服务设置]菜单项开启 VNC 服务。
- 使用 VNC 功能前请先下载并安装 VNC 客户端，如 TightVNC 等。

1. 操作步骤

(1) 打开 VNC 客户端，如图 7-23 所示，输入 HDM 管理 IP 地址，单击<Connect>按钮，进入登录页面，如图 7-24 所示。

图7-23 VNC 客户端（以 TightVNC 为例）

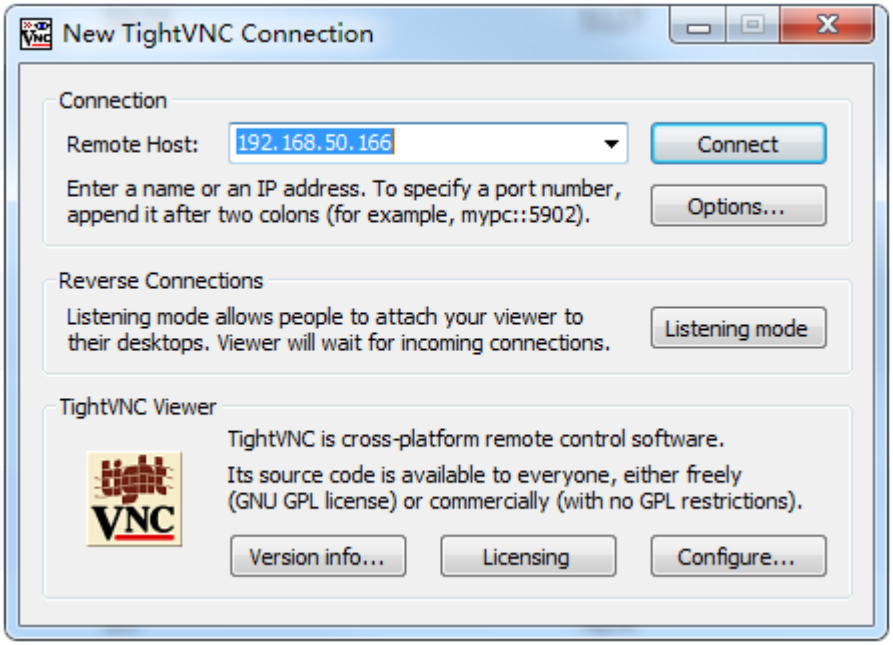
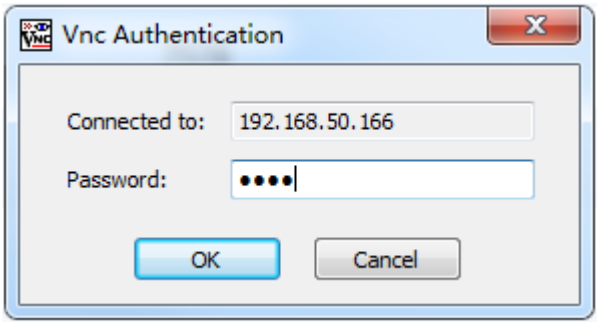
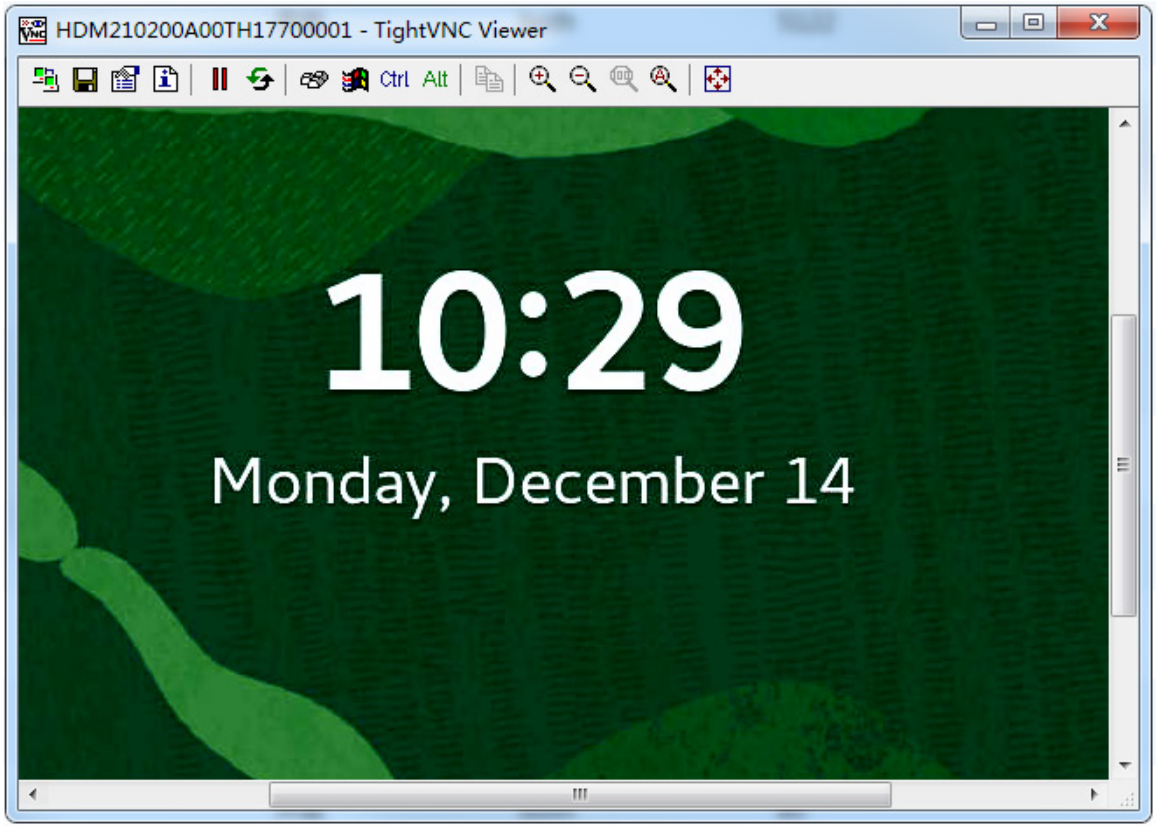


图7-24 登录页面



(2) 输入 VNC 密码（缺省为 root），连接 VNC 远程控制台，如图 7-25 所示。

图7-25 VNC 远程控制台



(3) 成功建立 VNC 会话后，可以在[远程服务/服务设置]查看到会话类型为 VNC， IP 地址为客户端 IP，如图 7-26 所示。

图7-26 会话信息

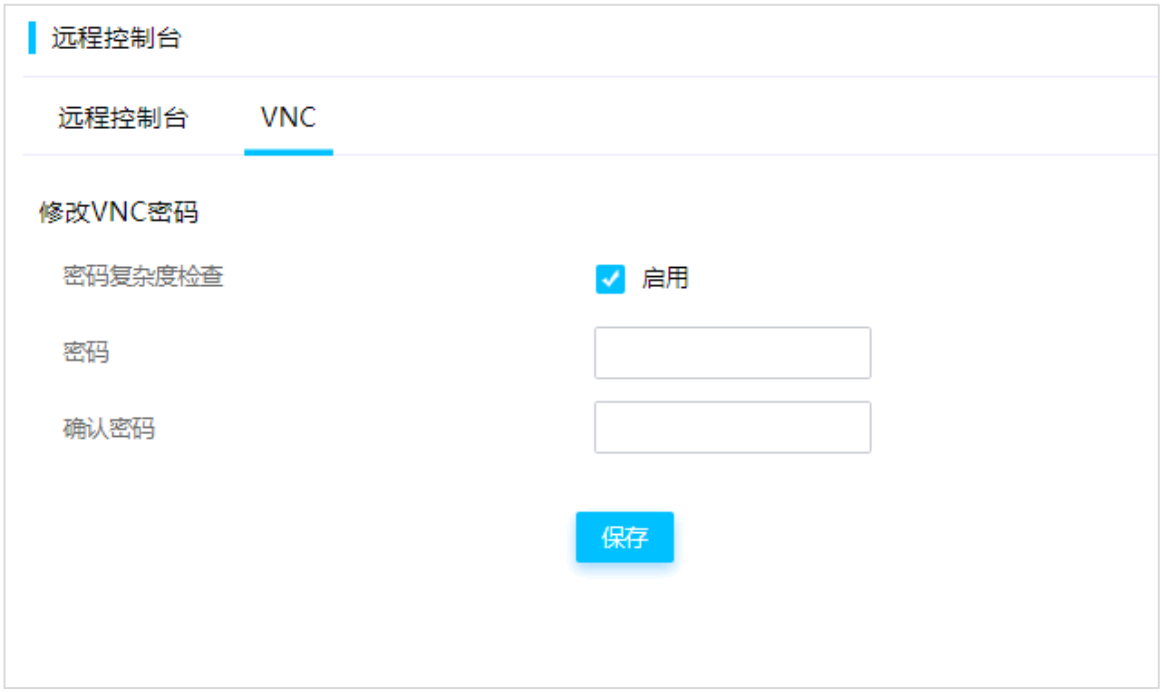
7.2.7 VNC 密码管理

VNC 密码管理用于 VNC 客户端登录。通过本功能可以设置密码复杂度，并可以修改 VNC 客户端登录密码。缺省 VNC 密码为 root。

1. 操作步骤

(1) 单击[远程服务/远程控制台]菜单项，选择“VNC”页签，进入 VNC 页面，如图 7-27 所示。

图7-27 VNC 密码管理



(2) 选择是否开启密码复杂度检查。

(3) 输入修改后的密码和确认密码。

(4) 单击<保存>按钮，完成操作。

2. 参数说明

- 密码复杂度检查：选择关闭或开启密码复杂度检查功能。
  - 关闭该功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。
    - 密码长度为 1～8 个字符；
    - 仅支持字母、数字、空格和特殊字符`~!@#$%^&*()_+-=[]\{}|;':",./<>?，区分大小写。
  - 开启该功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。
    - 密码长度为 8 个字符，仅支持字母、数字、空格和特殊字符 `~!@#$%^&*()_+-=[]\{}|;':",./<>?，区分大小写；
    - 至少包含大写字母、小写字母和数字中的两种字符；
    - 至少包含一个空格或特殊字符；

7.3 虚拟媒体

通过本功能可以把远程服务器上的镜像文件挂载至服务器操作系统。完成镜像挂载后，用户可以在服务器操作系统中发现挂载的镜像文件。

7.3.1 启用远程媒体功能

1. 配置限制和指导

- 使用远程媒体挂载时，必须在[远程服务/服务设置]中启用相应的虚拟媒体服务，比如：CD-Media（CD/DVD）、FD-Media（软盘）和 HD-Media（硬盘）。
- 通过远程控制台或镜像挂载功能挂载镜像文件时，CD/DVD 和硬盘类型支持挂载两个镜像文件，软盘媒体类型支持挂载一个镜像文件。
- CD/DVD 镜像文件必须是.iso 格式。
- Floppy、Hard disk 镜像文件是.img 或.ima 格式，且 Floppy 文件大小不能超过 1.44MB。
- 请检查并确保 NFS 或 CIFS 服务器源路径中 CD-Media（CD/DVD）、FD-Media（软盘）和 HD-Media（硬盘）三种类型的镜像文件数量都不超过 60 个。

2. 操作步骤

(1) 配置远程镜像挂载服务，请参见 11.1 虚拟媒体配置。

(2) 单击[远程服务/虚拟媒体]菜单项，进入虚拟媒体页面，如图 7-28 所示。

图7-28 远程镜像挂载

(3) 单击<高级设置>按钮，在对话框中开启远程媒体支持的功能，如图 7-29 所示。

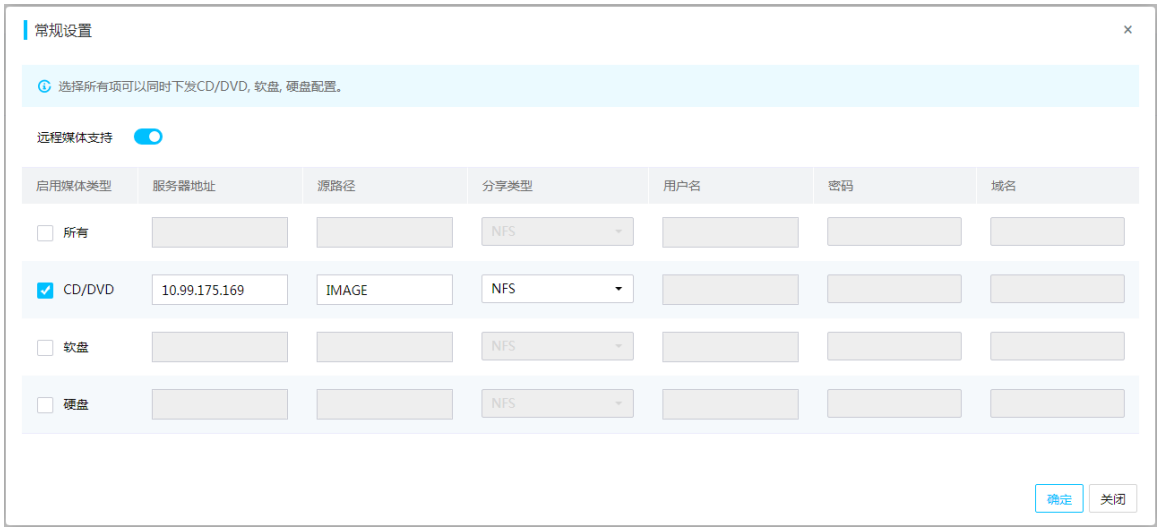
(4) 勾选启用媒体类型（CD/DVD、软盘、硬盘、所有），显示相对应的介质设置。

(5) 输入介质设置信息，请尽量避免使用特殊字符（如#等），否则可能会导致挂载失败。

- 如果分享类型选择 NFS，需输入服务器地址、源路径两项信息。
- 如果分享类型选择 CIFS（Samba），需输入服务器地址、源路径、用户名、密码和域名，其中域名为可选信息。

(6) 单击<确定>按钮，完成操作。

图7-29 高级设置



7.3.2 停用远程媒体功能

1. 操作步骤

(1) 单击[远程服务/虚拟媒体]菜单项，进入镜像挂载页面，如图 7-28 所示。

(2) 单击<高级设置>按钮，弹出常规设置对话框，如图 7-29 所示。

(3) 在对话框勾选远程媒体支持的<关闭>按钮。

(4) 单击<确定>按钮，完成操作。

2. 注意事项

如果已经启动镜像挂载，修改高级设置时，请确保所有的镜像挂载已停止。

7.3.3 挂载远程媒体

通过本功能可以将远程设备上的镜像文件挂载至服务器操作系统。

1. 操作步骤

(1) 单击[远程服务/虚拟媒体]菜单项，进入远程镜像挂载页面，如图 7-30 所示。

(2) 在远程媒体列表选择一个镜像文件，单击<开始>或<结束>按钮完成操作。

图7-30 远程镜像挂载

2. 参数说明

- 媒体类型：远程镜像文件的类型，包括：CD/DVD、软盘和硬盘三种类型。
- 状态：远程镜像文件挂载过程状态，包括：未启动和已启动。其中常见的停止状态包含以下情况：
  - 未启动-无法打开：表示使用非法的镜像文件。
  - 未启动-在使用连接：表示挂载会话数目已超上限。
  - 未启动-连接丢失：表示虚拟媒体服务已失效。
  - 未启动-无法连接：表示对应的虚拟媒体服务未开启。
  - 未启动-会话终止：表示对应的虚拟媒体会话已终止。
- 会话索引：服务器远程媒体挂载所挂载类型的会话索引。

3. 注意事项

只有拥有 Administrator、Operator 或者远程媒体权限的用户可以启动挂载。

7.4 SNMP

SNMP（Simple Network Management Protocol，简单网络管理协议）广泛用于网络设备的远程管理和操作。SNMP 允许管理员通过 NMS 对网络上不同厂商、不同物理特性、采用不同互联技术的设备进行管理，包括状态监控、数据采集和故障处理。

通过本功能可以设置 SNMP 的信息，包括选择 SNMP 版本、只读团体名和读写团体名。

1. 操作步骤

(1) 单击[远程服务/SNMP]菜单项，进入 SNMP 设置页面，设置 SNMP 信息，如图 7-31 所示。

a. 选择 SNMP 版本。

b. 选择是否开启超长口令。

c. 勾选“编辑只读团体名”或“编辑读写团体名”后，输入或删除只读团体名、读写团体名。

(2) 单击<保存>按钮，完成操作。

图7-31 SNMP

2. 参数说明

- SNMP 版本：可选择 v1、v2c，勾选表示支持该版本进行 SNMP get/set 操作， SNMP v3 默认支持。
- 超长口令：缺省为关闭状态。
  - 关闭超长口令，只读团体名长度为 1~32 字符；读写团体名长度为 1~32 字符或设置为空。
  - 开启超长口令，只读团体名长度为16~32字符；读写团体名长度为16~32字符或设置为空。
- 只读团体名：SNMP 协议只读团体名，默认为 rocommstr。
- 读写团体名：SNMP 协议读写团体名，默认为空。

3. 注意事项

- 只读团体名和读写团体名仅支持输入英文、数字以及特殊字符`~!@$%^&*()_+-=[]{}|:,./?。
- 读写团体名为空时不支持 SNMP set 操作。

- 读写团体名和只读团体名不能相同。
- 读写团体名和只读团体名在 Web 端以密文形式显示。

8 远程运维

8.1 日志

8.1.1 查看下载事件日志

通过本功能可以配置事件日志的存储策略（线性策略或循环策略），查看、下载或清除对应的事件日志。

1. 操作步骤

(1) 单击[远程运维/日志]菜单项，进入事件日志页面，如图 8-1 所示。

(2) 在日志策略栏选择事件日志的策略。

(3) 在日志筛选栏选择日志等级、传感器类型和日期信息，或者输入关键字来筛选日志。

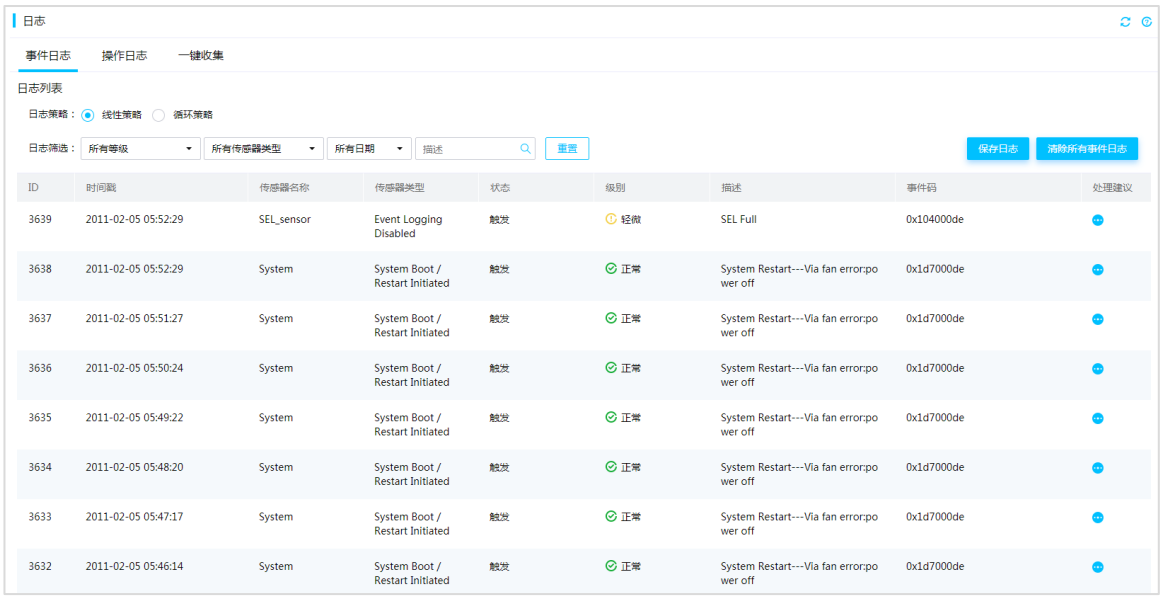
(4) （可选）在查询框中输入关键字，单击图标，可以查询日志。

(5) （可选）单击<重置>按钮，可以清除事件日志的所有筛选条件。

(6) （可选）单击页面右上方<保存日志>按钮，可以下载.csv 文件到本地。

(7) （可选）单击页面右上方<清除所有日志>按钮，完成清除操作后，事件日志无法恢复。

图8-1 事件日志



2. 参数说明

- 线性策略：当事件日志存储空间满后，将不会存储新的事件日志。
- 循环策略：当事件日志存储空间满后，新产生的事件日志会覆盖最早产生的事件日志。
- ID：事件编号。对事件按其发生的顺序进行编号。缺省情况下，按编号对事件日志进行排序。

- 时间戳：记录事件日志的时间。
- 状态：该事件的状态。触发表示事件发生，解除表示事件得到解决。
- 级别：检测到事件的严重性。
  - 正常：表示对系统不会产生影响的事件，例如正常的状态变化，告警事件解除。
  - 轻微：表示对系统不会产生大的影响，需要尽快采取相应的措施，防止故障升级。
  - 严重：表示对系统产生较大的影响，有可能中断部分系统的正常运行，导致业务中断。
  - 紧急：表示可能会使服务器下电，系统中断。需要马上采取相应的措施进行处理。
- 事件码：系统事件在 HDM 系统中的标识码。
- 处理建议：事件日志的简要处理建议。

3. 注意事项

- 当记录的事件日志达到事件日志支持的最大存储空间（最多支持约 3639 条事件日志），系统会根据设置的事件日志策略来存储事件日志。
- 清除所有事件日志后，会自动生成一条成功清除事件日志的日志信息。

8.1.2 查看下载操作日志

本功能用于查看并下载操作日志，包括审计日志、固件更新日志、硬件更新日志和配置日志。

- 审计日志：记录访问 HDM 的操作信息，包括：通过浏览器登录 HDM、启动远程控制台等信息。
- 固件更新日志：记录固件更新的操作信息及操作结果。
- 硬件更新日志：记录硬件更新的操作信息及操作结果，包括 CPU、内存、硬盘(包括 NVMe 硬盘)和电源的更新。
- 配置日志：记录用户的配置操作及操作结果。

1. 操作步骤

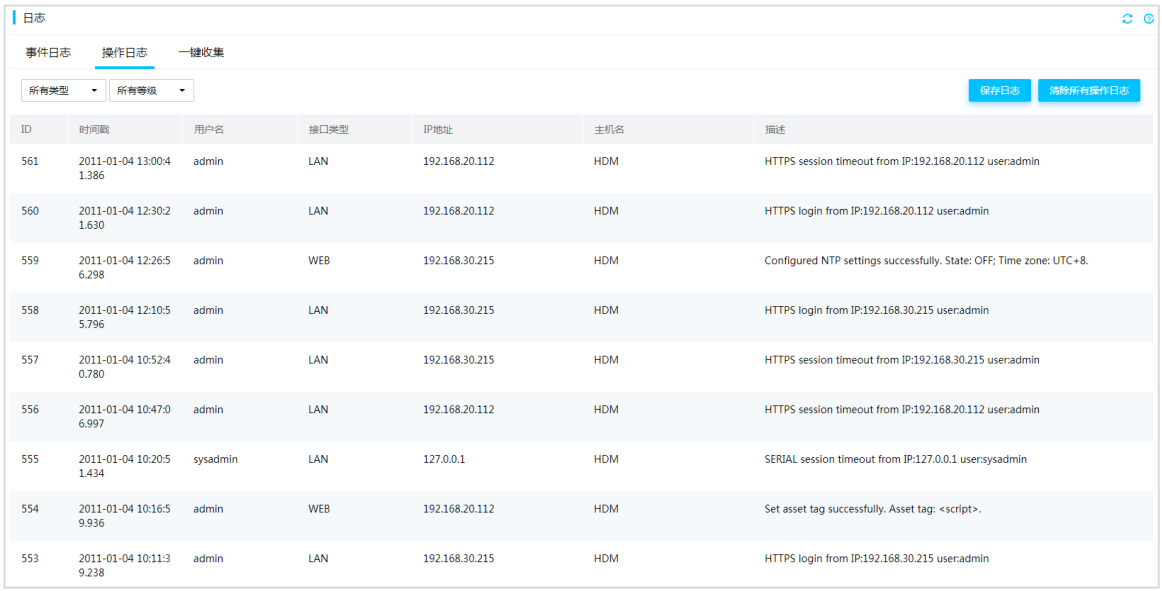
(1) 单击[远程运维/日志]菜单项，选择“操作日志”页签，进入操作日志页面，如图 8-2 所示。

(2) 在日志筛选栏选择日志类型和等级来筛选日志。

(3) （可选）单击页面右上方<保存日志>按钮，可下载.csv 文件到本地。

(4) （可选）单击页面右上方<清除所有操作日志>按钮，清除所有操作日志，完成清除操作日志操作后，操作日志无法恢复。

图8-2 操作日志



2. 参数说明

- ID：事件编号，对事件按其生成顺序进行编号。缺省情况下，按序号对操作日志进行排序，最多支持显示 1000 条日志，最晚发生的事件位于顶部。
- 时间戳：事件发生的时间。
- 接口类型：事件的操作通道。
- IP 地址：登录用户的 IP 地址。
- 主机名：HDM 设备名。
- 描述：事件的详细信息。

3. 注意事项

清除所有操作日志后，会自动生成一条成功清除日志的操作日志信息。

8.1.3 一键收集

本功能用于收集服务器的 SDS 日志信息，包括事件日志、软硬件信息和故障诊断信息。同时可以添加联系人信息，用于日志解析问题咨询等。

1. 操作步骤

(1) 单击[远程运维/日志]菜单项，选择“一键收集”页签，进入一键收集页面，如图 8-3 所示。

图8-3 一键收集

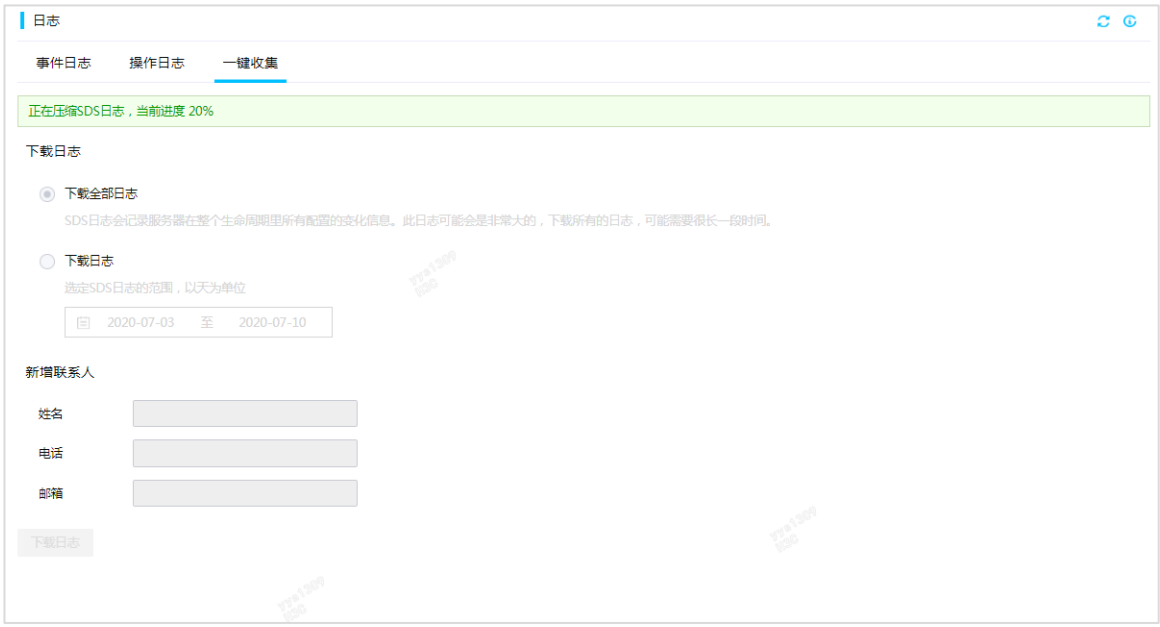
(2) 选择下载全部日志或下载指定时间段内的日志。

- 下载全部日志：选择<下载全部日志>。
- 下载指定时间段内的日志：在“下载日志”栏中，输入起始时间和截止时间。

(3) （选填）填写联系人信息，输入“姓名”、“电话”和“邮箱”信息。

(4) 单击<下载日志>按钮，开始下载日志，界面会显示下载进度，如图 8-4 所示。

图8-4 下载进度



(5) 下载完成后，将.sds 日志文件保存到本地，完成操作。

2. 注意事项

- 不支持多用户同时下载日志。
- SDS 日志记录的是 UTC 时间，HDM 时间以 NTP 页面设置为准，下载 SDS 日志时会把 HDM 时间自动转换成 UTC 时间，两者之间可能存在时间差。

3. 信息说明

表8-1 信息说明

一级目录	二级目录	文件名	文件内容说明
dump		dump_end	dump结束时间信息
		HDM_SDS_DUMP_DUP_01	dump加密信息
		HDM_SDS_DUMP_DUP_02	dump加密信息
		HDM_SDS_DUMP_DUP_03	dump加密信息
		HDM_SDS_DUMP_DUP_04	dump加密信息
event		*.sbe	事件日志的内部记录
		*.sme	事件日志的内部记录
hdm		pack.info	SDS日志压缩打包信息
sdmmc0p4	log	auth	HDM登录认证信息
		operate	操作日志
		update	更新日志

一级目录	二级目录	文件名	文件内容说明
		visible	审计日志
static		board_cfg	主板信息
		hdm.json	HDM配置信息
		bios.json	BIOS配置信息
		raid.json	RAID配置信息
		firmware_version	系统固件版本信息
		FruInfo	FRU信息
		dcpmm_info	DCPMM内存信息
		gpu_info	GPU信息
		hardware.info	硬件信息
		hardware_info	硬件信息
		net_cfg	Net配置信息
		PCIe_arguments_table	PCIe设备配置信息
		Pdb_Node_dump_info	仅记录R6900 G3、R8900 G3机型的节点板以及电源板的cpld寄存器值
		nvme_info	NVMe硬盘信息
		psu_cfg	电源配置信息
		sensor_info	传感器列表信息
		test	SDS日志，方便运维人员查看定位问题

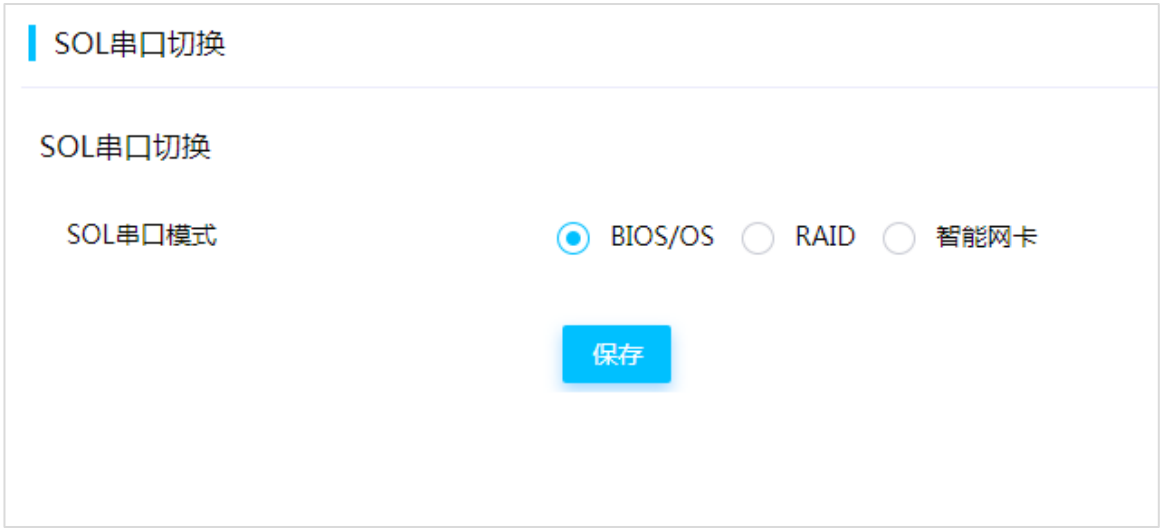
8.2 SOL串口切换

通过本功能可以选择启用 SOL（Serial Over Lan，串口重定向）功能时所连接的串口。

1. 操作步骤

(1) 单击[远程运维/SOL 设置]，进入 SOL 设置页面，如图 8-5 所示。

图8-5 SOL 串口



(2) 选择串口模式。

(3) 单击<保存>按钮，完成操作。

2. 参数说明

- BIOS/OS：选择 BIOS/OS，启用 SOL 功能时会连接到 BIOS 或 OS 串口。
- RAID：选择 RAID，启用 SOL 功能时会连接到 RAID 串口。
- 智能网卡：选择智能网卡，启用 SOL 功能时会连接到智能网卡串口。

3. 注意事项

- RAID 串口仅支持 RAID 扣卡串口。
- 智能网卡串口目前仅支持部分智能网卡。
- 切换 SOL 串口模式前，需要先关闭 SOL 功能。

8.3 截屏&录像

8.3.1 录像功能设置

通过本功能可以开启服务器的自动录像功能。当服务器操作系统发生崩溃、重启或关机时，系统会自动录制事件发生前的录像。技术人员可以通过服务器操作系统在崩溃、重启或关机前录制的视频，对操作系统崩溃、重启或关机的原因进行分析。

1. 配置限制和指导

- 在配置录像回放操作前，请先通过[远程服务/服务设置]菜单项开启 KVM 服务。
- 录制视频过程中，必须保持远程控制台处于关闭状态。
- Windows 系统和 Linux 系统支持录制崩溃前视频。

2. 操作步骤

(1) 单击[远程运维/截屏&录像]菜单项，进入截屏&录像页面。

(2) 单击<配置>按钮，在对话框中设置录像功能，如图 8-6 所示。

(3) 选择是否启用录像功能。

(4) 设置录制时间，时长范围为 15 秒～255 秒。

(5) 点击<崩溃前>、<重启前>、<关机前>选框，选择触发录像的视频类型。

(6) 单击<确定>按钮，完成服务器录像功能配置。

图8-6 录像回放设置

8.3.2 查看录像回放

在录像回放页面可以对已录制的视频进行播放、下载、删除等操作。

目前支持记录三个视频文件，文件信息中有视频文件生成的时间，按照文件生成时间，新生成的视频文件将覆盖最早的视频文件。

1. 操作步骤

(1) 单击[远程运维/截屏&录像]菜单项，进入截屏&录像页面，如图 8-7 所示。

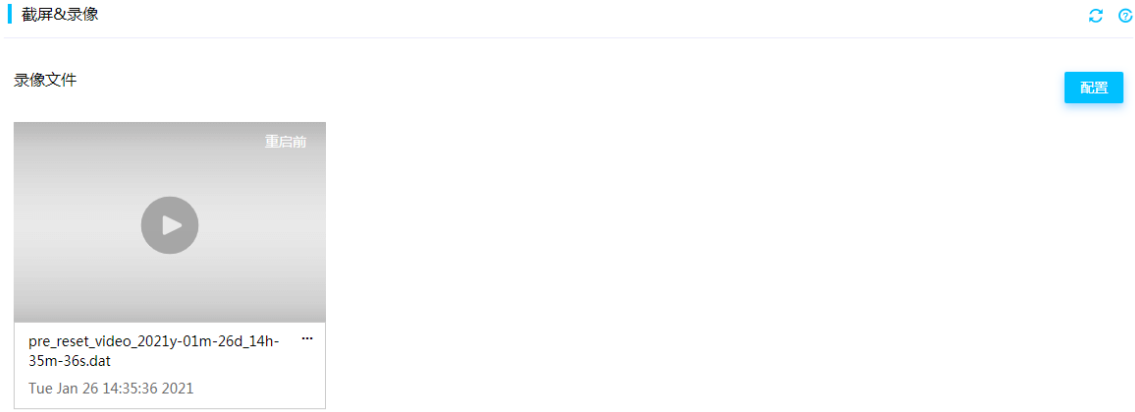
(2) 单击目标视频，视频会在当前页面中播放。

(3) （可选）视频加载完后，单击<下载>按钮，完成下载视频操作。

(4) （可选）视频播放完后，单击<关闭>按钮，完成关闭视频操作。

(5) （可选）单击目标视频右下角的...，再单击<删除>按钮，完成删除视频操作。

图8-7 录像播放



2. 注意事项

如果事件发生时，操作系统处于关机状态，查看录像回放时会显示无信号。

8.3.3 蓝屏快照

本功能用于查看服务器 Windows 操作系统发生故障重启前自动捕获的蓝屏快照，通过蓝屏快照可对故障进行快速分析。HDM 最多可保存十张蓝屏快照，并以快照捕获时间及序号命名。当蓝屏快照超过十张时，新的快照会覆盖最早生成的快照。

1. 配置限制和指导

在查看蓝屏快照前，请先通过[远程服务/服务设置]菜单项开启 KVM 服务。

2. 操作步骤

(1) 单击[远程运维/截屏&录像]菜单项，进入截屏&录像页面，如图 8-8 所示。

(2) 查看当前的蓝屏快照。

图8-8 蓝屏快照

3. 注意事项

如果服务器安装了 Windows 以外的操作系统，当服务器检测到 MCA 故障时，HDM 会也记录 MCA 触发时的快照。

8.4 告警设置

通过本功能，可以执行以下操作：

- 设置服务产生告警时的处理策略，包括 NMI 控制策略和 MCA 策略。
- 将服务器产生的事件日志通过“电子邮件”发送给指定用户，帮助用户监控服务器的运行状态。
- 发送 SNMP Trap 信息到目的主机。
- 发送 Syslog 信息到目的主机。
- 设置服务器的应急诊断功能。

8.4.1 告警策略

通过本功能设置服务器产生告警时的处理策略，包括 NMI 控制和 MCA 策略。

- NMI（Non Maskable Interrupt，不可屏蔽中断）是一种不能被标准屏蔽中断技术忽略的特殊中断。不可屏蔽中断特别用于不可恢复硬件错误的信号提示。
- MCA（Machine Check Architecture，硬件错误检测架构）是 Intel CPU 的一种特性机制，目的是实现错误检测上报和一定程度上的故障恢复。通过本功能可以配置当 HDM 检测到不可纠正的 IERR 错误时，主机是否需要重启的策略。

1. NMI 控制操作步骤

注意

- NMI 仅用于内部调试，使用时需要操作系统中有对应的 NMI 中断处理程序，否则可能引起系统崩溃。
- 该功能主要在无法使用操作系统的情况下使用。在服务器正常运行期间，不要使用该功能。
- 通过使用特殊方法，某些不可屏蔽中断也能够被屏蔽。

(1) 单击[远程运维/告警设置]菜单项，进入告警策略页面，如图 8-9 所示。

(2) 单击 NMI 控制栏的<执行动作>按钮，完成操作。

图8-9 告警策略

2. MCA 策略操作步骤

说明

R3830 G3、R3630 G5、R3830 G5、R4950 G5、R5500 G5 AMD 不支持 MCA 策略。

(1) 单击[远程运维/告警设置]菜单项，进入告警策略页面，如图 8-9 所示。

(2) 选择主机重启策略。

(3) 单击<保存>按钮，完成操作。

3. 参数说明

- 主动重启主机：当 HDM 检测到不可纠正的 IERR 错误时，会主动重启服务器。
- 不主动重启主机：当 HDM 检测到不可纠正的 IERR 错误时，不会主动重启服务器。

4. 注意事项

操作系统重启策略不受 MCA 策略影响。

8.4.2 邮件通知设置

告警邮件通过 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）协议，实现将告警邮件以邮件的形式发送到指定接收人。

通过本功能可以设置 SMTP 服务器和告警邮件发件人和接收人，设置成功后，可以发送测试邮件以验证配置是否生效。

1. 设置 SMTP 服务器操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择邮件通知页签，进入邮件通知页面，如图 8-10 所示。

(2) 单击<配置>按钮，在对话框中配置 SMTP 服务器。

a. 勾选 SMTP 功能的<启用>按钮。

b. 输入 SMTP 服务器地址和 SMTP 服务器端口。

c. 如果不勾选是否使用匿名的<启用>选项，需输入连接 SMTP 服务器的用户名和密码，用户名仅支持字母、数字及字符（_）、（@）和（.）。

d. 发件人邮件地址：发送电子邮件时使用的可连接 SMTP 服务器的邮箱地址。

e. 选择告警发送级别：包括紧急、轻微+严重+紧急和所有级别三个选项。

(3) 完成告警邮件相关配置后，请单击<确定>按钮。

图8-10 告警邮件

2. 设置接收告警的邮件地址操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择邮件通知页签，进入邮件通知页面，如图 8-10 所示。

(2) 单击<添加新邮件地址>按钮，弹出接收告警设置对话框。

(3) 在对话框中，设置收件人信息。

a. 选择收件人用户名后，会自动关联邮箱地址。

b. （可选）如果需要为选择的收件人添加邮箱地址，请单击“前往修改”链接进入[用户&安全/用户访问设置]页面，选择用户，单击“修改”按钮配置用户的电子邮箱 ID。

(4) 请输入邮件主题，仅支持字母、数字和特殊字符（_）。

(5) 添加成功后，单击“测试”按钮，发送测试告警邮件，再单击“结果”按钮，查看测试邮件发送结果。

(6) （可选）单击操作栏的<修改>按钮，修改收件人信息。

(7) （可选）单击操作栏的<删除>按钮，删除收件人信息。

8.4.3 告警 Trap 报文设置

通过本功能可以配置服务器将 Trap 告警发送给目的主机。管理员可以通过 Trap 告警来监控服务器的运行状态，及时发现设备异常情况。

1. 设置告警 Trap 报文通知操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择“告警 Trap 报文设置”页签，进入 Trap 报文设置页面。

(2) 单击<配置>按钮，在对话框中配置 Trap 报文通知相关信息，如图 8-11 所示。

a. 选择启用 Trap 功能。

b. 选择 Trap 模式，模块 OID 模式或者事件 OID 模式。

c. 选择 Trap 版本，如果选择 v3 版本，还需要选择 v3 用户。

d. （可选）输入节点位置和联系方式。

e. 输入团体名并选择告警发送级别。

(3) 单击<确定>按钮，完成操作。

图8-11 告警 Trap 报文设置

2. 设置告警 Trap 服务器操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择“告警 Trap 报文设置”页签，进入 Trap 报文设置页面。

(2) 单击设置告警 Trap 服务器栏的<修改>按钮，弹出修改告警 Trap 服务器对话框，如图 8-12 所示。

图8-12 修改告警 Trap 服务器对话框

(3) 修改配置信息。

(4) 单击<确定>按钮，完成操作。

(5) （可选）单击设置告警 Trap 服务器栏的<测试>按钮，发送测试告警信息。

3. 参数说明

- 模块 OID 模式：缺省模式，以与事件相关传感器模块对应的 SNMP 节点的 OID 作为 Trap 事件的标识。
- 事件 OID 模式：以与事件一一对应的 SNMP 节点 OID 作为 Trap 事件的标识，相较模块 OID 模式，可提供更为精确的定位信息。
- SNMP Trap 版本：选择 v1、v2c 或 v3 版本。
- 选择 v3 用户：选择发送 SNMP v3 版本 Trap 需要使用的用户名。
- 节点位置：服务器的位置描述，最多只能输入 31 个字符。
- 联系方式：设备联系人的名字及联系方式，最多只能输入 31 个字符。
- Trap 团体名：管理端进行的接收认证，最多只能输入 31 个字符，缺省值为 public。
- 告警发送级别：包括严重+紧急、轻微+严重+紧急和所有级别三个选项。
- 序号：Trap 发送告警的通道 ，最多可定义八个通道。
- 当前状态：勾选<启用>选项，表示通道处于启用状态，可以发送告警 Trap 信息；勾选<停用>选项，表示通道处于停用状态。
- Trap 服务器地址：接收 SNMP 告警信息的目的主机地址，支持 IP 地址和域名地址。
- 端口号：目的主机接收 SNMP 告警信息的端口号。端口号范围为 1～65535，缺省值为 162。

4. 注意事项

- 节点位置、联系方式、Trap 团体名仅支持输入英文、数字以及特殊字符 `~!@$%^&*()_+-=[]{}|:,./?。

8.4.4 Syslog 设置

通过本功能可以配置服务器以 Syslog 报文方式发送以下信息到目的服务器。

- 告警日志信息，包括操作日志、事件日志和安全日志。
- 传感器信息，包括传感器名称、读数和状态。
- 串口信息，包括 BIOS 启动信息和 OS 串口下的信息。

启用本功能前需要先配置 Syslog 服务器，具体操作请参见 11.3 搭建 Syslog 服务器。

1. 设置 Syslog 报文通知操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择“Syslog 设置”页签，进入 Syslog 设置页面。

(2) 单击<配置>按钮，进入“告警日志报文通知”配置页面，配置相关信息，如图 8-13 所示。

(3) 选择开启告警日志功能。

(4) 选择告警日志主机标识和传输协议。

a. 如果传输协议选择 TLS。

b. 需要选择认证方式，单向认证或双向认证。

– 如果选择单向认证，只需要上传 CA 证书。

– 如果选择双向认证，需要上传 CA 证书、本地证书和私钥文件。

(5) 单击<确定>按钮，完成操作。

图8-13 Syslog 设置

(6) 单击“设置告警日志服务器”栏的<修改>按钮，弹出“设置告警日志服务器”对话框，如图 8-14 所示。

(7) 修改配置信息。

(8) 单击<确定>按钮，完成操作。

图8-14 设置告警日志服务器

2. 传感器信息设置操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择“Syslog 设置”页签，进入 Syslog 设置页面。

(2) 单击“传感器信息设置”栏的<配置>按钮，在弹窗中配置相关信息，如图 8-15 所示。

a. 选择开启传感器信息功能。

b. 选择传输协议。

c. 输入 Syslog 服务器地址，端口号和发送时间间隔。

(3) 单击<确定>按钮，完成操作。

图8-15 传感器信息设置

3. 串口信息设置操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择“Syslog 设置”页签，进入 Syslog 设置页面。

(2) 单击“串口信息设置”栏的<配置>按钮，在弹窗中配置相关信息，如图 8-16 所示。

a. 选择开启串口信息功能。

b. 选择传输协议。

c. 输入 Syslog 服务器地址和端口号。

(3) 单击<确定>按钮，完成操作。

图8-16 串口信息设置

4. 参数说明

- 告警日志主机标识：标识告警日志的信息来源，包括主机名、主板序列号、产品资产标签和产品序列号。
- 传输协议：服务器发送 Syslog 报文使用的传输协议，包括 TCP、UDP 和 TLS 三种协议。
  - TCP：面向连接的协议，在正式收发数据前，必须在收发方建立可靠的连接。
  - UDP：无连接协议，在正式收发数据前，收发方不建立连接，直接传输正式的数据。
  - TLS：面向连接的协议，并保证数据传输的保密性和数据完整性。
    - 单向认证：只认证 Syslog 服务器端的证书。
    - 双向认证：Syslog 服务器端和客户端（即 HDM）的证书都需要认证。
    - CA 证书：建立数据连接时，使用此处上传的 CA 证书对 Syslog 服务器发送的报文进行验证，证书文件的格式应为.pem。
    - 本地证书：建立数据连接时，HDM 向 Syslog 服务器发送报文时会携带本地证书信息，用于 Syslog 服务器对客户端（即 HDM）的验证，证书文件的格式应为.pem。
    - 私钥：解密本地证书的密码，私钥文件的格式应为.pem。
- 序号：Syslog 报文发送通道，最多可定义八个通道。
- 服务器地址：接收 Syslog 报文的目的主机的地址，仅支持 IP 地址和域名地址，缺省值为 127.0.0.1，如果输入域名地址，长度不能超过 48 个字符。
- 端口：目的主机接收 Syslog 报文的端口号，端口号范围为 1～65535，缺省值为 514。
- 日志类型：Syslog 报文包含的日志类型，包括操作日志、事件日志和安全日志，可多选。
- 时间间隔：发送传感器信息的时间间隔，取值范围为 10 秒～2592000 秒。

5. 注意事项

修改告警日志报文通知设置后，告警日志服务器设置会恢复为缺省状态。

8.4.5 应急诊断

当服务器因可更换硬件故障导致启动进程挂死在 POST 阶段时，可以通过本功能配置应急诊断功能，包括最小启动功能和诊断隔离启动功能。

- 最小启动是指服务器仅启用单 CPU、单核、单通道内存来启动仅安装到 SATA M.2 硬盘的操作系统或 UEFI SHELL。
- 诊断隔离启动是指当服务器启动失败时，对服务器的硬件部件进行诊断，诊断出故障部件后，隔离该部件并重新启动。

说明

- 仅 HDM-2.26 及以后的版本支持应急诊断功能。
- 仅 R4300 G5、R4700 G5、R3800 G5、R5300 G5 服务器支持应急诊断功能。
- 开启应急诊断功能前，请确保 BIOS 未处于固件更新状态。
- 若同时开启最小启动和诊断隔离启动两个功能，仅诊断隔离启动功能生效。
- 本章节提到的“重启服务器”，仅限于在“设备上下电”页面选择“关机并重新开机”选项来重启服务器。
- 进入最小启动或诊断隔离模式后，服务器的 USB 接口处于禁用状态，HDM 的无线网络会断开连接，用户无法通过无线网络访问 HDM，请做好网络备份。
- 服务器进入最小启动或应急诊断模式后，HDM 和服务器之间的 USB 通道和 PCIe 通道会保持正常通信状态。

1. 操作步骤

(1) 单击[远程运维/告警设置]菜单项，选择“应急诊断”页签，进入应急诊断页面，如图 8-17 所示。

图8-17 应急诊断

(2) 查看最小启动和诊断隔离功能的状态。

(3) 单击<配置>按钮，在对话框中配置相关信息，如图 8-18 所示。

- 选择是否开启最小启动功能。
- 选择是否开启诊断隔离启动功能，如果开启，需要选择模式，诊断隔离启动功能包括“仅诊断”和“诊断+隔离”两个模式。

图8-18 应急诊断配置

(4) 单击<确定>按钮，完成操作。

(5) 重启服务器使配置生效。

- 如果开启了最小启动功能，服务器将进入最小启动模式。
- 如果开启了诊断隔离启动功能，服务器将进入诊断模式或诊断+隔离模式。

2. 参数说明

- 诊断隔离启动：包括开启和关闭两种状态。
  - 开启：开启诊断隔离启动功能时，请直接选择模式，包括“仅诊断”和“诊断+隔离”两个模式。
    - 仅诊断：对服务器的启动失败进行诊断，诊断结束后，仅显示诊断结果。
    - 诊断+隔离：对服务器的启动失败进行诊断，诊断结束后，显示诊断结果并隔离故障部件，然后再重新启动。
  - 关闭：关闭诊断隔离启动功能。
- 设备名称：服务器诊断的硬件部件名称。
- 诊断结果：硬件部件的诊断结果。
- 描述：诊断结束后的结果。

3. 注意事项

- 诊断过程时间较长，如需中断诊断或更改模式，需要先在 Web 端关闭诊断隔离启动功能，重启服务器退出当前模式。退出当前模式后才能更改模式，在 Web 端设置新的模式后，再重启服务器使配置生效。
- 诊断开始后，会先进行预检查，如果服务器在预检查阶段启动成功或最小启动到 UEFI SHELL 失败，诊断会直接终止。
- 服务器进入最小启动模式后，最小启动时未启动的设备会被 BIOS 隔离，导致 HDM 无法识别这些设备。

8.5 配置管理

通过本功能可以执行以下操作：

- 导入配置：将 HDM/BIOS/RAID 配置文件导入到系统中，覆盖当前配置。

- 导出配置：导出当前的 HDM/BIOS/RAID 配置信息，并生成一份配置文件。
- 恢复 HDM 配置：将当前的 HDM 配置还原为默认配置或出厂配置。
  - 默认配置：恢复 HDM 固件的缺省配置。
  - 出厂配置：当 HDM 存在客户定制化出厂配置时，支持将 HDM 当前配置还原为出厂配置。

8.5.1 导出配置

通过本功能可以导出服务器当前的 HDM、BIOS 或 RAID 配置信息，并生成一份配置文件。

说明

- RAID 配置导出前，请确保存储控制卡已完成初始化。
- PMC 存储控制卡不支持 RAID 配置导出。
- RAID 配置导出前，请确保 RAID 卡下的逻辑盘处于正常状态，且未执行扩容、迁移、重建、擦除等操作。

1. 操作步骤

(1) 单击[远程运维/配置管理]菜单项，进入配置管理页面，如图 8-19 所示。

(2) 在导出配置栏选择配置类别。

(3) 单击<导出>按钮，完成操作。

图8-19 配置管理

8.5.2 导入配置

用户导入配置文件后，可以覆盖服务器之前的配置。

注意

- 导入 RAID 和 BIOS 配置文件前，确保设备型号和组件配置（如存储控制卡型号、硬盘数量和槽位）都相同。导入 RAID 配置时，请确保存储控制卡模式为 RAID 模式，主机处于上电状态。
- 导入 HDM 配置前，确保设备型号相同。
- 导入 HDM 配置前，请确保待导入设备和配置文件中的 Bonding 模式处于同样的状态，否则会导入失败。
- 导入 RAID 配置时，如果硬盘之前的 RAID 信息未清除，会产生 Foreign 状态，导致 RAID 配置失败。请先在 BIOS 下清除该硬盘的 RAID 配置信息。
- 导入 HDM 配置前，如果配置文件中的某项配置信息被删除或不存在，则该项配置将在配置导入后依然保持原来的状态。
- 导入配置过程中，请勿对服务器进行上下电，否则可能会导致 HDM 部分功能以及操作系统出现异常。
- 导入 HDM/BIOS/RAID 配置时，如果 Web 页面提示出现失败项，将暂停导入，请修改失败项后再重新导入，直到导入完成。
- 导入配置前，请确保仅当前登录用户在执行操作，否则可能会导致导入配置失败。

1. 操作步骤

(1) （可选）使用文本工具打开配置文件，编辑配置文件信息，如图 8-20 所示。

说明

- 请谨慎修改配置文件，确保修改后配置信息的合法性，否则可能会导入失败。
- 编辑配置文件时，如果配置信息里包含“This_is_comment”信息，需要删除该信息。
- 配置文件中的密码显示为空，如果导入原服务器，不需要手动添加密码，导入后将保留原来的密码。如果导入其它服务器，需要手动添加密码，导入成功后，添加的密码会生效。

图8-20 配置文件

```
"machine information":  {
    "This_is_comment":  "If need to config some items, delete this comment",
    "baseboard id": 16978692,
    "host name":    "HDM-test-manu7",
    "product name": "RS32M2C9S1",
    "serial number":    "02A3FQH17B000275",
    "hdm version":  "1.30.18P56 HDM V100R001B03D018SP56_DEBUG",
    "bios version": "2.00.37 V100R001B02D037",
    "cpld version": "V004",
    "ME version":   "4.1.4.339",
    "config id":    1
```

(2) 单击[远程运维/配置管理]菜单项，进入配置管理页面，如图 8-19 所示。

(3) 在导入配置栏选择配置类别。

(4) 选择并导入配置文件。

(5) 在对话框中单击<确定>按钮，完成操作。

说明

- HDM 配置导入后，如果配置文件中包括网络设置信息，HDM 会自动重启使配置生效；否则配置会直接生效。
- HDM 配置导入后，如果配置文件中包含 HDM 配置管理 IP 地址，当前 HDM 管理 IP 地址会因为被覆盖而无法访问。如果配置文件里面的 HDM 管理 IP 地址是静态地址，导入成功后会直接替换原来的 IP 地址。如果配置文件里面的 HDM 管理 IP 地址是通过 DHCP 方式获取的，导入后 HDM 管理 IP 地址的获取方式会变成 DHCP，并重新获取一个 IP 地址。
- BIOS 配置导入后需要服务器重启后生效。
- PMC 存储控制卡不支持 RAID 配置导入。
- RAID 配置导入后需要等待约 40 秒后才能生效。

8.5.3 恢复 HDM 配置

注意

- 恢复 HDM 配置后，需要使用首次登录 HDM 的方法才可以登录 HDM，非专业人员请谨慎使用此功能。
- 恢复 HDM 配置过程中不要刷新页面，否则可能会导致 HDM Web 界面无法访问。

1. 操作步骤

(1) 单击[远程运维/配置管理]菜单项，进入配置管理页面，如图 8-19 所示。

(2) 单击恢复 HDM 配置栏下的<恢复默认配置>或<恢复出厂配置>按钮。

(3) 在弹出的对话框中单击<确定>按钮。

(4) HDM 会自动重启，重启后配置生效。

8.6 固件更新

可以通过 HDM 来完成 HDM、BIOS、各类 CPLD、PSU、LCD、GPUFPGA、FANMCU、存储控制卡固件、网卡固件和硬盘固件的固件更新。不同产品支持的固件类型不一样，如表 8-2 所示。

表8-2 固件类型差异表

机型	固件类型
• R2900 G3 • R4100 G3 • R4400 G3 • E3200 G3	• HDM • BIOS • CPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）

机型	固件类型
• B5700 G3 • AE100	
R3800 G3	• HDM • BIOS • CPLD • BPCPLD • PSU • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
• R2700 G3 • R4300 G3 • R4700 G3 • R3830 G3 • B5800 G3	• HDM • BIOS • CPLD • BPCPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
R5300 G3	• HDM • BIOS • CPLD • PSU • GPUCPLD • BPCPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
R6700 G3	• HDM • BIOS • CPLD • DBCPLD • STBCPLD • LCD • BPCPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
R6900 G3	• HDM • BIOS • CPLD • PDBCPLD • NDCPLD • BPCPLD • LCD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
R8900 G3	• HDM • BIOS • CPLD

机型	固件类型
	• BPCPLD • PDBCPLD • NDCPLD • PDBSCPLD • LCD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
B7800 G3	• HDM • BIOS • CPLD • AUXCPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
R3630 G5	• HDM • BIOS • CPLD • BPCPLD • PSU • LCD • PFRCPLD
• R4700 G5 • R3800 G5 • R3830 G5 • R4950 G5 • R4300 G5	• HDM • BIOS • CPLD • BPCPLD • PSU • LCD • PFRCPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
R5300 G5	• HDM • BIOS • CPLD • BPCPLD • PSU • PFRCPLD • OCPCPLD • GPUFPGA • REPO（包括存储控制卡固件、网卡固件和硬盘固件）

机型	固件类型
R5500 G5	• HDM • BIOS • CPLD • BPCPLD • PFRCPLD • PSWCPLD • PSU • FANMCU • REPO（包括存储控制卡固件、网卡固件和硬盘固件）
R5800 G5	• HDM • BIOS • CPLD • DBCPLD • BPCPLD • PSU • LCD • PFRCPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件） • OCPCPLD
B5700 G5	• HDM • BIOS • CPLD • PFRCPLD • REPO（包括存储控制卡固件、网卡固件和硬盘固件）

8.6.1 配置限制和指导

(1) 在开始固件更新操作前，请检查以下配置：

- 咨询厂家获取最新的服务器固件。
- HDM 一次仅支持一个用户执行固件更新操作，否则可能会导致更新失败。
- 选择的固件镜像必须与固件类型一致，包括厂商签名信息且未被篡改，否则会导致固件镜像验证失败。

(2) 在固件升级过程中，请注意如下事项：

- 进入固件更新模式之后，固件更新过程中不要刷新固件升级所在页面，其他登录用户可以使用除如表 8-3 所示功能外的网页和服务。

表8-3 无法使用功能

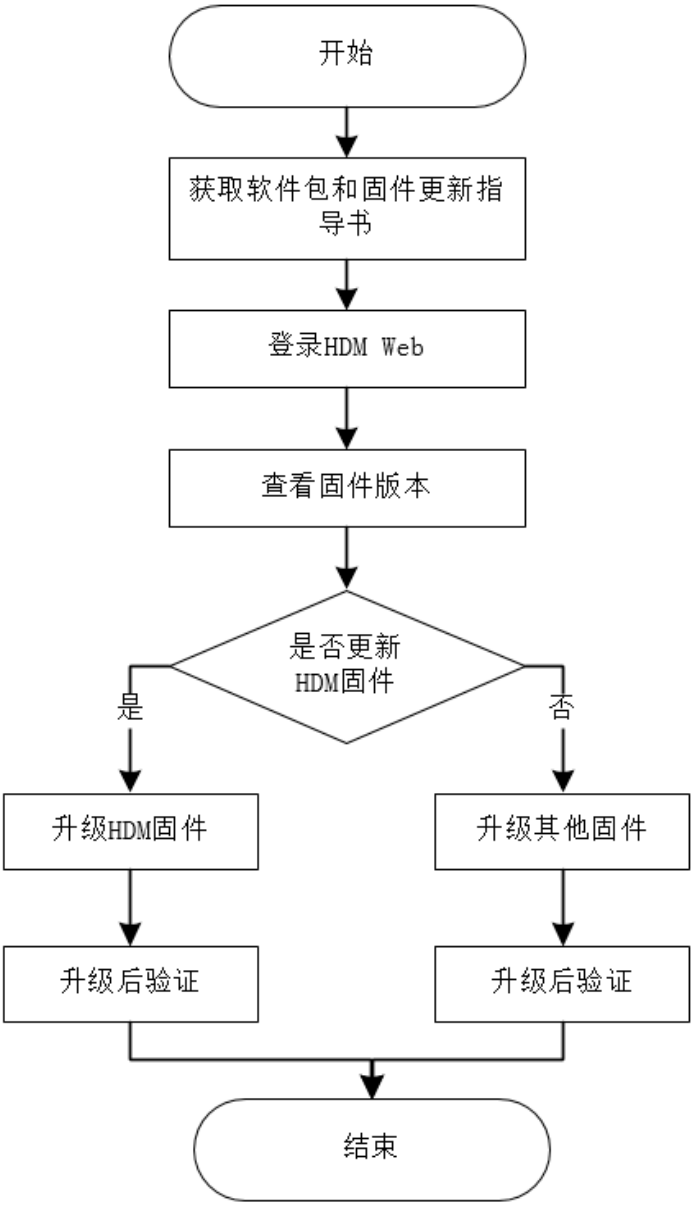
页面	功能
网络设置	共享网口配置
	专用网口配置
	网卡选择
	DNS配置
	网口模式配置
	无线网络配置
NTP	NTP设置
远程服务	服务配置
用户&安全	防火墙
	SSL证书
电源管理	设备上下电管理
	功率封顶配置
远程运维	NMI控制
	导入导出配置
	恢复HDM配置
	重启HDM
	主备切换
	重启CPLD

- 固件更新过程中，请勿对服务器进行上下电操作，否则可能会导致 HDM 部分功能以及操作系统出现异常。
- 如果多用户同时进行固件升级操作，非第一个操作的用户会被强制登出。
- 固件更新过程中，KVM 中屏蔽了“键盘”里的操作项，H5 KVM 中屏蔽了“发送热键”和“热键”的操作项，所以这些选项不可用。

8.6.2 固件更新流程

固件更新的流程如图 8-21 所示。

图8-21 固件更新流程



8.6.3 更新 HDM 固件

通过本功能可以更新 HDM 固件。

注意

- 更新 HDM 固件前，请先备份 HDM 配置，避免 HDM 配置意外丢失。
- 选择“恢复出厂配置”完成 HDM 固件更新后，需要使用登录 HDM Web 里的方法才可以登录 HDM，非专业人员请谨慎使用此功能。

1. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面，如图 8-22 所示。

图8-22 固件更新

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面，如图 8-23 所示。

图8-23 固件更新

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件。

- 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在弹出对话框选择固件镜像。
- 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

(4) 选择“HDM 更新配置”选项及是否启用“恢复出厂配置”，单击<下一步>按钮。

(5) HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，确认当前运行分区固件版本、待升级分区固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮，如图 8-24 所示。

图8-24 固件信息确认

(6) 服务器开始更新固件，页面提示固件升级成功时，表示完成烧写固件。

(7) 重启 HDM 使新固件生效。

- 如果步骤（4）选择的是<更新后立即重启 HDM>选项，HDM 将会自动重启，使新固件生效。
- 如果步骤（4）选择的是<更新后手动重启 HDM>选项，需要手动执行重启 HDM 操作，使新固件生效。

(8) 固件更新针对的是备分区镜像，HDM 重启后会自动执行主备切换。

2. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。
- 恢复出厂配置：更新 HDM 固件时，请根据实际需求选择是否勾选该选项。
  - 勾选<恢复出厂配置>选项，服务器将使用固件的出厂配置覆盖当前配置。如果没有出厂配置，则恢复默认配置。更新完成后，需要使用首次登录 HDM 的方法才可以登录 HDM，非专业人员请谨慎使用此功能。
  - 不勾选<恢复出厂配置>选项，固件更新后将继续使用当前配置。
- HDM 更新配置：HDM 升级完成后需要重启才能生效，可以选择自动重启或手动重启。
  - 勾选<更新后立即重启 HDM>选项，HDM 将在升级完成后自动重启。
  - 勾选<更新后手动重启 HDM>选项，HDM 升级完成后需要手动重启。

3. 注意事项

更新 HDM 固件后，请清除浏览器的缓存后再登录 HDM Web 界面，否则界面显示可能存在问题。

8.6.4 更新 BIOS 固件

通过本功能可以更新 BIOS 固件。

注意

- 更新 BIOS 固件前，请先检查电源是否处于冗余正常状态，如果否，可能会导致固件更新过程出现异常。
- 选择“配置覆盖”或“强制覆盖”完成 BIOS 固件更新后，BIOS 启动模式会变为缺省的 UEFI 模式。如果操作系统是在 Legacy 模式下安装的，请进入 BIOS 界面将 BIOS 启动模式修改为 Legacy 模式，否则操作系统无法正常启动。
- 在重启服务器使新固件生效过程中，请勿再次更新 BIOS 固件或重启 HDM，否则会导致 BIOS 功能异常。
- 安装 Intel 处理器的服务器选择“强制覆盖”完成 BIOS 固件更新后， 如需通过 HDM Web 端重启服务器，请在“设备上下电”页面选择除“正常关机”以外的其他选项来重启服务器，否则可能会导致 ME 异常。
- 安装海光处理器的服务器在使用 HDM 更新 BIOS 固件时，如果选择了<配置保留>或<配置覆盖>，请勿挂载 CD/DVD 镜像文件；如已挂载，在升级前请先卸载或者在固件更新过程中不要进行卸载操作，否则可能会因卸载操作导致传输 BIOS 文件的通道断开而更新失败。

1. 配置限制和指导

- BIOS 固件升级时勾选<配置保留>选项，不保证所有外接卡的配置保留：
  - mLOM 网卡的配置保存在 BIOS ROM 芯片的 ME 区域，因此升级 BIOS 固件后，mLOM 网卡配置无法保留。
  - 存储控制卡或网卡等部分外接卡的配置保存在卡上，所以这些卡的配置保留与否跟是否勾选<恢复出厂配置>无关。
- BIOS 固件向上升级版本可以保留配置，不保证向下回退版本可以保留配置。

2. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面，如图 8-23 所示。

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件。
  - 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在弹出对话框选择固件镜像。
  - 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

(4) （仅适用于安装 Intel 处理器的服务器）勾选“BIOS 更新选项”，选择待更新的组件。

(5) 选择“BIOS 更新配置”选项及是否启用“恢复出厂配置”，单击<下一步>按钮，如图 8-25 所示。

图8-25 BIOS 更新

(6) HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，确认当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮，如图 8-26 所示。

图8-26 固件信息确认

(7) 服务器开始更新固件，页面提示固件升级成功时，表示完成烧写固件。

(8) 更新 BIOS 固件后，必须重启服务器并完成 POST 阶段后，HDM Web 界面才能正常显示 BIOS 版本。

3. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。

- BIOS 更新选项：包括“更新 BIOS+ME”、“仅更新 BIOS”和“仅更新 ME”三个选项，默认勾选“更新 BIOS+ME”。
- 恢复出厂配置：更新 BIOS 固件时，请根据实际需求选择是否勾选该选项。当“BIOS 更新选项”选择“仅更新 ME”时，无需勾选此选项。
  - 勾选<配置保留>选项，更新 BIOS 后将继续使用 BIOS 当前配置。
  - 勾选<配置覆盖>选项，服务器将使用待升级的 BIOS 固件的出厂配置覆盖当前配置，如果没有出厂配置，则恢复默认配置。
  - 勾选<强制覆盖>选项，HDM 将直接烧写 BIOS 的 Flash，更新完成后 BIOS 将恢复默认配置。
    - 请确认服务器进入操作系统或关机后再选择强制覆盖，否则可能会导致 BIOS 功能异常。
    - 该选项可以在 BIOS 异常的情况下，用于恢复 BIOS。
- BIOS 更新配置：当固件类型选择为 BIOS 时，在服务器开机状态下，选择控制服务器重启时间。

8.6.5 更新 CPLD 固件

通过本功能可以更新多种 CPLD 固件，包括 CPLD、DBCPLD、STBCPLD、AUXCPLD、PDBCPLD、NDCPLD、PDBSCPLD、PFRCPLD 和 OCPCPLD。

1. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面，如图 8-27 所示。

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件。
  - 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在弹出对话框选择固件镜像。
  - 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

图8-27 CPLD 更新

(4) 单击<下一步>按钮，HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，进入固件信息确认页面，如图 8-28 所示。

(5) 确认当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮。

图8-28 固件信息确认

(6) 服务器开始更新固件，页面提示固件升级成功时，表示完成烧写固件。

(7) 更新 CPLD 固件后，新固件生效方式因产品而异，具体方式请参考《固件更新指导书》。

2. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。

3. 注意事项

- 不同产品支持的 CPLD 固件类型不完全一样，具体差异请以界面显示为准。
- 更新 CPLD 固件后，如果更新失败会导致设备无法正常使用。

8.6.6 更新 BPCPLD 或 PSWCPLD 固件

说明

- G3 系列服务器中，仅 R2700 G3、R4300 G3、R4700 G3、R3800 G3、R3830 G3、R5300 G3、R6700 G3、R6900 G3、R8900 G3、B5800 G3 支持更新 BPCPLD 固件。
- G5 系列服务器中，仅 B5700 G5 不支持更新 BPCPLD 固件。
- 仅 HDM-2.17 及以后的版本支持更新 PSWCPLD 固件。
- 当前仅 R5500 G5 支持更新 PSWCPLD 固件。

通过本功能可以更新硬盘背板和 PCIe Switch 板的 CPLD 固件，即 BPCPLD 和 PSWCPLD 固件。

1. 配置限制和指导

- 有多个硬盘背板在位时，只有 BPCPLD 镜像文件支持升级的背板，才能进行固件更新。

- 服务器保持关机状态 9 秒后才开始更新 BPCPLD 或 PSWCPLD 固件，更新过程中请勿开机或插拔电源，否则可能会导致更新失败。
- 更换硬盘背板或 PCIe Switch 板后，请先开机再进行固件更新。

2. 操作步骤

说明

BPCPLD 和 PSWCPLD 固件更新的操作步骤一样，本文以 BPCPLD 固件为例进行介绍。

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面，如图 8-29 所示。

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件，如图 8-29 所示。

- 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在弹出对话框选择固件镜像。
- 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

图8-29 BPCPLD 更新

(4) 单击<下一步>按钮，HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，如图 8-30 所示。

(5) 选择待升级的组件，并确认支持升级的组件信息、当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮。

图8-30 固件信息确认

(6) 如果服务器处于开机状态，将在关机之后开始更新固件。如果服务器处于关机状态，直接开始更新固件。

(7) 固件更新完成后，需要重启 HDM 使新 BPCPLD 固件生效。如果更新的是 PSWCPLD 固件，请断电重启服务器使新固件生效。

3. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。

4. 注意事项

- 更新过程中，如果某个组件更新失败，将会尝试再次进行更新，最多重复 2 次。
- 如果固件更新失败，请再次更新 BPCPLD 或 PSWCPLD 固件。如果多次更新失败，请联系技术支持，尝试通过其他方式更新固件。

8.6.7 更新 PSU 固件

通过本功能可以更新电源固件。

说明

仅 R3800 G3、R5300 G3、R4400 G3、R3630 G5、R4700 G5、R3800 G5、R3830 G5、R4950 G5、R5300 G5、R5500 G5、R5800 G5 支持更新 PSU 固件。

1. 配置限制和指导

- 在电源固件更新过程中，被更新电源无法正常供电，至少保证有一个电源在位维持服务器主板正常供电。
- 有多个电源在位时，必须保证所有在位电源都处于正常状态，且型号都和 PSU 固件一致，才能进行固件更新。

- R5500 G5 服务器的电源根据供电主体不同，分为主板电源和 GPU 电源两组，两组电源独立运行，支持独立更新各自的 PSU 固件。

- PSU 固件升级方式支持直接升级和关机后升级两种方式，升级方式由固件镜像文件决定，获取固件镜像文件时，请和技术支持人员确认升级方式。
  - 直接升级：固件上传校验通过后，直接开始更新 PSU 固件，更新过程中请勿开关机或拔插电源，否则可能会导致电源异常。
  - 关机后升级：固件上传校验通过后，需要服务器保持关机状态 9 秒后才开始更新 PSU 固件，更新过程中请勿开机或插拔电源，否则可能会导致电源异常。

2. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

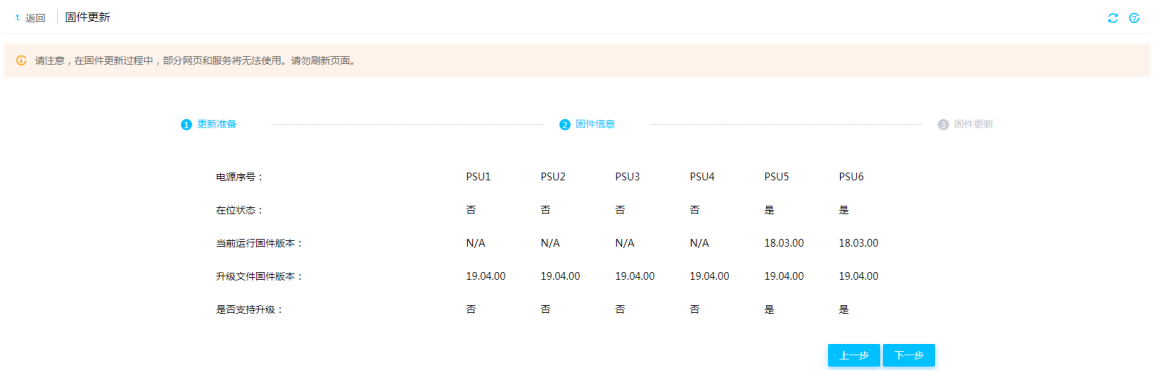
(2) 单击<固件更新>按钮，进入上传固件镜像文件页面。

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件，如图 8-31 所示。
  - 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在弹出对话框选择固件镜像。
  - 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

图8-31 PSU 更新

(4) 单击<下一步>按钮，HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，如图 8-32 所示。

图8-32 固件信息确认



(5) 确认支持升级的电源信息、当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮。

(6) 服务器会根据固件镜像文件的升级方式，直接更新固件或在关机之后开始更新固件。

3. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。
- 在位状态：电源是否在位。

4. 注意事项

- 更新的电源个数较多时，升级时间可能较长。
- 更新 PSU 固件后，新固件会在每个电源更新完成后自动生效。
- 更新 PSU 固件后，请在操作日志页面查看更新结果。如果某一电源更新失败，可能会导致该电源无法使用。

8.6.8 更新 LCD 固件

通过本功能可以升级 LCD 显示屏的固件。

说明

- HDM-2.09 及以后的版本支持更新 LCD 固件。
- R6700 G3、R6900 G3、R8900 G3、R3630 G5、R4700 G5、R3800 G5、R3830 G5、R4950 G5 和 R5800 G5 支持更新 LCD 固件。

1. 配置限制和指导

LCD 固件更新过程中，请勿重启 HDM 或者拔插电源，否则可能会造成 LCD 显示屏功能异常。

2. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

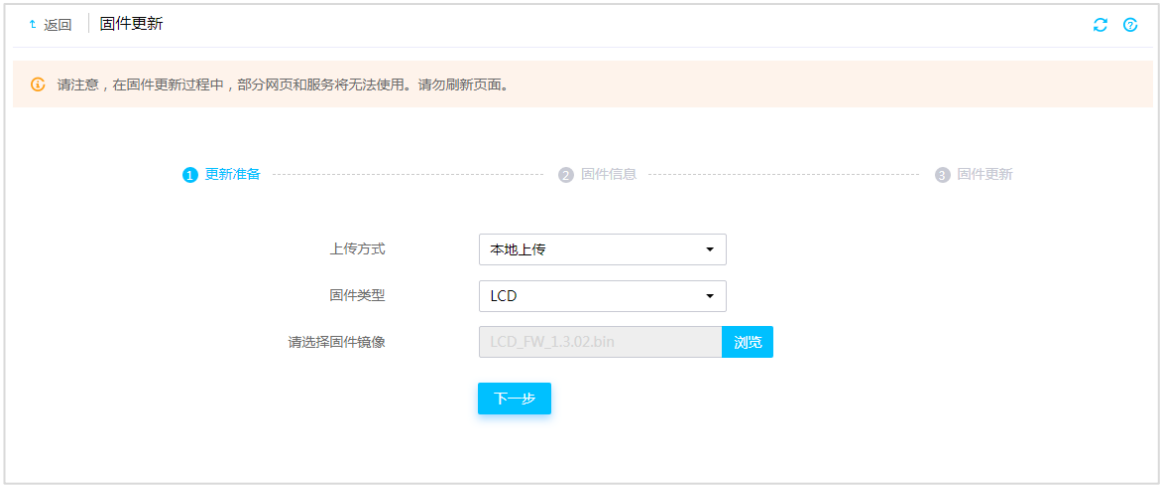
(2) 远程运维/固件更新配置上传固件镜像的方式，建议优先使用本地上传方式上传固件，如图 8-33 所示。

- 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在弹出对话框选择固件镜像。
- 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

说明

服务器接入 LCD 显示屏后，才会上传并更新 LCD 固件。

图8-33 LCD 固件更新



(3) 单击<下一步>按钮，HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，如图 8-34 所示。

(4) 确认支持升级的 LCD 信息、当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮。

图8-34 固件信息确认

(5) 开始更新固件，更新完成后，LCD 会自动重启使新固件生效。

3. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。

4. 注意事项

- LCD 固件更新时间可能较长，固件更新过程中 LCD 显示屏不可用。
- 如果 LCD 固件更新失败，可能会导致 LCD 显示屏功能异常，可以尝试再次更新固件。

8.6.9 更新 GPUCPLD 固件

通过本功能可以更新 GPU 的 CPLD 固件。

说明

- HDM-2.16 及以后的版本支持更新 GPUCPLD 固件。
- 仅 R5300 G3 支持更新 GPUCPLD 固件。

1. 配置限制和指导

- 有多个 GPU 在位时，只有 GPUCPLD 镜像文件支持升级的 GPU，才能进行固件更新。
- 目前只支持在开机状态时更新 GPUCPLD 固件，更新过程中请勿关机或插拔电源，否则可能会导致更新失败或 GPU 无法识别。

2. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面，如图 8-35 所示。

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面。

图8-35 GPUCPLD 固件更新

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件。

- 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在对话框中选择固件镜像。
- 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

(4) 单击<下一步>按钮，HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，如图 8-36 所示。

图8-36 固件信息确认

(5) 选择待升级的 GPU，并确认支持升级的 GPU 信息、当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮开始更新固件。

(6) 固件更新完成后，需要服务器断电重启使新固件生效。

3. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。

4. 注意事项

- 此功能目前仅支持部分型号的 GPU。
- 更新过程中，如果某个 GPU 更新失败，将会尝试再次更新，最多重复 2 次。
- 更新过程中，BIOS 会多次重启。

8.6.10 更新 GPUFPGA 固件

通过本功能可以更新 GPU 的 FPGA (Field Programmable Gate Array，现场可编程逻辑门阵列)固件。

说明

- HDM-2.25 及以后的版本支持更新 GPUFPGA 固件。
- 仅安装 Redstone GPU 模块的 R5300 G5 服务器支持更新 GPUFPGA 固件。

1. 配置限制和指导

- 有多个 GPU 在位时，只有 GPUFPGA 镜像文件支持升级的 GPU，才能进行固件更新。
- 目前只支持在开机状态时更新 GPU 的 FPGA 固件，更新过程中请勿关机或插拔电源，否则可能会导致更新失败或 GPU 无法识别。

2. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面。

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件，如图 8-37 所示。

- 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在对话框中选择固件镜像。
- 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

图8-37 GPUFPGA 固件更新

(4) 单击<下一步>按钮，HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面，如图 8-38 所示。

(5) 确认支持升级的 GPU 信息、当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮，开始更新固件。

图8-38 固件信息确认

(6) 更新完成后，需要重启服务器使新固件生效。

3. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。

4. 注意事项

更新过程中，如果更新失败，将会尝试再次更新，最多重复 2 次。

8.6.11 更新 FANMCU 固件

通过本功能可以更新风扇的 MCU (Micro Control Unit，单片机)固件。

说明

- HDM-2.42 及以后的版本支持更新 GPUFPGA 固件。
- 仅 R5500 G5 支持更新 FANMCU 固件。

1. 配置限制和指导

- 有多个风扇在位时，只有 FANMCU 镜像文件支持升级的风扇，才能进行固件更新。
- 仅支持在开机状态下更新 FANMCU 固件，更新过程中请勿关机或插拔电源，否则可能会导致更新失败或风扇无法识别。

- FANMCU 固件更新过程中风扇以最大转速旋转，调速模式可以设置成功但不会立即生效，将在固件更新结束后生效。
- 如果固件更新失败，风扇的 MCU 会无法正常运行，风扇会以最大速度旋转，请尝试再次固件更新，更新成功后 MCU 将恢复正常。

2. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面。

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件，如图 8-39 所示。

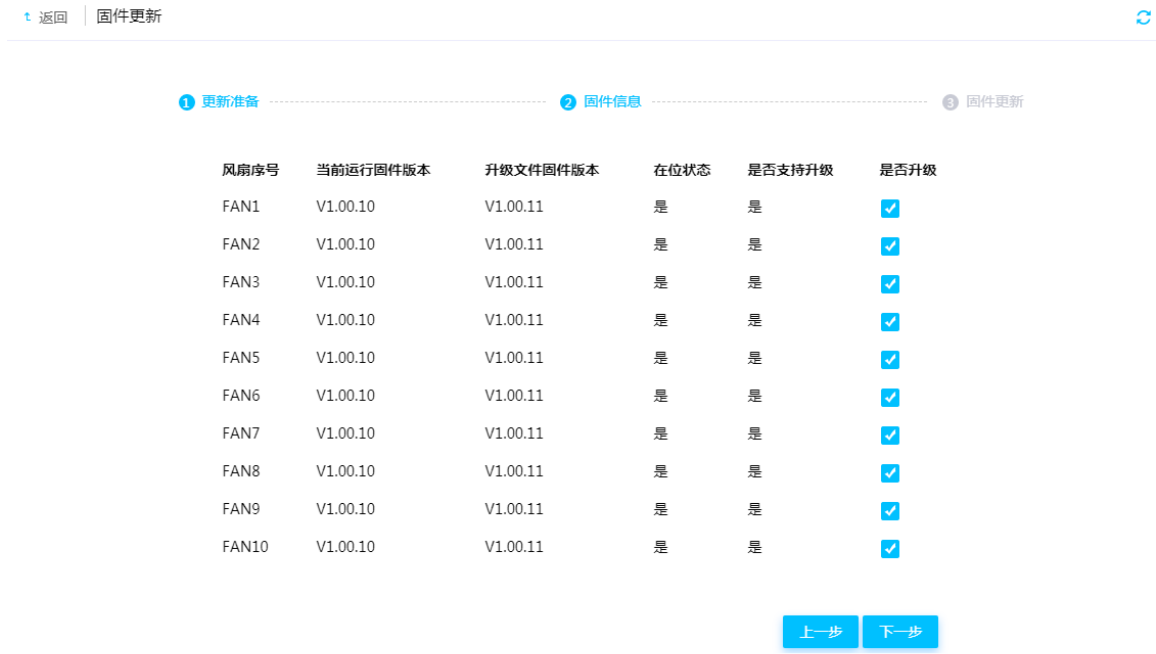
- 选择本地上传方式时，先选择固件类型，然后在“请选择固件镜像”栏，单击<浏览>按钮，在对话框中选择固件镜像。
- 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。

图8-39 FANMCU 固件更新

(4) 单击<下一步>按钮，HDM 会校验固件镜像文件的签名信息，校验通过后进入固件信息确认页面。

(5) 确认支持升级的风扇信息、当前运行固件版本和升级文件固件版本的版本号正确后，单击<下一步>按钮，开始更新固件。

图8-40 固件信息确认



(6) 更新完成后，固件立即生效。

3. 参数说明

- 镜像名称：固件镜像的文件名（包含后缀名）。
- 服务器地址：TFTP 服务器的地址，注意与 tftpd 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。

4. 注意事项

- 目前仅部分服务器支持更新风扇的 MCU 固件，具体支持情况请以界面实际显示为准。
- 更新过程中，如果某个风扇更新失败，将会尝试再次更新，最多重复 2 次。

8.6.12 通过 REPO 更新固件

本功能可以通过 REPO 带外更新服务器的各类存储控制卡、网卡和硬盘等部件的固件。关于 REPO 固件镜像文件的下载和使用指导，请联系技术支持。

说明

- 仅 HDM-2.52、iFIST-1.32 及以后的版本支持通过 REPO 更新固件。
- 如果服务器不支持 iFIST 软件，则无法通过 HDM Web 上传 REPO 固件镜像文件并更新固件。

1. 配置限制和指导

- 通过 REPO 更新固件后，需要配合 iFIST 软件使新固件生效，请确保 iFIST 已更新到和当前 HDM 版本配套的版本，软件版本配套信息请联系技术支持。

- 固件更新完成后，服务器首次重启会自动进入 iFIST 使新固件生效，固件生效期间请勿重启服务器或拔插电源。待新固件生效后，服务器会再次自动重启进入固件更新前的启动项。
- 下载 REPO 固件镜像文件时，MD5 文件会和镜像文件一起打包下载。
- 上传 REPO 固件时，请确保固件镜像文件的大小不超过 300MB，且 MD5 文件的大小不超过 1024 个字节。

2. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面。

(2) 单击<固件更新>按钮，进入上传固件镜像文件页面。

(3) 配置上传固件镜像的方式，建议优先使用本地上传方式上传固件，如图 8-41 所示。

- 选择本地上传方式时，先选择固件类型。然后在“请选择固件镜像”栏，单击<浏览>按钮上传固件镜像文件。（可选）最后在“MD5 文件(可选)”栏，单击<浏览>按钮上传 MD5 校验文件。
- 选择 TFTP 方式时，先输入 TFTP 服务器地址和镜像名称，再选择固件类型。（可选）最后输入 MD5 文件名称。

图8-41 上传 REPO 固件

(4) 选择固件更新配置和更新选项。

(5) 单击<下一步>按钮，进入固件信息确认页面，如图 8-42 所示。

图8-42 固件信息确认页面

(6) 确认无误后，单击<下一步>按钮，开始更新固件。

(7) 固件更新成功后，需要手动或自动重启服务器进入 iFIST 使新固件生效。

(8) 新固件生效后，可以进入“操作日志”页面查看更新结果。

3. 参数说明

- 镜像名称：REPO 固件镜像的文件名（包含后缀名.iso）。
- MD5 文件：存储固件镜像的 MD5 校验值的文件名（包含后缀名.txt），上传该文件后 HDM 会对 REPO 固件的完整性进行校验。
- 服务器地址：TFTP 服务器的地址，注意与 TFTP 工具 Server interfaces 栏的地址相同。
- 固件类型：选择和固件镜像文件一致的固件类型。
- 更新配置：通过 REPO 更新固件后，需要重启服务器才能生效，可以选择自动重启或手动重启。
  - 勾选<立即重启服务器>选项，固件更新完成后会自动重启服务器使新固件生效。
  - 勾选<稍后手动重启服务器>选项，固件更新完成后需要手动重启服务器使新固件生效。
- 更新选项：选择通过 REPO 更新固件的方式。
  - 勾选<仅高版本升级>选项，HDM 只更新 REPO 固件中高于当前运行的固件版本的部件固件，其他部件将忽略升级。
  - 勾选<强制升级>选项，HDM 会更新 REPO 固件中的所有部件固件。

8.6.13 重启 HDM

重启 HDM 会导致当前 HDM 连接全部中断，正常启动后恢复。重启 HDM 不影响 HDM 当前配置。

1. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面，如图 8-22 所示。

(2) 单击<重启 HDM>按钮，弹出“确认重启 HDM”对话框，单击<确定>按钮。

2. 注意事项

- 重启 HDM 会导致之前保存的录像文件丢失，请在重启 HDM 前备份录像文件。
- 重启 HDM 过程中，请勿对服务器进行上下电，否则可能会导致 HDM 部分功能以及操作系统出现异常。

8.6.14 重启 CPLD

CPLD 和 PFRCPLD 固件升级后，可以通过重启 CPLD 使新固件立刻生效，不需要断电后再重新上电。

说明

- G3 服务器中，仅 R2700 G3、R2900 G3、R4400 G3、R4700 G3、R3800 G3、R5300 G3 支持重启 CPLD。
- G5 系列服务器（B5700 G5 除外）支持通过重启 CPLD 功能使 PFRCPLD 新固件生效。

1. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面，如图 8-22 所示。

(2) 单击<重启 CPLD>按钮，弹出“确认重启 CPLD”对话框，单击<确定>按钮。

2. 注意事项

- 重启 CPLD 会导致 HDM 立刻重启。
- 只有服务器处于关机状态时，才允许重启 CPLD。开机状态时，不允许重启 CPLD。

8.6.15 HDM 主备切换

为了提升系统的可靠性，对升级 HDM 固件使用双镜像备份技术。用户登录的 HDM 界面使用的是主分区镜像。使用主备机制可以保证在 HDM 升级过程中，不影响 HDM 正常业务。

HDM 主备切换的方式有以下两种：

- 方式一：对 HDM 进行固件更新，更新的是备分区镜像。固件更新完成后，HDM 重启会自动进行主备切换。
- 方式二：单击<主备切换>按钮，进行主备切换。

1. 操作步骤

(1) 单击[远程运维/固件更新]菜单项，进入固件更新页面，如图 8-22 所示。

(2) 在主备切换部分，检查主备分区镜像版本，单击<HDM 主备切换>按钮。

2. 注意事项

主分区镜像升级后请进行主备切换，然后再次进行固件更新，将主备镜像升级到同一版本。

8.7 开机自检码

系统开机过程中，每个阶段都会生成自检码，通过自检码可以监测本次或最近一次开机的进程。

说明

如需了解开机自检码的具体含义，请联系技术支持。

1. 操作步骤

(1) 单击[远程运维/开机自检码]菜单项，进入开机自检码页面，如图 8-43 所示。

(2) 在该页面查看系统开机自检码的记录。

图8-43 开机自检码

2. 参数说明

- 当前开机自检码：系统启动到当前阶段时的自检码。
- 开机自检码：显示系统本次或最近一次开机过程中的所有自检码。

8.8 安全面板

说明

- 仅 G5 系列服务器支持安全面板功能，R5300 G5、R5500 G5 和 B5700 G5 服务器不支持安全面板。
- 仅 HDM-2.13 及以后的版本支持安全面板功能。

通过本功能可以查看安全面板的在位状态，开启面板的 Logo 灯和氛围灯状态，并设置氛围灯的模式。

1. 操作步骤

(1) 单击[远程运维/安全面板]菜单项，进入安全面板设置页面，如图 8-44 所示。

(2) 查看安全面板是否处于在位状态。

(3) 如果是，在面板设置栏选择是否开启 Logo 灯、氛围灯，并设置氛围灯的模式。

- 如果氛围灯的模式选择“状态关联”，氛围灯会根据服务器的运行阶段变化而变化，还可以选择是否关联服务器的健康状态。

(4) 如果氛围灯的模式选择“自定义”，可以设置氛围效果和灯光颜色。

(5)　单击<保存>按钮，完成操作。

图8-44 面板控制

2. 参数说明

- 氛围灯：包括“明亮”、“柔和”和“关闭”三个状态，如果选择开启氛围灯，建议选择“柔和”选项以降低服务器能耗。
- 健康状态关联：开启关联后，氛围灯的状态会根据服务器的健康灯状态变化而变化，具体显示状态请参见服务器用户指南。

8.9 服务U盘

通过 U 盘刻录工具把 U 盘诊断工具的镜像文件烧写到普通 U 盘中，烧写成功后该 U 盘就变成了服务 U 盘，服务 U 盘目前仅支持“自动下载 SDS 日志”功能。将服务 U 盘接入服务器后，可以查看并设置服务 U 盘的状态和功能。

说明

- 仅 G5 系列服务器支持服务 U 盘功能， B5700 G5 服务器不支持服务 U 盘功能。
- 仅 HDM-2.25 及以后的版本支持服务 U 盘功能。

1. 操作步骤

(1) 单击[远程运维/服务 U 盘]菜单项，进入服务 U 盘页面，如图 8-45 所示。

(2) 查看 U 盘的状态。

(3) 选择是否启用服务 U 盘。

(4) 启用服务 U 盘后，可以选择开启“自动下载 SDS 日志”功能。

(5) 单击<保存>按钮，完成操作。

(6) （可选）如果服务 U 盘处于运行状态，请重新拔插 U 盘使配置生效。

图8-45 服务 U 盘

2. 参数说明

- U 盘状态：服务 U 盘的状态，包括“在位”，“不在位”和“运行中”三种状态。

- 是否自动下载 SDS 日志：开启此功能后，服务 U 盘会在接入服务器后，自动下载服务器的 SDS 日志到 U 盘中的“Sds_And_SmartTest/ServiceUdisk”路径。

3. 注意事项

- 通过服务 U 盘下载 SDS 日志时，如有其他用户正在下载 SDS 日志，U 盘会自动弹出。请等待其他用户下载完成后，再将 U 盘重新接入服务器。
- 通过服务 U 盘下载 SDS 日志前，请确保 U 盘的可用空间大于 500MB。
- 当服务 U 盘处于运行状态时，请勿强制拔出 U 盘，否则可能会导致 U 盘异常。
- 请勿频繁拔插服务 U 盘，否则可能会导致 U 盘异常。
- 当服务器同时接入多个服务 U 盘时，服务器只能识别到最先接入的那个 U 盘。

9 用户&安全

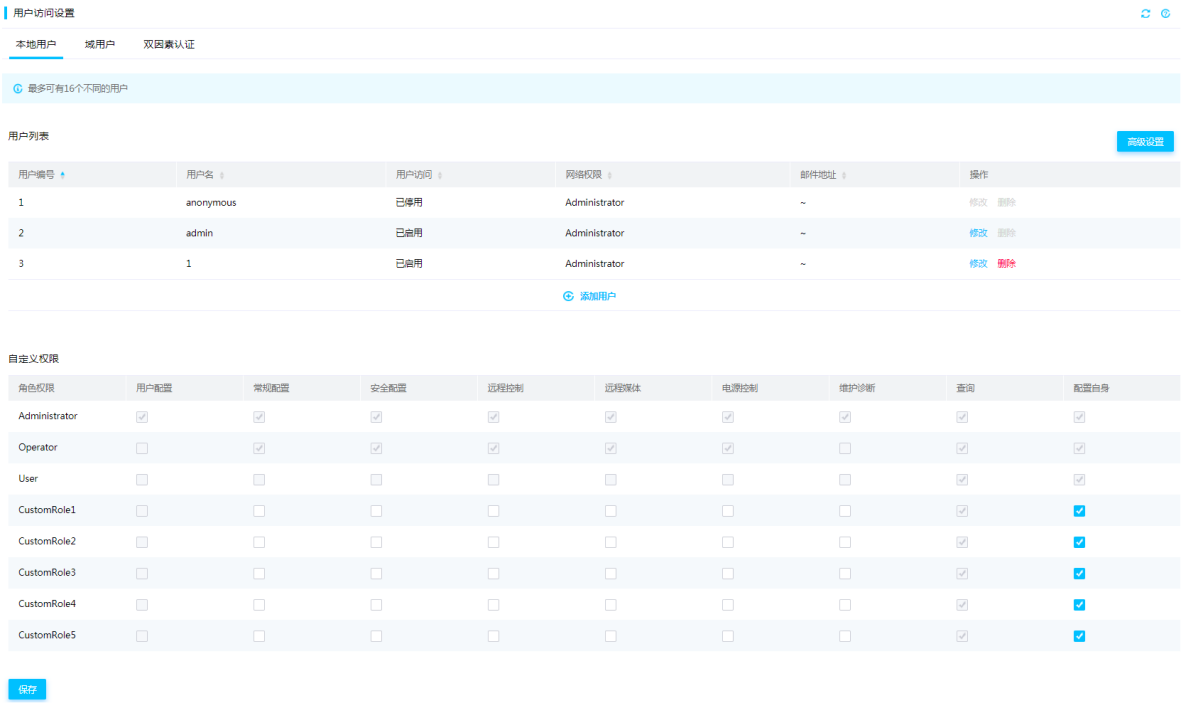
9.1 用户访问设置

在用户访问配置页面可以配置本地用户和域用户（包括 LDAP 和 AD 用户），通过这些用户可以访问 HDM Web 界面。用户还可以开启双因素认证功能，对登录 HDM 的用户执行“静态密码”+“动态密码”的双重认证。

9.1.1 查看本地用户

通过本功能可以查看 HDM 所有本地用户的详细信息，如图 9-1 所示。

图9-1 查看本地用户



1. 操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，进入本地用户页面。

(2) 通过页面中的列表，可以查看 HDM 所有用户的详细信息。

2. 参数说明

- 用户名：用户名称。
- 用户访问：用户能否访问 HDM Web 界面。
- 网络权限：用户所拥有的网络访问等级，包括以下等级。

- Administrator：管理员，对所有功能具有读取和写入权限。
- Operator：操作员，对所有功能具有读取权限，对部分功能具有写入权限，能执行日常的基础操作。
- User：用户，具有只读访问权限，无法修改 HDM 配置。
- CustomRole1～CustomRole5：自定义权限组用户，管理员可以配置用户所拥有的权限。
- None：预设账户。

- 邮件地址：HDM 用户作为收件人的电子邮箱地址。

9.1.2 本地用户密码规则高级设置

该功能用于配置本地用户的密码规则。

1. 操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，进入本地用户页面。

(2) 单击<高级设置>按钮，弹出对话框，如图 9-2 所示：
- 勾选开启/关闭密码复杂度检查。
- 输入密码有效期等信息。

(3) 单击<确定>按钮，完成操作。

图9-2 密码规则高级设置

2. 参数说明

- 密码复杂度检查：选择关闭或开启密码复杂度检查功能。
  - 关闭该功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。
    - 密码长度为 2～20 个字符；
    - 仅支持字母、数字、空格和特殊字符`~!@#$%^&*()_+-=[]\{}|;':",./<>?，区分大小写。
  - 开启该功能时，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。
    - 密码长度为 8～20 个字符，仅支持字母、数字、空格和特殊字符 `~!@#$%^&*()_+-=[]\{}|;':",./<>?，区分大小写；
    - 至少包含大写字母、小写字母和数字中的两种字符；
    - 至少包含一个空格或特殊字符；
    - 不能与用户名或用户名的倒序相同；
    - 需符合“禁用历史密码”要求。
- 密码有效期：用户密码的使用期限，临近使用期限前，HDM 会提醒用户更换密码。默认管理员不受密码有效期配置影响。

- 禁用历史密码：用户修改密码时，禁止使用设置次数内的历史密码。
- 登录失败锁定：用户登录失败的次数达到设定的次数后，系统会锁定该用户的登录。
- 登录失败锁定时长：用户由于登录失败达到登录失败锁定次数后，被系统锁定的时长。用户被锁定后，在失败锁定时长内不能登录 HDM。

9.1.3 自定义用户权限

自定义用户的网络权限，通过本功能可以为 CustomRole1～CustomRole5 配置名称和操作权限。

说明

仅 HDM-2.03 及以上版本支持自定义用户权限。

1. 操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，进入本地用户页面。

(2) 单击角色权限右侧的图标，可以修改 CustomRole 1～CustomRole 5 的权限名称。

(3) 在自定义权限栏配置 CustomRole1～CustomRole5 的操作权限，如图 9-3 所示。

(4) 单击<保存>按钮，完成操作。

图9-3 自定义用户权限

2. 参数说明

- 角色权限：角色组的网络权限。
- CustomRole1～CustomRole5：管理员可以配置自定义权限组所拥有的名称和操作权限，缺省拥有查询的权限。权限组名称长度为 1～16 个字符，仅支持字母、数字、句点（.）、连接符（-）和下划线（_）和特殊字符（@），区分大小写。
- 用户配置：包括本地用户配置、LDAP 用户配置、AD 用户配置、双因素认证、导入/导出配置和 HDM 联合管理的操作权限。

- 常规配置：包括设置资产标签、网络配置、NTP 配置、SNMP 配置和告警设置（SMTP、Trap、Syslog、应急诊断）、事件日志、操作日志、录像回放和安全面板设置的操作权限。
- 安全配置：包括服务配置、防火墙、SSL 证书、PFR 固件保护、登录安全性信息的操作权限。
- 远程控制：包括存储信息管理（RAID 配置和物理盘管理）、系统资源监控设置、硬分区配置、KVM（电源控制、镜像挂载除外）、H5 KVM（电源控制、镜像挂载除外）、VNC 密码管理、系统启动项、UID 灯控制、SOL 串口设置和 MCA 策略的操作权限。
- 远程媒体：包括虚拟媒体配置、KVM 镜像挂载、H5 KVM 镜像挂载的操作权限。
- 电源控制：包括电源管理、物理电源按钮控制、NMI 控制和风扇配置的操作权限。
- 维护诊断：包括硬盘点灯、蓝屏快照、固件更新、恢复 HDM 配置、HDM 主备切换、重启 HDM、重启 CPLD 和服务 U 盘的操作权限。
- 查询：Administrator 权限用户拥有查看所有信息的权限，非 Administrator 权限用户拥有查看除其他用户信息外的所有信息的权限。
- 配置自身：可以配置用户（仅限本地用户）自身的密码和 SSH 密钥。

9.1.4 添加本地用户

1. 操作步骤

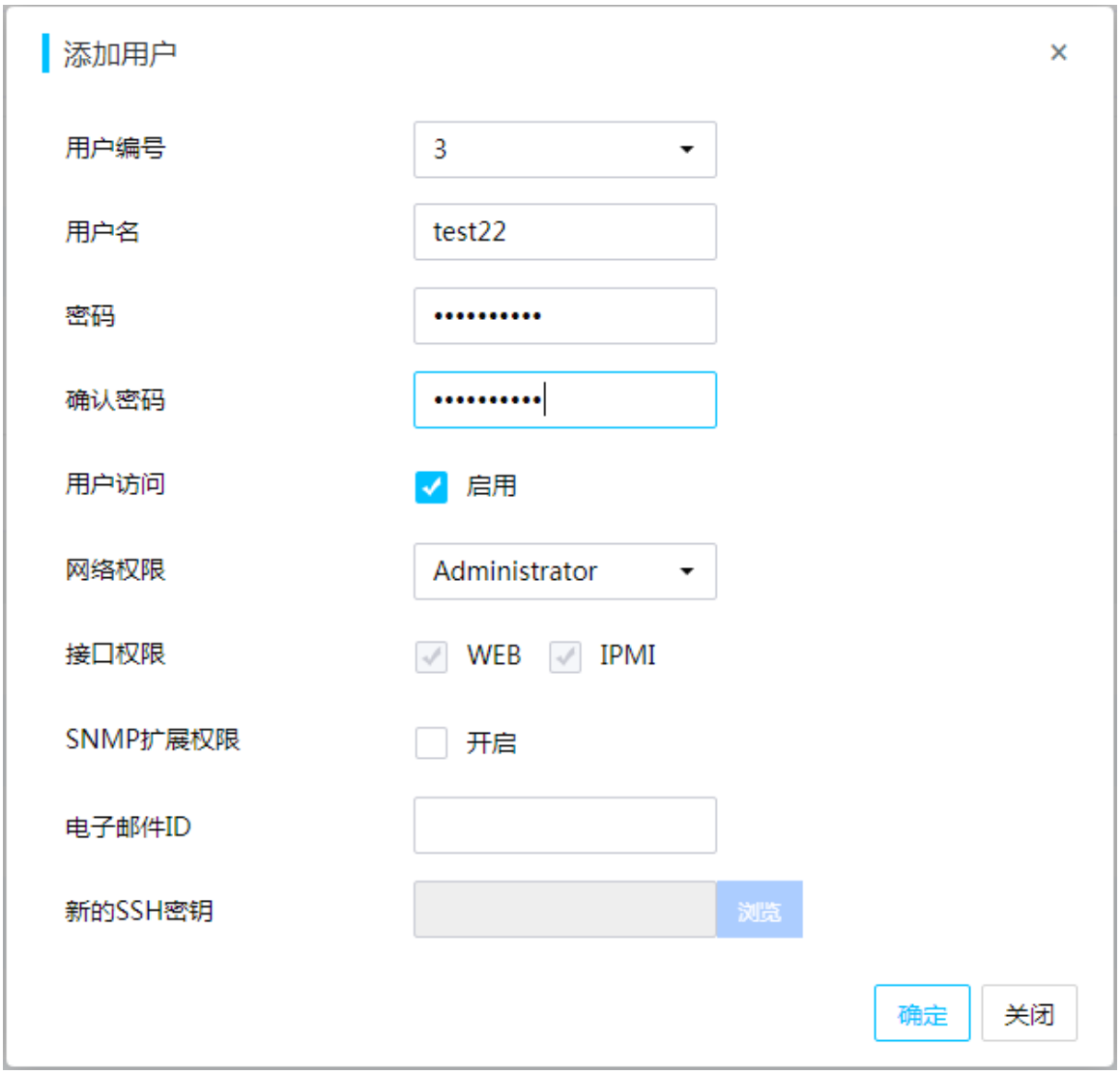
(1) 单击[用户&安全/用户访问设置]菜单项，进入本地用户页面。

(2) 单击<添加用户>按钮，弹出“添加用户”对话框，如图 9-4 所示。

(3) 在对话框中输入新用户的用户信息。

(4) 单击<确定>按钮，完成操作。

图9-4 添加用户



2. 参数说明

- 用户编号：用户的编号。
- 用户名：待创建的用户名称，长度为 1～16 个字符，仅支持字母、数字、句点（.）、连接符（-）和下划线（_）和特殊字符（@），区分大小写。
- 密码：用户的密码。密码需要符合的要求请参见本地用户密码规则高级设置。
- 用户访问：用户能否访问 HDM Web 界面。
  - 已启用：表示该用户可以通过 Web 接口和 IPMI 接口访问 HDM。
  - 已停用：表示该用户不可以通过 Web 接口和 IPMI 接口访问 HDM。
- 网络权限：用户所拥有的网络访问权限，包括以下权限。
  - Administrator：管理员，对所有功能具有读取和写入权限。

- Operator：操作员，对所有功能具有读取权限，对部分功能具有写入权限，能执行日常的基础操作。
- User：用户，对部分功能具有读取权限，无法修改 HDM 配置。
- CustomRole1～CustomRole5：自定义权限组用户，管理员可以配置用户所拥有的权限。
- None：预设账户。

- 接口权限：选择用户是否拥有 WEB 和 IPMI 的权限。
  - Administrator 和 Operator 用户缺省拥有 WEB 和 IPMI 权限，且不支持修改。
  - 其他用户可以选择是否拥有以上所有权限。
- SNMP 扩展权限：用户所拥有的 SNMP 的操作权限。开启 SNMP 扩展权限要求用户开启访问 HDM 权限且密码最小长度为 8 个字符
  - 读取：用户拥有 SNMP v3 只读的权限，通过 SNMP 进行 GET 操作，并且可接收 Trap 消息。
  - 读/写：用户拥有 SNMP v3 读写的权限，通过 SNMP 进行 GET 以及 SET 操作，并且可接收 Trap 消息。
- SNMP v3 鉴权算法：支持的鉴权算法为 SHA、MD5，缺省值为 SHA。
- SNMP v3 加密算法：支持的加密算法为 DES、AES，缺省值为 DES。
- 电子邮件 ID：HDM 用户作为收件人的电子邮箱地址。
  - 该功能需要和告警设置页面中的告警邮件配置配合使用。
  - 该邮箱地址可用于忘记登录密码时找回密码。
  - 请输入长度不超过 63 位字符的合法邮箱地址。
- SSH 密钥：SSH 密钥由登录 HDM 命令行的客户端工具生成，生成密钥时用户可以选择是否设置密码。如果设置，上传 SSH 密钥后，该用户登录 HDM 命令行时无需输入用户密码，只需要输入设置的密码；如果不设置，上传 SSH 密钥后，该用户可以免密登录 HDM 命令行。当前支持 RSA、ECDSA 和 ED25519 格式的密钥。
  - 当密钥格式为 RSA 时，支持长度为 1024 位、2048 位、4096 位。
  - 当密钥格式为 ECDSA 时，支持长度为 256 位、384 位、521 位。
  - 当密钥格式为 ED25519 时，支持长度为 256 位。

9.1.5 修改本地用户

1. 操作步骤

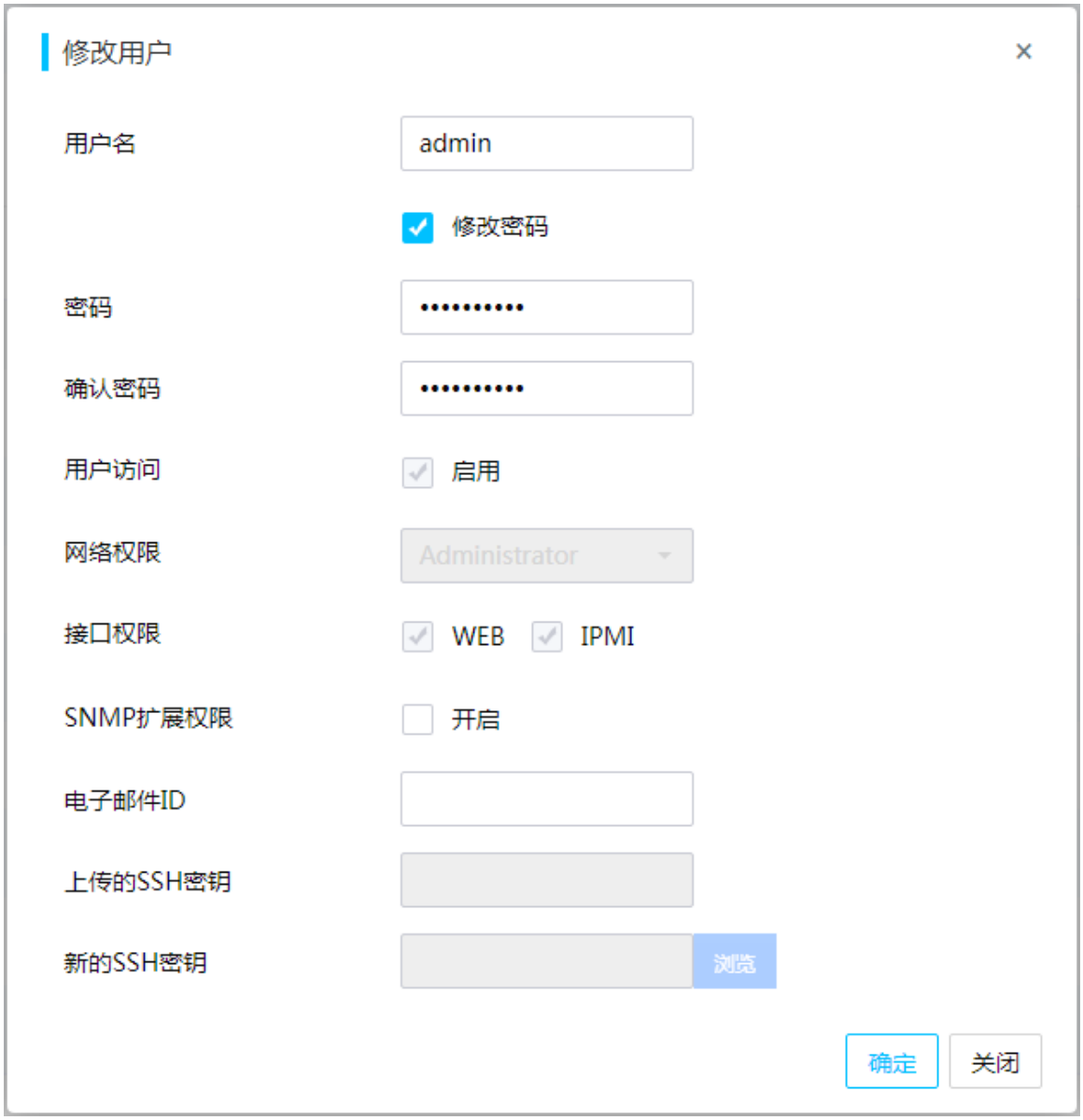
(1) 单击[用户&安全/用户访问设置]菜单项，进入本地用户页面。

(2) 在用户列表中选择一个用户，单击<修改>按钮，弹出“修改用户”对话框，如图 9-5 所示。

(3) 在“修改用户”对话框中，输入需修改的用户配置信息。

(4) 单击<确定>按钮，完成操作。

图9-5 修改用户



2. 注意事项

当前已存在会话的用户，不支持修改该用户的用户名。

9.1.6 删除本地用户

1. 操作步骤

(1) 单击[配置/用户配置]菜单项，进入用户配置页面。

(2) 在用户列表中选择一个用户，单击<删除>按钮，跳出对话框。

(3) 在对话框中单击<确定>按钮，完成操作。

2. 注意事项

不允许删除当前已存在会话的用户。

9.1.7 用户权限

用户的网络权限，不同机型支持的功能不完全一样，具体差异请以界面显示为准。

表9-1 HDM 用户权限列表

模块/功能		Administrator	Operator	User
用户配置	本地用户配置	√	×	×
	LDAP配置	√	×	×
	AD配置	√	×	×
	双因素认证	√	×	×
	导入/导出配置	√	×	×
	HDM联合管理	√	×	×
常规配置	设置资产标签	√	√	×
	配置专用网口	√	√	×
	配置共享网口	√	√	×
	DNS配置	√	√	×
	设置网口模式	√	√	×
	设置LLDP	√	√	×
	无线管理	√	√	×
	设置NTP服务器	√	√	×
	SNMP配置	√	√	×
	邮件通知设置	√	√	×
	Trap设置	√	√	×
	Syslog设置	√	√	×
	事件日志设置（策略设置、保存、清除）	√	√	×
	保存或清除操作日志	√	√	×
	录像回放设置（设置、查看、下载）	√	√	×

模块/功能		Administrator	Operator	User
	安全面板设置	√	√	×
安全配置	服务配置	√	√	×
	防火墙配置	√	√	×
	SSL证书配置	√	√	×
	PFR固件保护配置	√	√	×
	登录安全性信息配置	√	√	×
远程控制	存储信息管理（RAID配置、物理盘管理）	√	√	×
	系统资源监控告警阈值设置	√	√	×
	硬分区配置	√	√	×
	KVM控制台（电源控制、镜像挂载除外）	√	√	×
	H5 KVM控制台（电源控制、镜像挂载除外）	√	√	×
	VNC密码管理	√	√	×
	设置系统启动项	√	√	×
	SOL串口配置	√	√	×
	UID灯设置	√	√	×
	MCA策略配置	√	√	×
远程媒体	虚拟媒体配置	√	√	×
	KVM镜像挂载	√	√	×
	H5 KVM镜像挂载	√	√	×
电源控制	设备上下电	√	√	×
	NMI控制	√	√	×
	电源配置（工作模式、AC恢复配置）	√	√	×
	挂耳电源按钮屏蔽	√	√	×
	电源功率配置（总功率告警阈值、功率封顶）	√	√	×
	风扇配置	√	√	×

模块/功能		Administrator	Operator	User
	节能设置	√	√	×
维护诊断	设置硬盘定位灯	√	×	×
	事件日志设置（策略设置、保存、清除）	√	×	×
	保存操作日志	√	×	×
	固件更新	√	×	×
	恢复HDM配置	√	×	×
	重启HDM	√	×	×
	HDM主备切换	√	×	×
	重启CPLD	√	×	×
	服务U盘设置	√	×	×
查询	查看基本信息	√	√	√
	查看基本状态	√	√	√
	查看设备健康状态	√	√	√
	查看用户会话	√	√	√
	查看存储信息	√	√	√
	查看系统信息	√	√	√
	查看温度海洋	√	√	√
	查看风扇配置信息	√	√	√
	查看系统启动项信息	√	√	√
	查看系统资源监控信息	√	√	√
	一键收集查看并下载	√	√	√
	查看事件日志	√	√	√
	查看操作日志	√	√	√
	查看蓝屏快照	√	√	√
	查看录像回放	√	√	√
	查看专用网口	√	√	√

模块/功能		Administrator	Operator	User
	查看共享网口	√	√	√
	查看DNS配置	√	√	√
	查看网口模式	√	√	√
	查看LLDP信息	√	√	√
	查看无线网络管理信息	√	√	√
	查看本地用户自身配置	√	√	√
	查看其他本地用户配置	√	×	×
	查看NTP服务器	√	√	√
	查看LDAP配置	√	√	√
	查看AD配置	√	√	√
	查看SNMP配置	√	√	√
	查看告警设置	√	√	√
	查看服务配置信息	√	√	√
	查看防火墙配置	√	√	√
	查看PFR固件保护设置	√	√	√
	查看SSL证书	√	√	√
	查看UID灯状态	√	√	√
	查看系统启动项	√	√	√
	查看SOL串口信息	√	√	√
	查看虚拟媒体信息	√	√	√
	查看安全面板设置	√	√	√
	查看服务U盘设置	√	√	√
	查看登录安全性信息	√	√	√
	查看双因素认证信息	√	√	√
	查看安全模块信息	√	√	√
	查看电源状态	√	√	√
	查看电源信息	√	√	√

模块/功能		Administrator	Operator	User
	查看电源配置（工作模式、AC恢复配置）	√	√	√
	电源功率配置（总功率告警阈值、功率封顶）	√	√	√
	查看历史功率信息	√	√	√
	查看开机自检码信息	√	√	√
	查看风扇配置	√	√	√
	查看节能设置	√	√	√
	查看HDM联合管理信息	√	√	√
	语言切换	√	√	√
	查看联机帮助	√	√	√
	刷新功能	√	√	√
	查看最新事件消息	√	√	√
	退出登录	√	√	√
配置自身	修改当前登录用户的密码和SSH密钥（仅限于本地用户）	√	√	√

9.1.8 启用 LDAP 配置功能

LDAP（Lightweight Directory Access Protocol，轻型目录访问协议）是一种基于网络的目录访问协议，以实现资源信息的高效管理。通过本功能，您可以启用 LDAP 认证并制定访问策略。完成配置后，您可以用 LDAP 目录服务器中设置的用户名和密码直接访问 HDM。

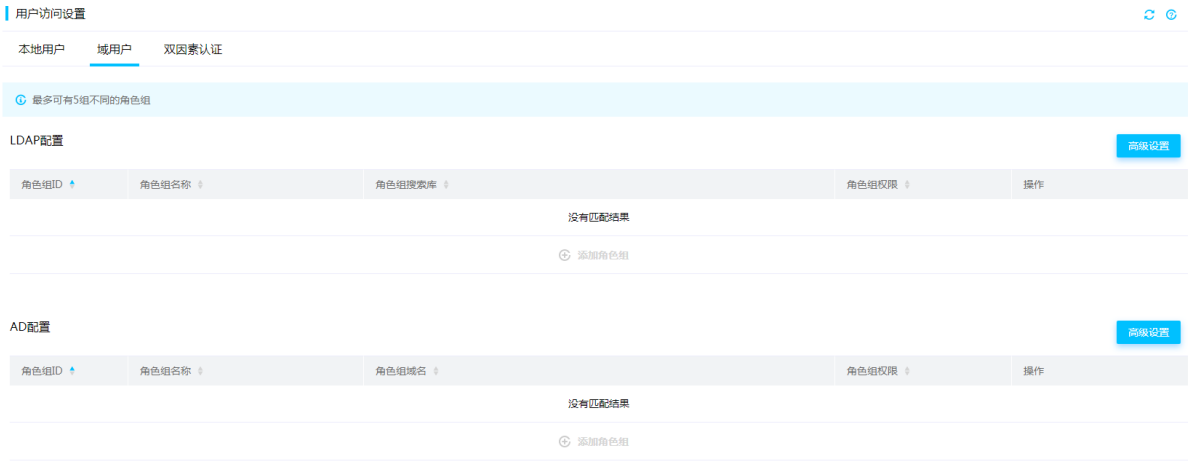
通过本功能可以对 LDAP 功能进行详细配置，并添加 LDAP 角色组。添加成功后，可以通过角色组里的用户可以直接访问 HDM。

启用 LDAP 功能之前，确保已有可以正常访问的 LDAP 服务器，如果没有，请参考 11.4 LDAP 配置搭建服务器。

1. 操作步骤

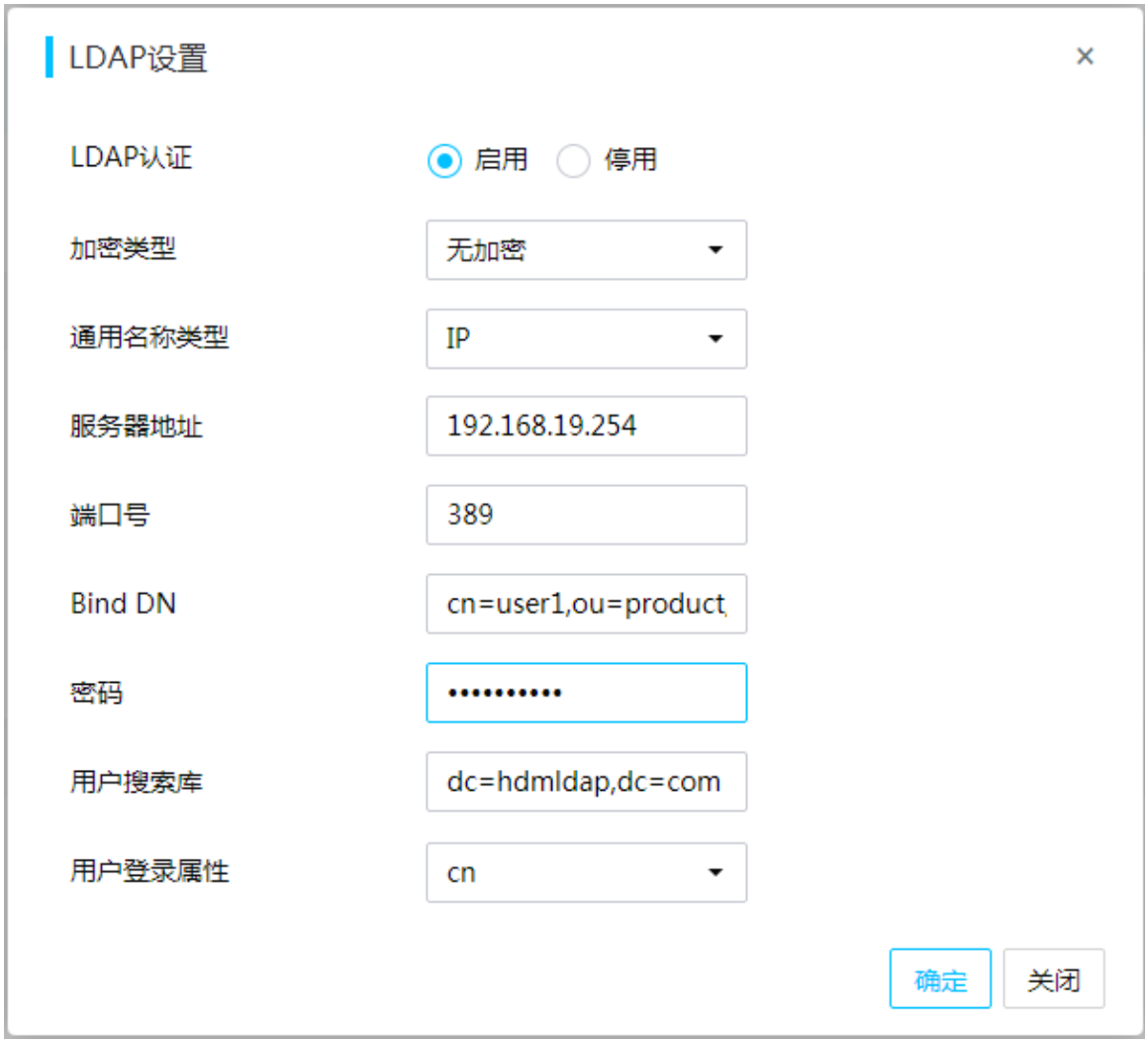
(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面，如图 9-6 所示。

图9-6 LDAP 配置



(2) 单击 LDAP 配置栏的<高级设置>按钮，跳出 LDAP 设置对话框，如图 9-7 所示。

图9-7 LDAP 高级设置



(3) 在对话框中勾选 LDAP 认证的<启用>选项，并配置相关信息。

(4) 单击<确定>按钮，完成操作。

2. 参数说明

- 加密类型：无加密表示 LDAP 和服务器之间建立的是无加密连接。SSL 表示 LDAP 和服务器之间建立的是 SSL 连接。
- 通用名称类型：IP 地址或域名地址。
- 服务器地址：LDAP 服务器的系统地址。支持 IPv4 地址、IPv6 地址和域名。
- 端口号：与 LDAP 服务器建立连接使用的指定端口号。对于 SSL 连接，缺省端口号为 636；对于其他连接，缺省端口号为 389；端口号范围为 1～65535，请确保与其他服务不冲突。
- Bind DN：绑定 LDAP 服务器和 HDM 的 LDAP 用户的 DN 信息，主要包括 CN 信息（或 UID 信息）、OU 信息和 DC 信息，字段之间以英文逗号隔开，长度最大支持 255 个字节。
  - CN：用户登录名。
  - UID：用户 ID。

- OU：组织单位信息，输入时从低级组织到高级组织。
- DC：用户所属的域名信息。

- 密码：Bind DN 中 LDAP 用户的登录密码。
- 用户搜索库：在 LDAP 服务器中搜索 Bind DN 中 LDAP 用户的文件夹路径，长度最大支持 255 个字节。
- 用户登录属性：LDAP 服务器识别用户的方法，支持 CN 或 UID 两种方法，需要和 Bind DN 中的 LDAP 用户信息保持一致。

9.1.9 添加/修改/删除 LDAP 角色组

1. 添加角色组操作步骤

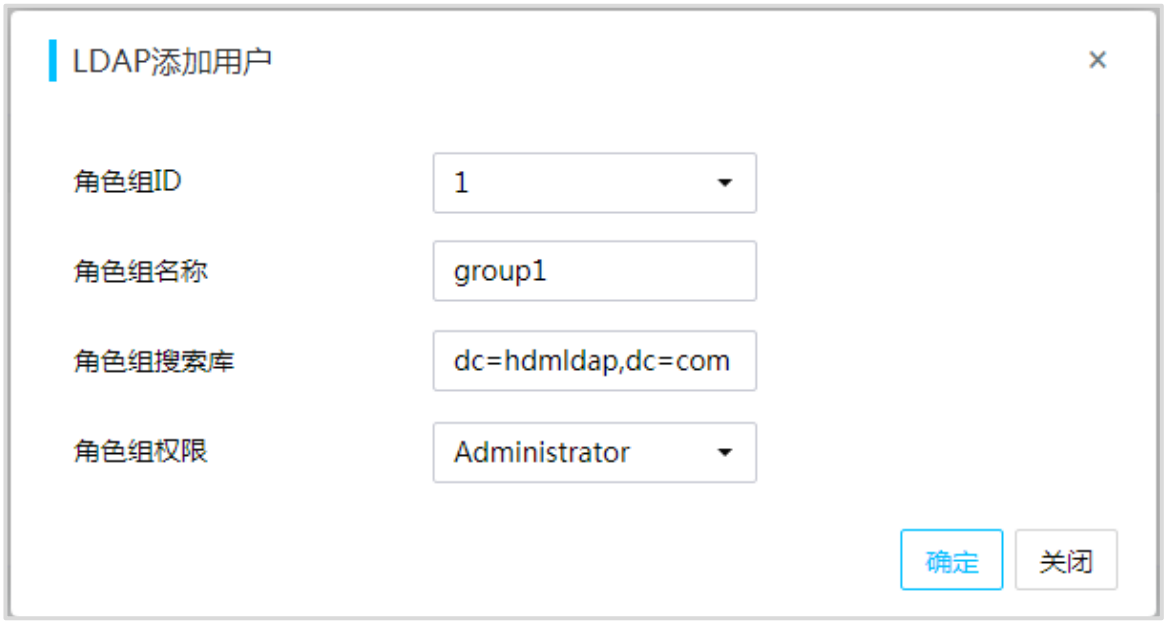
(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面。

(2) 单击 LDAP 配置栏的<添加角色组>按钮，完成操作。

(3) 在对话框中配置相关信息，如图 9-8 所示。

(4) 单击<确定>按钮，完成操作。

图9-8 添加用户



2. 修改角色组操作步骤

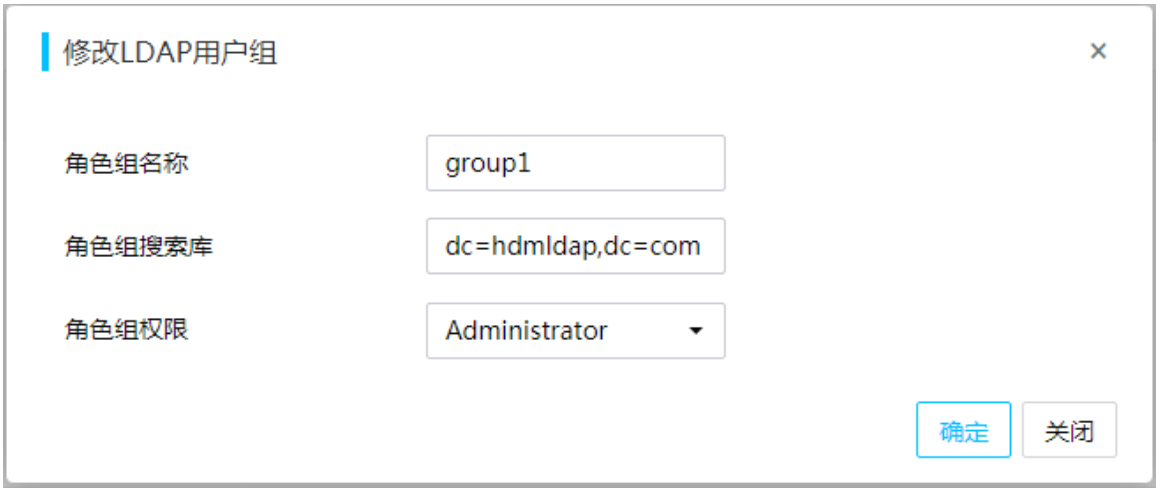
(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面。

(2) 在角色组列表选择一个角色组，单击<修改>按钮，完成操作。

(3) 在对话框中根据需要修改相关信息，如图 9-9 所示。

(4) 单击<确定>按钮，完成操作。

图9-9 修改 LDAP 用户组



3. 删除角色组操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面。

(2) 在角色组列表选择一个角色组，单击<删除>按钮，完成操作。

4. 参数说明

- 角色组 ID：角色组编号。
- 角色组名称：LDAP 服务器里已存在的角色组的名称。
- 角色组搜索库：角色组在 LDAP 服务器中搜索的文件夹路径，长度最大支持 255 个字节。
- 角色组权限：该角色组对应的网络权限。

9.1.10 启用 AD 配置功能

启用 AD 认证并制定访问策略后，可以通过 AD 目录服务器中设置的用户名和密码直接访问 HDM。通过本功能可以启用 AD 配置功能，添加 AD 角色组。添加成功后，可以通过角色组里的用户可以直接访问 HDM。

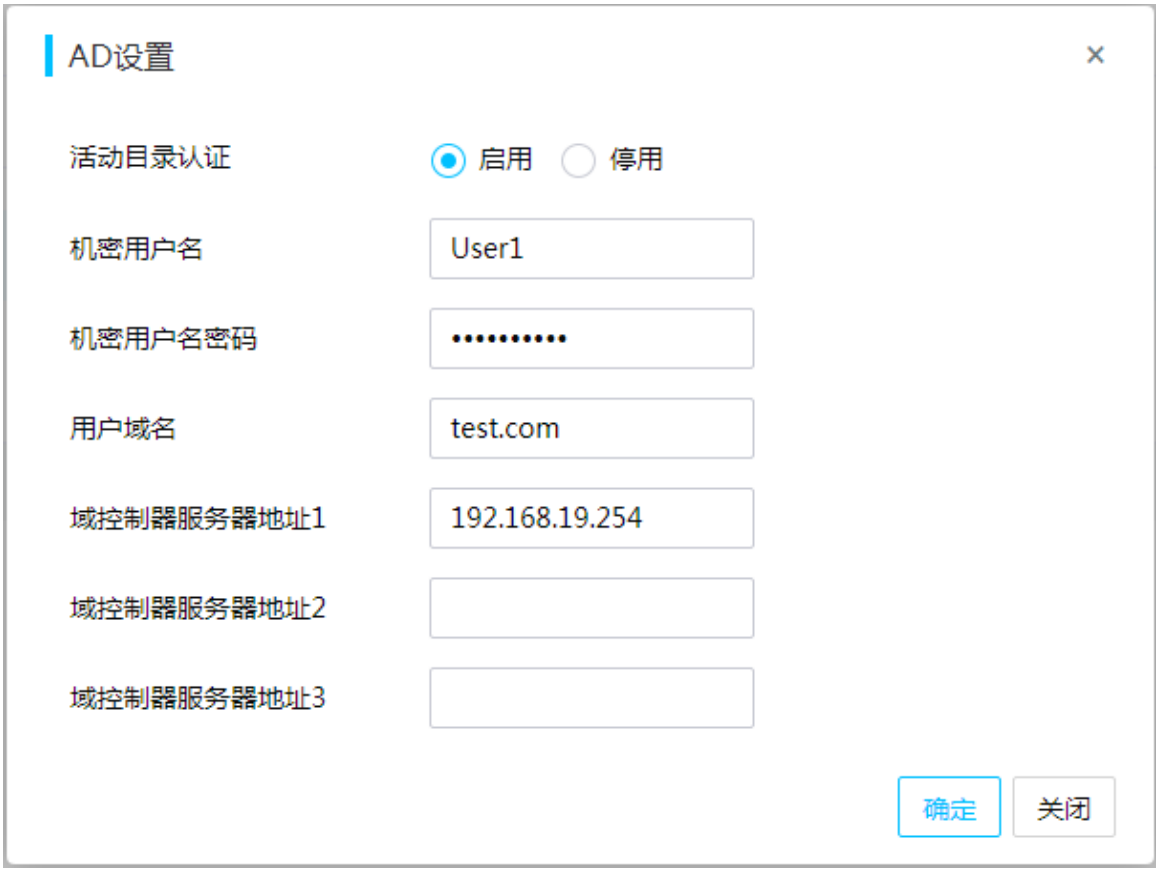
启用 AD 功能之前，确保已有可以正常访问的 AD 服务器。

1. 操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面，如图 9-6 所示。

(2) 单击 AD 配置栏的<高级设置>按钮，跳出 AD 设置对话框，如图 9-10 所示。

图9-10 AD 设置



(3) 在对话框中勾选活动目录认证的<启用>选项，并配置相关信息。

(4) 单击<确定>按钮，完成操作。

2. 参数说明

- 机密用户名：指定 AD 服务器的用户名。
  - 仅支持数字、字母，必须以字母开头。
  - 最大长度支持 64 个字符，可以为空。
- 机密用户名密码：指定 AD 服务器的密码。
  - 长度为 6～96 个字符，可以为空。
- 用户域名：指定机密用户的域名。
- 域控制服务器地址：AD 服务器的地址，支持 IP 地址和域名地址，第一组地址不能为空。

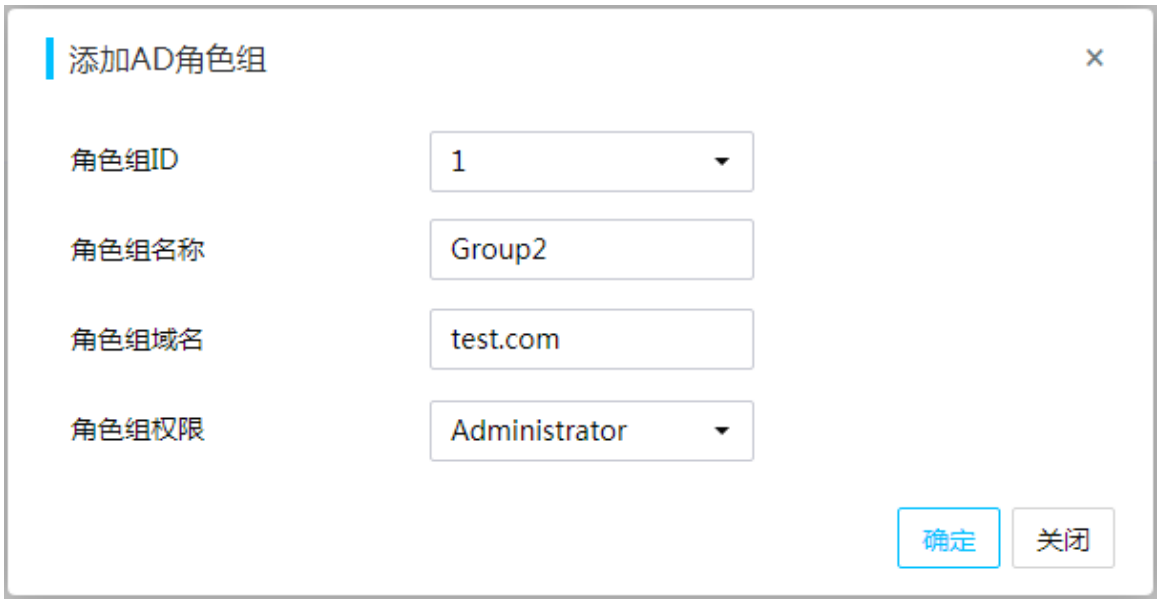
9.1.11 添加/修改/删除 AD 角色组

1. 添加角色组操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面，如图 9-6 所示。

(2) 在角色组列表选择一个空栏位，单击<添加>按钮，弹出添加 AD 角色组对话框，如图 9-11 所示。

图9-11 添加 AD 角色组



(3) 在对话框中配置相关信息。

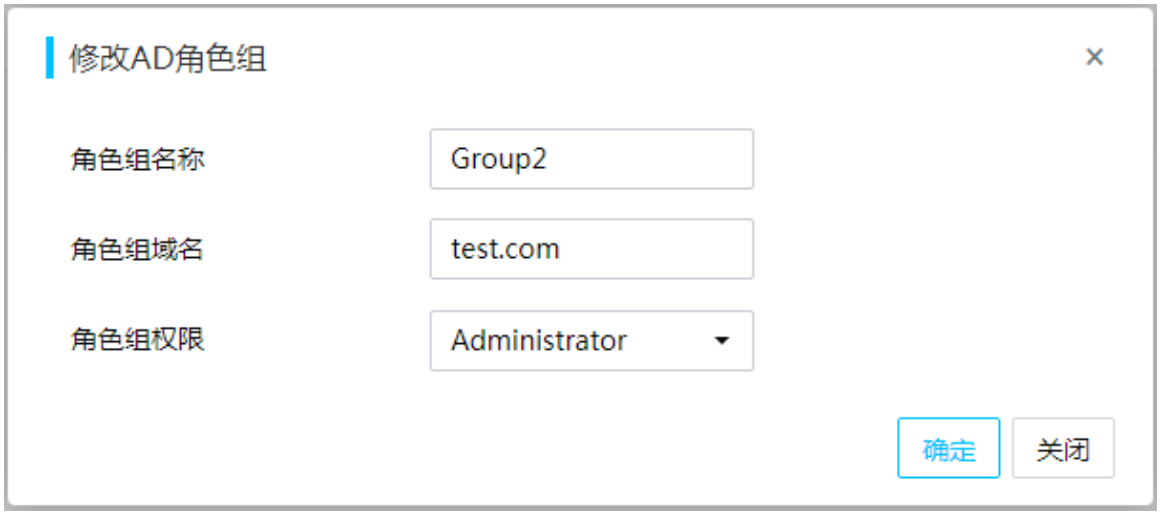
(4) 单击< 确定>按钮，完成操作。

2. 修改角色组操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面。

(2) 在角色组列表选择一个角色组，单击<修改>按钮，弹出修改 AD 角色组对话框，如图 9-12 所示。

图9-12 修改 AD 角色组



(3) 在对话框中根据需要修改相关信息。

(4) 单击<确定>按钮，完成操作。

3. 删除角色组操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，选择“域用户”页签，进入域用户页面。

(2) 在角色组列表选择一个角色组，单击<删除>按钮，弹出删除确认对话框。

4. 参数说明

- 角色组 ID：角色组编号。
- 角色组名称：AD 服务器里已存在的角色组的名称。
  - 仅支持数字、字母和特殊字符（_）和（-）。
  - 长度为 1～64 个字符。
- 角色组域名：角色组所在的域。
  - 仅支持数字、字母和特殊字符（_）、（-）和（.）。
  - 最大长度支持 255 个字符。
- 角色组权限：该角色组对应的网络权限。

9.1.12 双因素认证

通过本功能可以开启并设置双因素认证功能，提升 HDM 的安全性。HDM 支持宁盾动态令牌方案，在 HDM 上绑定 OTP（One-Time Password，一次性密码）服务器后，可以对登录 HDM 的用户执行“静态密码”+“动态密码”的双因素认证。开启双因素认证后，用户登录 HDM 时不仅需要输入用户名和静态密码，还要输入手机令牌或硬件令牌上的动态密码，所有信息校验通过后，才能登录成功。

说明

- 刀片服务器和 AE 模块不支持双因素认证功能。
- 仅 HDM-2.25 及以后的版本支持双因素认证功能。
- 开启双因素认证前，请保证有可访问的 OTP 服务器，并在 OTP 服务器上完成相关配置，包括添加 HDM 管理 IP 地址、添加 HDM 用户（包括本地用户和域用户）、设置用户的认证策略和令牌。
- 请谨慎配置双因素认证功能，可能会影响用户正常登录 HDM。
- 动态密码错误导致的用户登录失败达到系统锁定次数后，HDM 不会锁定该用户。

1. 操作步骤

(1) 单击[用户&安全/用户访问设置]菜单项，选择“双因素认证”页签，进入双因素认证配置页面，如图 9-13 所示。

图9-13 双因素认证

(2) 选择开启“双因素认证”功能。

(3) 输入 OTP 服务器地址、服务端口号和共享秘钥。

(4) 单击<保存>按钮，完成操作。

(5) 配置完成后，新建 HDM Web 会话需要在登录页面输入 HDM 用户名、静态密码和动态密码，才能登录 HDM，如图 9-14 所示。

图9-14 登录页面

2. 参数说明

- OTP 服务器地址：OTP 服务器的地址，支持 IPv4 地址及域名地址。
- 服务端口：OTP 服务器的服务端口号，缺省为 1812。
- 共享秘钥：在 OTP 服务器上添加 HDM 管理 IP 地址时设置的共享秘钥，长度为 1~64 个字符，支持英文字符、数字、特殊字符`~!@$%^&*()_+-=[]\{}|;':",./?，区分大小写。

3. 注意事项

- 开启双因素认证后，服务器的部分接口会受到影响，影响范围如表 9-2 所示。但接口的服务配置状态并不会被修改，关闭双因素认证后这些接口会恢复到功能开启之前的状态。

表9-2 双因素认证影响范围

接口类型	是否中断已存在会话或连接	是否屏蔽新建会话或连接
Web	否	否
SSH	否	是
Telnet	否	否
VNC	是	是

接口类型	是否中断已存在会话或连接	是否屏蔽新建会话或连接
Redfish	否	是
IPMI	是	是
SNMPv3	否	是
SOL	是	是

- 开启双因素认证后，其他不支持双因素认证的管理软件或功能（包括但不仅限于 HDM Mobile、其他服务器的 HDM 联合管理）无法通过 HDM 管理 IP 地址添加并管理当前服务器。

9.2 安全设置

9.2.1 防火墙

防火墙可以根据访问 HDM 的设备的 IP 地址、IP 地址段和 MAC 地址设置防火墙黑名单和白名单规则，黑名单的优先级比白名单高，仅允许符合规则的设备访问 HDM。

由于防火墙规则设置不当导致 HDM 无法访问时，可以通过 BIOS 恢复 HDM 默认设置，清除防火墙规则，具体操作请参考《BIOS 用户指南》。

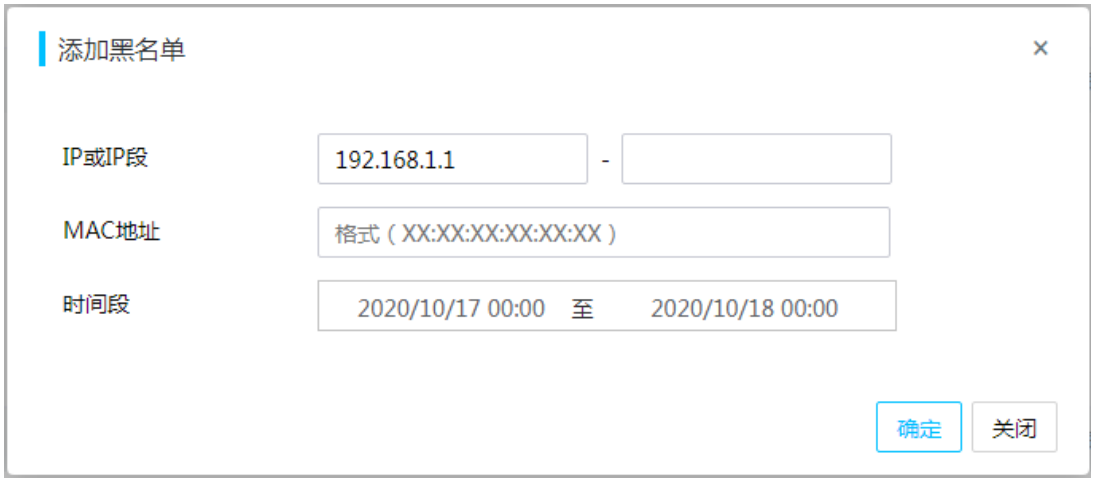
1. 添加黑名单规则操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择“防火墙”页签，进入防火墙页面，如图 9-15 所示。

图9-15 防火墙页面

(2) 单击黑名单栏的<添加新规则>按钮，跳出添加黑名单对话框，如图 9-16 所示。

图9-16 添加黑名单



(3) 输入 IP 地址（或 IP 地址段）、MAC 地址和时间段。

(4) 单击<确定>按钮，完成操作。

2. 删除黑名单规则操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择“防火墙”页签，进入防火墙页面，如图 9-15 所示。

(2) 选择要删除的黑名单规则条目。

(3) 单击<删除>按钮，在对话框中单击<确认>按钮，完成操作。

3. 修改黑名单规则操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择“防火墙”页签，进入防火墙页面，如图 9-15 所示。

(2) 选择要修改的黑名单规则条目。

(3) 单击<修改>按钮，跳出修改黑名单对话框，如图 9-17 所示。

图9-17 修改黑名单

(4) 修改 IP 地址（或 IP 地址段）、MAC 地址和时间段。

(5) 单击<确定>按钮，完成操作。

4. 添加白名单规则操作步骤

注意

- 添加白名单规则时，请先添加本机 IP 地址或 MAC 地址，以保证正常访问 HDM。
- 添加白名单规则后，白名单以外的地址均不能访问 HDM。

(1) 单击[用户&安全/安全设置]菜单项，选择“防火墙”页签，进入防火墙页面，如图 9-15 所示。

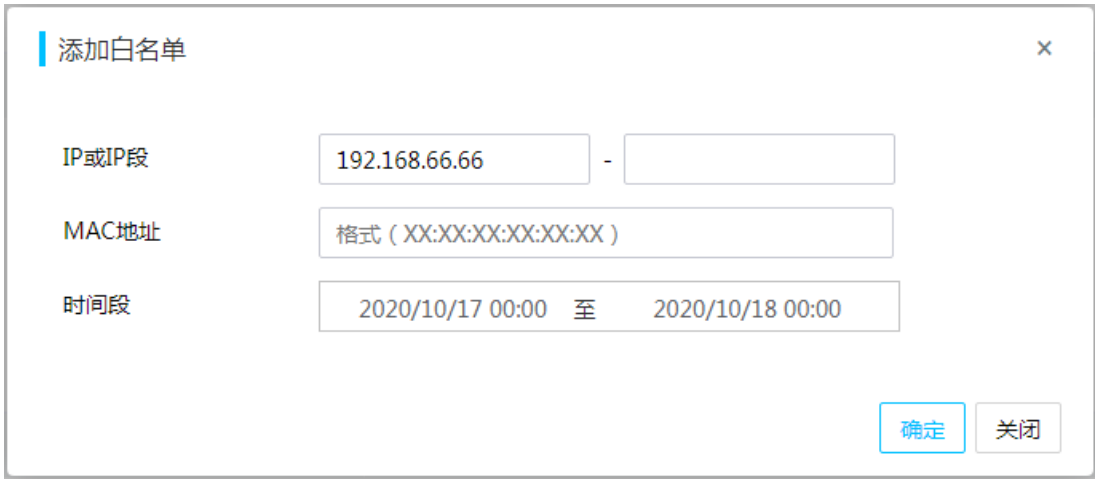
(2) 单击白名单栏的<添加新规则>按钮，跳出添加白名单对话框，如图 9-18 所示。

(3) 输入本机的 IP 地址（或 IP 地址段）、MAC 地址。

(4) 单击<确定>按钮，完成操作。

(5) 再重复步骤（1）～（4），添加其他 IP 地址（或 IP 地址段）和 MAC 地址。

图9-18 添加白名单



5. 删除白名单规则操作步骤

注意

删除白名单规则时，请谨慎操作。

(1) 单击[用户&安全/安全设置]菜单项，选择“防火墙”页签，进入防火墙页面，如图 9-15 所示。

(2) 选择要删除的白名单规则条目。

(3) 单击<删除>按钮，在对话框中单击<确认>按钮，完成操作。

6. 修改白名单规则操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择“防火墙”页签，进入防火墙页面，如图 9-15 所示。

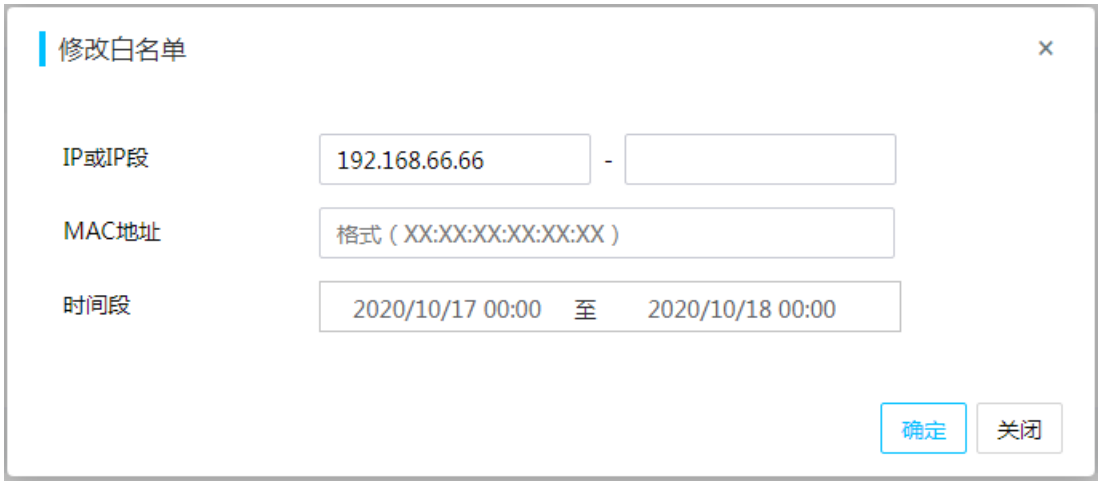
(2) 选择要修改的白名单规则条目。

(3) 单击<修改>按钮，跳出修改白名单对话框，如图 9-19 所示。

(4) 修改 IP 地址（或 IP 地址段）、MAC 地址和时间段。

(5) 单击<确定>按钮，完成操作。

图9-19 修改白名单



7. 参数说明

- IP 或 IP 段：访问 HDM 的设备 IP 地址或 IP 地址范围。
- MAC 地址：访问 HDM 的设备 MAC 地址。
- 时间段：防火墙规则有效期的开始时间和结束时间，缺省为空，表示规则永久生效。

8. 注意事项

- IP 地址（或 IP 地址段）与 MAC 地址可以组合设置，不能同时为空。
- 时间段开始时间和结束时间均以 HDM 时间为基准，且与 HDM 时间所在时区保持一致。
- 配置相同规则时，页面只显示一条。

9.2.2 SSL 证书

SSL（Secure Sockets Layer，安全套接字层）是一个安全协议，为基于 TCP 的应用层协议（如 HTTP）提供安全连接。使用 SSL 传输数据，会在客户端和 Web 服务器之间建立一条安全通道，可以保证数据传输的机密性，验证数据源的身份，并保证数据的完整性。

通过本功能，可以实现以下几个操作：

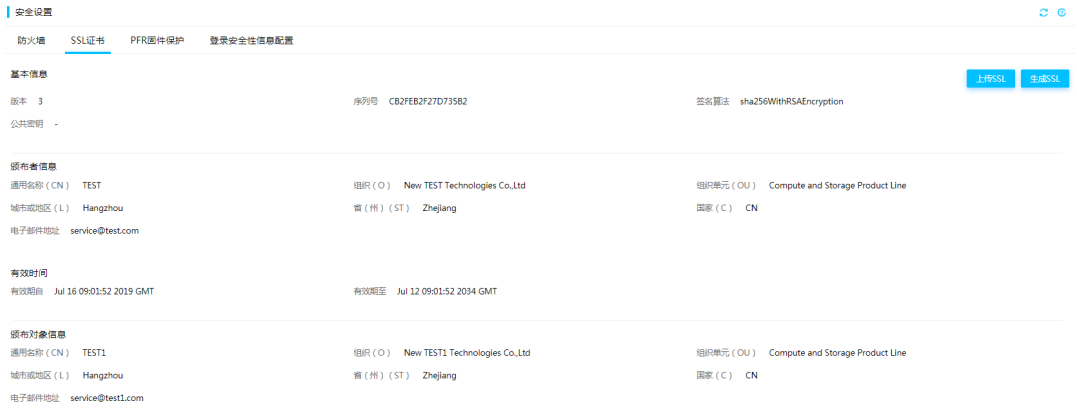
- 查看当前 SSL 证书的详细信息
- 上传 SSL 证书
- 生成 SSL 证书

1. 查看 SSL 证书信息操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择“SSL 证书”页签，进入 SSL 证书页面，如图 9-20 所示。

(2) 通过本页面，可以查看当前 SSL 证书的详细信息。

图9-20 查看 SSL



2. 上传 SSL 操作步骤

说明

SSL 证书根据来源可以分为两种:

- 从正式的证书颁发机构获取的 SSL 证书。（推荐）
- 用户自己使用工具生成的证书。

(1) 单击[用户&安全/安全设置]菜单项，选择“SSL 证书”页签，进入 SSL 证书页面,如图 9-20 所示。

(2) 单击<上传 SSL>按钮，弹出“上传 SSL”对话框，如图 9-21 所示。

图9-21 上传 SSL

(3) 单击新的证书选项的<浏览>按钮，弹出对话框，选择正确的 SSL 证书文件。

(4) 单击新的私钥选项的<浏览>按钮，弹出对话框，在窗口选择正确的私钥文件。

(5) 单击<确认>按钮，上传 SSL 证书文件和私钥文件到 HDM，完成操作。

说明

如果上传的是自己使用工具生成的证书，在上传后还需要确认客户端浏览器中是否已存在对应的根证书。下面以 IE 11.0 浏览器为例介绍如何在浏览器中查看并添加认证机构的根证书。

---

(6) 打开 IE 浏览器。

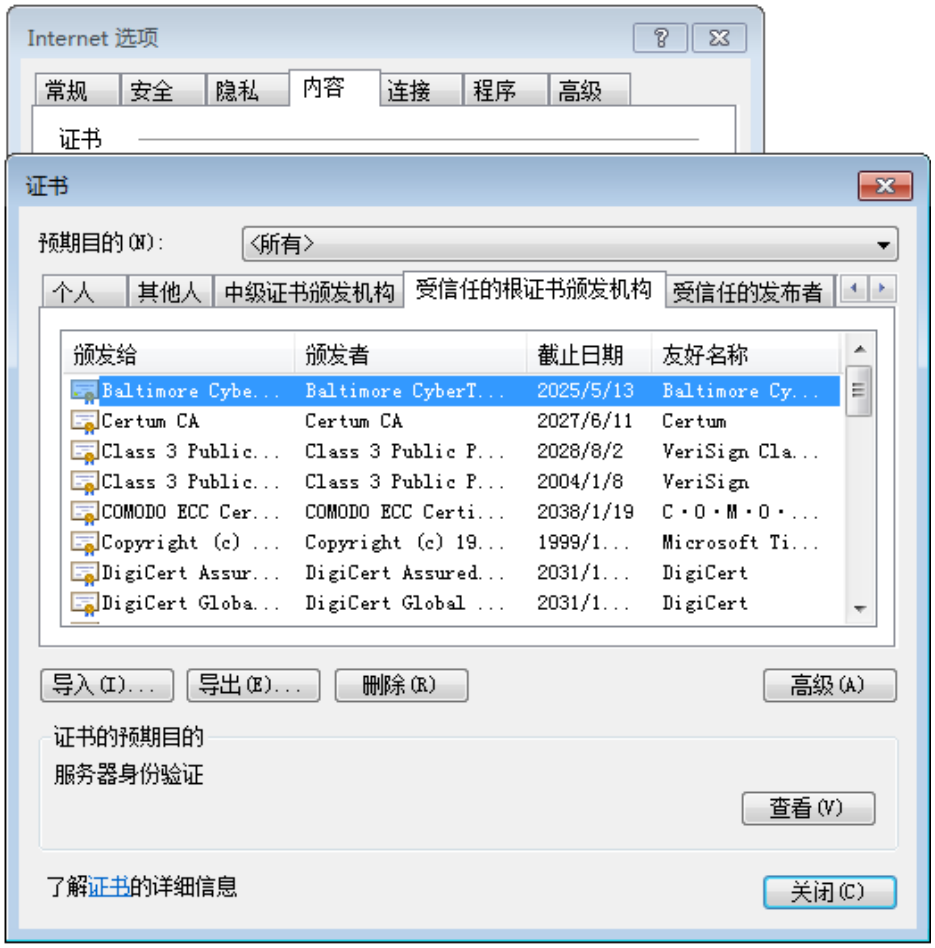
(7) 在工具栏中选择“工具>Internet 选项”，弹出“Internet 选项”窗口。

(8) 单击“内容”页签，再选择“证书”，弹出“证书”窗口。

(9) 在“受信任的根证书颁发机构”页签中查看颁发 SSL 证书的机构是否在列表中，以及证书截止日期。

(10) 如果颁发机构不在列表中，单击右下方的“导入”，重新导入根证书，如图 9-22 所示。

图9-22 根证书



3. 生成 SSL 证书操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择 SSL 证书页签，进入 SSL 证书页面，如图 9-20 所示。

(2) 单击<生成 SSL>按钮，跳出生成 SSL 证书对话框，如图 9-23 所示。

图9-23 生成 SSL

(3) 输入通用名称、组织、组织单元、城市或地区、省（州）、国家、电子邮件地址、有效期等信息，并选择密钥长度。

(4) 单击<确定>按钮，跳出确认对话框，单击<确定>按钮。

(5) 弹出“生成 SSL 证书成功”对话框，表示新的 SSL 证书生成成功。

(6) 重新登录 HDM，将使用新生成的 SSL 证书。

4. 参数说明

- 当前的证书：当前证书上传的日期和时间。
- 新的证书：新的证书文件，证书文件的格式应为.pem。
- 当前的私人密钥：当前私钥上传的日期和时间。
- 新的私钥：新的私钥文件，私钥文件的格式应为.pem。
- 通用名称（CN）：拥有此 HDM 的全称域名。
  - 长度为 1～64 个字符。
  - 不允许使用纯数字。

    - 仅支持字母、数字、空格和特殊字符_-.。
- 组织（O）：拥有此 HDM 的公司或组织的名称。
    - 长度为 1～64 个字符。
    - 不允许使用纯数字。
    - 仅支持字母、数字、空格和特殊字符_-.,。
- 组织单元（OU）：公司或组织中拥有此 HDM 的单位。
    - 长度为 1～64 个字符。
    - 不允许使用纯数字。
    - 仅支持字母、数字、空格和特殊字符_-.。
- 城市或地区（L）：拥有此 HDM 的公司或组织所在的市/县。
    - 长度为 1～128 个字符。
    - 不允许使用纯数字。
    - 仅支持字母、数字、空格和特殊字符_-.。
- 省（州）（ST）：拥有此 HDM 的公司或组织所在的省/直辖市/自治区。
    - 长度为 1～128 个字符。
    - 不允许使用纯数字。
    - 仅支持字母、数字、空格和特殊字符_-.。
- 国家（C）：拥有此 HDM 的公司或组织所在的国家/地区。
    - 只允许使用两个字母。
- 电子邮件地址：拥有此 HDM 的公司或组织的电子邮件地址。
- 有效：SSL 证书的有效期，取值范围为 1～5475，单位为天。
- 密钥长度：证书的密钥长度。
- 基本信息：当前 SSL 证书的基本信息。
    - 版本：此 SSL 证书的版本。
    - 序列号：证书签证机关（CA）为证书分配的序列号。
    - 签名算法：此 SSL 证书所采用的签名加密算法。
    - 公共密钥：公共密钥信息。
- 颁布者信息：颁发 SSL 证书的 CA。
- 有效时间：当前 SSL 证书的有效时间。
    - 有效期自：证书生效的第一天。
    - 有效期至：证书的到期日。
- 颁布对象信息：向其颁发 SSL 证书的实体。

5. 注意事项

- SSL 证书的时间以 HDM 时间为基准。上传 SSL 证书时，请在[首页]页面检查 HDM 的时间。
- SSL 成功上传之后，需要重新登录 HDM Web 以使用新上传的 SSL 证书。
- 只有网络权限为“Administrator”、“Operator”或拥有安全配置权限的用户才可以上传 SSL。

9.2.3 PFR 固件保护

说明

- 仅 G5 系列服务器支持 PFR 固件保护功能。
- 仅 HDM-2.13 及以后的版本支持 PFR 固件保护功能。

PFR （Platform Firmware Resilience，通用平台固件保护恢复方案）是一种安全技术，用于保护 HDM 免受攻击。PFR 固件保护功能开启后，PFR 会在 HDM 启动时对固件镜像文件进行校验。

- 如果主分区校验通过，HDM 会直接从主分区启动。
- 如果主分区检测到固件损坏，会对备分区镜像文件进行校验，校验通过后 HDM 会从备分区启动。
- 如果主备分区都检测到固件损坏，而主分区的损坏不影响正常启动，HDM 还是会从主分区启动。

1. 操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择“PFR 固件保护”页签，进入 PFR 固件保护页面，如图 9-24 所示。

(2) 查看 PFR 固件保护功能状态和当前固件状态。

(3) 选择是否开启“校验失败从备分区启动”功能。

图9-24 PFR 固件保护

2. 参数说明

- 是否启用：显示 PFR 固件保护功能的状态。
- 当前固件状态：HDM 本次启动过程中，PFR 对 HDM 固件镜像文件的校验结果。

- 校验失败从备分区启动：缺省关闭。开启后，如果 PFR 对 HDM 主分区镜像文件校验失败，会对备分区镜像文件进行校验，校验通过后 HDM 会从备分区启动。

3. 注意事项

- 如果 PFR 检测到某个分区固件镜像文件损坏，需要更新该分区固件使固件恢复正常。
- 开启 PFR 固件保护功能后，HDM 启动时间会略有延长。

9.2.4 登录安全性信息设置

说明

仅 HDM-2.13 及以后的版本支持设置登录安全性信息功能。

本功能可以开启并设置登录安全性信息功能，设置完成后，登录安全性信息会显示在登录页面。

1. 操作步骤

(1) 单击[用户&安全/安全设置]菜单项，选择“登录安全性信息配置”页签，进入登录安全性信息配置页面，如图 9-25 所示。

(2) 选择开启“登录安全性信息”功能。

(3) 输入登录安全性信息内容，允许设置为空。

(4) 单击<保存>按钮，完成操作。

(5) 保存成功后，进入登录页面，可以查看已设置的安全性信息内容，如图 9-26 所示。

图9-25 登录安全性信息

图9-26 登录安全性信息

2. 注意事项

登录安全性信息内容长度为 1～1024 个字节，支持中英文字符、数字和其它字符，（<）和（>）字符除外。

9.3 安全模块

说明

仅 HDM-2.14 及以后的版本支持查看安全模块信息。

通过本功能可以查看 TPM/TCM 的状态。

- TPM 是内置在主板上的微芯片，拥有独立的处理器和存储单元，用于存储加密信息（如密钥），为服务器提供加密和安全认证服务。
- TCM 是可信计算平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。

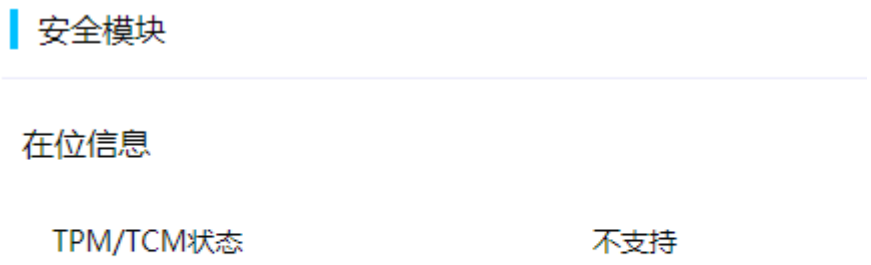
关于 TPM/TCM 模块的更多信息，请参见服务器用户指南。

1. 操作步骤

(1) 单击[用户&安全/安全模块]菜单项，进入安全模块页面，如图 9-27 所示。

(2) 查看 TPM/TCM 的状态。

图9-27 安全模块



2. 参数说明

表9-3 TPM/TCM 状态

TPM/TCM 状态	状态含义
TPM已启用	TPM功能已开启
TPM已禁用	TPM模块已安装，但功能未开启
TPM/TCM不在位	未安装TPM/TCM模块
TCM已启用	TCM功能已开启
TCM已禁用	TCM模块已安装，但功能未开启
不支持	TPM/TCM功能不支持

10 联合管理

通过本功能，可以实现服务器的批量管理，最多支持添加 10 台设备，可执行以下操作：

- 添加设备
- 查看设备信息
- 访问 HDM
- 电源操作
- 连接 H5 KVM
- 删除设备

10.1 添加设备

通过设备添加可以实现单台或批量添加服务器。

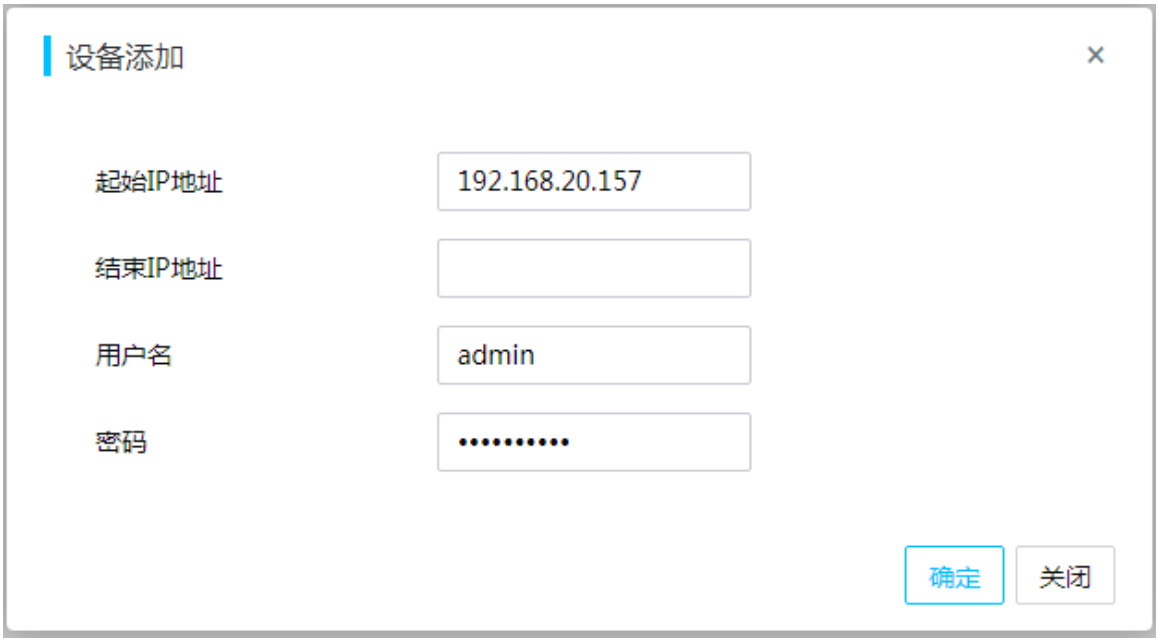
1. 操作步骤

(1) 单击[联合管理]菜单项，进入联合管理页面，如图 10-1 所示。

图10-1 联合管理

(2) 单击<设备添加>按钮，在对话框中输入待添加的设备信息，如图 10-2 所示。

图10-2 设备添加



(3) 单击<确定>按钮，完成操作。

2. 参数说明

- 起始 IP 地址：HDM 管理 IP 地址的起始地址，目前仅支持 IPv4 地址，必填项。
- 结束 IP 地址：HDM 管理 IP 地址的结束地址，目前仅支持 IPv4 地址，可以为空。
- 用户名：HDM 登录用户名，包括 Administrator 权限用户和非 Administrator 权限用户。
- 密码：和 HDM 登录用户名匹配的密码。

3. 注意事项

- 添加设备时，建议输入 Administrator 权限的用户名和密码，非 Administrator 权限的用户添加的设备，部分功能不可用。
- 添加设备时，起始 IP 地址和结束 IP 地址范围内的设备 IP 不能超过 255 个，当设备 IP 超过 10 个时，会添加先获取到信息的 10 台设备。
- 已添加的设备用户名或密码发生变化后，该设备将处于不可用状态。
- 不支持多用户同时添加设备。

10.2 查看设备信息

添加设备后，可以查看设备信息，包含设备 IP、产品名称、产品序列号、健康状态、服务器电源状态和 UID 状态。

1. 操作步骤

(1) 单击[联合管理]菜单项，进入联合管理页面。

(2) 查看已添加设备的信息，如图 10-3 所示。

图10-3 设备信息

2. 参数说明

- 设备 IP：HDM 管理 IP 地址。
- 健康状态：服务器的整体健康状态。
  - 正常：HDM 监测的服务器所有组件均正常运行。
  - 紧急、严重、轻微：HDM 监测的服务器部分组件发生故障。
- 电源状态：服务器的电源状态。
  - 开启：电源处于开启状态。
  - 关闭：电源处于关闭状态。
- UID 状态：服务器的 UID 灯状态。
  - 开启：UID 灯蓝色常亮，表示服务器被选中。
  - 关闭：UID 灯熄灭，表示服务器未被选中。
  - 闪烁：UID 灯蓝色闪烁，表示服务器正在进行固件更新，或者远程控制台被打开。

10.3 访问HDM

通过本功能可以通过设备 IP 地址的链接访问设备的 HDM。

1. 操作步骤

(1) 单击[联合管理]菜单项，进入联合管理页面，如图 10-3 所示。

(2) 单击设备 IP 地址，访问 HDM，如图 10-4 所示。

图10-4 访问 HDM

2. 注意事项

- 访问 HDM 前，需要先确认添加设备时输入的用户是否拥有登录 HDM 的权限。
- 访问 HDM 的用户权限由添加设备时输入的用户的权限决定。

10.4 电源操作

通过本功能可以管理设备的电源状态。操作前请先确认添加该设备时输入的用户的权限，只有拥有 Administrator、Operator 或电源控制权限的用户才有操作权限。

1. 操作步骤

(1) 单击[联合管理]菜单项，进入联合管理页面，如图 10-3 所示。

(2) 在操作栏单击<电源操作>按钮，在下拉选项中选择要执行的操作按钮，如图 10-5 所示。

图10-5 电源操作

2. 参数说明

注意

- 下列参数中，除“正常关机”外的其他关机方式可能会损坏用户的程序或者未保存的数据，请根据实际情况谨慎选择操作方式。
- 请确保仅当前登录用户在执行电源操作，否则可能会导致操作无法生效。

- 立即重启：强制重启服务器。此过程不会断开服务器的电源。
- 强制关机：立即强制关闭服务器，此操作与长按服务器前面板上的开机/待机按钮 5 秒以上效果相同。此过程中会断开服务器电源。
- 正常关机：正常关闭服务器，即先关闭操作系统，再关闭电源。此过程中会断开服务器电源。
- 开机：正常启动服务器。
- 关机并重新开机：立即强制重启服务器。此过程中会断开服务器电源。

10.5 连接H5 KVM

通过本功能可以启动设备的 H5 KVM。

启动 H5 KVM 前，请检查以下配置：

- 确认添加设备时输入的用户是否拥有远程控制权限，如果没有，需要先修改该用户的权限，具体操作请参见修改本地用户。

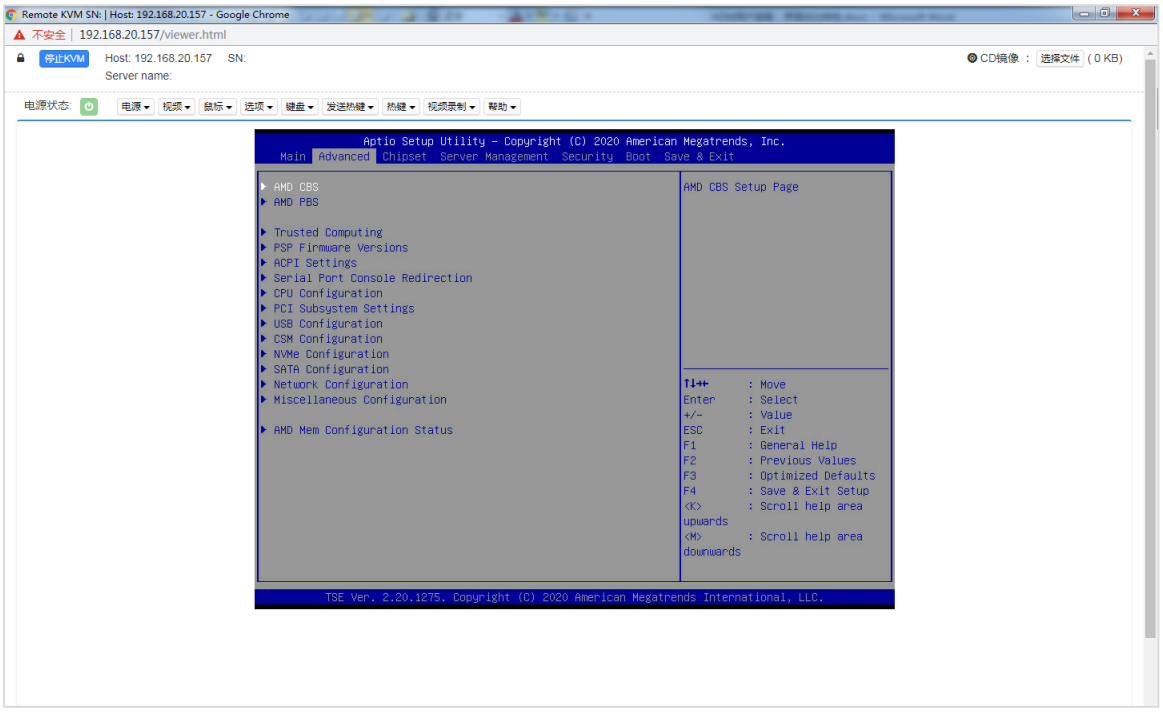
- 确认添加设备时输入的用户是否开启 KVM 服务，如果没有，需要先开启该用户的 KVM 服务，具体操作请参见服务设置。

1. 操作步骤

(1) 单击[联合管理]菜单项，进入联合管理页面，如图 10-3 所示。

(2) 在操作栏单击<H5 KVM>按钮，启动 H5 KVM，如图 10-6 所示。

图10-6 H5 KVM



(3) H5 KVM 相关操作请参见使用 H5 KVM 远程控制台。

10.6 删除设备

通过本功能可以删除已添加的设备。删除设备前请确保仅当前登录用户在删除设备，否则可能会导致操作无法生效。

1. 操作步骤

(1) 单击[联合管理]菜单项，进入联合管理页面，如图 10-3 所示。

(2) 选择待删除的设备，单击<设备删除>按钮。

(3) 在对话框中单击<确定>按钮，如图 10-7 所示，完成操作。

图10-7 设备删除


联合管理
设备添加
设备删除
设备IP
产品名称
产品序列号
健康状态
电源状态
UID状态
操作
192.168.20.157
开启
关闭
电源操作
H5 KVM
消息
确定要删除所选的设备？
确定
取消

11 常用操作

11.1 虚拟媒体配置

11.1.1 Windows 环境搭建 CIFS 服务

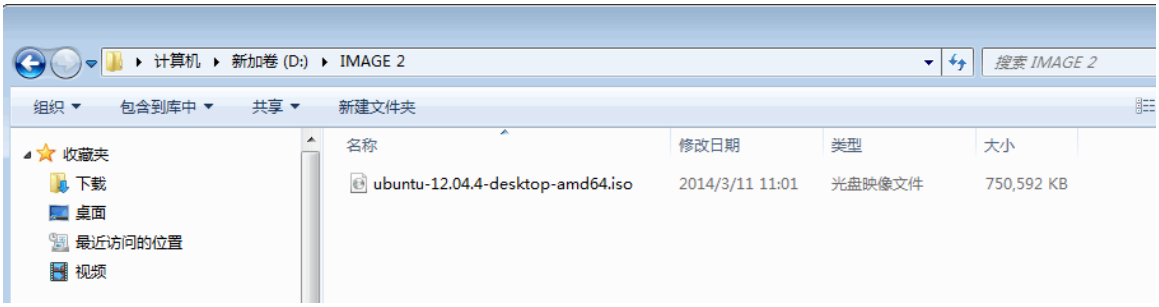
CIFS（Common Internet File System，通用 Internet 文件系统），使 HDM 可以远程访问设备上的文件。Windows 系统中已包括 CIFS 软件，无需下载安装。

本文以 Windows 7 的环境为例介绍如何设置 CIFS 服务。

1. 镜像文件

把镜像文件拷贝到本地路径，以“D:\IMAGE 2”为例，如图 11-1 所示。

图11-1 镜像文件

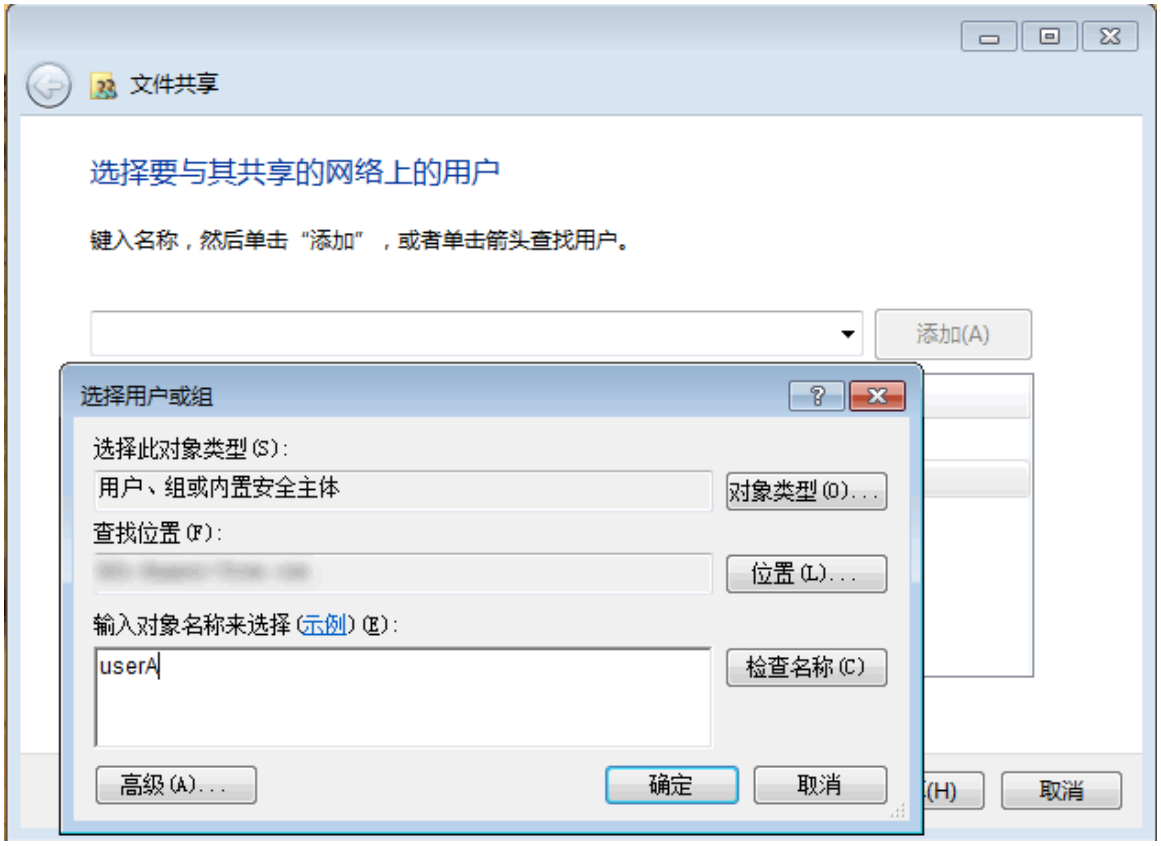


2. 设置访问权限

(1) 选择“IMAGE 2”文件夹，单击右键，选择共享/特定用户，在文件共享窗口设置镜像文件的读写权限。

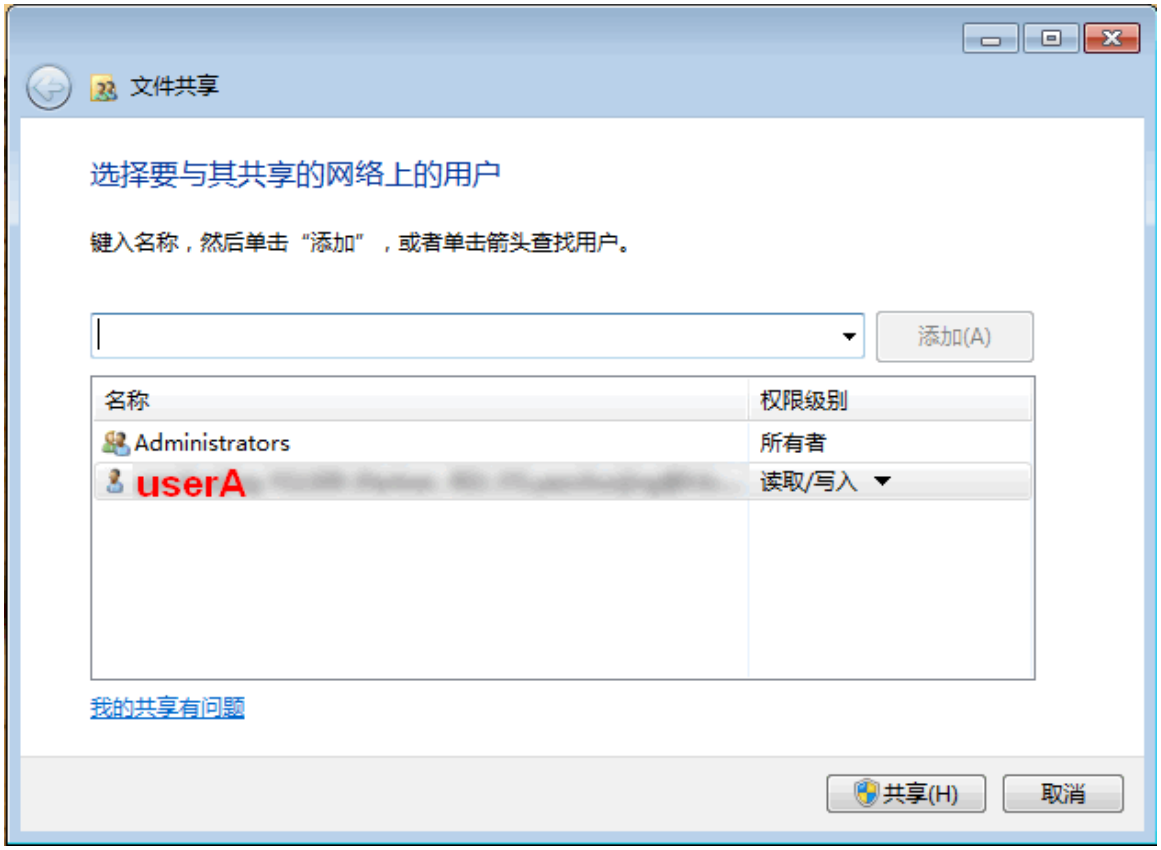
(2) 在文本框里选择查找用户，在对话框中搜索并添加用户，以 userA 为例，如图 11-2 所示。

图11-2 文件共享窗口



(3) 添加用户（可多个）后，设置用户的权限为读取写入，如图 11-3 所示，该用户就拥有访问该文件的权限。

图11-3 添加共享用户



3. 登录 HDM

(1) 登录 HDM，单击[远程服务/虚拟媒体]菜单项，进入虚拟媒体页面。

(2) 单击<高级设置>按钮，开启远程媒体支持功能，如图 11-4 所示。

(3) 启用媒体类型勾选 CD/DVD。

(4) 服务器地址输入 CIFS 服务器地址，以 192.168.32.48 为例，源路径输入 IMAGE 2。

(5) 分享类型选择 CIFS。

(6) 用户名和密码，输入 userA 访问共享镜像文件的用户名和密码。

图11-4 开启远程媒体

(7) 单击<确定>按钮，与 CIFS 服务器成功建立连接，访问共享路径，如图 11-5 所示。

图11-5 访问共享路径

11.1.2 Linux 环境搭建 CIFS 服务器

CIFS（Common Internet File System，通用 Internet 文件系统）使应用程序可以远程访问服务器上的文件。CIFS 是 SMB（Server Messages Block，服务器信息块）协议的开放版本。

Samba 是在 Linux 系统中实现 SMB 协议的一个免费软件，由服务端及客户端程序构成。在 Linux 系统中安装 Samba 后即可使用 CIFS 服务。

本文以 Red Hat Enterprise Linux 7.3 的环境为例介绍下载、安装和设置 Samba 软件。

1. 安装 Samba 软件

(1) 输入以下命令，安装 Samba 软件。

```
yum –y install samba samba-common samba-client
```

建议同时安装 Samba 服务端和客户端。

- samba-common 代表 Samba 服务端。
- samba-client 代表 Samba 客户端。

(2) 安装完成后，输入以下命令，查看安装软件列表。

```
yum list installed | grep samba
```

(3)　安装完成后，输入以下命令，校验 Samba 配置是否正确，正确如图 11-6 所示。

```
testparm
```

图11-6 testparm

```
[root@localhost ~]# testparm
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Registered MSG_REQ_POOL_USAGE
Registered MSG_REQ_DMALLOC_MARK and LOG_CHANGED
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
        printcap name = cups
        security = USER
        workgroup = SAMBA
        idmap config * : backend = tdb
        cups options = raw


[homes]
        browseable = No
        comment = Home Directories
        inherit acls = Yes
        read only = No
        valid users = %S %D%w%S


[printers]
        browseable = No
        comment = All Printers
        create mask = 0600
```

2. 启动 Samba 服务

输入以下命令启动并查看 Samba 服务。

```
systemctl start smb
systemctl status smb
```

3. 关闭防火墙

输入以下命令，关闭防火墙，把 SELinux 设为安全值。

```
systemctl stop firewalld
getenforce
setenforce 0
```

4. 查询并添加 Samba 用户

(1) 输入以下命令，查询 Samba 用户。

```
pdbedit –L
```

(2) 如果没有 Samba 用户，输入以下命令，添加用户，以 ldt 为例，如图 11-7 所示。

```
smbpasswd  -a ldt
```

图11-7 添加 Samba 用户

```
[root@localhost ~]# smbpasswd -a ldt
New SMB password:
Retype new SMB password:
Added user ldt.
```

添加的 Samba 用户必须是服务端 OS 下已经存在的用户，可以输入以下命令查看用户信息。

```
cat /etc/passwd
```

5. 访问 Samba 服务器

输入以下命令，访问 Samba 服务器，即 OS 侧 IP 地址，以 10.99.205.165 为例，查看服务端共享信息，如图 11-8 所示。

```
smbclient -L //10.99.205.165
```

图11-8 Samba 服务器

```
[root@localhost ~]# smbclient -L//10.99.205.165
Enter SAMBA\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        mnt             Disk      /mnt dir
        IPC$            IPC       IPC Service (Samba 4.9.1)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

6. 配置 Samba 服务端

输入以下命令，修改/etc/samba/smb.conf 配置文件，创建共享路径。

```
vi /etc/samba/smb.conf
[mnt]
comment = /mnt dir
path = /test
```

7. 重启 Samba 服务

输入以下命令，重启 Samba 服务。

```
systemctl restart smb
```

8. 放入共享文件

在/test 路径下放入共享文件，以 test.iso 为例。

9. 登录 HDM

(1) 登录 HDM，单击[远程服务/虚拟媒体]菜单项，进入虚拟媒体页面。

(2) 单击<高级设置>按钮，开启远程媒体支持功能，如图 11-9 所示。

(3) 启用媒体类型勾选 CD/DVD。

(4) 服务器地址输入 Samba 服务端 OS 侧 IP 地址，以 10.99.205.165 为例，源路径输入/mnt。

(5) 分享类型选择 CIFS。

(6) 域名可以不填。

(7) 输入查询并添加 Samba 用户添加的 Samba 用户名和密码。

图11-9 开启远程媒体支持

(8) 单击<确定>按钮，与 CIFS 服务器成功建立连接，访问共享路径，如图 11-10 所示。

图11-10 访问共享路径

11.2 导入HDM配置

11.2.1 导入 HDM 用户信息

注意

- 导入 HDM 配置前，确保设备型号相同。
- 配置文件中的密码显示为空，如果导入原服务器，不需要手动添加密码，导入后将保留原来的密码。如果导入其他服务器，需要手动添加密码，导入成功后，添加的密码会生效。

1. 打开配置文件

使用文本工具打开配置文件，搜索“User Accounts”，找到用户配置信息，如图 11-11 所示。

图11-11 用户配置信息

```
"User Accounts":    {
    "Custom privileges":    {
        "role customrole1": 384,
        "role customrole2": 384,
        "role customrole3": 448,
        "role customrole4": 384,
        "role customrole5": 384,
        "rolename_oem1":    "CustomRole1",
        "rolename_oem2":    "CustomRole2",
        "rolename_oem3":    "CustomRole3",
        "rolename_oem4":    "CustomRole4",
        "rolename_oem5":    "CustomRole5"
```

2. 配置已有用户的密码

以用户“ycj”为例举例说明，删除 comment 语句，输入用户密码 Password@_，如图 11-12 所示。

图11-12 配置密码

```
"This_is_comment":  "If need to config this user, delete this comment",
"User ID":  3,
"User role":    4,
"Access to HDM":    1,
"WEB":  1,
"IPMI": 1,
"Password": "Password@_",
"Username": "ycj",
"EMail address":    "",
"SNMP extended privileges": 0,
"SNMP v3 R/W permission":   "",
"SNMP v3 authProtocol": "",
"SNMP v3 privProtocol": ""
```

如果图 11-11 中的 Complexity check 的值为 1，即密码复杂度检查为开启状态，输入的密码需要符合密码复杂度检查。

3. 添加新用户

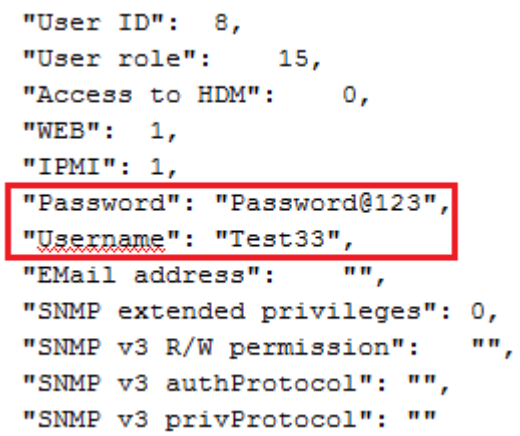
(1) 选择 Username 为空的用户，以 User ID 8 为例，删除 comment 语句，如图 11-13 所示。

图11-13 删除 comment 语句

```
"User ID":  8,
"User role":    15,
"Access to HDM":    0,
"WEB":  1,
"IPMI": 1,
"Password": "",
"Username": "",
"EMail address":    "",
"SNMP extended privileges": 0,
"SNMP v3 R/W permission":   "",
"SNMP v3 authProtocol": "",
"SNMP v3 privProtocol": ""
```

(2) 输入新用户信息，以用户名 Test33，密码 Password@123 为例，如图 11-14 所示。

图11-14 设置用户名和密码



如果图 11-11 中的 Complexity check 的值为 1，即密码复杂度检查为开启状态，输入的密码需要符合密码复杂度检查。

(3) 设置用户的网络权限（User role，以 Administrator 为例），开启访问 HDM 的权限，把 HDM Access to HDM 的值设置为 1，如图 11-15 所示。

图11-15 设置权限

4. 修改其它信息

修改用户的其它信息，请保证输入信息的合法性，具体请参考表 11-1。

表11-1 用户配置信息

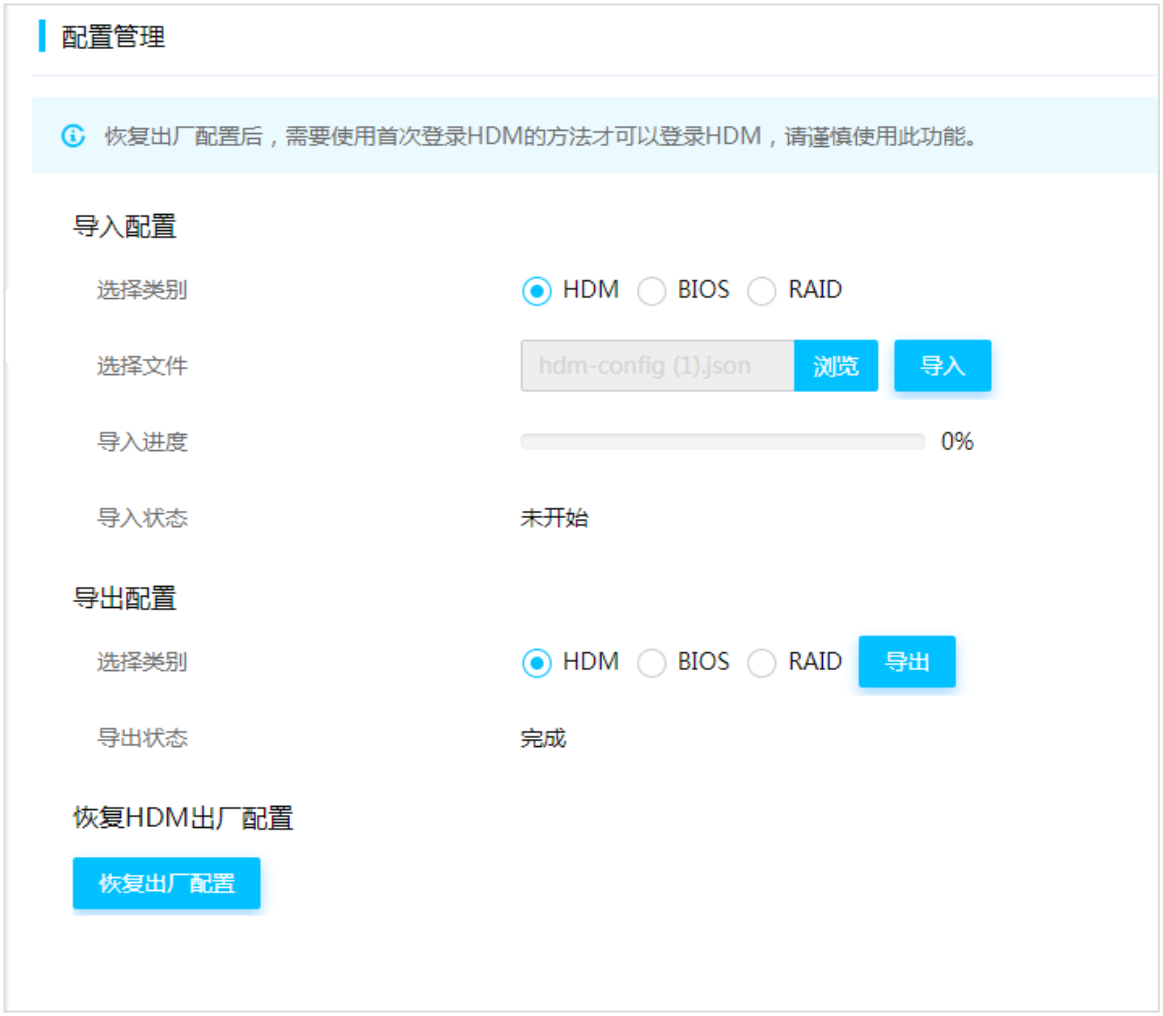
信息项	含义及合法值
role customrole 1～5	自定义权限组的权限。以435的状态值为例，先转换成二进制110110011，Bit0到Bit8依次表示远程控制、远程媒体、安全配置、用户配置、常规配置、电源控制、维护诊断、查询、配置自身权限的状态 • 1：开启 • 0：关闭
User ID	用户编号，2～16，不能和已有的用户编号重复

信息项	含义及合法值
User role	用户的网络权限： • 2：User • 3：Operator • 4：Administrator • 6～10：CustomRole 1～CustomRole 5 • 15：None
Access to HDM	访问HDM的权限，开启后用户才能登录HDM Web端 • 1：开启 • 0：关闭
WEB	Web扩展权限，当用户的网络权限为Administrator和Operator时，缺省开启，不可修改 • 1：开启 • 0：关闭
IPMI	IPMI扩展权限，当用户的网络权限为Administrator和Operator时，缺省开启，不可修改 • 1：开启 • 0：关闭

5. 保存并导入修改后的配置文件

(1) 单击[远程运维/配置管理]菜单项，进入配置管理页面，导入修改后的 HDM 配置文件，如图 11-16 所示。

图11-16 导入配置文件



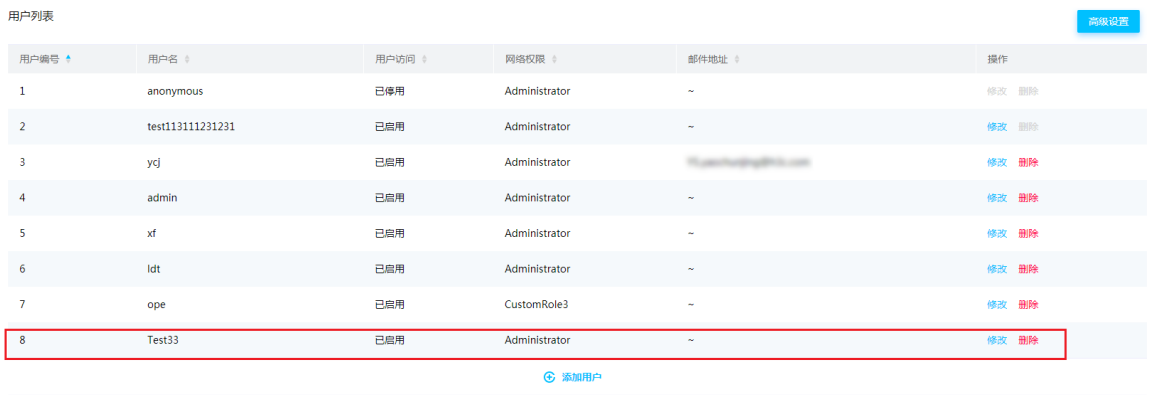
(2) 导入成功后，配置会立即生效。

(3) 注销当前用户回到登录页面，输入用户名 Test33，密码 Password@123，重新登录 HDM，如图 11-17 所示。

图11-17 登录页面

(4) 进入[用户&安全/用户访问设置]页面，查看用户信息，如图 11-18 所示。

图11-18 用户列表



11.2.2 导入 SNMP Trap 信息

1. 打开配置文件

使用文本工具打开配置文件，搜索“SNMPTrap”，找到 SNMP Trap 信息，如图 11-19 所示。

图11-19 SNMP Trap


```
"SNMPTrap": {
    "SnmpEnable":   1,
    "TrapMode": 0,
    "Version":  1,
    "V3_User":  0,
    "Location": "",
    "Contact":  "",
    "Trap_Community":   "public",
    "AlarmSendLevel":   2,
    "Port": 162,
    "Enable_1": 1,
    "Destination_1":    "10.99.160.71",
    "Port_2":   162,
    "Enable_2": 1,
    "Destination_2":    "10.99.160.72",
    "Port_3":   162,
    "Enable_3": 1,
    "Destination_3":    "1oobm-wan.jd.com",
    "Port_4":   162,
    "Enable_4": 1,
    "Destination_4":    ""
```

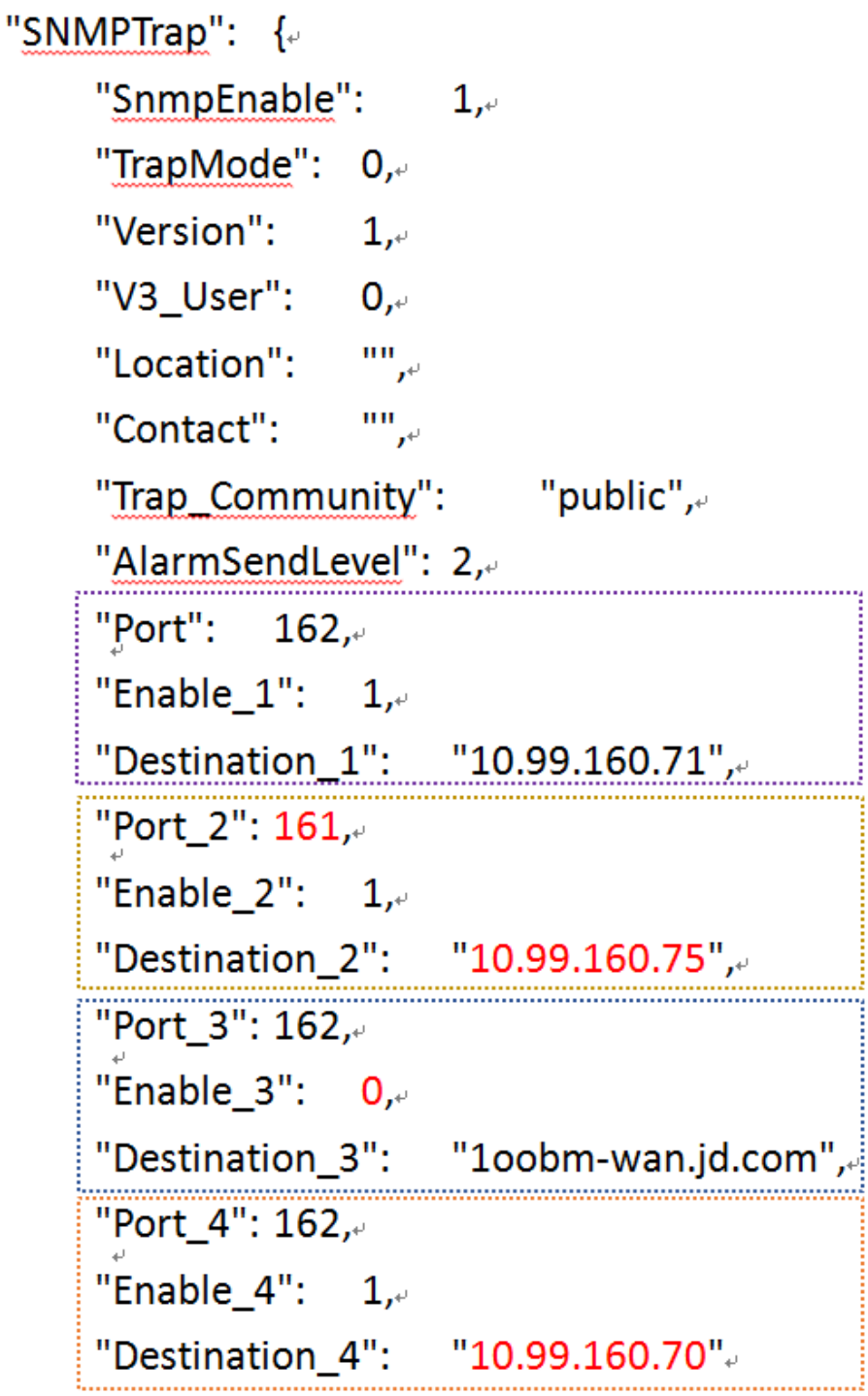

2. 修改服务器地址信息

(1) 修改目标地址 2 为 10.99.160.75，端口号为 161。

(2) 修改目标地址 3 的状态为 0，关闭该目标地址的通道。

(3) 新增目标地址 4 的地址为 10.99.160.70，如图 11-20 所示。

图11-20 修改服务器地址



3. 修改其它信息

修改 SNMP Trap 其它信息，请保证修改后信息的合法性，具体请参考表 11-2。

表11-2 用户配置信息

信息项	含义及合法值
SnmpEnable	是否开启SNMP Trap 功能： • 0：关闭 • 1：开启
Trap Mode	SNMP Trap 模式： • 0：模块 OID 模式 • 1：事件 OID 模式
Version	SNMP Trap版本 • 0：v1 • 1：v2c • 2：v3
V3_User	选择v3用户
Location	节点位置：服务器的位置描述，最多只能输入31个字节
Contact	联系方式：设备联系人的名字及联系方式，最多只能输入31个字节
Trap_Community	Trap团体名：管理端进行的接收认证，最多只能输入31个字节，缺省值为public
AlarmSendLevel	告警发送级别： • 0：轻微+严重+紧急 • 1：严重+紧急 • 2：所有级别
Port~Port_8	目的主机接收SNMP告警信息的端口号。端口号范围为1～65535，缺省值为162
Enable_1～Enable_8	通道是否开启： • 0：停用 • 1：启用
Destination_1～Destination_8	接收SNMP告警的目标地址，支持IP地址和域名地址

4. 保存并导入修改后的配置文件

(1) 单击[远程运维/配置管理]菜单项，进入配置管理页面，导入修改后的 HDM 配置文件。

(2) 导入成功后，配置会自动生效。

(3) 进入“告警 Trap 报文设置”页面，在告警 Trap 页面查看修改后的 Trap 服务器信息，如图 11-21 所示。

图11-21 告警 Trap 页面

告警Trap服务器

序号	当前状态	Trap服务器地址	Trap端口	操作
1	启用	10.99.160.71	162	测试 修改
2	启用	10.99.160.75	161	测试 修改
3	停用	1oobm-wan.jd.com	162	测试 修改
4	启用	10.99.160.70	162	测试 修改

11.3 搭建Syslog服务器

本文以 Red Hat Enterprise Linux 7.7 的环境为例介绍下载、安装和配置 Syslog 服务器。Syslog 服务器包括 UDP、TCP 和 TLS 三种协议。

11.3.1 Linux 环境搭建 UDP 和 TCP 协议环境

1. 配置 rsyslog.conf 文件

打开配置文件/etc/rsyslog.conf，如图 11-22 所示。

图11-22 配置文件

```
#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
```

2. 启用 UDP 和 TCP 模块

去掉＃注释，启用接收 UDP 和 TCP 的模块，设置 UDP 和 TCP 服务器端口分别为 514 和 518，并设置 remotelogs 存储路径为/var/log/hdm/messages.log，如图 11-23 所示。

图11-23 配置后文件

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 518

$template RemoteLogs,"/var/log/hdm/messages.log"
*.* ?RemoteLogs
#&~
```

- UDP 和 TCP 模块同时启用时，需要设置不同的端口。
- $template RemoteLogs 指令，使 rsyslog 后台进程隔开本地/var/log/下的文件去写日志信息，而日志文件名为 messages.log。
- *.* ?RemoteLogs 指令，用 RemoteLogs 模板来接收所有的日志。
- & ~指令告诉 rsyslog 后台进程停止对日志进行本地化写入，日志信息只会写入到 messages.log 这个路径下。

3. 重启和查看 rsyslog 服务

输入以下命令，重启并查看 rsyslog 服务，如图 11-24 所示。

图11-24 重启和查看 rsyslog 服务

```
[root@localhost ~]# systemctl restart rsyslog.service
[root@localhost ~]#
[root@localhost ~]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-03-09 13:44:46 CST; 8s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 11171 (rsyslogd)
    Tasks: 9
   CGroup: /system.slice/rsyslog.service
           └─11171 /usr/sbin/rsyslogd -n

Mar 09 13:44:46 localhost.localdomain systemd[1]: Starting System Logging Service...
Mar 09 13:44:46 localhost.localdomain rsyslogd[11171]:  [origin software="rsyslogd" swVersion="8.24.0-38.el7" x-pid="11171" x-info="http://www.rsyslog.com"] start
Mar 09 13:44:46 localhost.localdomain systemd[1]: Started System Logging Service.
[root@localhost ~]#
```

4. HDM Web 端配置

(1) 登录 HDM Web 端。

(2) 进入[远程运维/告警设置/Syslog 设置]页面。

(3) 单击<配置>按钮，在“Syslog 设置”对话框中，配置相关信息，如图 11-25 所示。

(4) 开启 Syslog 功能，选择告警日志主机标识为主机名和传输协议为 UDP。

图11-25 开启 Syslog 功能

(5) 单击<确定>按钮，完成操作。

(6) 单击告警日志服务器栏的<修改>按钮，弹出修改 Syslog 服务器对话框。

(7) 设置 Syslog 服务器的地址和端口分别为 172.16.18.48（OS 侧 IP 地址）和 514，选择日志类型为操作日志和事件日志，如图 11-26 所示。

图11-26 设置 Syslog 服务器

(8) 单击<确定>按钮，完成操作。

11.3.2 Linux 环境搭建 TLS 协议环境

TLS 是一种加密的传输协议，分为单向认证与双向认证两种：

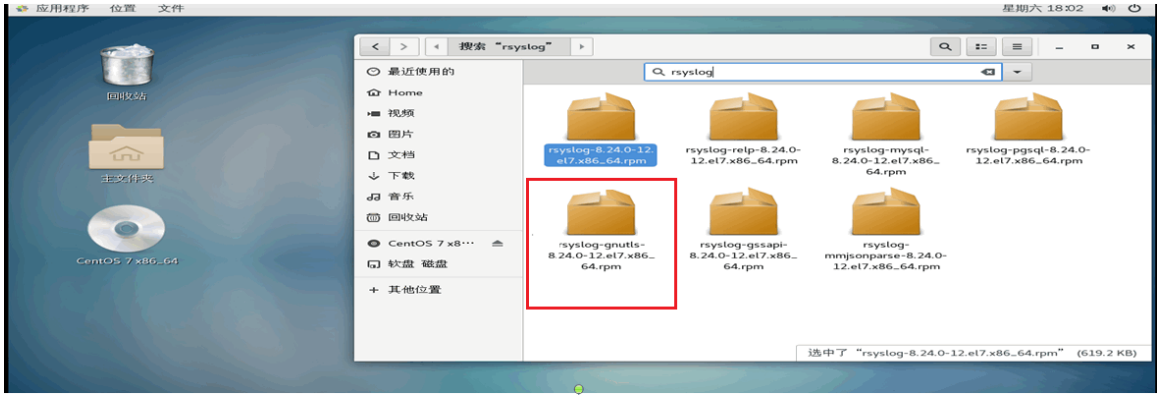
- 单向认证：只认证 Syslog 服务器端的证书。
- 双向认证：Syslog 服务器端和客户端（即 HDM）的证书都需要认证。

1. 下载依赖包 rsyslog-gnutls

服务器安装 OS 之后，OS 默认会安装 rsyslog，但是要想实现 TLS 传输，则还需要安装依赖包 rsyslog-gnutls。

- 如果设备能联网，可以使用 sudo yum install -y rsyslog-gnutls 或 apt 命令下载依赖包。
- 如果不能联网，OS 系统默认配置了 rsyslog，而且 OS 镜像内也有对应的 rsyslog-gnutls 依赖包，如图 11-27 所示。

图11-27 rsyslog-gnutls 依赖包



2. 安装依赖包 rsyslog-gnutls

图11-28 安装依赖包 rsyslog-gnutls

```
[root@localhost Packages]#
[root@localhost Packages]# rpm -ivh rsyslog-g
rsyslog-gnutls-8.24.0-38.el7.x86_64.rpm
rsyslog-gssapi-8.24.0-38.el7.x86_64.rpm
[root@localhost Packages]# rpm -ivh rsyslog-gnutls-8.24.0-38.el7.x86_64.rpm
warning: rsyslog-gnutls-8.24.0-38.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY
Preparing...                          ################################# [100%]
Updating / installing...
   1:rsyslog-gnutls-8.24.0-38.el7     ################################# [100%]
[root@localhost Packages]#
```

3. 生成自签 CA 证书

使用 openssl 命令在控制台依次输入以下命令生成自签 CA 证书。

(1) 生成根证书私钥(pem 文件)。

```
# cd /root/Desktop
# mkdir tls
# cd tls
# mkdir server
# mkdir client
# openssl genrsa -out cakey.pem 2048
```

(2) 生成根证书签发申请文件(csr 文件) 。

```
# openssl req -new -key cakey.pem -out ca.csr -subj
"/C=CN/ST=myprovice/L=mycity/O=myorganization/OU=mygroup/CN=myCA"
```

(3) 自签发根证书(cer 文件)

```
# openssl x509 -req -days 365 -sha1 -extensions v3_ca -signkey cakey.pem -in ca.csr -out
cacert.pem
```

4. 生成服务端私钥和证书

使用 openssl 命令在控制台依次输入以下命令生成服务端私钥和证书。

(1) 生成服务端私钥。

```
# cd server
# openssl genrsa -out key.pem 2048
```

(2) 生成证书请求文件，以 rsyslog 服务器 OS 侧 IP 地址 172.16.18.48 为例。

```
# openssl req -new -key key.pem -out server.csr -subj
"/C=CN/ST=myprovice/L=mycity/O=myorganization/OU=mygroup/CN=172.16.18.48"
```

(3) 使用根证书签发服务端证书。

```
# openssl x509 -req -days 365 -sha1 -extensions v3_req -CA ../cacert.pem -CAkey ../cakey.pem
-CAserial ca.srl -CAcreateserial -in server.csr -out cert.pem
```

(4) 使用 CA 证书验证服务端证书。

```
# openssl verify -CAfile ../cacert.pem cert.pem
```

5. 生成客户端私钥和证书

(1) 生成客户端私钥。

```
# cd ../client
# openssl genrsa -out key.pem 2048
```

(2) 生成证书请求文件，以 HDM 客户端 IP 地址 172.16.20.168 为例。

```
# openssl req -new -key key.pem -out client.csr -subj
"/C=CN/ST=myprovice/L=mycity/O=myorganization/OU=mygroup/CN=172.16.20.168"
```

(3) 使用根证书签发客户端证书。

```
# openssl x509 -req -days 365 -sha1 -extensions v3_req -CA ../cacert.pem -CAkey ../cakey.pem
-CAserial ../server/ca.srl -CAcreateserial -in client.csr -out cert.pem
```

(4) 使用 CA 证书验证客户端证书。

```
# openssl verify -CAfile ../cacert.pem cert.pem
```

6. 配置 rsyslog.conf 文件

(1) 保留配置 TCP 和 UDP 部分的不动，修改标红内容，如图 11-29 所示。

图11-29 配置文件

```
#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
$ModLoad immark  # provides --MARK-- message capability


#make gtls driver the default
$DefaultNetstreamDriver gtls

#cerificate files
$DefaultNetstreamDriverCAFile /root/Desktop/tls/cacert.pem
$DefaultNetstreamDriverCertFile /root/Desktop/tls/server/cert.pem
$DefaultNetstreamDriverKeyFile /root/Desktop/tls/server/key.pem

$ModLoad imtcp # load TCP listener
$InputTCPServerRun 516

#shuangxiangrenzheng
$InputTCPServerStreamDriverAuthMode x509/certvalid

#danxiangrenzheng
#$InputTCPServerStreamDriverAuthMode anon

$InputTCPServerStreamDriverMode 1 # run driver in TLS-nly mode

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 518
```

(2) 设置服务器端口为 516。

(3) 单向认证仅支持客户端验证服务端的证书，服务端无需验证客户端的证书。所以在服务端的 rsyslog.conf 下，需要取消对客户端证书的验证，设置后重启 rsyslog 服务端就不用再验证了。配置信息如下：

```
$InputTCPServerStreamDriverAuthMode anon
```

(4) 而双向认证需要验证服务器端和客户端的证书，配置信息如下：

```
$InputTCPServerStreamDriverAuthMode x509/certvalid
```

7. 关闭防火墙

输入以下命令，将 SELINUX 设置为 disabled，关闭防火墙。

```
# systemctl stop firewalld
# setenforce 0
# sed -i 's#SELINUX=enforcing#SELINUX=disabled#g' /etc/selinux/config
```

8. 重启和查看 rsyslog 状态

输入以下命令，重启并查看 rsyslog 状态。

```
systemctl restart rsyslog
systemctl status rsyslog
```

9. HDM Web 端配置

(1) 把步骤 3～5 生成的证书拷贝到 HDM 客户端所在的环境。

(2) 登录 HDM Web 端。

(3) 进入[远程运维/告警设置/Syslog 设置]页面。

(4) 开启告警日志功能，如图 11-30 所示。

(5) 选择告警日志主机标识为主机名和传输协议为 TLS。

- 认证方式选择单向认证，需要上传步骤 3 生成的自签 CA 证书去验证服务端。
- 认证方式选择双向认证，需要上传步骤 3 和 5 生成的自签 CA 证书、客户端证书（即本地证书）和私钥。

图11-30 开启 Syslog 功能

(6) 单击<确定>按钮，完成操作。

(7) 设置告警日志服务器的地址和端口分别为 172.16.18.48 和 516，选择日志类型为操作日志和事件日志，如图 11-31 所示。

图11-31 设置告警日志服务器

(8) 单击<确定>按钮，完成操作。

11.3.3 查看 rsyslog 日志

(1) 通过 SSH 方式登录 rsyslog 服务器：172.16.18.48。

(2) 查看/var/log/hdm/messages.log 路径下的日志，如图 11-32 所示。

图11-32 查看日志

```
[root@localhost ~]# ls -lh /var/log/hdm/messages.log
-rw-------. 1 root root 3.1M Mar  9 13:41 /var/log/hdm/messages.log
[root@localhost ~]#
[root@localhost ~]#
```

11.4 LDAP配置

LDAP（Lightweight Directory Access Protocol，轻型目录访问协议）是一个访问在线目录服务的协议，主要的优点是可以快速响应用户的查询需求，可用于实现用户认证的统一管理。

HDM 支持与 Windows Active Directory 和 Linux OpenLDAP 的对接，本文以 Windows Server 2012 R2 Datacenter 为例说明 LDAP 服务的配置过程，主要包括安装操作系统、搭建 LDAP 服务器、配置 LDAP 服务器、HDM Web 端配置 LDAP 和验证 LDAP 配置五个部分。

11.4.1 安装操作系统

安装 Windows Server 2012 R2 Datacenter，具体操作步骤请参见《操作系统安装指导》。

11.4.2 搭建 LDAP 服务器

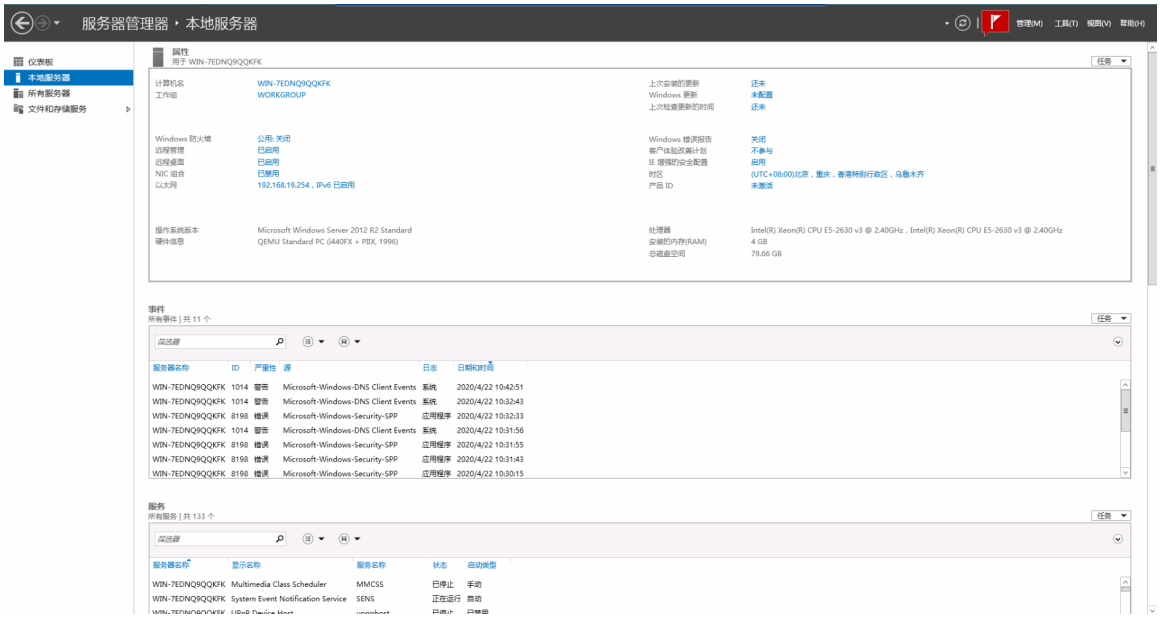
操作系统安装完成后，以管理员权限登录，进入操作系统，开始搭建 LDAP 服务器。

1. 安装 DNS 服务

(1) 单击 [服务器管理器]菜单项，进入服务器管理器页面。

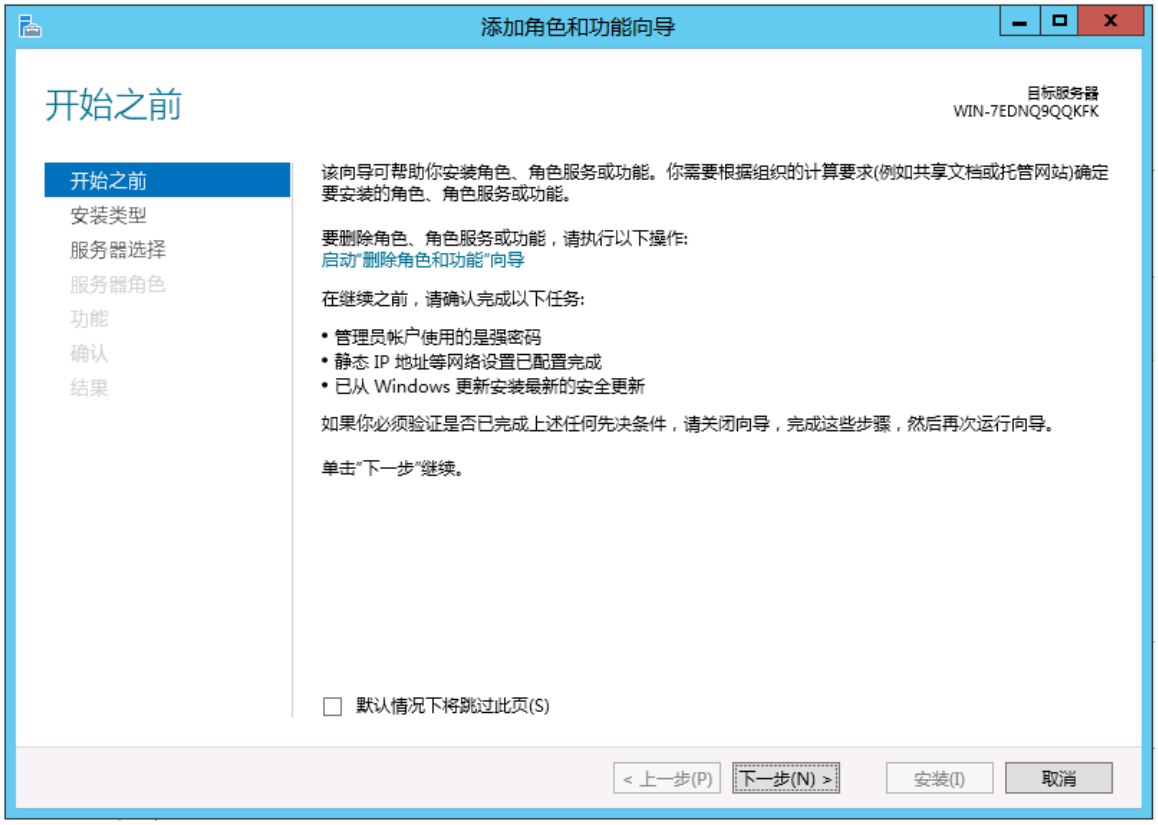
(2) 单击左侧导航栏的[本地服务器]菜单，右侧显示本地服务器的属性，如图 11-33 所示。

图11-33 本地服务器



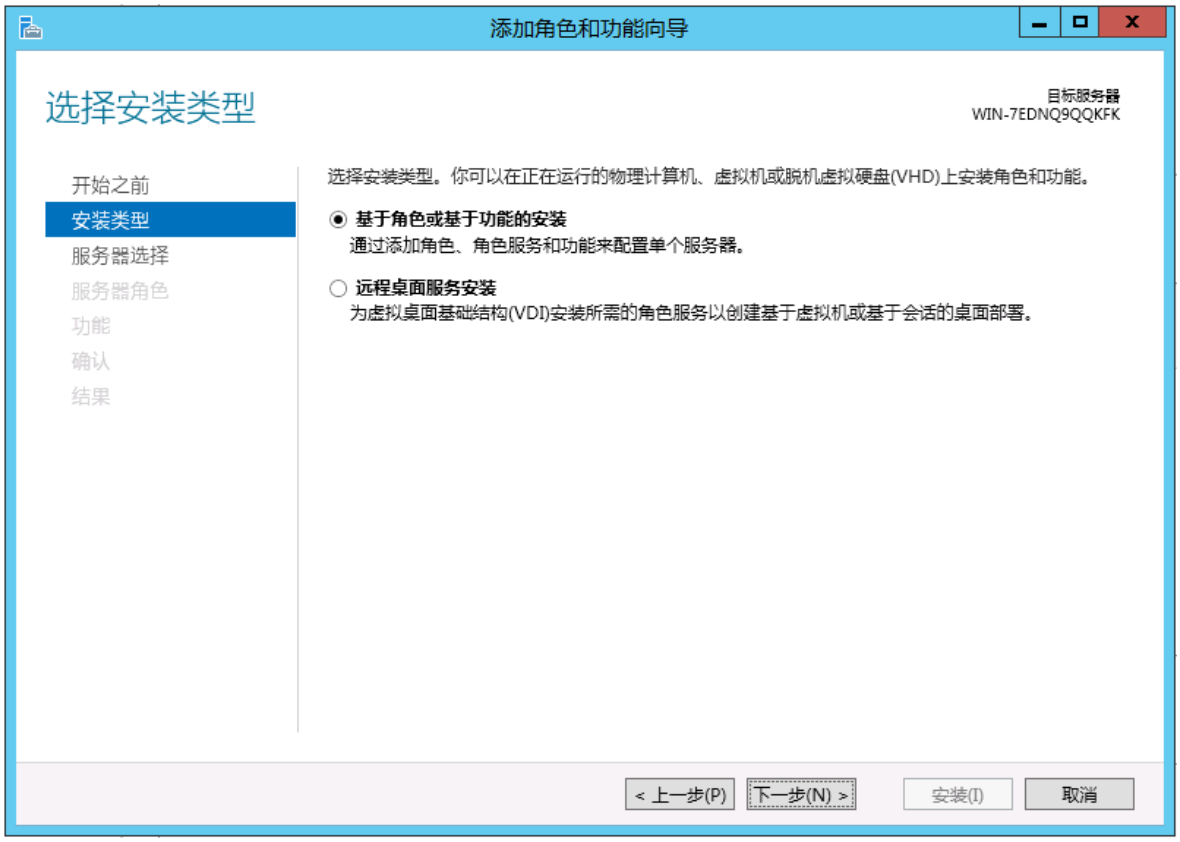
(3) 单击右上角的[管理]菜单，选择“添加角色和功能”，打开添加角色和功能向导，如图 11-34 所示。

图11-34 添加角色和功能向导



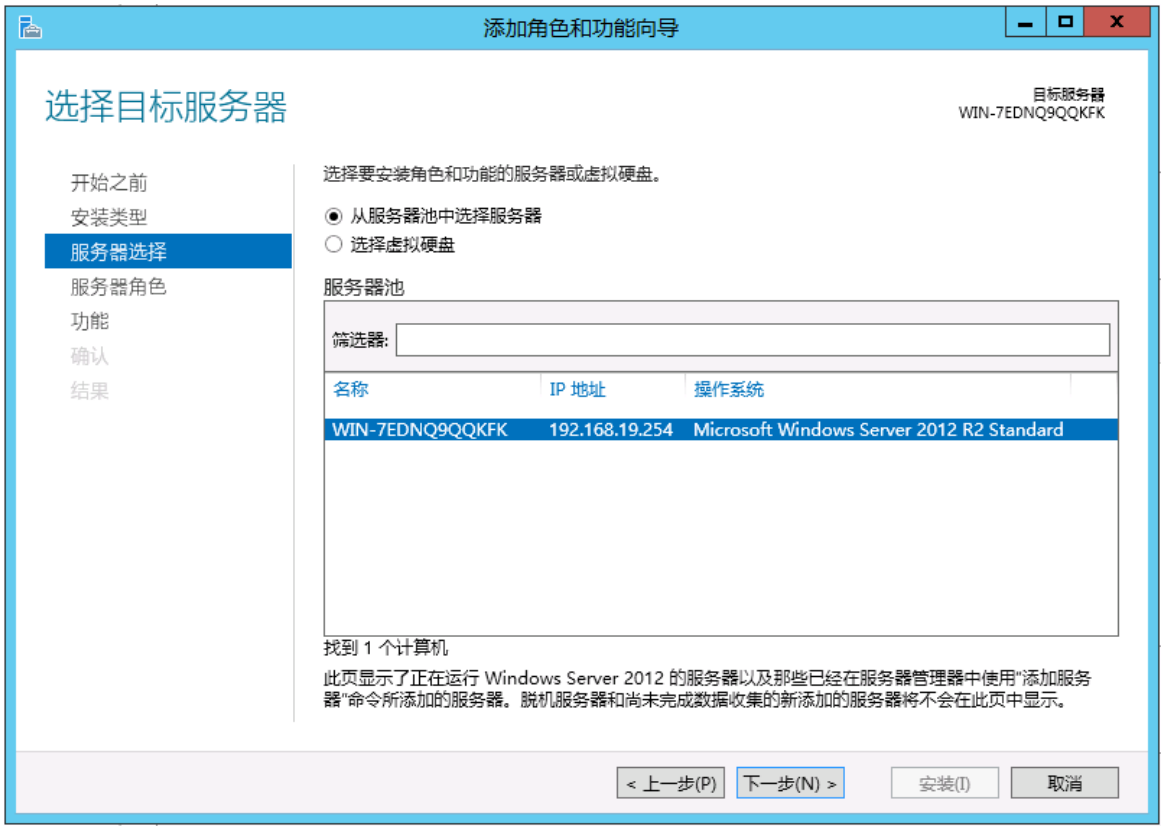
(4) 单击<下一步>按钮，进入安装类型选择界面，选择基于角色或基于功能的安装，如图 11-35 所示。

图11-35 安装类型



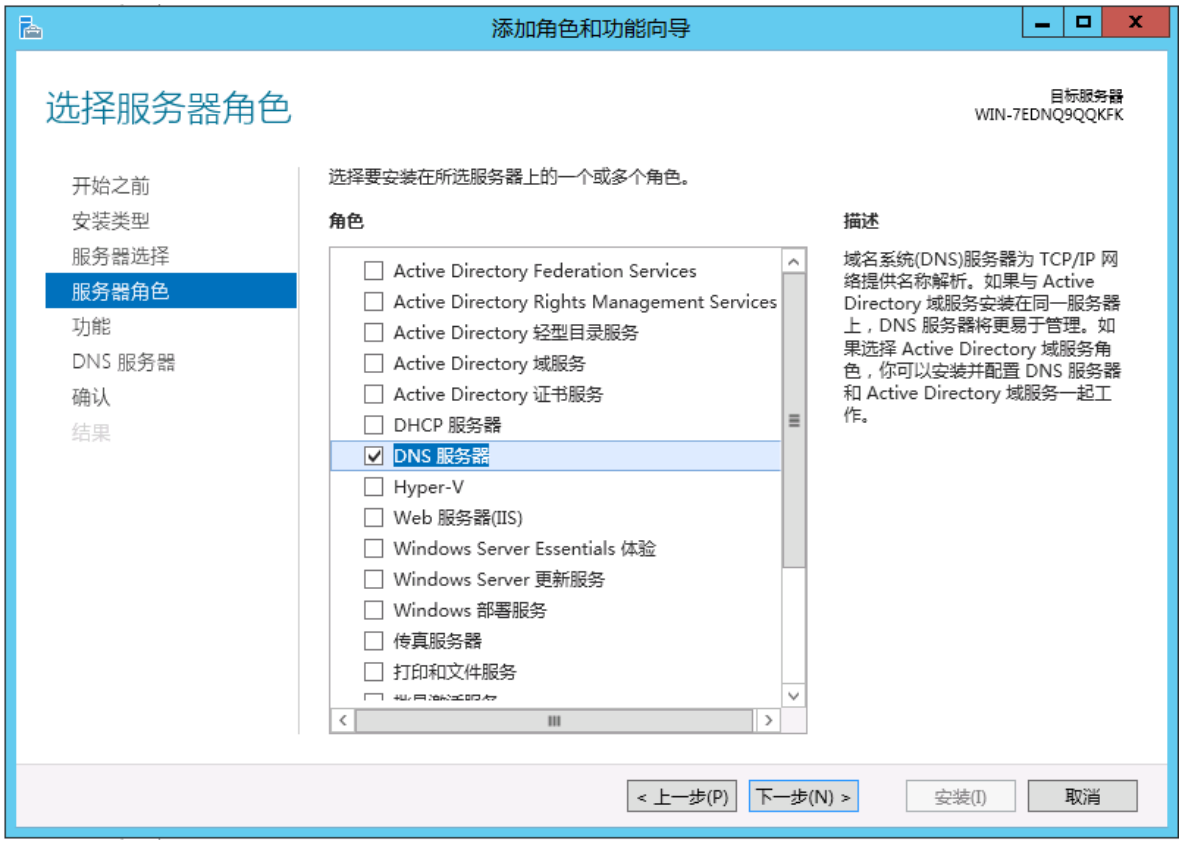
(5) 单击<下一步>按钮，进入服务器选择界面，选择从服务器池中选择服务器，选择本机作为目标服务器，如图 11-36 所示。

图11-36 选择目标服务器



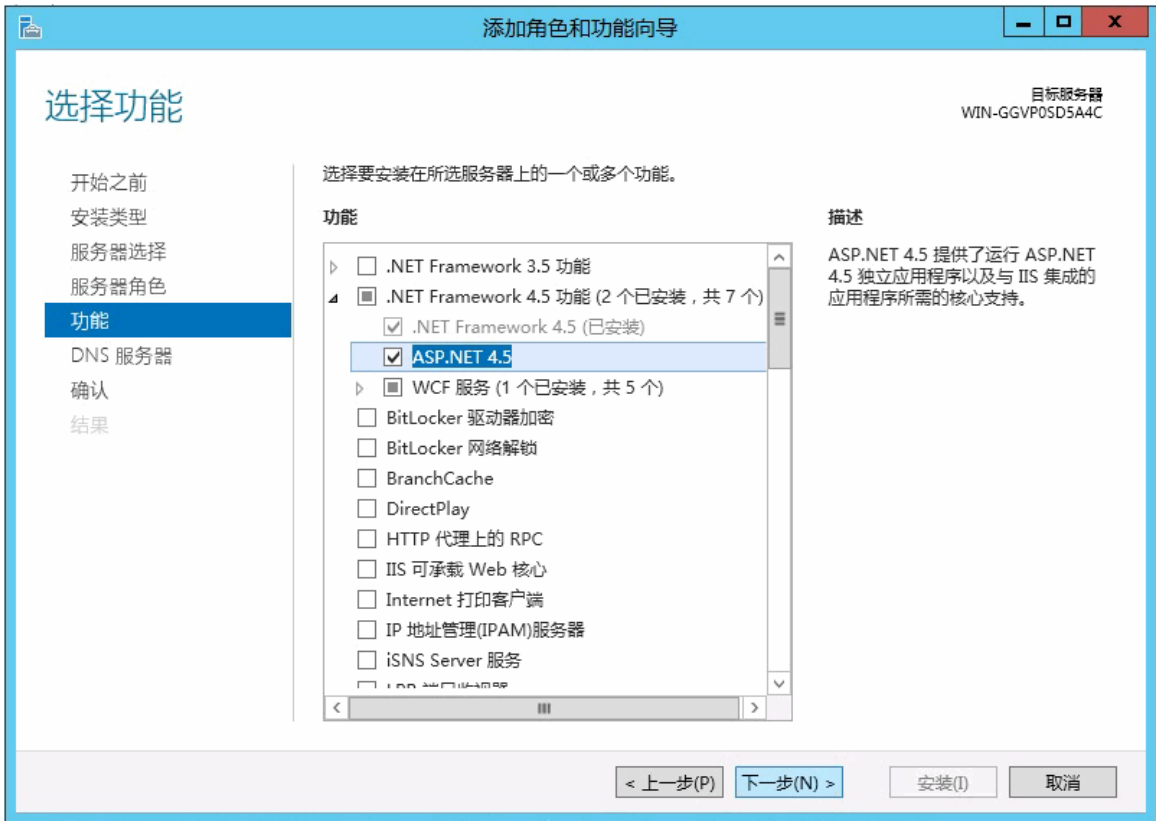
(6) 单击<下一步>按钮，进入服务器角色界面，勾选 DNS 服务器选项，如图 11-37 所示。

图11-37 服务器角色



(7) 单击<下一步>按钮，进入选择功能界面，勾选 NET Framework 4.5 功能，如图 11-38 所示。

图11-38 选择功能



(8) 单击<下一步>按钮，进入注意事项界面。

(9) 单击<下一步>按钮，进入功能确认界面。

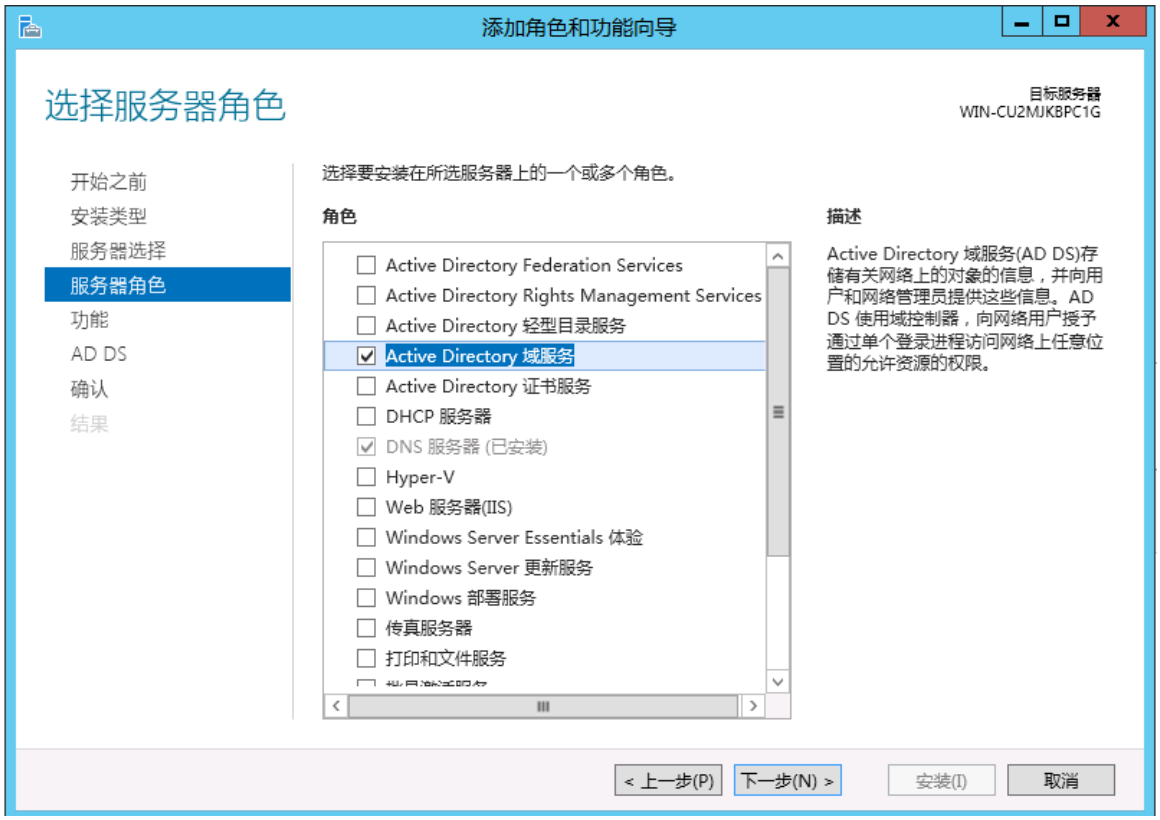
(10) 单击<安装>按钮，安装 DNS 服务。

2. 安装 Active Directory 域服务

(1) 参考安装 DNS 服务的步骤 1～5，继续添加新服务。

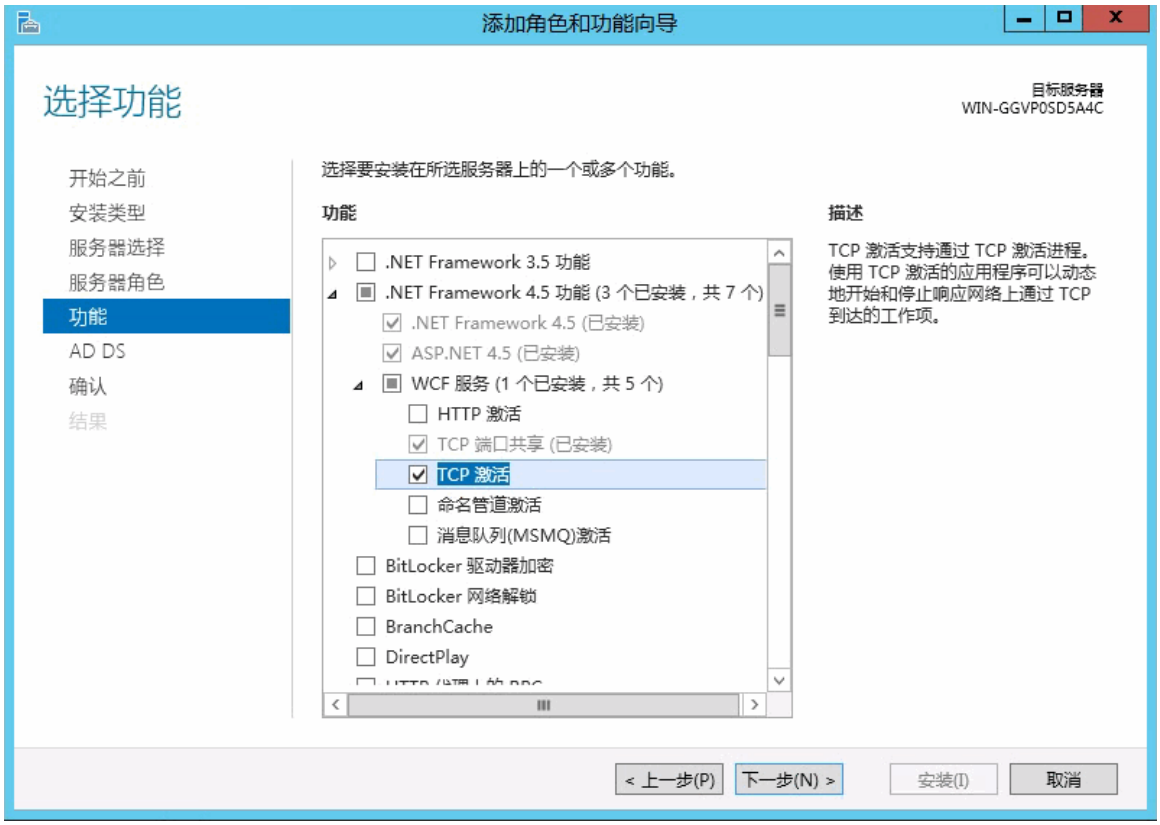
(2) 进入服务器角色界面，勾选 Active Directory 域服务，如图 11-39 所示。

图11-39 服务器角色



(3) 单击<下一步>按钮，进入选择功能界面，勾选 NET Framework 4.5 功能，如图 11-40 所示。

图11-40 选择功能



(4) 单击<下一步>按钮，进入注意事项界面。

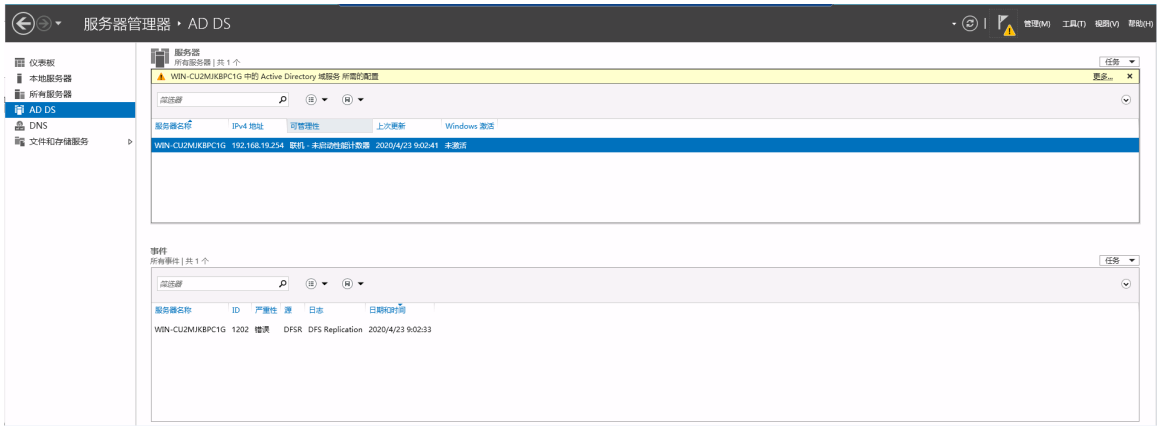
(5) 单击<下一步>按钮，进入功能确认界面。

(6) 单击<安装>按钮，安装 Active Directory 域服务。

3. 配置 Active Directory 域服务

(1) 单击服务器管理器页面左侧的[AD DS]菜单，右侧显示 Active Directory 域服务的属性，如图 11-41 所示。

图11-41 AD DS

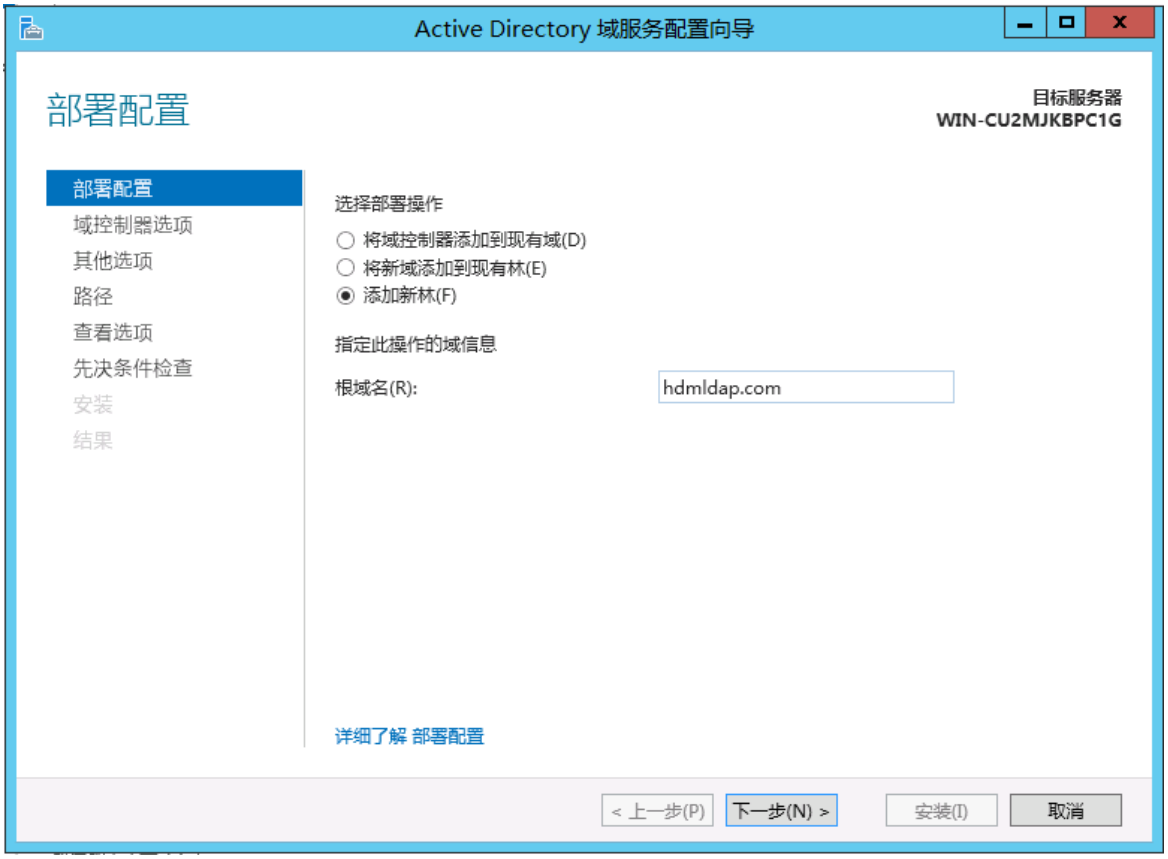


(2) 单击页面右上方的“更多...”，打开所有服务器任务详细信息的对话框，如图 11-42 所示。

图11-42 任务详细信息

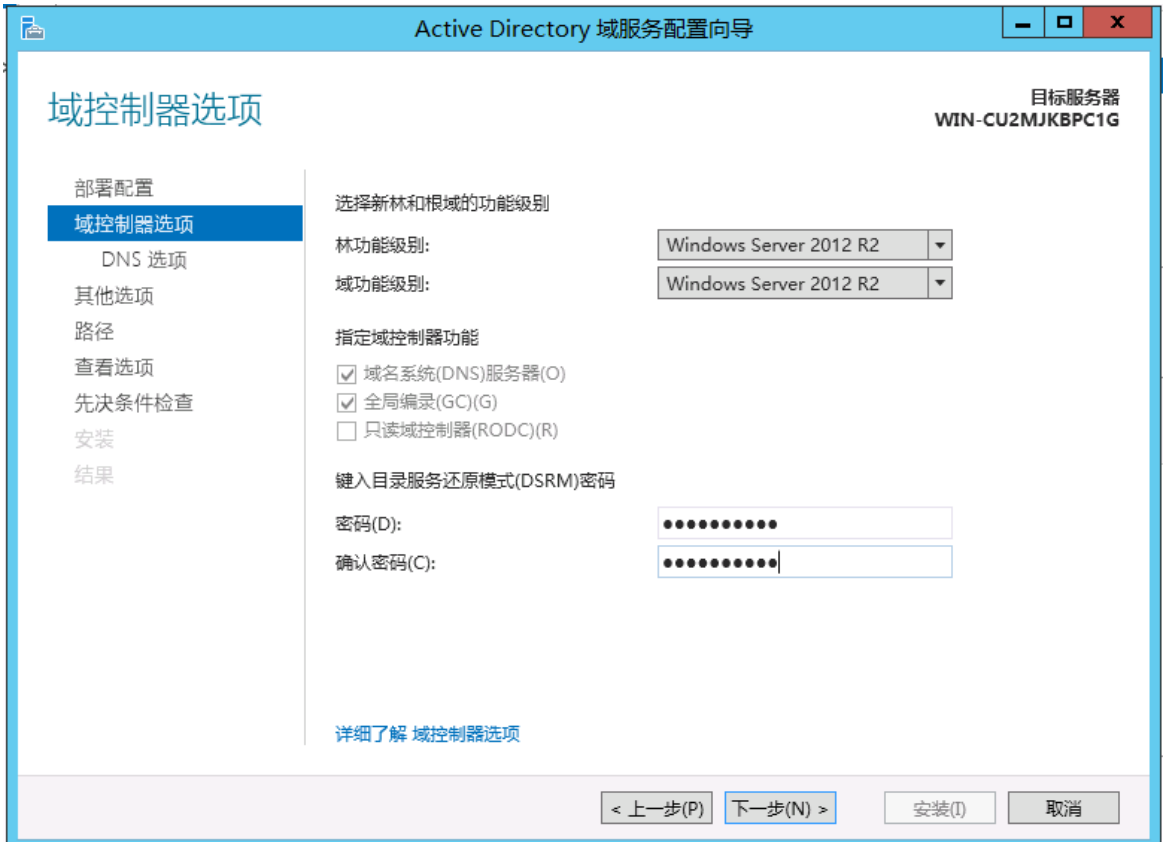
(3) 单击操作栏的“将此服务器提升为域控制器”，打开 Active Directory 域服务配置向导，如图11-43 所示。

图11-43 Active Directory 域服务配置向导



(4) 选择添加新林，在根域名栏输入 Active Directory 域名，以 hdmldap 为例，单击<下一步>按钮，打开域控制器界面，如图 11-44 所示。

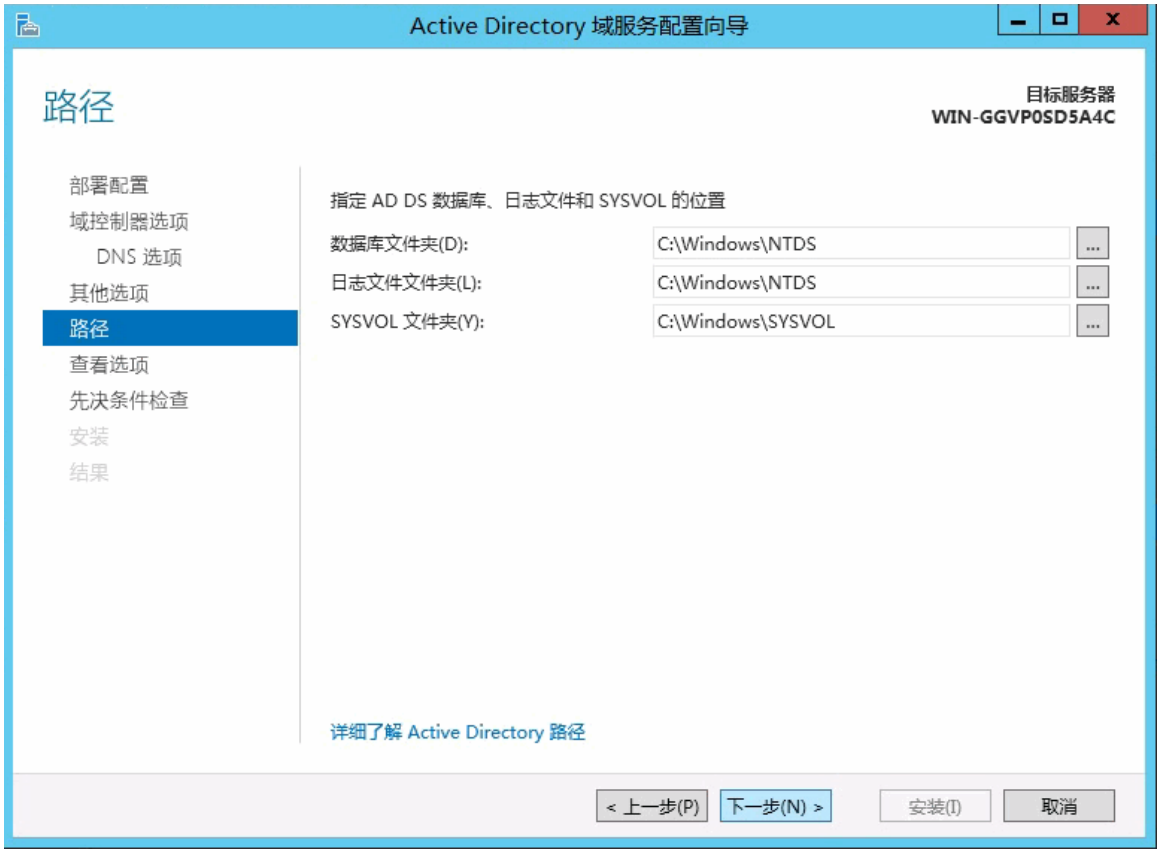
图11-44 域控制器



(5) 输入 Active Directory 域控制器的密码，单击<下一步>按钮。

(6) 根据指引继续单击<下一步>按钮，直至进入域服务路径界面，如图 11-45 所示。

图11-45 域服务路径



(7) 根据实际需求设置 Active Directory 域服务相关路径，也可以使用默认配置，单击<下一步>按钮。

(8) 根据指引继续单击<下一步>，直至进入先决条件检查界面，如图 11-46 所示。

图11-46 先决条件检查

(9) 单击<安装>按钮，开始配置 Active Directory 域服务器，配置完成后，操作系统将会自动重启。

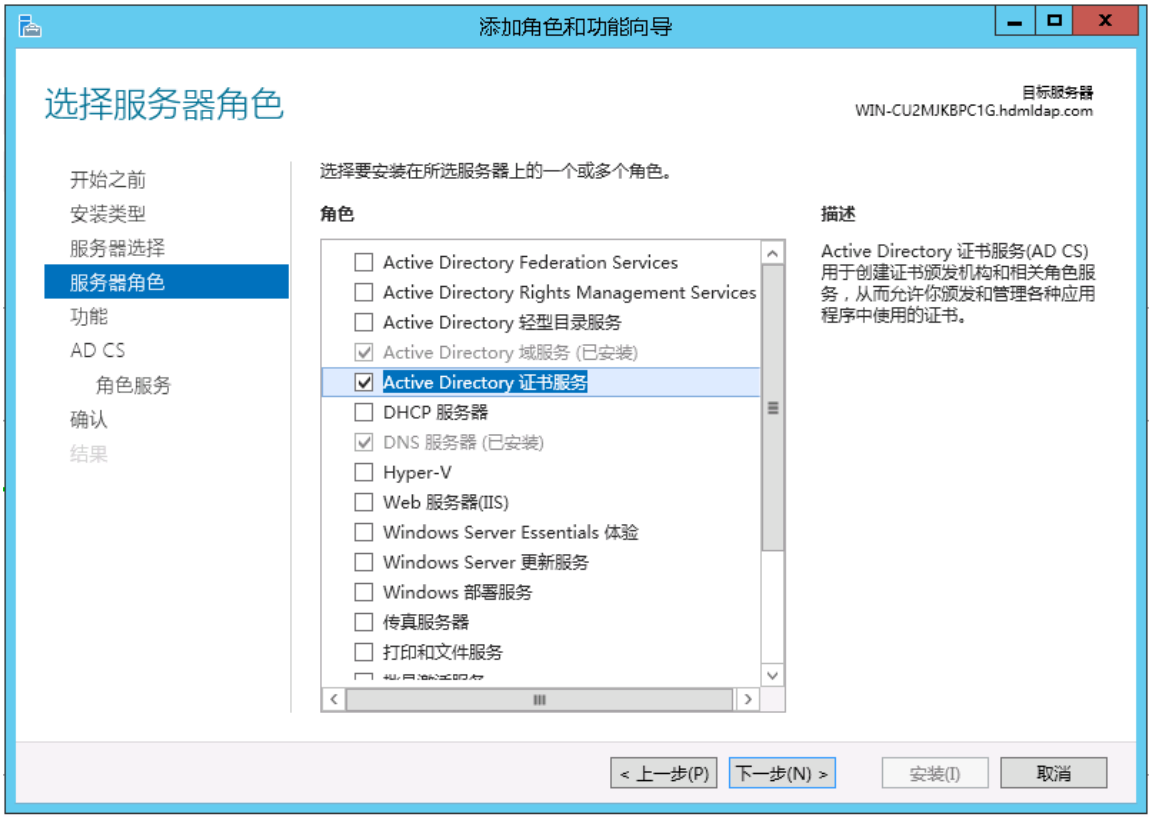
4. 安装 Active Directory 证书服务

操作系统重启后，需要以管理员权限重新登录，登录时要在用户名前面加上域名才能登录成功。

(1) 参考安装 DNS 服务的步骤 1～5，继续添加新服务。

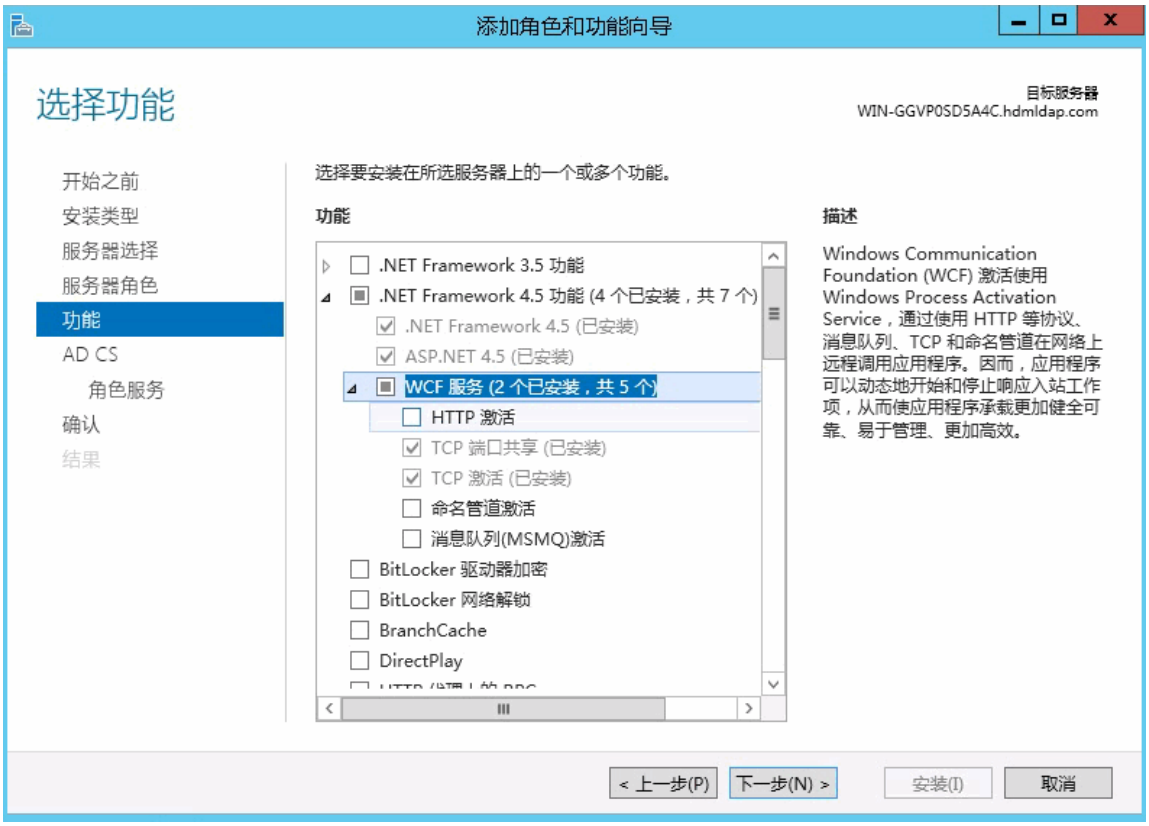
(2) 进入服务器角色界面，勾选 Active Directory 证书服务，如图 11-47 所示。

图11-47 服务器角色



(3) 单击<下一步>按钮，进入选择功能界面，勾选 NET Framework 4.5 功能，如图 11-48 所示。

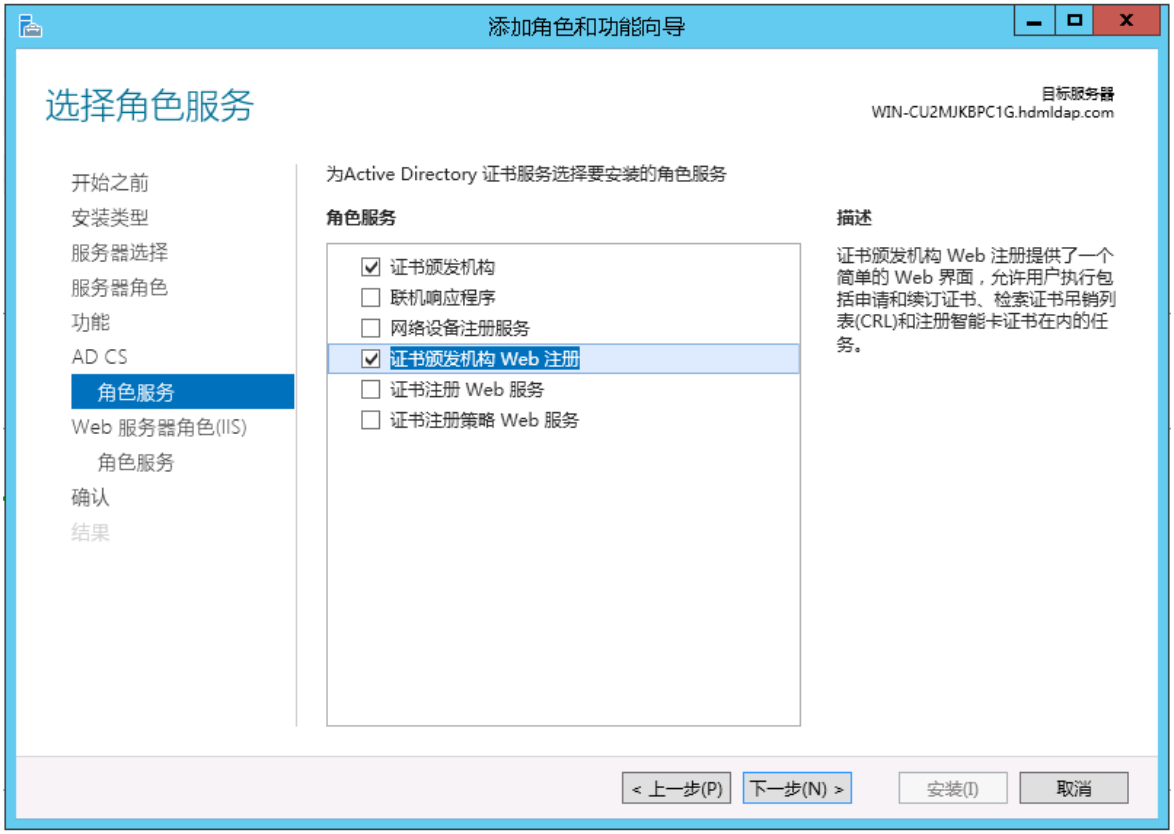
图11-48 选择功能



(4) 单击<下一步>按钮，进入注意事项界面。

(5) 单击<下一步>按钮，进入为 Active Directory 证书服务添加角色服务界面，勾选证书颁发机构和证书颁发机构 Web 注册，如图 11-49 所示。

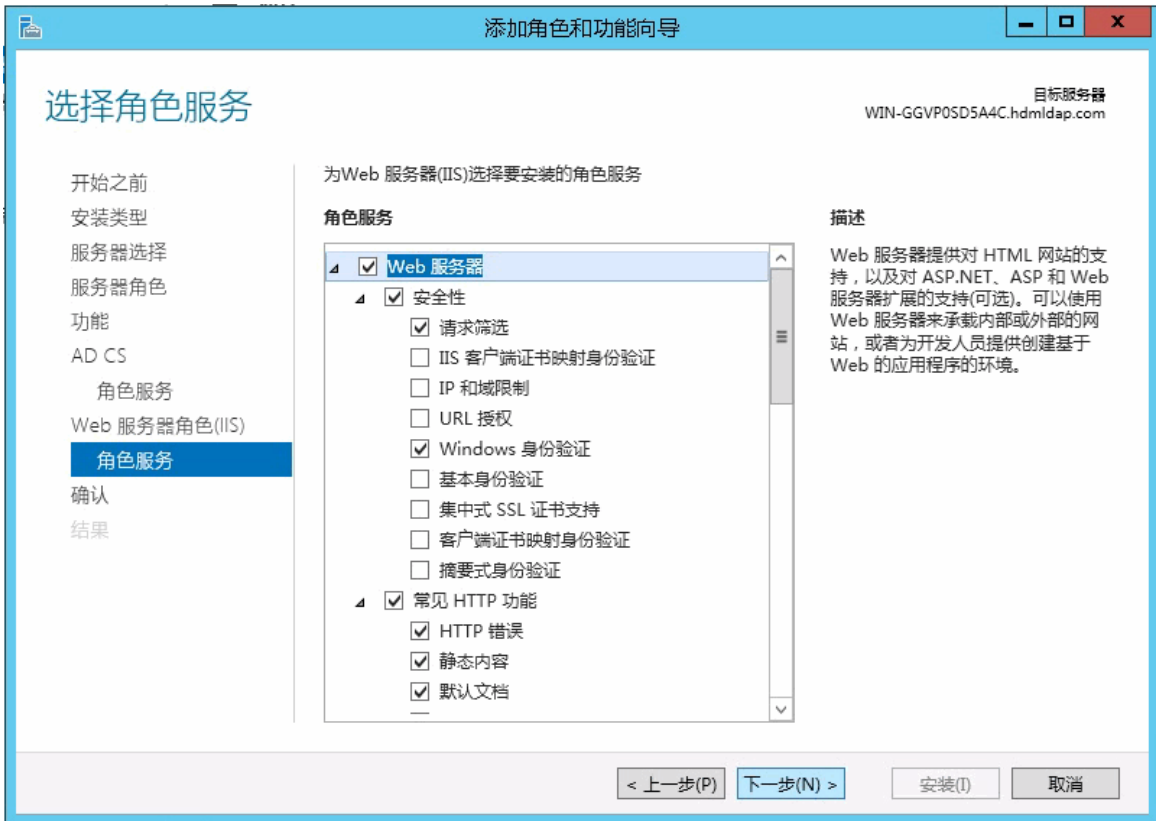
图11-49 添加角色服务



(6) 单击<下一步>按钮，进入注意事项界面。

(7) 单击<下一步>按钮，进入为 Web 服务器添加角色服务界面，推荐使用默认配置，如图 11-50 所示。

图11-50 添加角色服务



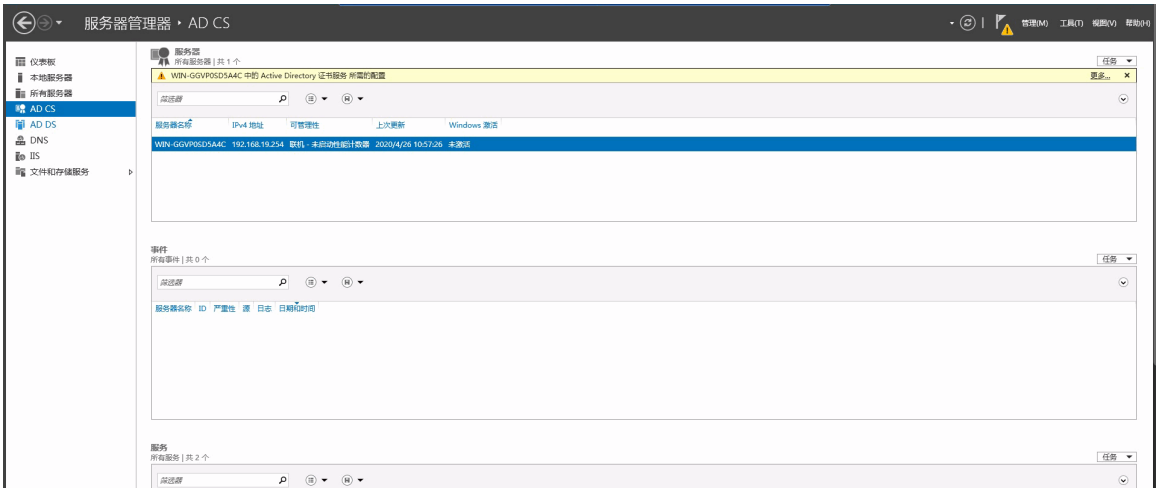
(8) 单击<下一步>按钮，进入确认界面。

(9) 单击<安装>按钮，开始安装 Active Directory 证书服务。

5. 配置 Active Directory 证书服务

(1) 单击服务器管理器页面左侧的[AD CS]菜单，右侧显示 Active Directory 证书服务的属性，如图 11-51 所示。

图11-51 AD CS

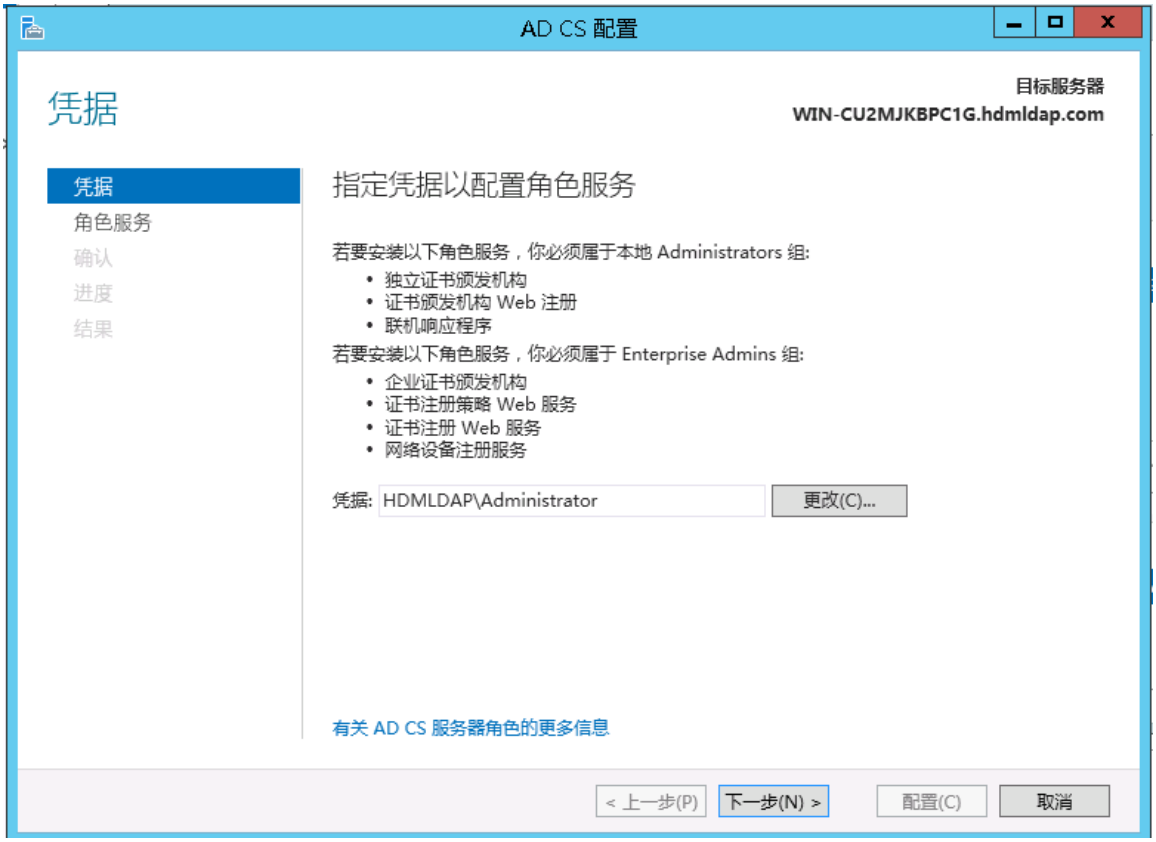


(2) 单击页面右上方的“更多...”，打开所有服务器任务详细信息的对话框，如图 11-52 所示。

图11-52 任务详细信息

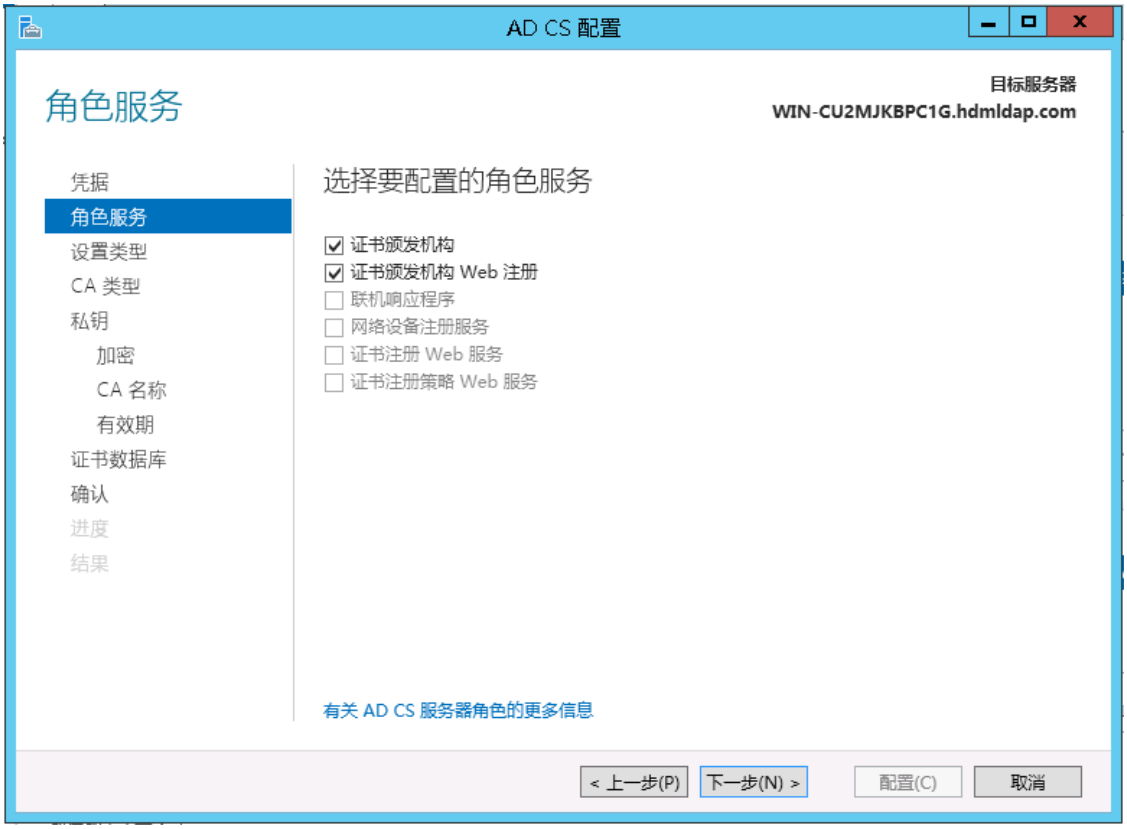
(3) 单击操作栏的配置目标服务器上的 Active Directory 证书服务，打开 Active Directory 证书服务配置向导，如图 11-53 所示。

图11-53 Active Directory 证书服务配置向导



(4) 单击<下一步>按钮，进入角色服务界面，勾选证书颁发机构和证书颁发机构 Web 注册，如图11-54 所示。

图11-54 角色服务



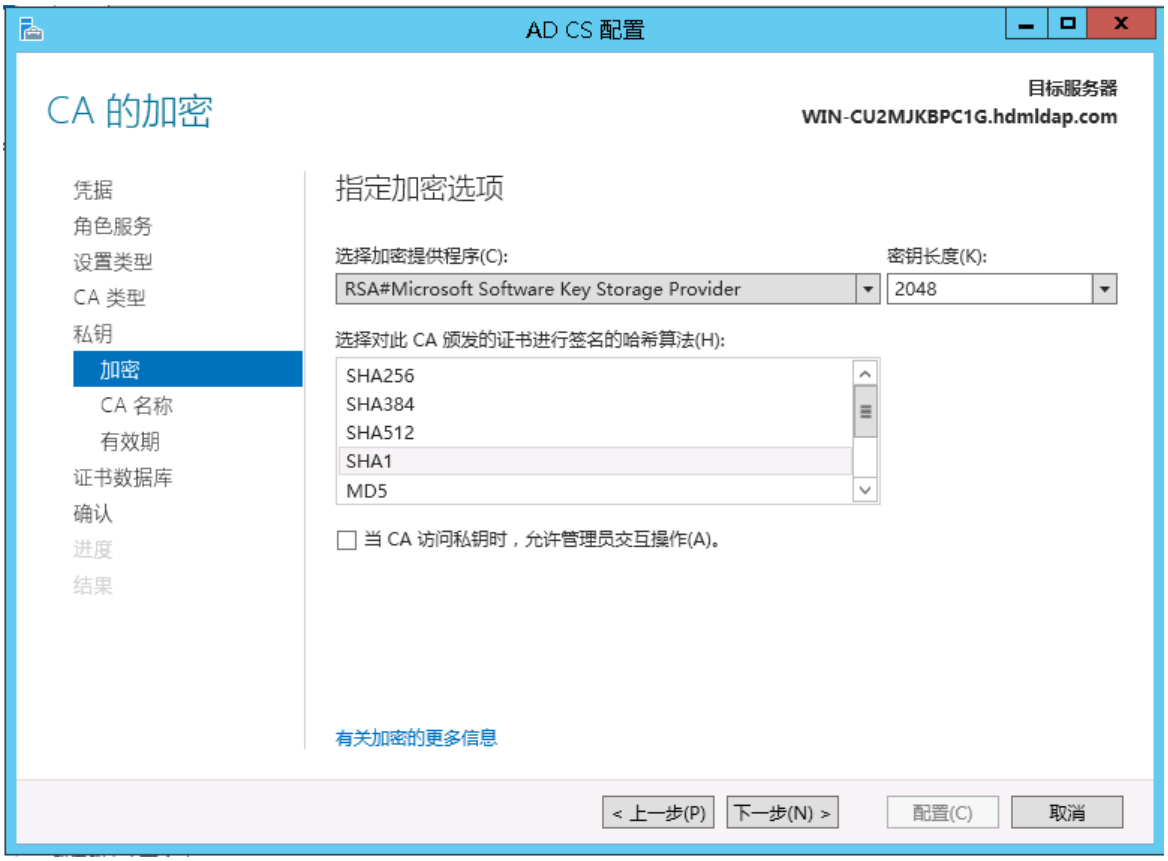
(5) 单击<下一步>按钮，进入设置类型界面，勾选企业 CA。

(6) 单击<下一步>按钮，进入 CA 类型界面，勾选根 CA。

(7) 单击<下一步>按钮，进入私钥界面，勾选创建新的私钥。

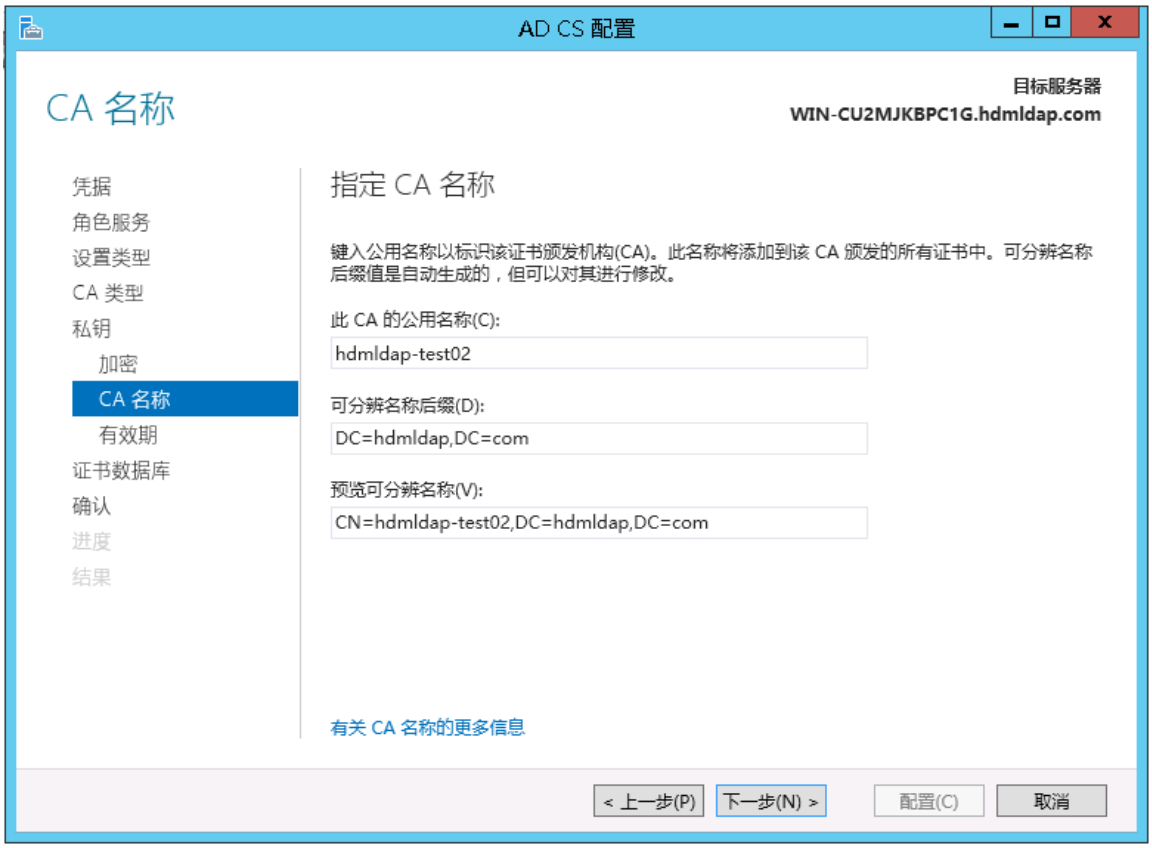
(8) 单击<下一步>按钮，进入加密界面，指定加密提供程序为 RSA，秘钥长度为 2048，哈希算法为 SHA1，如图 11-55 所示。

图11-55 CA 加密界面



(9) 单击<下一步>按钮，进入 CA 名称界面，设置 CA 名称为 hdmldap-test02，如图 11-56 所示。

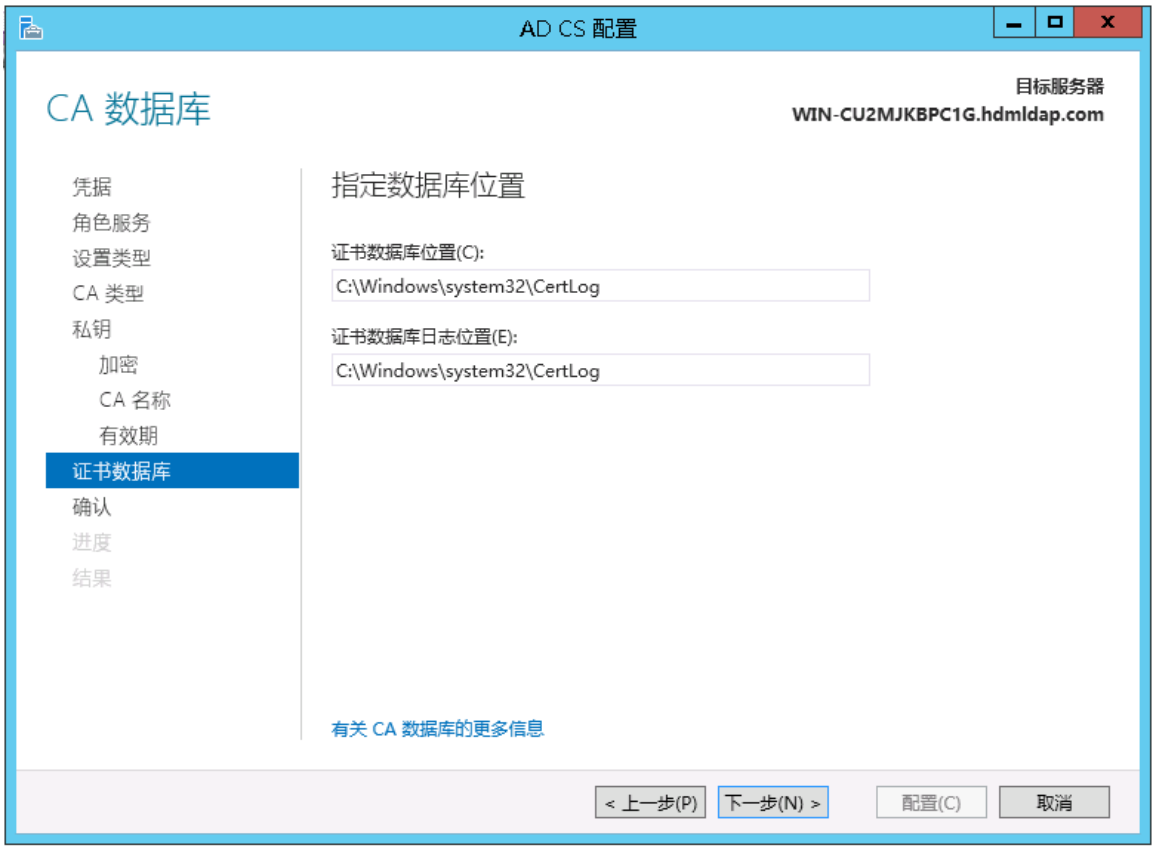
图11-56 CA 名称



(10) 单击<下一步>按钮，进入有效期界面，指定 CA 证书有效期，默认为 5 年。

(11) 单击<下一步>按钮，进入证书数据库界面，设置证书数据库位置，如图 11-57 所示。

图11-57 数据库



(12) 单击<下一步>按钮，进入确认界面。

(13) 单击<配置>按钮，开始配置 Active Directory 证书服务。

(14) 配置完成后，需要重启服务器使配置生效。

11.4.3 配置 LDAP 服务器

操作系统重启后，以管理员权限重新登录进入操作系统，登录时要在用户名前面加上域名才能登录成功，登录成功后开始配置 LDAP 服务器。

1. 新建组织单位

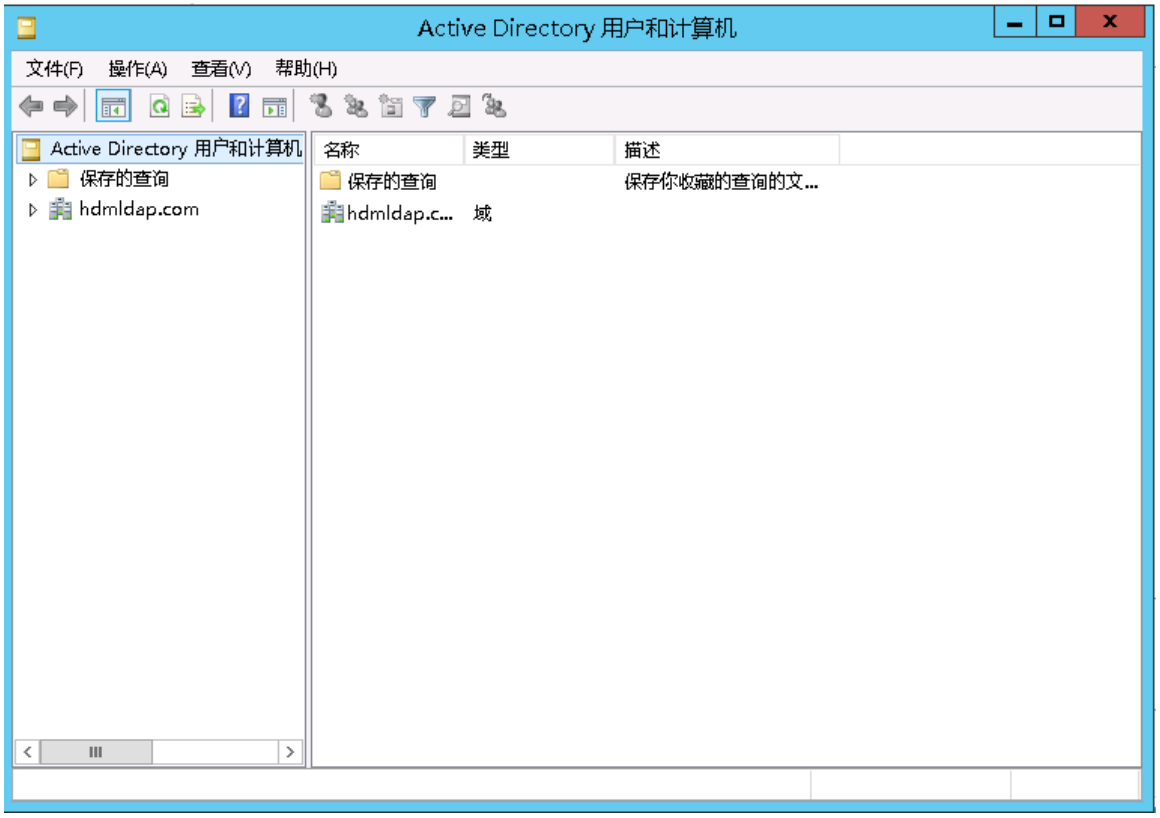
说明

- 新建组织单位时，可以根据实际需要在 LDAP 服务器上规划新的一级组织单位和低级别组织单位，也可以在已有的组织单位下面新建低级别组织单位。
- 本文以新建一级和二级组织单位为例进行说明。

(1) 单击 [服务器管理器]菜单项，进入服务器管理器页面。

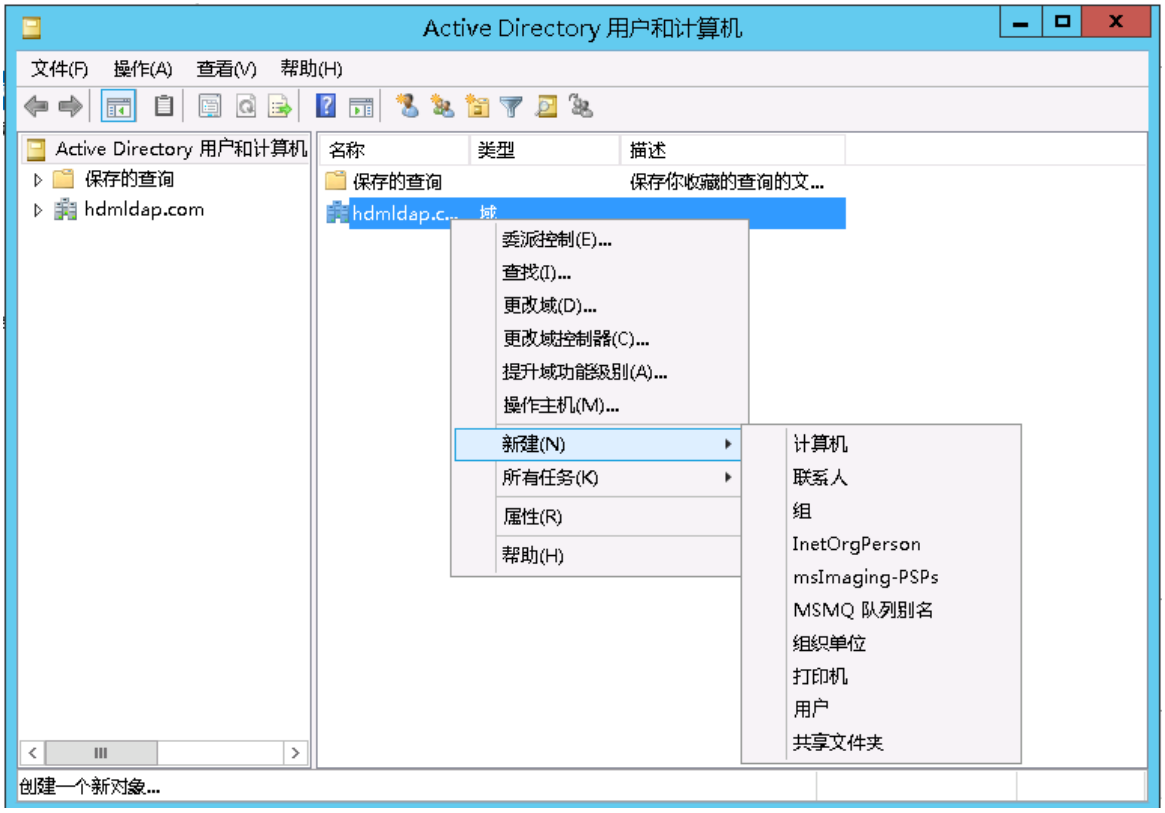
(2) 单击页面右上方的<任务>按钮，在下拉列表中选择 Active Directory 用户和计算机，打开域的服务组件，如图 11-58 所示。

图11-58 Active Directory 用户和计算机



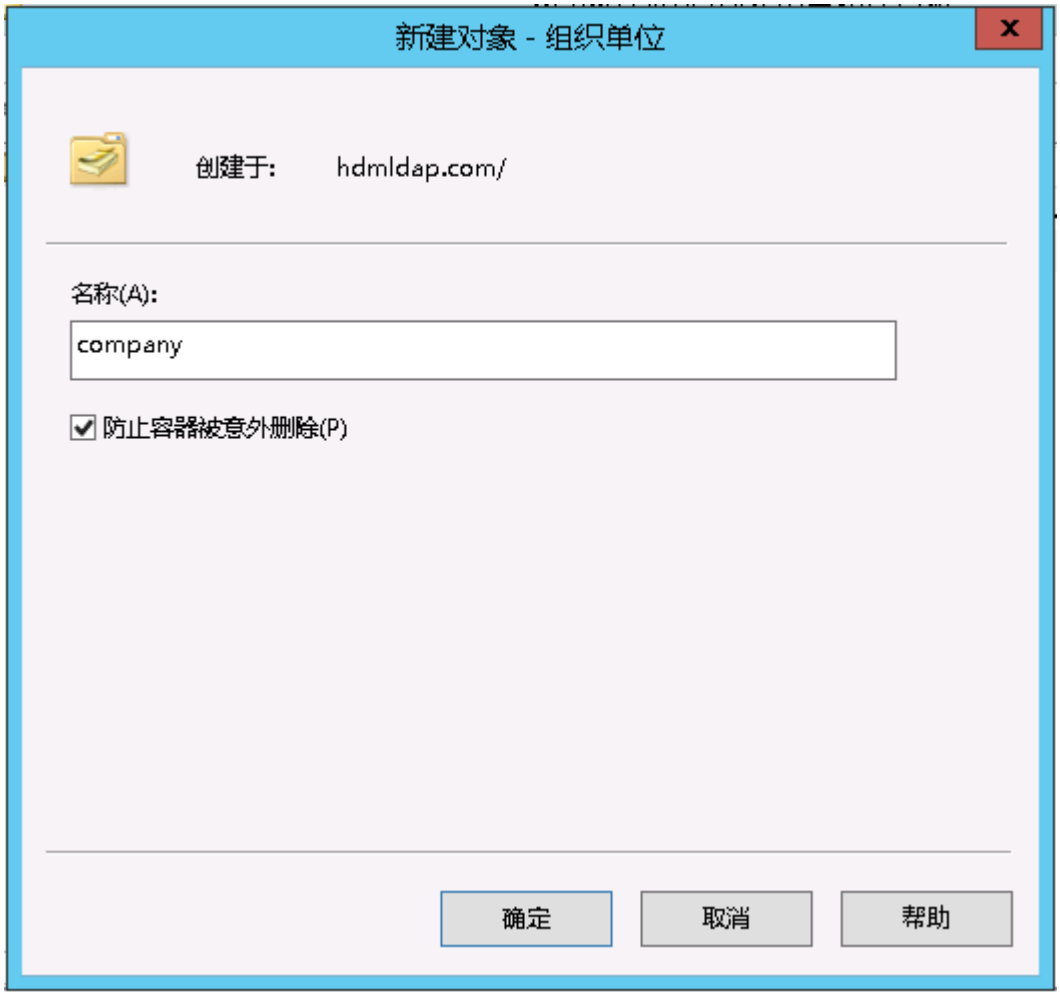
(3) 右键单击 hdmldap.com，选择[新建/组织单位]菜单项，如图 11-59 所示。

图11-59 hdmldap.com



(4) 打开新建对象的组织单位对话框，输入组织名称，以 company 为例，如图 11-60 所示。

图11-60 新建组织

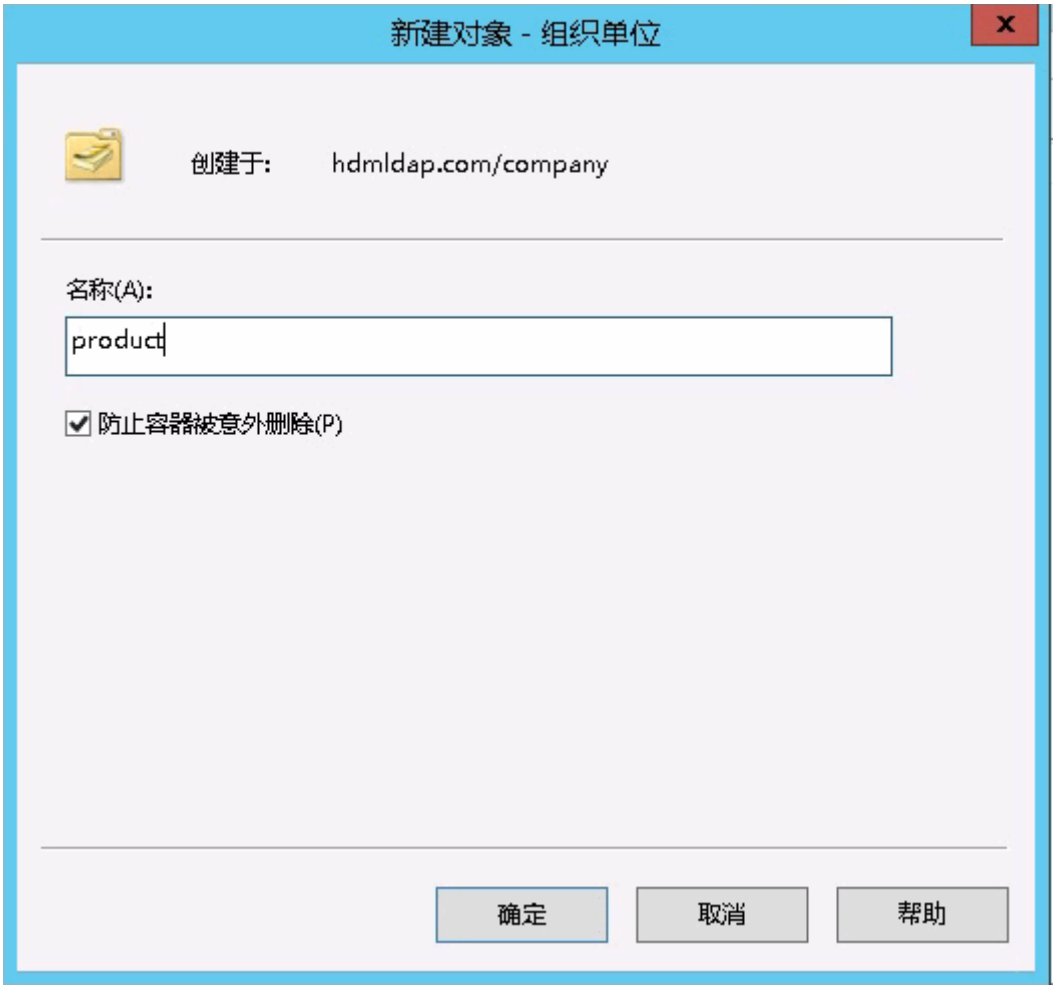


(5) 单击<确定>按钮，一级组织 company 创建成功。

(6) 右键单击 company，选择[新建/组织单位]菜单项，打开新建组织单位对话框。

(7) 输入组织名称，以 product 为例，如图 11-61 所示。

图11-61 新建组织



(8) 单击<确定>按钮，二级组织 product 创建成功。

(9) 重复以上操作，可以新建多个组织单位。

2. 新建角色组

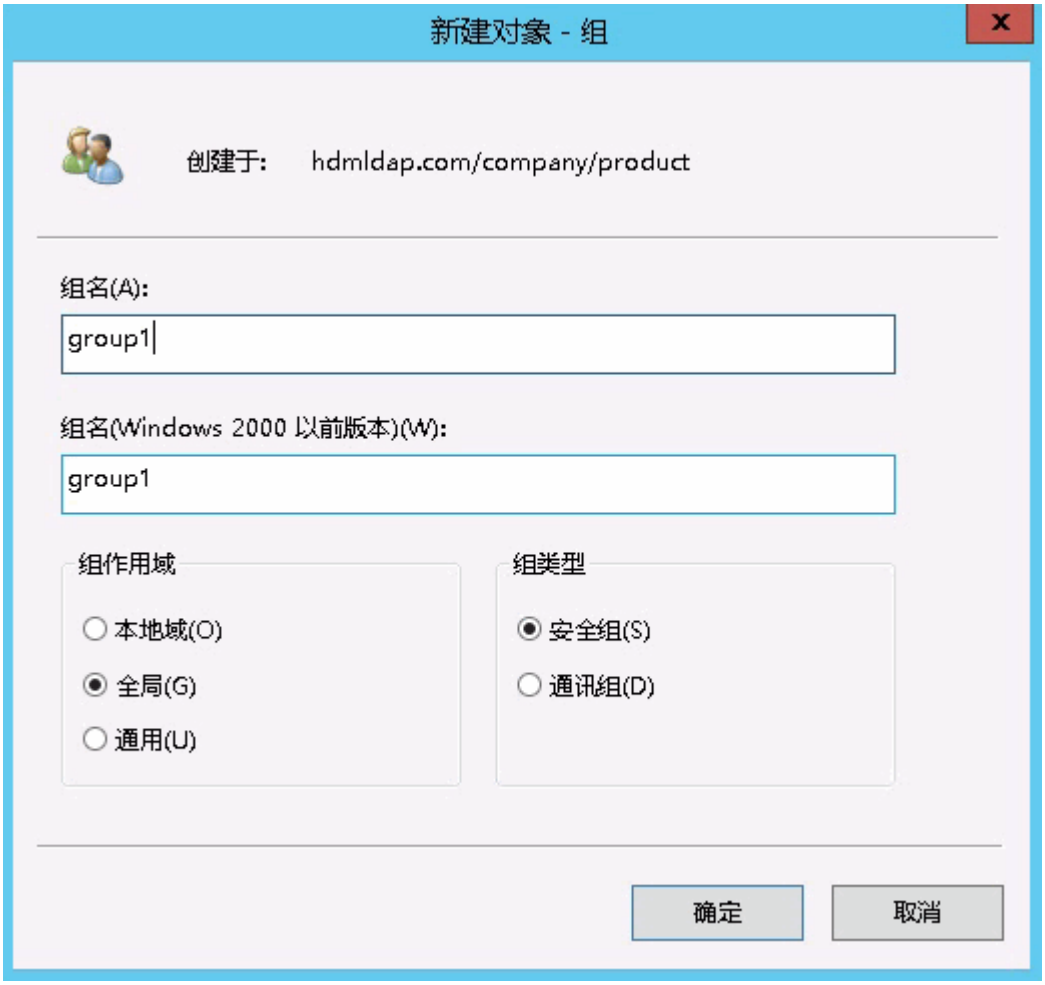
说明

新建角色组时，可以选择任意级别的组织单位。

(1) 右键单击 product，选择[新建/组]菜单项，打开新建组对话框。

(2) 输入组名，以 group1 为例，勾选组作用域和组类型，如图 11-62 所示。

图11-62 新建组



说明

“组名（A）”和“组名（Windows 2000 以前版本）”建议保持一致。

(3) 单击<确定>按钮，创建角色组成功。

(4) 重复以上操作，可以新建多个角色组。

3. 新建用户

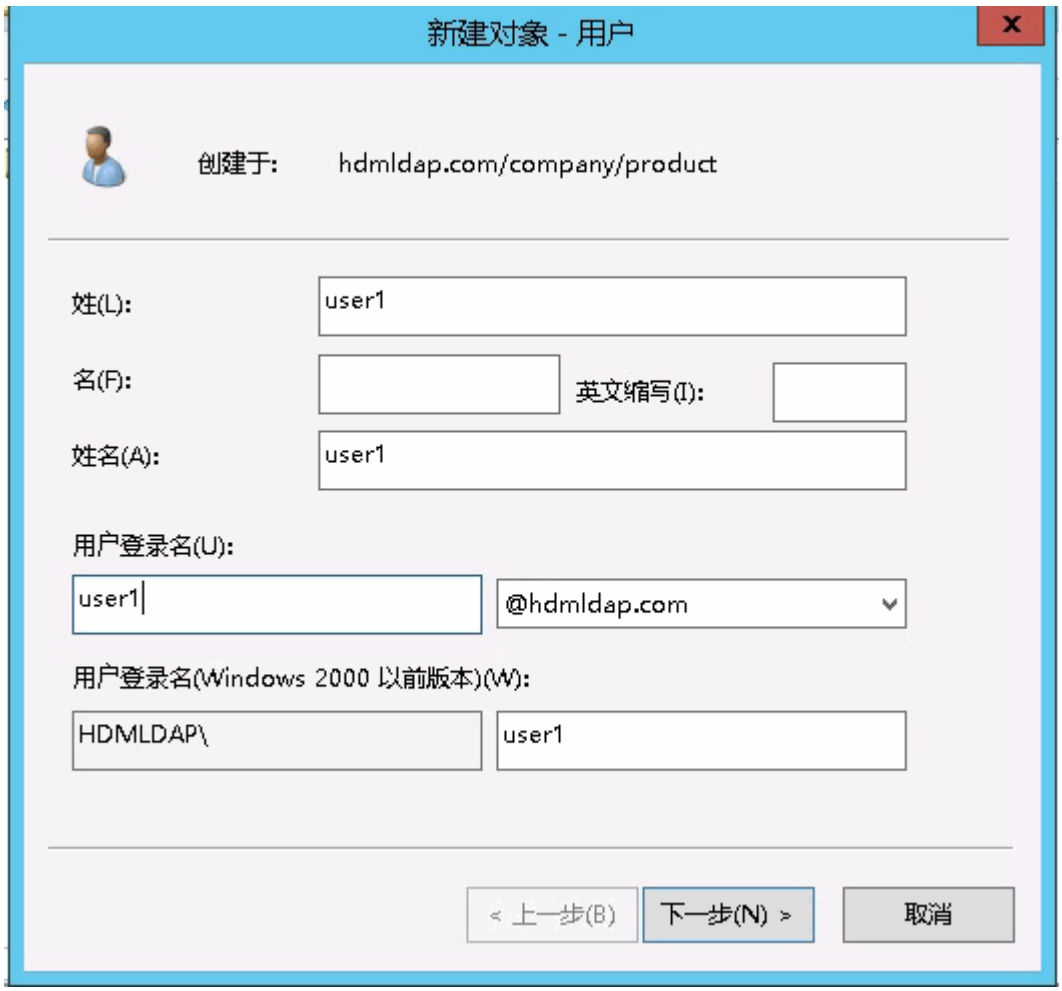
说明

新建用户时，可以选择任意级别的组织单位。

(1) 右键单击 product，选择[新建/用户]菜单项，打开新建用户对话框。

(2) 输入用户信息，以 user 为例，如图 11-63 所示。

图11-63 新建用户

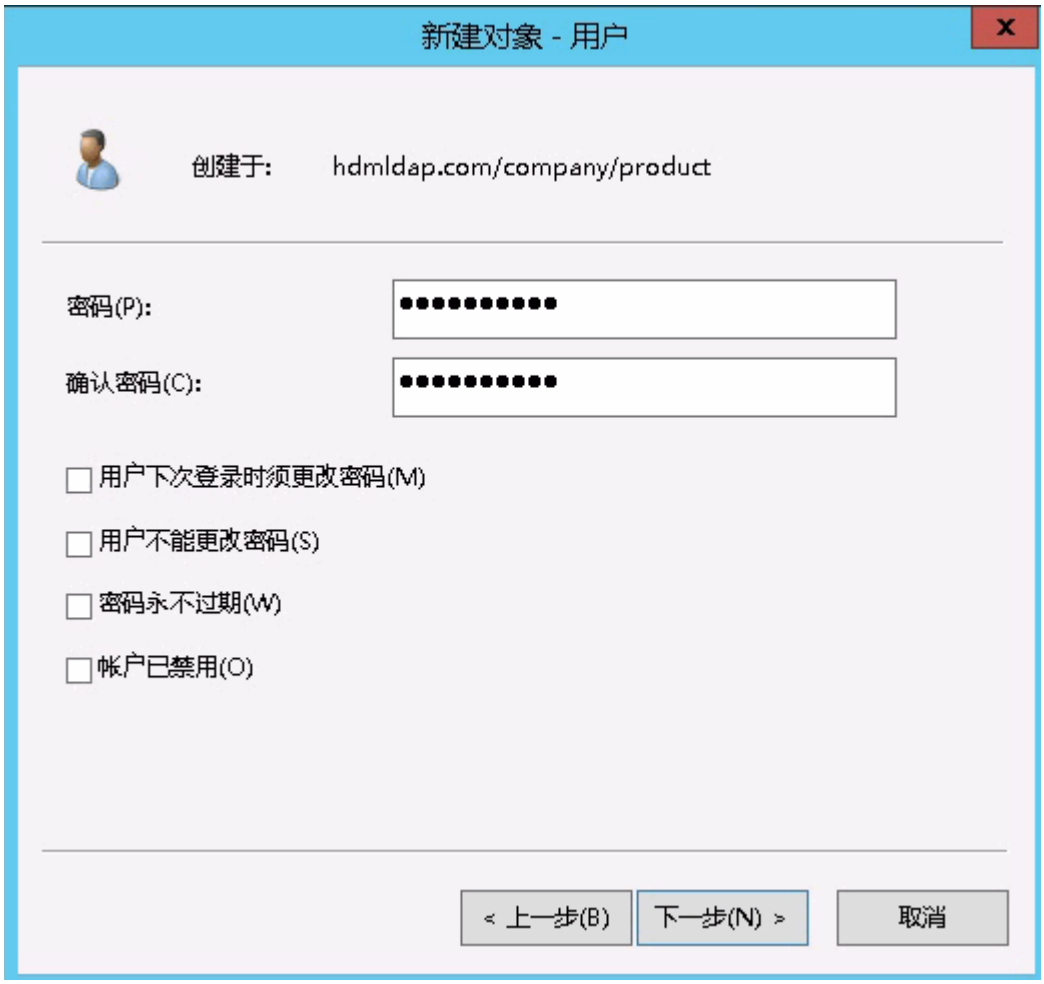


说明

用户登录名和下一步的登录密码是访问 HDM 的登录名和密码，请谨慎设置和保存。

(3) 单击<下一步>按钮，进入设置密码界面，输入用户登录密码，取消勾选“用户下次登录时须更改密码”选项，如图 11-64 所示。

图11-64 设置密码



(4) 单击<下一步>按钮，进入确认界面，单击<完成>按钮，创建成功。

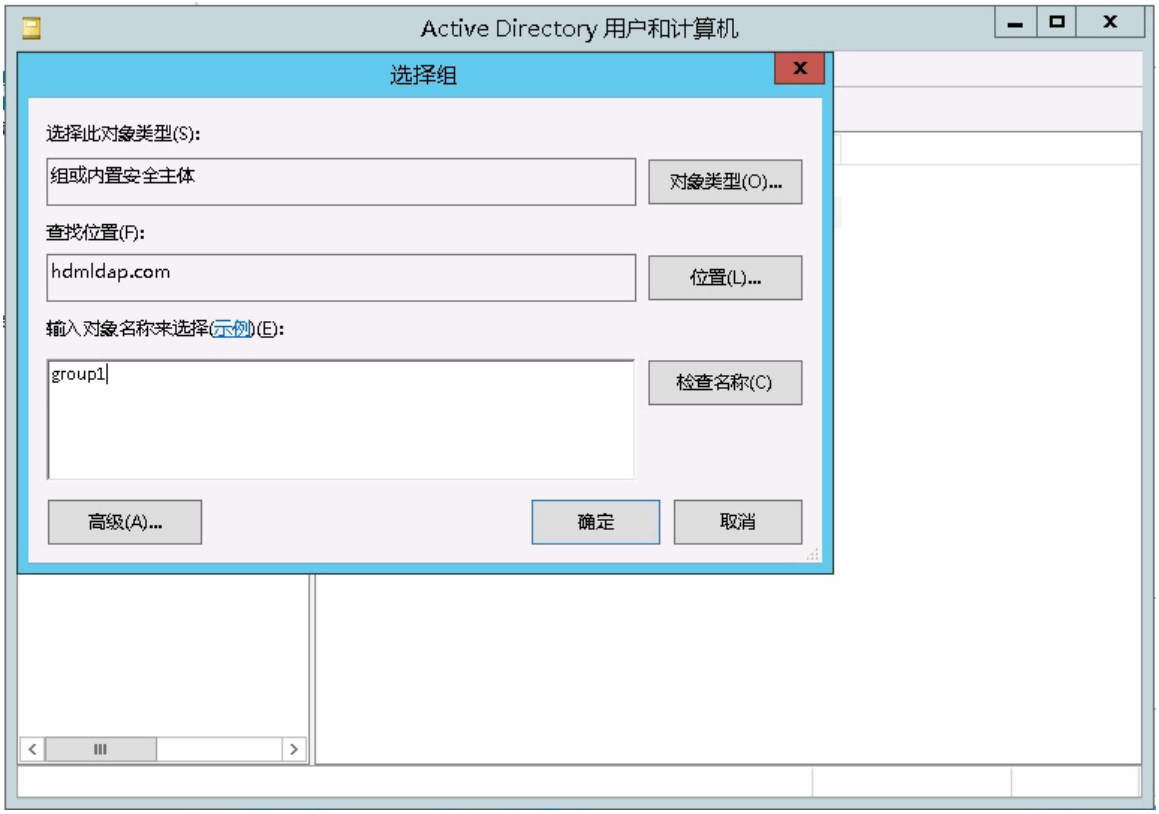
(5) 重复以上操作，可以新建多个用户。

4. 把用户添加到组

可以通过对组的操作来添加用户，也可以通过对用户的操作来添加到组，本文以对用户的操作为例进行说明。

(1) 右键单击 user1，选择添加到组，打开选择组对话框，如图 11-65 所示。

图11-65 选择组



(2) 输入要加入的组名，以 group1 为例，单击<确定>确定按钮，完成操作。

(3) 重复以上操作，可以将多个用户添加到组。

11.4.4 HDM Web 端配置 LDAP

HDM 提供 LDAP 用户的接入功能。通过 HDM Web 启用 LDAP 功能，添加角色组后，可以直接使用角色组里的 LDAP 用户访问 HDM。

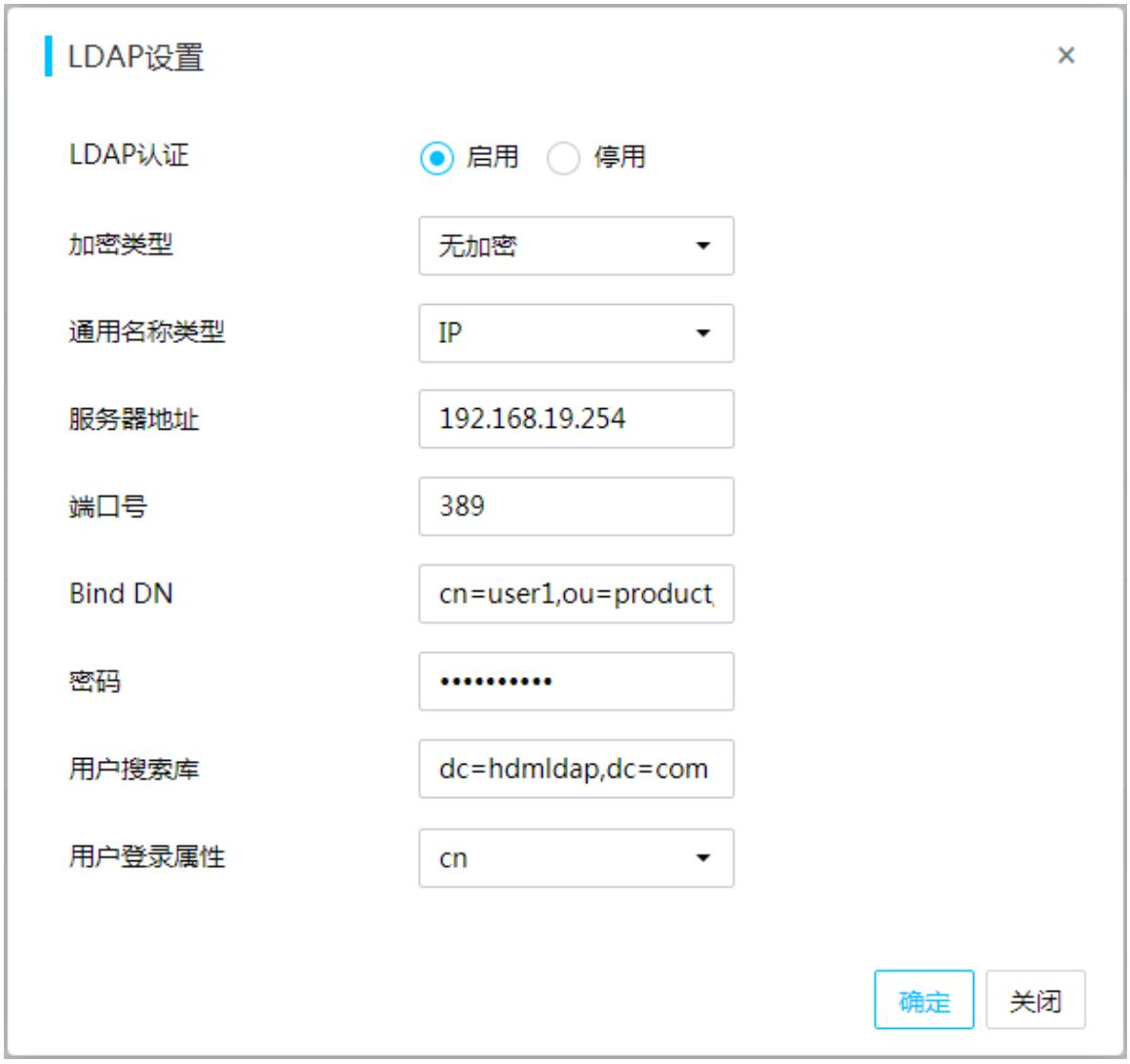
1. 启用 LDAP 功能

(1) 单击[用户&安全/用户访问设置]菜单项，选择域用户页签，进入域用户页面。

(2) 单击 LDAP 配置栏的<高级设置>按钮，弹出“LDAP 设置”对话框。

(3) 在对话框中勾选 LDAP 认证的<启用>选项，并配置相关信息，如图 11-66 所示。

图11-66 LDAP 配置



a. 加密类型选择无加密。
b. 通用名称类型选择 IP。
c. 服务器地址输入 LDAP 服务器所在的操作系统的 IP 地址。
d. 端口号使用默认端口即可。
e. Bind DN 输入 user1 的 dn 信息，包括公共名称、组织单位（从低级到高级组织）和域名信息，信息之间用英文逗号隔开。
   - 公共名称：cn=user1
   - 组织单位：ou=product,ou=company
   - 域名：dc=hdmldap,dc=com
f. 密码输入 user1 的登录密码。
g. 用户搜索库输入 user1 的域名信息，dc=hdmldap,dc=com。
h. 用户登录属性选择 cn。

(4) 单击<确定>按钮，完成操作。

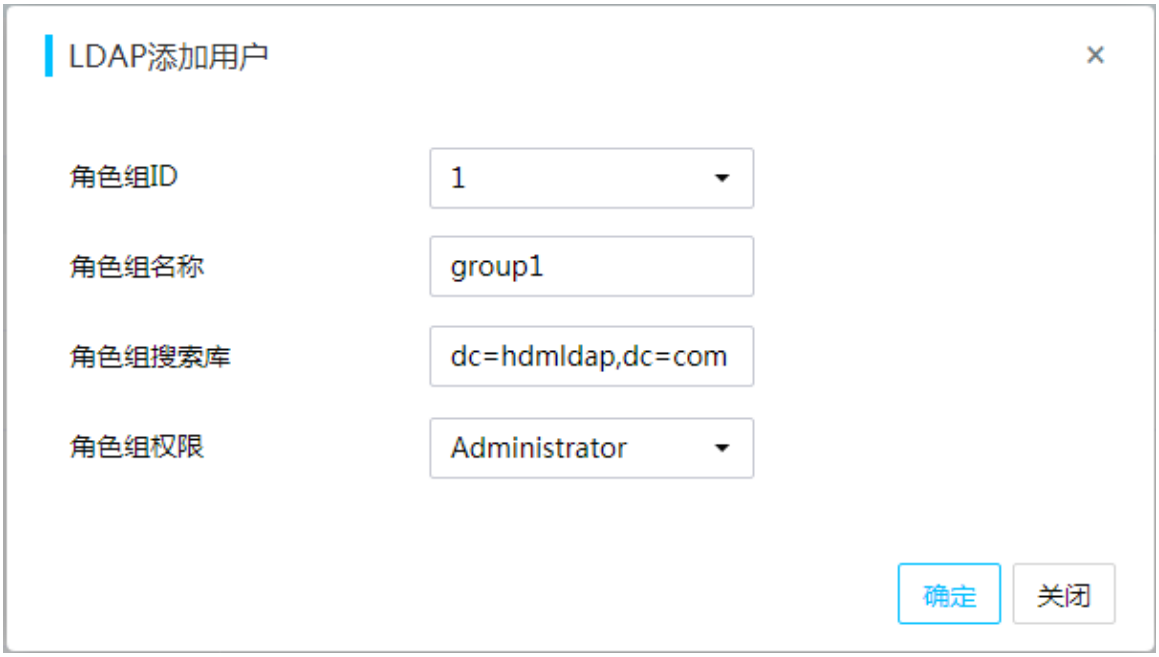
2. 添加角色组

(1) 单击[用户&安全/用户访问设置]菜单项，选择域用户页签，进入域用户页面。

(2) 单击 LDAP 配置栏的<添加角色组>按钮，完成操作。

(3) 在对话框中输入角色组的名称和域名信息，如图 11-67 所示。

图11-67 添加角色组



(4) 选择角色组权限。

(5) 单击<确定>按钮，完成操作。

11.4.5 验证 LDAP 配置

添加角色组成功后，使用角色组里的用户名和密码登录 HDM，如果登录成功，说明配置正确且已经生效。

1. LDAP 用户登录 HDM Web

(1) HDM 登录页面输入 group1 里的用户名和登录密码，以 user1 为例，如图 11-68 所示。

图11-68 登录 HDM

(2) 单击<登录>按钮，登录 HDM。

11.4.6 LDAP 关键字说明

表11-3 LDAP 关键字

关键字	英文全称	含义
dc	Domain Component	域名，域名example.com的正确写法是dc=example,dc=com
uid	User ID	用户ID，如LDAPuser1
ou	Organizational Unit	组织单位，是一个容器对象
cn	Common Name	公共名称，如 user1
sn	Surname	姓，如 Yang
dn	Distinguished Name	可分辨名称，每个条目都有一个唯一的可分辨名称
c	Country	国家，如 CN
o	Organization	组织名，如 Example. Inc