



深信服超融合 HCI

用户手册

产品版本 6.8.0

文档版本 06

发布日期 2023-02-21

深信服科技股份有限公司

版权声明

版权所有 © 深信服科技股份有限公司 2022。保留一切权利（包括但不限于修订、最终解释权）。

除非深信服科技股份有限公司（以下简称“深信服公司”）另行声明或授权，否则本文件及本文件的相关内容所包含或涉及的文字、图像、图片、照片、音频、视频、图表、色彩、版面设计等的所有知识产权（包括但不限于版权、商标权、专利权、商业秘密等）及相关权利，均归深信服公司或其关联公司所有。未经深信服公司书面许可，任何人不得擅自对本文件及其内容进行使用（包括但不限于复制、转载、摘编、修改、或以其他方式展示、传播等）。

特别提示

您购买的产品、服务或特性等应受深信服科技股份有限公司商业合同和条款的约束，本文件中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，深信服科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新，如有变更，恕不另行通知。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保，深信服科技股份有限公司不对本文档中的遗漏、变更及错误所导致的损失和损害承担任何责任。

联系我们

售前咨询热线：400-860-6868

售后服务热线：400-630-6430（中国大陆）

深信服科技官网：www.sangfor.com.cn

7*24小时智能客服：<https://bbs.sangfor.com.cn/>（点击右侧智能客服）



打开微信扫一扫
可在手机端咨询

文档说明

本文档针对深信服超融合 HCI (Hyper-Converged Infrastructure) 产品，介绍了 HCI 的架构、特性、安装、操作、运维管理和常见问题与排查方法。

适用对象

- 技术服务工程师
- 运维人员

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

日期	文档版本	更新记录
2023-02-21	06	1. 新建虚拟机，磁盘动态分配方式下，最大容量更新。 2. 虚拟机热迁移（含集群内迁移和跨集群迁移），批量迁移允许并发个数更新。
2023-01-11	05	新增支持“ 磁盘空间回收 ”功能的虚拟机操作系统列表。
2023-01-03	04	“ vGPU 管理 ”章节新增虚拟机安装完显卡驱动后的授权步骤，包括 Windows 虚拟机和 Linux 虚拟机。
2022-11-14	03	6.8.0 存储通信网络聚合模式，去掉了“其他”选项。
2022-10-20	02	1. “ USB 映射 ”章节新增 USB 管理内容。 2. “ RAID 故障管理 ”章节新增隔离主机内容。 3. “ 虚拟机集群内热迁移 ”章节新增虚拟机迁移记录 4. “ 虚拟机编辑 ”章节新增虚拟机变更操作日志记录功能
2022-09-13	01	本文档第一次发布

符号说明

在本文中可能出现下列标志，它们所代表的含义如下。

图形	文字	使用原则
 危险	危险	若用户忽略危险标志，可能会因误操作发生危害人身安全、环境安全等严重后果。

 警告	警告	该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。
 小心	小心	若用户忽略警告标志，可能会因误操作发生严重事故（如损坏设备）或人身伤害。
 注意	注意	提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。。
 说明	说明	对操作内容的描述进行必要的补充和说明。

在本文中会出现图形界面格式，它们所代表的含义如下。

文字描述	代替符号	举例
窗口名、菜单名等	方括号“[]”	弹出[新建用户]窗口。
		选择[系统设置/接口配置]。
按钮名、键名	尖括号“<>”	单击<确定>按钮。

目录

目录.....	III
1. 产品说明.....	1
1.1. 产品简介.....	1
1.2. 产品架构.....	1
1.3. 关键特性.....	3
1.3.1. 云平台关键特性.....	3
1.3.2. aSV 关键特性.....	6
1.3.3. aSAN 关键特性.....	9
1.3.4. aNET 关键特性.....	15
2. 安装部署.....	17
2.1. 安装组网介绍.....	17
2.1.1. 组网注意事项.....	17
2.1.2. HCI 标准集群组网介绍.....	18
2.1.3. HCI 延伸集群组网介绍.....	19
2.2. 安装前准备.....	21
2.2.1. 文档和工具准备.....	21
2.2.2. 超融合集群配置要求.....	21
2.2.3. 仲裁节点配置要求.....	23
2.2.4. 交换机配置要求.....	24
2.3. 安装流程介绍.....	25
2.4. HCI 虚拟化系统安装.....	25
2.4.1. aServer 一体机.....	25
2.4.2. 第三方服务器.....	26
2.4.2.1. 服务器配置.....	26
2.4.2.2. ISO 安装.....	34
2.4.2.3. U 盘安装.....	44
2.5. 仲裁节点接入.....	46
2.5.1. 配置要求.....	46
2.5.2. aServer 一体机.....	46
2.5.3. 第三方服务器.....	47
2.5.4. VMware 平台.....	52
2.6. 补丁升级.....	55
2.6.1. 补丁升级设置.....	55
2.6.2. 补丁信息获取.....	66
2.7. 终端检测响应平台 EDR 安装.....	67
2.7.1. 安装 EDR 服务器.....	68
2.7.1.1. VMA 格式安装.....	68
2.7.1.2. ISO 格式安装.....	69

2.7.2. EDR 服务器授权.....	71
2.7.3. 安装 EDR 客户端.....	72
2.7.4. EDR 客户端卸载.....	74
3. HCI 集群初始化.....	76
3.1. HCI 集群初始化条件.....	76
3.2. 组建集群.....	76
3.2.1. 配置集群 IP.....	76
3.2.2. 配置集群时间.....	77
3.2.3. 配置告警通知（可选）.....	78
3.2.4. 添加主机.....	82
3.2.5. 设置控制节点资源池.....	84
3.3. 管理通信口配置.....	85
3.4. 数据通信口配置.....	86
3.5. 虚拟存储配置.....	91
3.5.1. 配置存储通信网络.....	91
3.5.2. 创建卷.....	93
3.5.2.1. 创建普通卷.....	93
3.5.2.2. 创建延伸卷.....	96
3.6. 终端通信口配置（可选）.....	101
3.7. 授权激活.....	103
3.7.1. USB KEY 授权.....	103
3.7.2. vKEY 授权.....	104
3.8. 配置 LLDP（可选）.....	105
3.9. 物理出口配置.....	107
3.10. 三网合一方案（可选）.....	108
3.11. 四网合一方案（可选）.....	112
3.12. 一键检测集群状态.....	121
3.13. 使用 ADEPLOY 工具进行检测.....	121
3.14. 云安全中心安装部署.....	121
3.14.1. aSEC 云安全中心安装.....	123
3.14.2. 虚拟机安全防护管理平台安装.....	127
3.14.3. 虚拟机安全组件安装.....	130
4. 平台登录.....	132
5. 虚拟机配置指导.....	107
5.1. 新建虚拟机.....	107
5.1.1. 创建全新虚拟机.....	107
5.1.2. 虚拟机安装操作系统.....	115
5.1.2.1. Windows 系统安装.....	115
5.1.2.2. Linux 系统安装.....	120
5.1.3. 导入 ova/vma/ovf 虚拟机.....	123
5.1.4. P2V 迁移.....	127
5.1.5. 虚拟机克隆.....	129
5.1.5.1. 全量克隆.....	129

5.1.5.2. 快速全量克隆	131
5.1.5.3. 链接克隆	133
5.1.6. 虚拟机模版部署	135
5.2. 虚拟机管理	137
5.2.1. 安装性能优化工具	137
5.2.1.1. Windows 操作系统	137
5.2.1.2. Linux 操作系统	141
5.2.2. 卸载性能优化工具	143
5.2.2.1. Windows 操作系统	143
5.2.2.2. Linux 操作系统	145
5.2.3. USB 映射	147
5.2.4. 虚拟机磁盘容量扩容	150
5.2.4.1. Windows 操作系统	150
5.2.4.2. Linux 操作系统	153
5.2.5. 使用物理磁盘（裸磁盘映射）	156
5.2.6. 使用 VHD 磁盘	159
5.2.7. 虚拟机编辑	161
5.2.7.1. 硬件配置	161
5.2.7.2. 高级配置	163
5.2.8. 导出虚拟机	165
5.2.9. 虚拟机集群内热迁移（支持批量操作）	167
5.2.10. 虚拟机跨集群热迁移（支持批量操作）	170
5.2.11. 虚拟机快照	174
5.2.12. 一致性组快照	177
5.2.13. 快照策略	179
5.2.14. vGPU 管理	182
5.2.14.1. 部署英伟达授权服务器	183
5.2.14.2. 显卡管理	190
5.2.14.3. 虚拟机添加显卡	194
5.2.14.4. Windows 虚拟机安装显卡驱动	197
5.2.14.5. Linux 虚拟机安装显卡驱动	199
5.2.14.6. 虚拟机修改显卡	202
5.2.15. 导出虚拟机报表	203
5.2.16. 虚拟机 Qos 上限限制	204
5.2.16.1. CPU 频率限制	204
5.2.16.2. 磁盘 IO 频率限制	205
5.2.16.3. 网卡流量限制	207
5.2.17. 多国语言键盘支持	208
5.3. 查看虚拟机运行状态	209
5.4. 删除虚拟机	212
6. 虚拟网络配置指导	214
6.1. 创建物理出口	214
6.1.1. 物理出口相关概念	214
6.1.2. 多网段端口组的物理出口创建	214

6.1.3. 单网段端口组的物理出口创建	216
6.1.4. 物理出口典型拓扑	219
6.2. 创建虚拟网络设备	219
6.2.1. 虚拟路由器创建	219
6.2.2. 分布式虚拟机交换机创建	225
6.2.3. 虚拟交换机路由器典型拓扑	227
6.2.4. 其他 NFV 设备创建	227
6.3. 配置流量镜像	228
6.4. 配置分布式防火墙	230
6.5. 网络可视化	232
6.6. 管理 NFV 设备（支持批量操作）	239
7. 存储配置指导	242
7.1. 查看存储状态	242
7.2. 虚拟存储配置指导	245
7.2.1. 查看虚拟存储状态	245
7.2.2. 添加卷	246
7.2.2.1. 添加普通卷	246
7.2.2.2. 添加延伸卷	271
7.2.3. 延伸卷修改故障域	277
7.2.4. 删除卷（高危操作）	278
7.2.5. 配置数据平衡计划	279
7.2.6. 配置定时坏道扫描	280
7.2.7. 配置数据重建等待时间	282
7.2.8. 配置快照熔断	283
7.2.9. 更改虚拟存储网络配置（高危操作）	284
7.2.10. 更改网络连通性探测 IP 地址（两主机场景）	289
7.2.11. 配置跨卷访问 IP 池	291
7.2.12. 配置读性能优化	292
7.2.13. 新增及配置虚拟共享盘	294
7.2.14. 删除虚拟共享盘	296
7.2.15. 存储策略	297
7.2.16. 配置虚拟 iSCSI 磁盘	298
7.2.17. 硬盘维护模式（硬盘隔离）	301
7.2.17.1. 硬盘隔离	302
7.2.17.2. 硬盘替换	303
7.2.18. 亚健康磁盘坏道预测	307
7.2.19. 智能预测	308
7.2.19.1. 坏道预测	308
7.2.19.2. 容量预测	309
7.2.19.3. SSD 寿命预测	310
7.2.20. 卡慢盘处理	311
7.2.20.1. HDD 卡慢盘处理	312
7.2.20.2. SSD 卡慢盘处理	314
7.2.21. 只读盘处理	317

7.3. 其他存储配置指导	318
7.3.1. 添加 FC 存储	318
7.3.2. 添加 iSCSI 存储	320
7.3.3. 添加 NFS	322
7.3.4. 添加本地存储	323
7.3.5. 删除存储（高危操作）	325
8. 可靠服务配置指导	327
8.1. HA 配置	327
8.2. 集群资源调度配置	328
8.3. 动态热添加配置	330
8.4. 虚拟机调度配置	333
8.4.1. 聚集虚拟机	333
8.4.2. 互斥虚拟机	334
8.4.3. 虚拟机组互斥	335
8.4.4. 虚拟机组到主机组	336
8.5. 资源预留配置	337
8.6. 主机亚健康监控	338
8.7. 内存 ECC 隔离	341
8.7.1. 内存 CE 错误隔离	341
8.7.2. 内存 UE 错误隔离	342
8.8. UPS 电源	343
8.9. RAID 卡故障处理	346
8.10. 虚拟机容灾与备份	347
8.10.1. 快速备份与恢复	348
8.10.1.1. 手动备份	348
8.10.1.2. 备份策略备份	350
8.10.1.3. 备份恢复	354
8.10.2. CDP 备份与恢复	356
8.10.2.1. 备份策略备份	356
8.10.2.2. CDP 恢复系统	360
8.10.3. 文件恢复	362
8.10.4. 备份管理	364
8.10.4.1. HCI 备份策略	365
8.10.4.2. HCI 备份复制策略	365
8.10.4.3. VMware 备份策略	366
8.10.4.4. HCI 备份文件	366
8.10.4.5. VMware 备份文件	368
8.10.4.6. 备份池	369
8.10.4.7. 设置	370
8.11. GPU 虚拟机调度	371
9. 云安全中心配置指导	373
9.1. 查看平台安全状态	373
9.2. 虚拟机安全	374
9.2.1. 资产管理	375

9.2.2. 病毒/漏洞扫描.....	377
9.2.3. 紧急隔离	380
9.2.4. 勒索应急恢复.....	381
9.2.5. 安全事件处置.....	386
9.2.6. 查看安全事件/漏洞信息	389
9.3. 漏洞管理.....	393
9.4. 安全设置.....	395
9.4.1. 数据保护策略设置	395
9.4.2. 告警设置	397
9.4.3. 安全能力管理.....	398
9.4.4. 云安全中心升级	400
9.4.5. 远程维护	401
10. 超融合平台配置指导.....	402
10.1. 查看主机/集群运行状态	402
10.2. 端口管理.....	403
10.3. 证书配置.....	404
10.4. 查看告警日志	405
10.5. 告警设置.....	406
10.6. SYSLOG 配置.....	409
10.7. 管理员与权限管理配置	409
10.7.1. 权限	409
10.7.2. 新增用户	412
10.7.3. 三员分立	415
10.7.4. 密码策略	417
10.7.5. 限制登录	418
10.7.6. UKey 双因子登录配置	420
10.7.7. Google OTP 双因子登录配置	422
10.8. 修改集群 IP 地址	424
10.9. 管理口不带 IP 切换	426
10.10. 修改仲裁节点 IP 地址	428
10.11. 数据通信口(VXLAN)配置修改	430
10.12. 一键检测的使用	433
10.13. 系统诊断.....	434
10.14. 修改平台日期时间	435
10.15. 备份和恢复系统配置	437
10.16. 恢复出厂设置（高危操作）	439
10.17. CPU 超配限制配置	441
10.18. 内存超配配置.....	442
10.19. 虚拟机逃逸检测	443
10.20. 合作伙伴服务.....	444
10.20.1. SIP 安全联动	444
10.20.2. PAAS 联动	448
10.21. VMWARE 异构管理	449
10.21.1. 添加 vCenter.....	449

10.21.2. 管理 VMware 虚拟机	450
10.21.2.1. 新建 VMware 虚拟机	450
10.21.2.2. 删除 VMware 虚拟机	452
10.21.2.3. 虚拟机开关机操作（开机、关机、重启、挂起）	453
10.21.3. VMware 虚拟机的备份	454
10.21.4. VMware 虚拟机的恢复	456
10.21.5. 迁移 VMware 虚拟机到 HCI 平台	458
10.22. 仲裁节点故障处理（高危操作）	460
10.23. 版本升级	461
10.24. 单主机维护模式	462
10.25. 虚拟机磁盘加密	464
10.26. 回收站	466
10.27. 剩余信息保护	467
10.28. 报表位置管理	468
10.29. 企业定制	468
10.30. 中/英文语言切换	470
11. 平台运维	472
11.1. 运维工具/模块	472
11.1.1. 日常运维模块	472
11.1.1.1. 告警监控	472
11.1.1.2. 一键检测	474
11.1.1.3. 智能交付工具	476
11.1.1.4. 云端智能大脑	477
11.1.1.5. Sangfor CLI	478
11.1.2. 问题排障模块	478
11.1.2.1. 系统诊断	478
11.1.2.2. 控制台抓包	479
11.1.2.3. 连通性探测（网络故障排查）	481
11.1.2.4. 端口管理	483
11.2. 平台日/周/月运维	484
11.2.1. 日维护	484
11.2.2. 周维护	487
11.2.3. 月维护	488
11.2.3.1. 月度巡检	488
11.2.3.2. 预警补丁	488
11.2.3.3. 可用性管理	489
11.2.3.4. 安全管理	490
11.3. 基础业务变更	491
11.3.1. 系统上下电	491
11.3.1.1. 单台主机上下电	491
11.3.1.2. 超融合集群上下电	494
11.3.2. 平台版本及补丁包升级	499
11.3.3. HCI 平台网络设置与变更	499
11.3.4. 虚拟网络设置与运维	500

11.3.5. 虚拟存储设置与运维	500
11.3.6. 扩容变更	500
11.3.6.1. 主机扩容	500
11.3.6.2. 硬盘扩容	507
11.4. 平台硬件维护	510
11.4.1. 硬件巡检	510
11.4.2. 硬件告警查看	510
11.4.2.1. 面板指示灯判断【9C、9S、9T、9D 均指服务器 SN 码编号的开头】	511
11.4.2.2. IPMI 信息判断	513
11.4.3. 服务器拆机规范	514
11.4.4. 硬件故障处理	516
11.4.4.1. 主机替换	516
11.4.4.2. 系统盘替换	520
11.4.4.3. 磁盘替换	527
11.4.4.4. 内存替换	530
11.4.4.5. 网卡替换	537
11.4.4.6. RAID 卡替换	538
11.4.4.7. 电源替换	542
11.5. 平台高危操作	543
11.5.1. 界面配置高危操作	543
11.5.1.1. 更改存储通信网口	543
11.5.1.2. 格式化集群	544
11.5.1.3. 集群备份恢复	544
11.5.1.4. 清空回收站	545
11.5.2. 硬件高危操作	545
11.5.2.1. 未加入超融合集群的服务器重装系统	545
11.5.2.2. 已加入超融合集群的服务器重装系统	545
11.5.2.3. 变更物理网络	546
11.5.2.4. 随意拔插服务器磁盘	546
11.5.2.5. 格式化服务器磁盘	546
11.5.2.6. iSCSI 存储重新扫描或重新发现目标	547
11.6. 通信矩阵	547
12. 术语表	549
13. 缩略语	552

1. 产品说明

HCI（Hyper-Converged Infrastructure，深信服超融合基础设施）是一款基于创新的超融合技术构建的产品，具备完整的IT基础设施服务能力和运维管理服务能力，并能承载核心数据库、ERP、财务系统、生产系统等企业关键业务应用。

不同于传统的云，深信服超融合构建的超融合更加轻便灵活，帮助用户快速构建业务驱动的云计算数据中心，将用户的IT资源池化、IT使用服务化、IT运维自动化，让关键业务轻松上云，是政府及广大企事业单位业务上云的优选方案。

本章主要从产品简介、产品架构和关键特性等不同方面对深信服HCI产品进行详细介绍和说明。

1.1. 产品简介

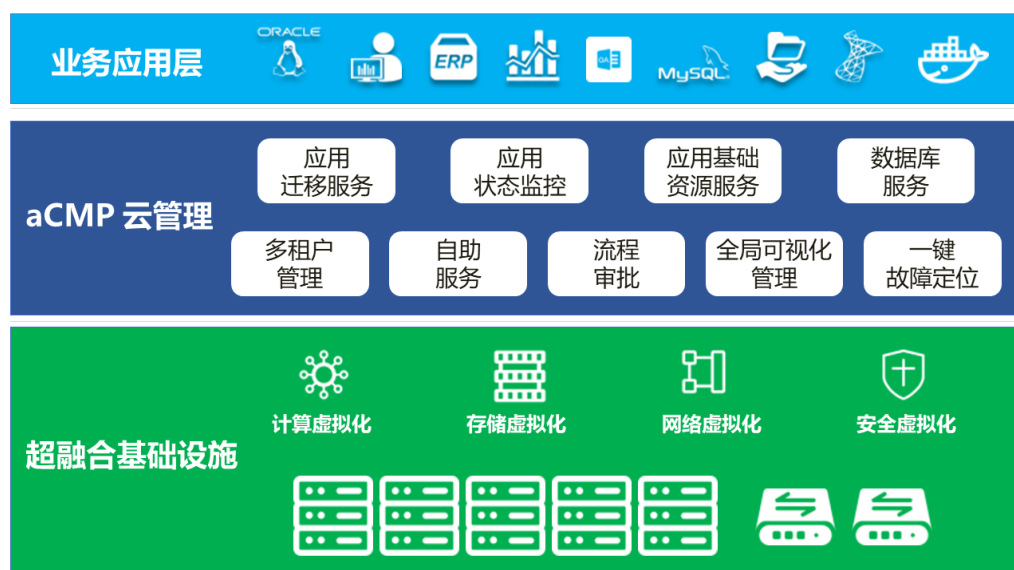
HCI将计算、网络 and 存储等资源作为基本组成元素，形成根据系统需求进行选择 and 预定义的一种技术架构。具体实现方式上一般是在同一套单元节点（x86 服务器）中融入软件虚拟化技术（包括计算、网络、存储、安全等虚拟化），而每一套单元节点可以通过网络聚合起来，实现模块化的无缝横向扩展（scale-out），构建统一的资源池。深信服基于超融合构建的超融合架构能够替代繁重复杂的传统云基础架构，实现云架构的极简。

HCI依托超融合技术将数据中心简化为2种设备：x86服务器和交换机，降低了初始投资成本和学习使用设备的成本。通过接入SCP云计算平台实现平滑扩容，以支撑业务高性能的需求。HCI提供了P2V迁移功能，可以实现一键迁移应用上云，提升IT的创新效率。HCI通过CDP技术、数据多副本技术、虚拟机备份技术、应用数据备份、网络行为管理等多项技术保障数据可靠。针对关键应用具备独特优化技术，支撑Oracle RAC集群、SQL Server集群、金蝶、用友和ERP类软件关键业务稳定运行，可以满足超高可靠业务需求。内置防火墙、WAF、云杀毒等运行在云平台上的业务应用，使其具备完善的安全防护体系，符合安全等保合规要求，能够有效防止数据中心内部的东西向安全威胁。HCI具备全局的资源管理能力，部署配置“所画即所得”，降低应用部署时间，减少故障定位和修复时间，无需专门培训即可掌握平台使用方法。

1.2. 产品架构

深信服超融合HCI架构由两部分组成：超融合基础设施、云计算管理平台。在超融合

架构之上，用户可以基于自身需求构建业务系统。



深信服超融合 HCI 基于超融合架构，以虚拟化技术为核心，利用计算虚拟化 aSV、存储虚拟化 aSAN、网络虚拟化 aNET、安全虚拟化 aSEC 等组件，将计算、存储、网络等虚拟资源融合到一台标准 X86 服务器中，形成基准架构单元。并且多套单元设备可以通过网络聚合起来，实现模块化的无缝横向扩展（Scale-Out），形成统一的资源池。

深信服云计算管理平台 SCP，提供对深信服超融合、第三方资源池的管理和资源调配能力；通过自动化运维工具，降低平台运维的难度，减少运营工作量；借助 IT 自助服务和流程管理，提升用户 IT 服务的敏捷性和快速响应的能力，从而提高 IT 的管理水平和服务效率；结合云计算管理平台的计量功能，对每个租户使用的 IT 服务和 IT 资源进行细粒度的计量与统计，从而更好的帮助企业和组织核算部门的成本与效益。

HCI 有四大主要组件为：aSV（服务器虚拟化）、aNET（网络虚拟化）和 aSAN（存储虚拟化）和 aSEC（安全虚拟化和 NFV），aSV 为整个 HCI 的内核，是必选项，aNET、aSAN 和 aSEC 可以根据具体的需求三选一或者全选。

aSV 是深信服超融合架构解决方案中的计算虚拟化组件，也是整个超融合架构中的核心组件，计算资源虚拟化技术将通用的 x86 服务器经过 aSV 组件，对最终用户呈现标准的虚拟机。这些虚拟机就像同一个厂家生产的系列化的产品一样，具备系列化的硬件配置，使用相同的驱动程序。

aSAN 是一款自主开发的分布式存储系统，利用虚拟化技术“池化”集群存储卷内通用 X86 服务器中的本地硬盘，实现服务器存储资源的统一整合、管理及调度，最终向上层提供 NFS/iSCSI 存储接口，供虚拟机根据自身的存储需求自由分配使用资源池中的存储空间。

aNET 是深信服超融合架构解决方案中的网络虚拟化组件，通过 Overlay 的方式来构

建大二层和实现业务系统之间的租户隔离，通过 NFV 实现网络中所需各类网络功能资源（包括基础的路由交换、安全以及应用交付等）按需分配和灵活调度，从而实现超融合架构中的网络虚拟化。

aSEC为深信服的安全虚拟化和NFV(包含：vAC、vAD、vAF、vSSL VPN、vWOC、vDAS)。其将深信服现有的网络设备（SSL、WOC、AD、AF、AC、DAS）进行虚拟化，并通过模板形式单独提供。

超融合底层配置信息

1. 使用到的开发语言：C，C++，Perl，Python，Golang。
2. 数据库/中间件：Sqlite，Redis，Zookeeper，MySQL，Kafka。
3. 基础操作系统：SangforOS，内核：Linux-4.18.0。

1.3. 关键特性

1.3.1. 云平台关键特性

1. 云计算平台

深信服SCP云计算平台能够提供丰富的管理功能，包括纳管HCI集群、VMware平台，支持软硬件多种授权方式，授权方式灵活，统一对多个HCI集群授权，支持多租户管理和自主服务管理；在安全方面，支持租户配置自己的分布式防火墙策略；容灾方面，SCP集成了“可靠中心”，能够为用户提供完整的虚拟机级别异地灾备方案。

2. 应用迁移服务

HCI迁移工具可以将现有物理主机或VMWare或Citrix平台上的Windows/Linux操作系统通过网络复制到HCI平台上。

3. 异构虚拟化管理

HCI可添加VMware vCenter并对其进行纳管，实现双平台的集中管理。VMware vCenter和HCI之间的虚拟机可以实现支持双向迁移。

4. 数据库向导部署

深信服超融合平台上的Oracle RAC支持向导式部署，也支持向导式部署 SQL Server AlwaysOn集群数据库。



5. 一键检测

一键检测能够识别系统硬件、配置、系统运行情况，快速定位问题位置（硬件、平台、业务），进行分层检查，提供故障详细解决方案。



6. 集群资源调度

集群资源调度是指在特定的场景下会调度集群资源，将虚拟机从CPU或者内存利用率比较高的主机迁移到利用率比较低的主机上，将负载过高的主机的利用率降到阈值以下。

7. 监控中心

监控中心能够全方位监控业务并提前预警，减少业务中断次数与时间，并支持大屏展示让整个数据中心可视，更好支撑关键业务上云。支持监控虚拟机、Oracle、SQL Server、Weblogic和业务系统。

8. 虚拟机数据保护

- 虚拟机快照类似于系统还原点，一个虚拟机可以存在多个快照。
- 虚拟机备份方式支持虚拟机全量备份和增量备份。用户首次虚拟机备份为虚拟机全量备份，备份保留周期内其他备份为增量备份。
- CDP 即持续数据保护，它能够记录虚拟机中业务系统对磁盘的每一个 IO，可以将虚拟机恢复到任意时刻的状态，也可以直接查看并下载某个时刻的文件，对于文件误删、病毒、系统崩溃、数据损坏等故障有十分明显的价值，做到 RPO 接近于 0。

9. 开机扩容

支持虚拟机开机状态扩容已存在的磁盘，避免因虚拟机扩容磁盘带来的停机。

10. 批量克隆迁移

- 支持虚拟机批量克隆。
- 支持集群内批量迁移。
- 支持跨集群批量迁移。

11. 单主机维护

支持单台主机设置维护模式，进入维护模式的主机，任务将不会调度到该主机上执行，减少物理主机维护时对业务的影响。

12. 短信告警

- 支持短信网关方式告警，包括联通、移动、电信。
- 支持联通一信通 http 方式短信告警。

13. 涉密级用户安全策略

- 支持 syslog 日志上报。
- 支持 UKey 双因子登录。
- 支持 IP+MAC、终端绑定策略。

14. 系统盘替换

- 支持对已有的系统盘进行健康检查和寿命预测。
- 支持对系统盘的系统配置和用户配置自动备份。
- 支持安全地替换主机的系统盘。

15. 云安全中心

- 上线即安全：主机终端防护的自动安装、识别资产、防护策略的自动开启，专业的安全处置固化，人人都是安全专家。

- 平台数据的绝对保护：全部虚拟机通过定时快照进行天级别的保护；当检测到安全软件被卸载、疑似存在勒索风险时，立即触发快照进行数据保护，同时持久化定时快照避免用病毒数据进行覆盖。
- 勒索应急向导式恢复：对勒索虚拟机进行向导式的专项恢复，通过对虚拟机进行隔离、快照、验证、恢复、扫描、处置等动作，完成勒索应急处理，无需专家介入即可快速安全的恢复业务，采用连接克隆进行业务验证，整个过程中环境完全独立，避免病毒扩散。
- 安全事件一键处置：云安全中心提供安全事件从网络隔离、快照兜底，病毒处置的全栈的向导化处置，处置过程保证异常发生最小的 RPO 和 RTO。
- 病毒查杀：云安全中心平台通过深信服人工智能检测引擎、基因特征检测引擎、行为分析检测引擎、云查杀检测引擎四大检测机制，支持对虚拟机下发病毒扫描任务，发现病毒并进行安全处置。
- 购买灵活弹性：仅需一个超融合，无需复杂的解决方案；授权灵活；处置固化，省去服务费用，加快闭环时间，减少业务中断时间。
- 漏洞管理：从云端及时更新漏洞情报，并主动扫描所有资产，展示受影响的资产，节省人工确认的时间和精力；漏洞修复快照兜底，解决客户后顾之忧。

16. Sangfor CLI

- 匹配用户习惯，支持 CLI 命令行用于自动化运维。

17. 滚动热升级

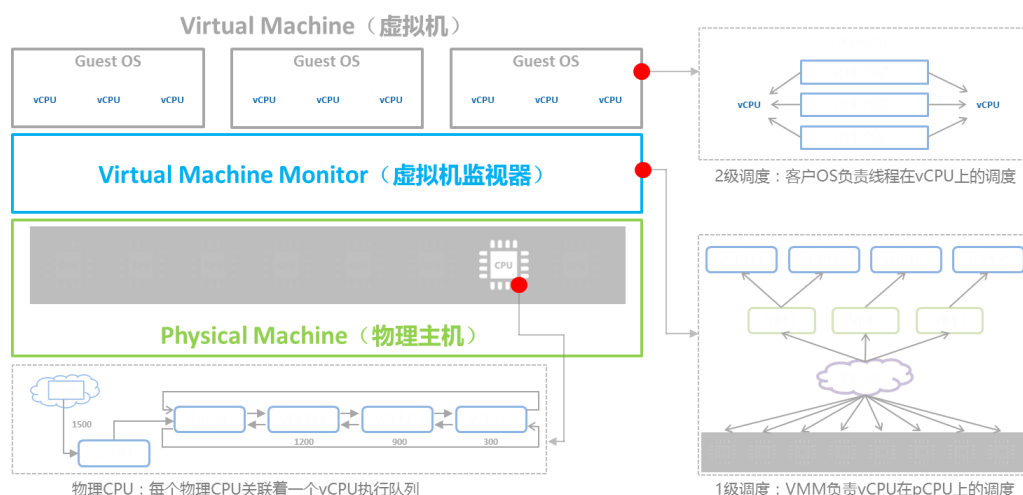
深信服超融合提供滚动热升级方案，将待升级主机上的虚拟机热迁移至其他主机，然后原地热升级该主机，以滚动的方式实现业务零中断的热升级能力，提高业务的连续性。

1.3.2. aSV 关键特性

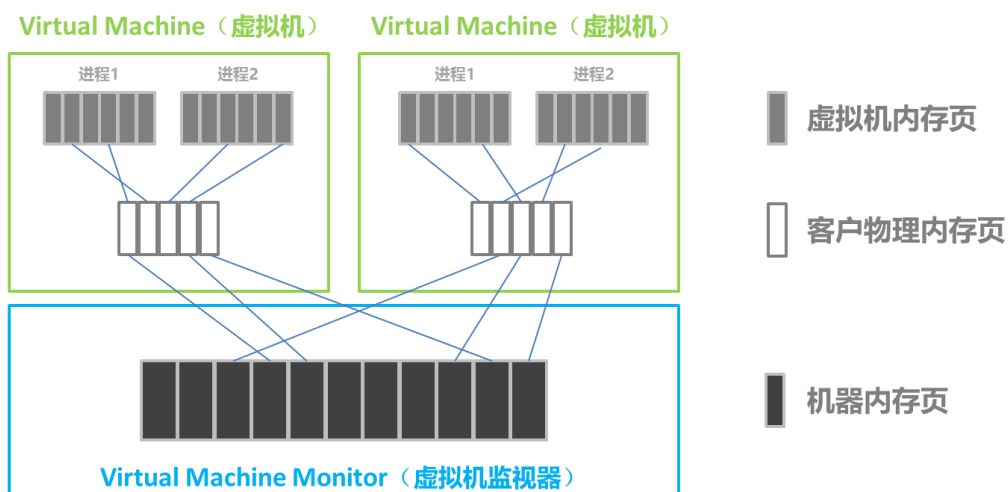
1. aSV的Hypervisor实现

aSV平台通过VMM(Virtual Machine Monitor, 虚拟机监视器)对CPU、内存以及IO设备进行虚拟化。

aSV基于硬件辅助虚拟化技术利用VMM实现X86架构的虚拟化，将单个物理CPU划分成多个vCPU。虚拟机只看到VMM呈现的vCPU，不直接感知物理CPU。用户操作系统负责第2级调度，即线程或进程在vCPU上的调度。虚拟机监视器负责第1级调度，即vCPU在物理处理单元上的调度。



aSV基于页表虚拟化技术完成内存虚拟化。VMM负责页式内存管理，维护虚拟地址到机器地址的映射关系，将物理内存虚拟化为虚拟机可以使用虚拟内存。



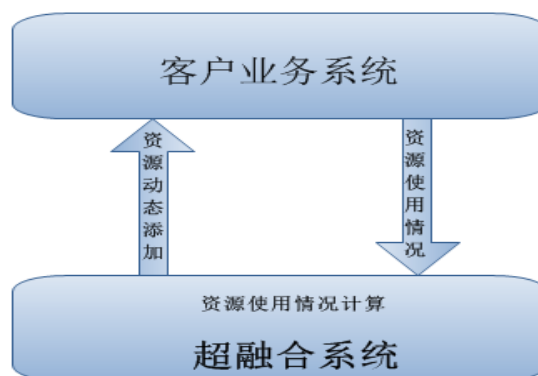
aSV利用VMM截获 Guest OS 对 I/O 设备的访问请求，然后通过软件模拟真实的硬件，实现I/O 虚拟化。

2. 虚拟机资源热添加

aSV支持对虚拟机的CPU，内存执行热添加，对虚拟机的网口和磁盘执行热插拔操作。

3. 动态热添加

动态热添加功能提供的自动化策略，快速响应业务状态增长变化对虚拟机CPU、内存资源进行动态扩展，既保证了业务的连续性，又解决用户业务增长带来的敏捷运维问题。



4. 虚拟机高可用HA

虚拟机高可用HA分为主机故障HA和虚拟机故障HA。

- 主机故障 HA 指当虚拟机所在节点发生意外（主机掉电、网口掉线等）时，将选择一台资源充足的节点重启该虚拟机，极大的降低了业务中断时间。
- 虚拟机故障 HA 指当虚拟机发生了蓝屏、黑屏等故障，将虚拟机关机并在原物理主机重启。

5. 虚拟机快速拉起

快速拉起功能可在需要恢复虚拟机时，立即创建虚拟机并启动，整个过程在3分钟内完成，15分钟内性能爬升到正常使用的状态，快速帮助用户恢复业务运行，极好地保障了业务连续性，RTO≤15分钟。

6. 智能NUMA调度

通过对核心业务的数据库进行建模，利用AI算法，生成核心数据库在通用场景下的NUMA绑定规则库，提高业务性能。

7. 内存隔离、内存超配和CPU超配限制

通过对各个模块的内存区进行隔离，保障系统不因内存被抢占导致系统假死、宕机，提升平台可靠性。同时支持虚拟机CPU和内存超配，实际使用量可超过物理限制，优先保障重要虚拟机的内存使用，提高CPU和内存使用率。

8. 亚健康主机监控

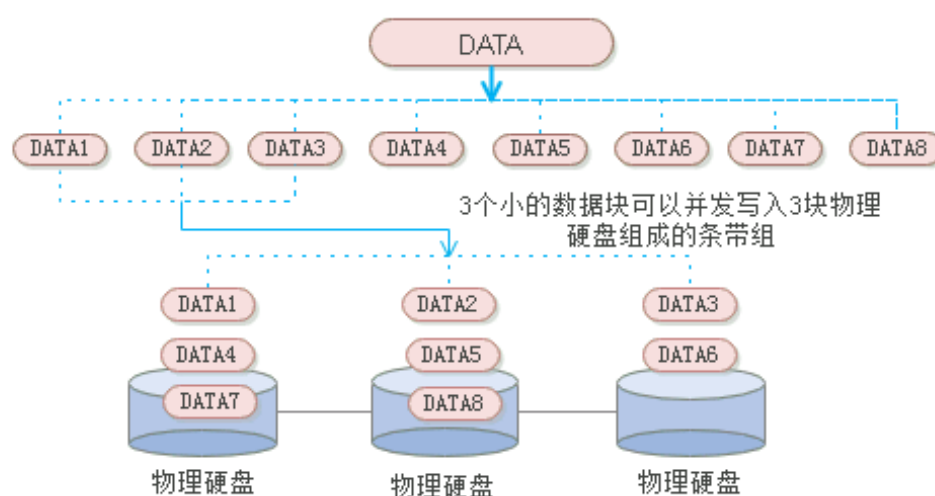
监控集群中主机的系统盘和内存是否处于亚健康状态，对于亚健康主机给予处理意见并降低亚健康主机在虚拟机开机（或者HA）选择主机过程中的优先级。目前支持对主机上内存CE和UE错误、系统盘只读、SSD寿命不足、HDD存在坏道这五种亚健康状态进行处理。

1.3.3. aSAN 关键特性

1. 数据条带化

aSAN利用条带化技术获得最大程度上的I/O 并发能力。条带化技术是将一块连续的数据切分成很多个小的数据块，然后并发地存储到不同物理硬盘上，实现对数据进行写入或读取时可以获得最大程度上的I/O 并发能力，从而获得优异的性能。

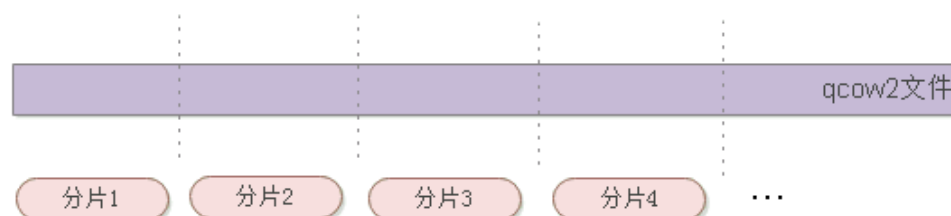
如下图所示，经过条带化处理的数据可以并发地写入到三块磁盘，而未经条带化处理的数据每次只能写入到一块磁盘中，因此数据经过条带化后的写入性能则是未经条带化的写入性能的3倍。



图示：三个物理硬盘组成的条带组 (RAID0组)

2. 分片

aSAN通过数据分片技术对单个qcow2文件按照固定单位大小进行切分成若干个颗粒度更小的分片。让数据在存储卷中分布更加地均衡，数据管理更加灵活。



3. 多副本机制：支持2副本、3副本

同时支持2副本及3副本策略，针对承载重要业务系统的虚拟机，用户可以选择配置3副本策略，进一步提高数据的可靠性。支持2副本虚拟机与3副本虚拟机相互转换，实现高可靠与高性能之间的最佳平衡。

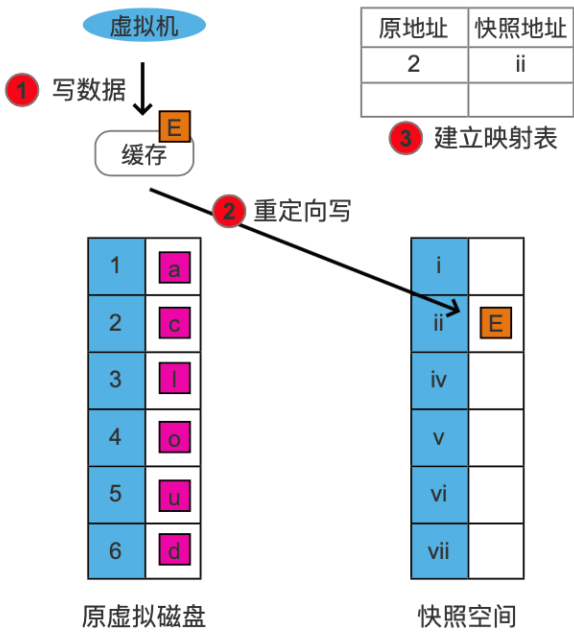
平台内置常用存储策略，用户根据业务系统的特点，新建虚拟机时可选择相应的存储策略；同时用户可依据业务系统特性，以虚拟机为粒度配置更精细的存储策略，配置更为灵活。包含以下四个属性：

- 副本数：可靠指标，依照业务重要程度，可选择两副本或三副本。
- 智能分层 QoS：性能指标，可选择高性能、默认性能、低性能。
- 条带数：性能指标，根据硬盘当前存储状态，系统自动设置条带数或自定义。
- 聚合副本：性能指标，为了保证 IO 本地化，提高读性能，聚合副本默认开启。

4. 存储快照

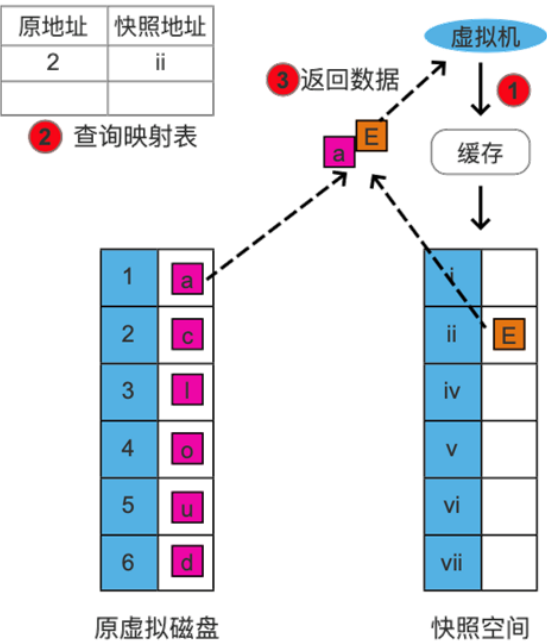
支持存储快照功能，在对虚拟机创建快照时，系统会将源虚拟磁盘设置为只读，并生成对应数量的新磁盘文件（即快照空间）。

快照创建完成后，该虚拟机的所有新增数据和对源数据的修改都将写入到新生成的快照空间，并将源虚拟磁盘和快照空间逻辑地址的对应关系写入映射表。



快照创建后，虚拟机对数据的读取存在两种情况：

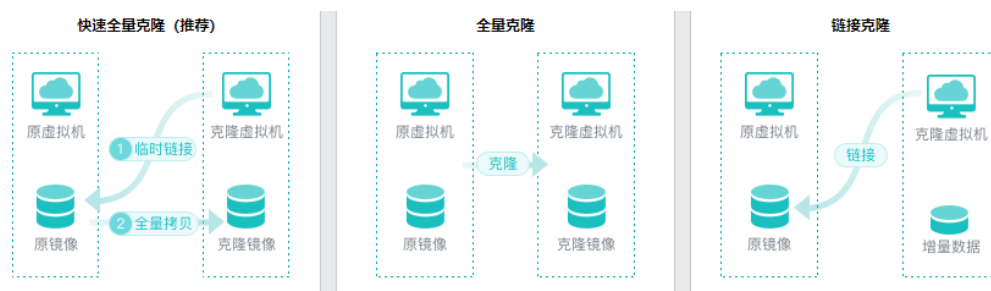
- 若读取的数据是快照创建之前已有的数据，且创建快照后未进行修改，则从源虚拟磁盘中读取。
- 若读取的数据是快照创建之后新增/修改的数据，则从快照空间读取。



- 该快照方式具有以下优点：
- 采用写时重定向（ROW）方式实现快照，快照后虚拟机性能不受影响。
 - 删除快照后可释放存储空间（发起快照残留文件清理任务）。
- 支持一致性组快照, 保证Oracle RAC及分布式业务的一致性：
- 支持将 Oracle RAC 中的虚拟机或承载同一业务系统的多个虚拟机添加为一致性组，对一致性组创建快照，保证组内所有虚拟机在同一时刻创建快照。
 - 当一致性组内的虚拟机出现故障时，组内的虚拟机利用一致性组快照可回滚到一致的状态。
- 支持定时快照, 简化运维，数据更可靠：
- 支持对单个虚拟机和一致性组自定义定时快照策略。
 - 快照频率可以选择按小时、天、周，同时为避免频繁快照占用大量存储资源，可设置快照自动清理策略，系统会自动合并快照点，有效利用存储空间。
 - 在开发测试场景下，定时快照能很大程度上简化运维工作、提高数据可靠性。
- ### 5. 虚拟机克隆
- 在全量克隆虚拟机的基础上，同时支持链接克隆与快速全量克隆虚拟机。
- 链接克隆生成的虚拟机始终依赖源镜像启动和运行，数据发生增改时才会记录并重定向到新的镜像上。具有虚拟机启动快、数据非独立，节省存储空间、克隆完成后，性能仍会有影响等特点。
- 快速全量克隆生成的虚拟机前期依赖源镜像，可秒级启动，虚拟机启动后仍持续克隆数据，最终数据会完整无依赖。具有虚拟机启动快、数据最终独立、克隆完成后

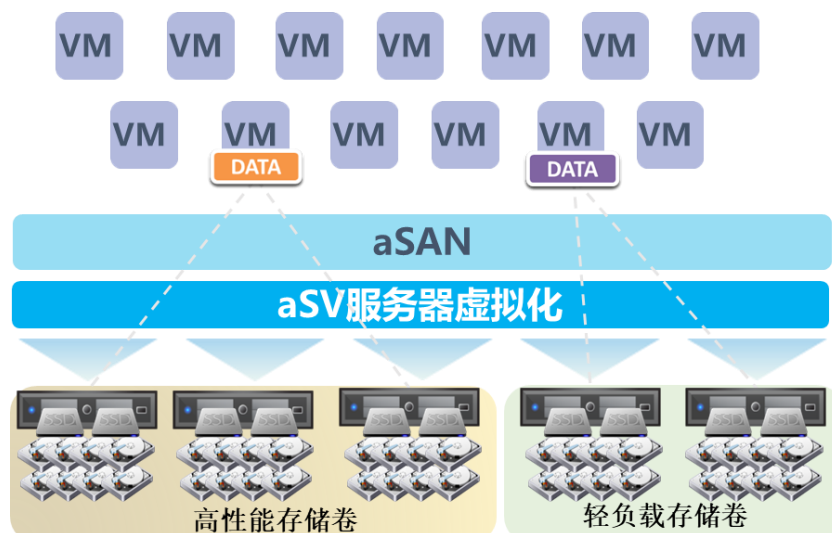
性能完全无影响等特点。

可灵活选择虚拟机克隆方式，默认推荐快速全量克隆方式。



6. 主机多卷

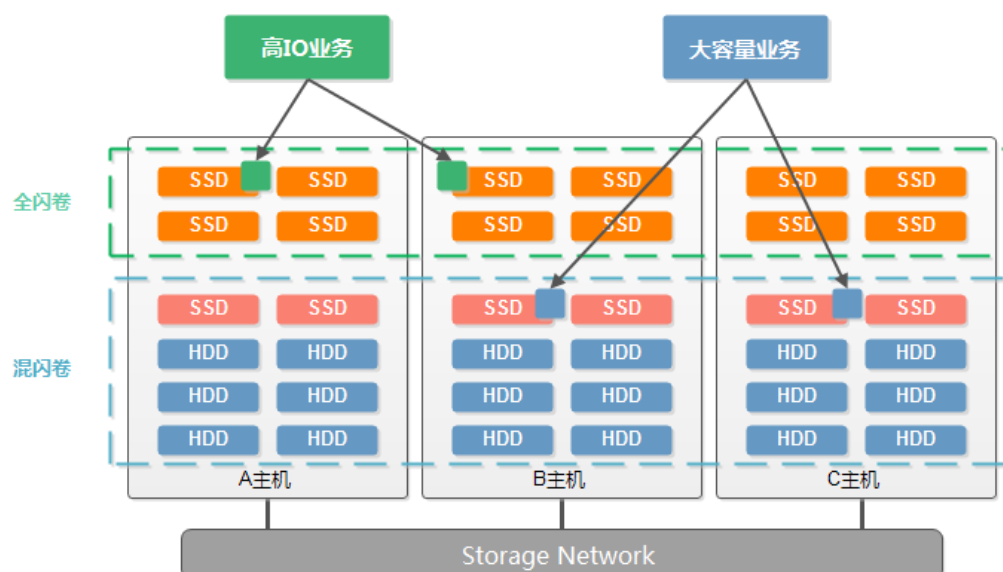
深信服超融合HCI在一个集群中，支持通过选择不同主机组建多个存储子卷，既满足了用户对不同业务的容量和性能隔离的需求，并且可以使得业务在不同的存储子卷进行切换，进而实现同一个业务在不同阶段的不同性能需求。



7. 磁盘多卷

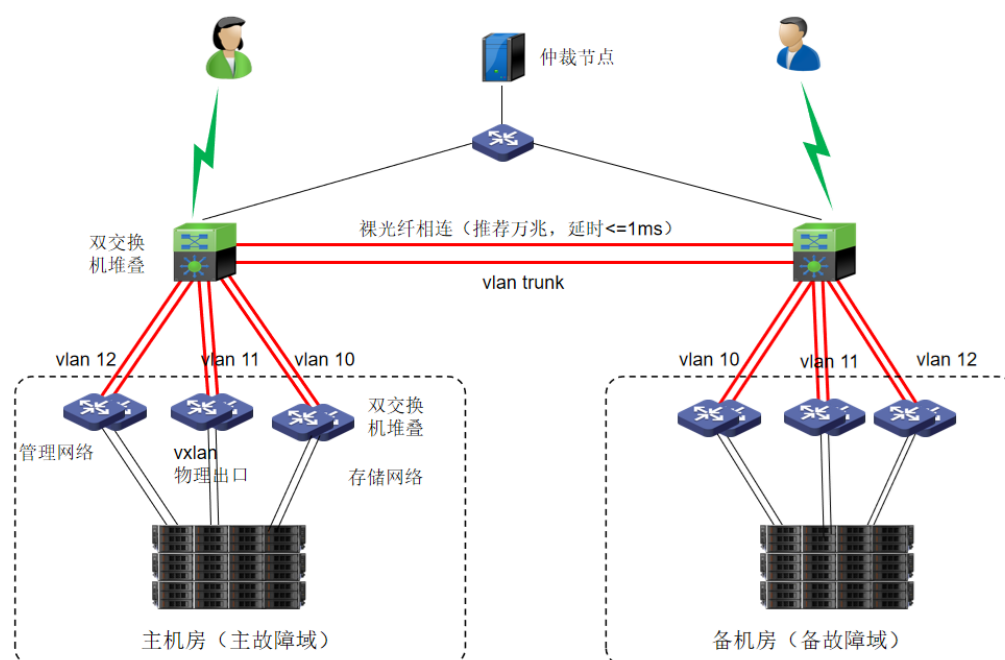
按主机划分多个卷至少6主机起步才能支持，对于承载业务节点较小的小集群，无法按主机划分为多个卷，可以采用按硬盘划分多个卷。

如下图所示，从3主机起步，aSAN支持按硬盘的粒度，划分为2个卷，相较按主机划分存储卷，降低了多卷的部署门槛。当客户存在高性能和大容量两种不同类型业务，可以按硬盘划分为2个卷：1个闪存卷 + 1个混合卷，闪存卷用来跑高性能业务，混合卷用来跑大容量业务。



8. 延伸卷

通过延伸集群的方案实现双活数据中心，该方案必须部署仲裁节点，解决脑裂问题，保证数据可靠性，HCI主机组建一个集群，平均部署到2个机房，每个机房配置成一个故障域，每个故障域保存一个副本，数据会被同时写入2个副本，任意一个机房故障，数据不丢失。



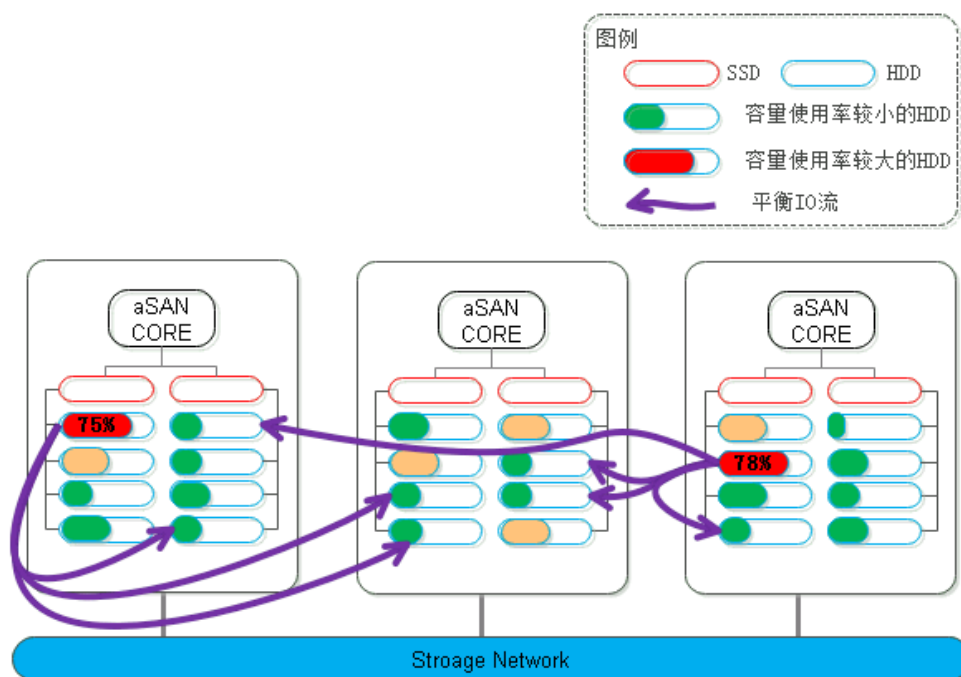
9. 仲裁机制

数据脑裂通常是由于网络发生故障，数据的多个副本出现隔离，无法及时相互同步信息，并且副本各自孤立地写入不同的数据，导致副本之间数据不一致，各自副本存在对方不存在的数据。aSAN引入仲裁副本来避免数据脑裂发生。仲裁副本是一种

特殊的副本，它只有少量的校验数据，占用的实际存储空间很小。

10. 数据平衡

随着分布式存储运行过程中，主机间的各磁盘也可能使用的不均匀。当发现卷内最高和最低的磁盘容量使用率之差超过一定阈值时，aSAN会以分片为单位计算出源端磁盘上的各个分片其即将落入的目的端磁盘的位置。目的端磁盘的个数可以是多个，位置可以是本主机内的其他磁盘或者其他主机内的磁盘。



11. 数据重建

aSAN通过数据重建功能，在组件（磁盘或主机）发生故障后，将以故障组件上数据的另一副本作为修复源，以分片为单位在目的组件上重建出新的副本，恢复副本的完整性，实现系统自愈。

12. 虚拟iSCSI技术

aSAN具备虚拟iSCSI技术，可以创建虚拟iSCSI硬盘，并且支持从虚拟存储通信网口接入。

13. 异构存储管理

- HCI 支持添加 FC 存储、iSCSI 存储作为外置存储，让虚拟机的存储位置放到 FC 存储或者 iSCSI 存储上，并实现虚拟机 HA 功能。
- HCI 支持添加 NFS 作为虚拟机的备份位置。
- HCI 支持添加服务器系统盘之外的本地磁盘或服务器上磁盘组建 RAID 之后的逻辑磁盘作为虚拟机的存储位置，但不支持虚拟机 HA 功能。

14. 磁盘亚健康扫描与修复

- aSAN 通过坏道主动扫描功能，及时发现潜藏的坏道，避免数据长期处于“单副本”状态。
- aSAN 发现坏道后，会立即触发坏道数据修复，从另一副本读取数据修复至坏道盘的保留扇区，及时恢复数据副本的冗余。
- aSAN 主动预先将坏道过多（或 SSD 寿命即将用尽）的硬盘上所有数据迁移至其他健康的硬盘上，始终保持副本的冗余度。
- 硬盘出现卡顿、变慢、拥塞等异常情况时，会影响性能，此时通过亚健康盘隔离和读写源切换保证性能的连续性。

15. 坏道预测

深信服通过收集分析大量客户真实使用场景中坏道硬盘的SMART数据、性能参数与硬盘日志信息，结合先进的算法训练模型，自主研发出高精度的坏道预测功能，通过大量差异业务场景测试，aSAN坏道预测准确率高达95%以上。

16. 容量预测

aSAN可以根据客户集群的容量使用情况动态预测出未来90天内的容量增长趋势。在容量预测界面，用户可以切换查看不同的存储卷裸容量、实际使用容量与动态预测曲线，并在界面提示用户预计xx天后，使用容量将达到容量告警阈值（90%）。

17. SSD寿命预测

aSAN收集分析集群中SSD硬盘IO数据，计算出SSD硬盘的剩余寿命，并结合上层业务压力显示预计SSD剩余可用时长，按照预测结果划分“健康”、“风险”、“高风险”三个寿命等级，提示用户及时更换集群中寿命告急的SSD硬盘。

1.3.4. aNET 关键特性

1. 网络虚拟化

- 虚拟分布式交换机可以保证虚拟机在主机之间迁移时网络配置的一致性，同时提供丰富的网络配置管理功能，端口动态绑定，静态绑定。
- 分布式防火墙提供 IP 接入控制、虚拟机网络 QoS，实现网络资源统一管理，实时化网络监控。
- 虚拟化路由器可解决虚拟化后出口路由的问题，同时提供其它包括 VLAN 子网口、NAT 规则、ACL 策略、DHCP 地址池、DNS 代理等功能。

2. 网络功能虚拟化

网络功能虚拟化（Network Function Virtualization，NFV）将网络功能与专有硬件设备分离，并将这些功能使用软件的方式实现，以支持虚拟化组件完全融合的基础架构。深信服的超融合平台在NFV的实现上十分完整，包括安全领域技术领先的深信

服网络设备软件，包括虚拟下一代防火墙vAF、虚拟应用交付vAD、虚拟行为管理vAC、虚拟广域网加速vWOC、虚拟vSSLVPN等。

3. 分布式虚拟防火墙

分布式防火墙，相当于在每台虚拟机出口和入口都放着一个防火墙，只要配置一条策略，无论拓扑如何变化、虚拟机在哪运行、IP是否更改，后台都可以动态进行调整，因此无论何时业务都能够进行安全防护。

4. 业务逻辑拓扑所画即所得

所画即所得的业务逻辑呈现，通过使用鼠标在管理平面上进行操作便可从资源池中调取相应的资源，即可呈现出不同的拓扑架构。

5. 网络可视化

网络可视化（aNI, Advanced Network Insight）实现虚拟机访问关系自动采集梳理，新增资产自动添加展示，及时同步资产情况。从业务的角度提供直观、清晰的虚拟机间的访问关系拓扑图和访问详情，便于优化策略配置、发现业务访问风险、减少风险端口暴露。

6. 网络流量镜像

深信服HCI支持将虚拟机/网络设备的网卡流量复制转发至超融合出口，运维场景下可以将业务虚拟机的网络流量镜像至安全审计设备以实现流量筛选和监控。

2. 安装部署

2.1. 安装组网介绍

2.1.1. 组网注意事项

表1 HCI 平台安装组网注意事项

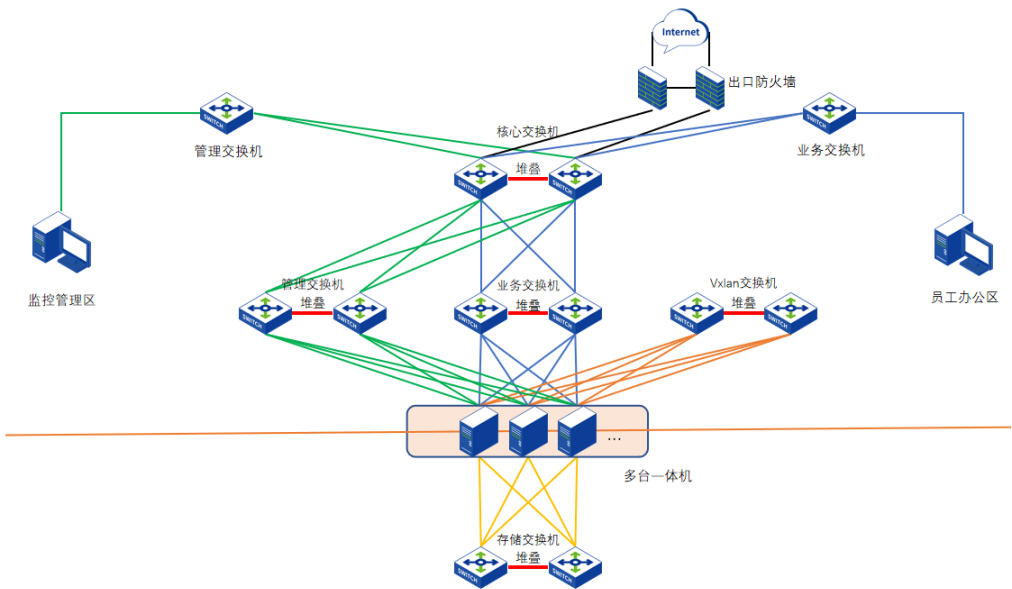
组网部署	主机网口	建议最低 6*GE+2*10GE	禁止使用千兆以下的网络。
	存储私网	推荐采用标准链路聚合	1. 必须采用万兆网口构建存储私网。 2. 禁止使用无链路聚合。
	管理网络	建议堆叠/M-LAG 部署、使用 2*GE 网口做聚合，采用 IP 地址方式进行负载，需要交换机相应的接口配置静态网口聚合，集群管理口、数据通信口的组网交换机，需要支持组播功能，否则无法建立集群。	-
	业务网络	建议堆叠/M-LAG 部署、使用 2*GE 网口做聚合，采用 IP 地址方式进行负载，需要交换机相应的接口配置静态网口聚合。	-
	VXLAN 网络	建议 2*GE 网口做聚合，采用 IP 地址方式进行负载，开启高性能模式，连接的交换机需要开启巨帧，设置为 1600 以上(锐捷交换机设置为 2000)，同时需要交换机相应的接口配置静态网口聚合。（设备网口不足的情况下允许将 VXLAN 网络与业务网络复用）	HCI 平台 VXLAN 网络设置必须开启高性能模式。
	交换机	需要将交换机上联网口关闭 STP 功能或配置边缘端口，交换机采用堆叠/M-LAG 部署。	禁止使用无冗余单台交换机部署。
	IP 地址规划	建议管理网段，VXLAN 网段和业务网段划分在不同网段，避免 IP 地址冲突。	-
	网线规范	1. 建议 50m 以内使用多模光纤，超过 50m 使用单模光纤。 2. 建议使用五类及以上双绞线。	1. 禁止单模光纤接多模模块。 2. 禁止多模光纤接单模模块。 3. 禁止使用 1~4 类双绞线。
	双活组网	1. 建议仲裁节点和主备故障域之间带宽在 100Mbps 以上，延时 ≤1ms(允许在 5ms 以内波动)。 2. 延伸集群卷主故障域和备故障域之间必须使用万兆裸光纤连接，	-

		延时<=1ms。	
--	--	----------	--

- 1. 数据通信口的组网交换机，应确认是否支持巨帧（Jumbo Frame）。如果支持，则建议开启数据通信口的高性能模式，即把VXLAN口的MTU改为1600。如果不支持，则禁止开启数据通信口的高性能模式，否则会导致虚拟机数据不通。
- 2. 一键检测的连通性探测只是ping检测，只要能ping通，即使组播不通，但是检测结果是正常。
- 3. 四种通信网口类型（管理通信口、VXLAN数据通信口、VS存储通信口、物理出口）不允许复用。但如果网口不够的情况下一定要复用网口就复用物理出口与VXLAN口。建议网口使用规划为：2个管理口，2个存储口，2个聚合做VXLAN和物理出口复用。
- 4. 无论是第三方服务器还是超融合一体机，不要对网卡进行热插拔，否则可能会出现网口乱序的情况。

2.1.2. HCI 标准集群组网介绍

HCI标准组网拓扑图如下。



名词解释：

- 1. 管理网络，用于平台管理，服务器IPMI/BMC/IDRAC等远程管理网口复用管理网络。

2. VXLAN网络，用于承载虚拟机的东西向流量，二层通信。
3. 存储网络，用于aSAN存储，负责HCI节点间存储数据通信；在使用IPSAN时，也作为与外置存储进行通信的接口，二层通信。
4. 业务网络，用于承载虚拟机的南北向通信。

组网说明：

1. 核心层

建议采用具备大容量网络报文转发能力的数据中心核心交换机，要求交换机型号支持堆叠/M-LAG或者集群技术，下行端口速率10GE。

2. 接入层

大规模部署场景下，建议管理、业务、VXLAN网络平面分别采用支持堆叠/M-LAG技术的两台数据中心千兆接入交换机，下行端口速率GE接入服务器，上行端口速率10GE，多条10GE链路使用链路聚合方式接入核心交换机，构建冗余、低收敛比、无阻塞业务交换网络。存储网络则采用支持堆叠/M-LAG技术的两台万兆交换机，多条10GE链路使用链路聚合方式接入服务器保证VS性能，同时提高整个网络架构的健壮性。

小规模部署场景下，建议管理、业务、VXLAN网络平面采用两台堆叠/M-LAG的数据中心千兆接入交换机，各个网络平面划分不同VLAN做逻辑隔离。存储网络同样采用支持堆叠/M-LAG技术的两台万兆交换机，采用链路聚合方式，保障VS性能，同时提高整个网络架构的健壮性。

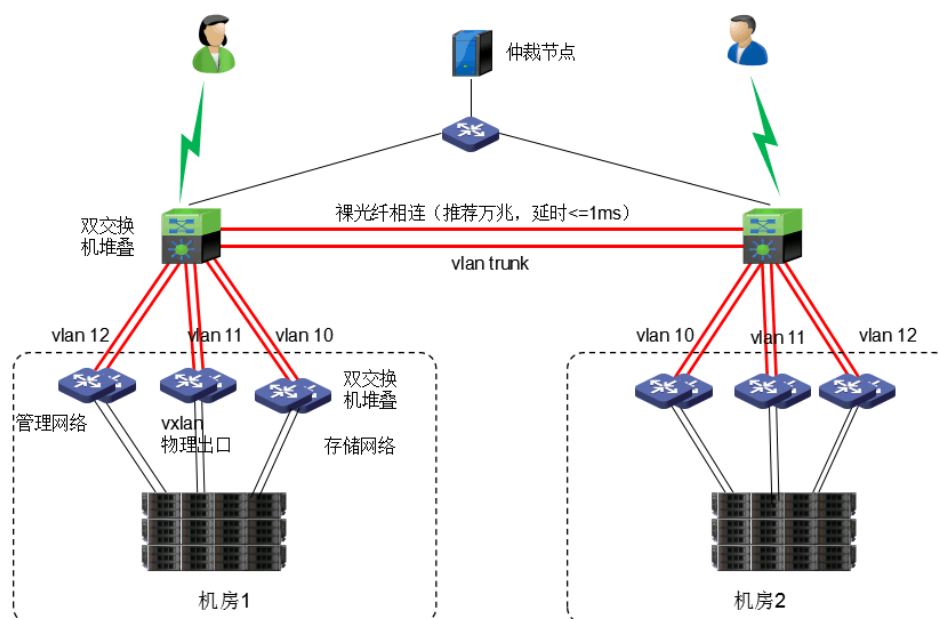
服务器配置6*GE、2*10GE网口时，管理、业务、VXLAN网络各采用2*GE网口，并做网口聚合绑定；存储网络采用2*10GE网口，并做网口聚合绑定，增加网络冗余性和传输带宽。

对于管理、业务、VXLAN、存储网络平面，服务器网卡聚合支持根据IP、MAC地址、轮询三种方式负载均衡模式，建议采用按照IP方式进行负载均衡，接入层交换机端口需要配置相应的端口聚合模式，如果接入交换机是思科交换机则配置mode on与底层聚合网卡进行对接。

另外，由于超融合平台无法感知机柜，建议超融合部署时尽量使用双机双柜的部署方式，即堆叠/M-LAG的双交换机放置于两个机柜中，单一集群中服务器建议放置于两个以上机柜中。

2.1.3. HCI 延伸集群组网介绍

HCI延伸集群组网拓扑图如下。



组网说明：

- 机房 1 和机房 2

机房1和机房2组成一个HCI集群，在保障两个机房的管理网络、VXLAN网络、存储网络互通的情况下，分别在机房内部对管理网络、VXLAN网络、存储网络配置相应的冗余策略，对这三种网络分别采用两个交换机做堆叠/M-LAG，同时在HCI集群上配置好相应的网络聚合。建议如下：

管理网络：每台主机用2*GE网口做聚合，采用2台单独的管理网交换机做堆叠/M-LAG。

VXLAN网络：每台主机用2*GE网口做聚合，采用2台单独的VXLAN网交换机做堆叠/M-LAG。

存储网络：每台主机用2*10GE网口做聚合，采用2台单独的存储网交换机做堆叠/M-LAG。

两个机房可以设置各自的业务出口，同样建议业务网络采用2*GE网口做聚合，对外提供业务。建议有条件的情况下，两个机房设置各自的业务出口，如果条件不允许，也可以只在主提供业务的机房设置业务出口。

- 机房间网络

机房1和机房2通过网络二层直连，推荐万兆裸光纤网络做聚合，机房间的网络延时应小于等于1ms；两个机房间的交换机分别做堆叠/M-LAG，同时在堆叠/M-LAG的交换机上划分三个不同的VLAN，用于承载两个机房间的管理网络、VXLAN网络、存储网络的相关数据。

- 仲裁节点

仲裁节点是延伸集群中的一个重要节点，它不同于HCI系统，配置仲裁节点需要单独安装仲裁节点的操作系统或者购买单独的仲裁节点一体机。通过仲裁节点与集群间的定期通信，可以及时发现不同机房的数据副本是否异常。对于发生异常的机房，在仲裁节点的指控下，可以让业务在数据副本正常的机房上继续提供服务。仲裁节点可部署于机房1和机房2之间用来承载业务的主机房，也可以部署于第三方站点，前提是仲裁节点需要跟HCI集群IP能够相互通信。仲裁节点与集群间链路要求延时不高于5ms，建议带宽为100M。

2.2. 安装前准备

2.2.1. 文档和工具准备

表2 文档和工具下载地址

工具/材料名称	下载地址
深信服超融合版本用户手册	深信服社区 - 知识库 - 资料库 - 超融合 HCI - 用户手册
深信服超融合版本安装镜像	深信服社区 - 自助服务 - 软件下载 - 超融合 HCI
深信服仲裁节点安装包	
深信服智能交付工具 aDeploy	深信服社区 - 自助服务 - 常用工具
深信服虚拟网络设备模板	深信服社区 - 自助服务 - 软件下载 - 超融合 HCI - 虚拟网络设备模板
操作系统镜像	自行获取
Chrome、UltraISO、MD5	自行获取

2.2.2. 超融合集群配置要求

表3 HCI 硬件配置要求

名称	项目	建议值	注意事项
服务器	RAID 卡	- 必须支持直通（JBOD、NON-RAID）模式。 - 缓存盘和数据盘必须配置成直通模式。 - 支持 RAID1。（第三方服务系统盘使用） - 使用 aDeploy 工具对 RAID 卡、RAID 卡固件进行兼容性检测，不满足要求的硬件将不被允许加入到虚拟存储中。	缓存盘和数据盘禁止使用 RAID0 模式。

	CPU	建议 CPU 主频大于 2.0GHz。（建议使用服务器级 CPU）	1. 禁止使用小于 8 线程的 CPU。 2. 支持 HCI 部署到搭载海光 7159 CPU 的服务器上。 3. 若使用海光 CPU： a. 不支持混合部署，同一集群内只能使用海光 CPU； b. 不支持 NUMA 调度功能； c. 不支持异构迁移； d. Windows 虚拟机禁止开启高性能时钟。
	内存	内存不低于 64G。	禁止内存小于 32 的主机三个全开 aSAN/aNET/aSV。
	系统盘	1. 系统盘推荐使用企业级硬盘。 2. 容量不低于 128G。 3. 第三方服务使用两块盘做成 RAID1。	1. 禁止服务器系统盘部署单盘 RAID0。 2. 禁止使用 SD 卡做超融合的系统盘，不能使用的原因是其可靠性、性能、稳定性方面存在问题。
	数据盘	分布式存储使用 SSD 作为缓存盘。 SATA（也可以是 SAS）作为数据盘。 SSD：HDD 容量比越高，整体性能越好。 使用 aDeploy 工具对 SSD 固件进行兼容性检测，若不满足要求将不被允许加入到虚拟存储中。	1. 禁止使用非企业级 HDD 盘。 2. 禁止使用 7200 转以下 HDD 硬盘。 3. 禁止使用小于 600G 硬盘作为数据盘。（推荐 4T 以上） 4. 禁止使用 4Kn 盘（低于 6.2.0 的版本或者 2 主机 vs 集群，6.2.0 开始 VS 支持 4kn 盘）。 5. 禁止缓存盘 SSD/数据盘 HDD 容量比例小于 1:20（最佳实践推荐容量比为 20%）。 6. 如果使用读密集型 SSD，则禁止 SSD 缓存盘/HDD 容量比例低于 7%。 7. 禁止缓存盘 SSD/数据盘 HDD 个数比例小于 1:7。 8. 各个主机之间的数据盘容量总和，最高的容量不能超过剩下所有主机之和的 80%。 9. 单个主机内数据盘容量的大小存在差异是允许的，但最大和最小的数据盘的

			容量差距不要超过 2 倍。 10. 无论是测试还是实施，不能出现缓存盘的数量大于数据盘的数量。 11. 要求 SSD 接口速率为 6Gbps，如果速率为 3Gbps，不允许加入虚拟存储卷。 12. 禁止速率低于 50MB/s 的 HDD 加入虚拟存储卷。 13. 禁止 IOPS 低于 1 万的 SSD 数据盘（全闪）加入虚拟存储卷。
	缓存盘		1. 禁止使用非企业级 SSD。 2. 缓存盘禁止使用小于 240GB 的 SSD。 3. 禁止使用 DWPD 小于 1 的 SSD。（SSD 的 spec 参数表可以查到） 4. 禁止使用不支持掉电数据保护的 SSD。 5. 禁止 IOPS 低于 3 万的 SSD 加入虚拟存储卷。
交换机	VXLAN 管理业务交换机	支持堆叠/M-LAG，VXLAN 交换机额外支持巨帧。（调整 MTU 值）	禁止选择不支持巨帧交换机。（有些厂商叫做网口 MTU）
	存储交换机	必须使用万兆交换机。	存储私网禁止使用千兆交换机。

2.2.3. 仲裁节点配置要求

硬件配置要求

部署延伸集群的时候需要部署仲裁节点，仲裁节点既可以部署于物理服务器上，也可以部署在VMware虚拟化环境上，可根据集群规模参考下表做相应的硬件规划。



注意：

仲裁盘不支持使用机械盘，必须为企业级 SSD，并且在兼容性列表中，否则无法通过。

表4 仲裁节点选型要求

集群规模	最低硬件要求	说明
------	--------	----

小型部署 (4~6 台 HCI 主机，每机房 2~3 台)	CPU: 6 核 内存: 32GB 系统盘: 容量>=128G 仲裁盘: 容量>100GB 的企业级 SSD，虚拟化部署要求不低于 1000 IOPS。	支持 VMware 虚拟化部署和物理机部署。
中型部署 (8~16 台 HCI 主机，每机房 4~8 台)	CPU: 8 核 内存: 32GB 系统盘: 容量>=128G 仲裁盘: 采用 2 块 128GB 或 248GB 的企业级 SSD，配置成 RAID1	推荐采用物理机部署。
大型部署 (18~24 台 HCI 主机，每机房 9~12 台)	CPU: 16 核 内存: 32GB 系统盘: 容量>=128G 仲裁盘: 采用 2 块 128GB 或 248GB 的企业级 SSD，配置成 RAID1	务必使用物理机部署。

2.2.4. 交换机配置要求

基本配置要求

- 管理、业务、存储、隧道等基于安全合规考虑采用不同 VLAN 隔离。
- 交换机关闭 STP 协议。
- 交换机 VXLAN 端口开启巨帧。
- 超融合采用标准链路聚合模式对接对端交换机堆叠组/M-LAG。

具体配置举例

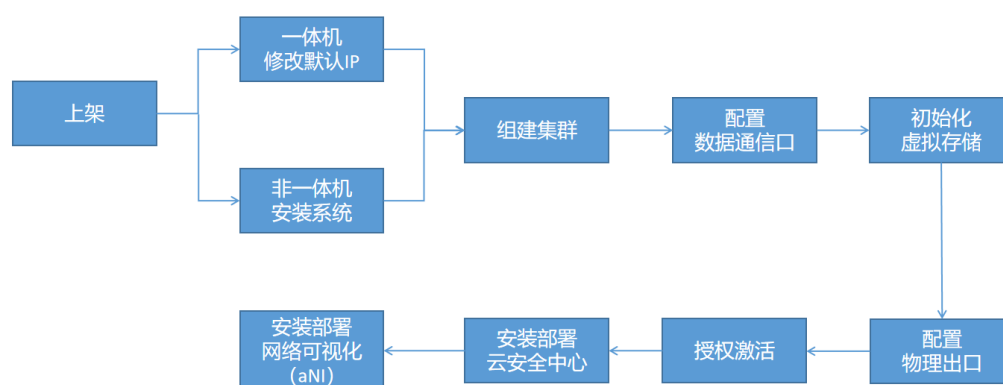
表5 交换机配置示例

网络类型	接口类型	配置举例（接口视图下配置）	备注
管理网络	access	Interface Ethernet1/0/48 switchport access VLAN 2	-
存储网络	access	Interface Ethernet1/0/48 switchport access VLAN 3	-
隧道网络	access	Interface Ethernet1/0/48 jumboframe enable switchport access VLAN 4	隧道口需要开启巨帧

外部网络	trunk	Interface Ethernet1/0/48 switchport mode trunk switchport trunk allowed VLAN 10-20	-
终端通信网络	access	Interface Ethernet1/0/48 switchport mode trunk switchport trunk allowed VLAN 30-40	

2.3. 安装流程介绍

HCI集群安装流程概要如图。



2.4. HCI 虚拟化系统安装

2.4.1. aServer 一体机

aServer一体机出厂时已预装超融合操作系统，并设置ETH0接口为管理接口，默认IP地址是10.250.0.7/24。使用PC配置同网段IP地址，直连ETH0口，用浏览器打开<https://10.250.0.7/>可以登录aServer一体机的控制台。

默认的管理员账号和密码均为admin，首次登录会提示修改默认密码，使用一个月后强制修改默认密码。

首次登录成功后会提示修改默认IP地址。如果有多台aServer主机，需要在组建集群之前分别登录以修改默认IP地址，且要求IP地址在同网段。

aServer一体机经过签名处理，只能使用具有签名的磁盘（原厂发货），如果一体机插入第三方磁盘，在虚拟存储中不能识别使用，只能用于本地存储。

使用了虚拟存储时，不支持删除主机，禁止将集群拆开后把主机拿出去单独使用。

一体机不可重装系统，重装系统后需要对主机和磁盘重新签名。

一体机磁盘不要进行低级格式化，格式化后需要重新签名。

配置IPMI接口方法请参考下面“[BIOS配置](#)”章节。

2.4.2. 第三方服务器

第三方服务器安装系统可以使用IPMI进行ISO安装和U盘安装两种方式。两种方式的
区别主要在于挂载镜像部分，安装部分是完全相同的。

2.4.2.1. 服务器配置

硬件配置要求

使用第三方服务器安装超融合时，要求每台主机硬件必须满足以下最低配置要求。
为了保证最佳使用效果，建议按推荐配置选配服务器硬件。



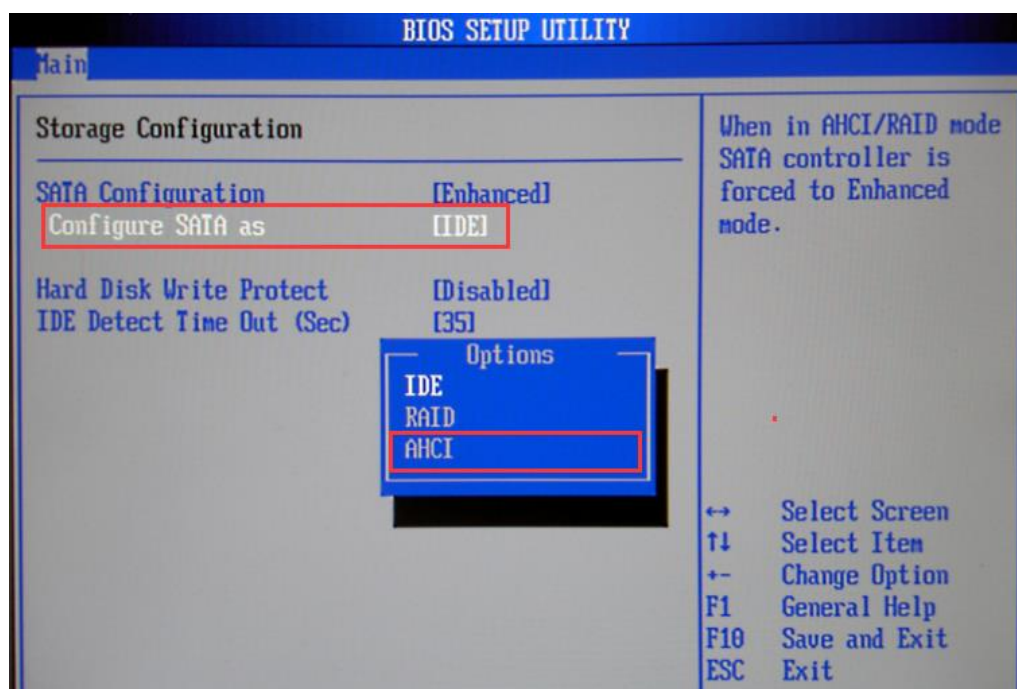
注意：

如果需要使用虚拟存储功能，则每台主机除系统盘以外，还必须配置至少 1 块 240GB 以上的企业级 SSD 固态硬盘（需要支持 TRIM/Discard 指令）作为缓存盘，以及若干块 1TB 以上的企业级 HDD 机械硬盘（转速大于等于 7200RPM）作为数据盘。

SSD 和 HDD 的个数比不能低于 1: 6，最低不能低于 1: 25，如果是读密集型 SSD，则禁止 SSD 缓存盘/HDD 容量比例低于 7%。

RAID卡配置要求

如果有RAID卡，建议选配支持JBOD/Non-RAID直通的RAID卡，支持TRIM指令透传。
如果RAID卡不支持JBOD/Non-RAID，则直接禁用RAID卡启用普通磁盘模式（AHCI/IDE）。



BIOS配置要求

使用第三方服务器时，需要修改一些BIOS选项，确保超融合平台的高效运行。BIOS配置要求：

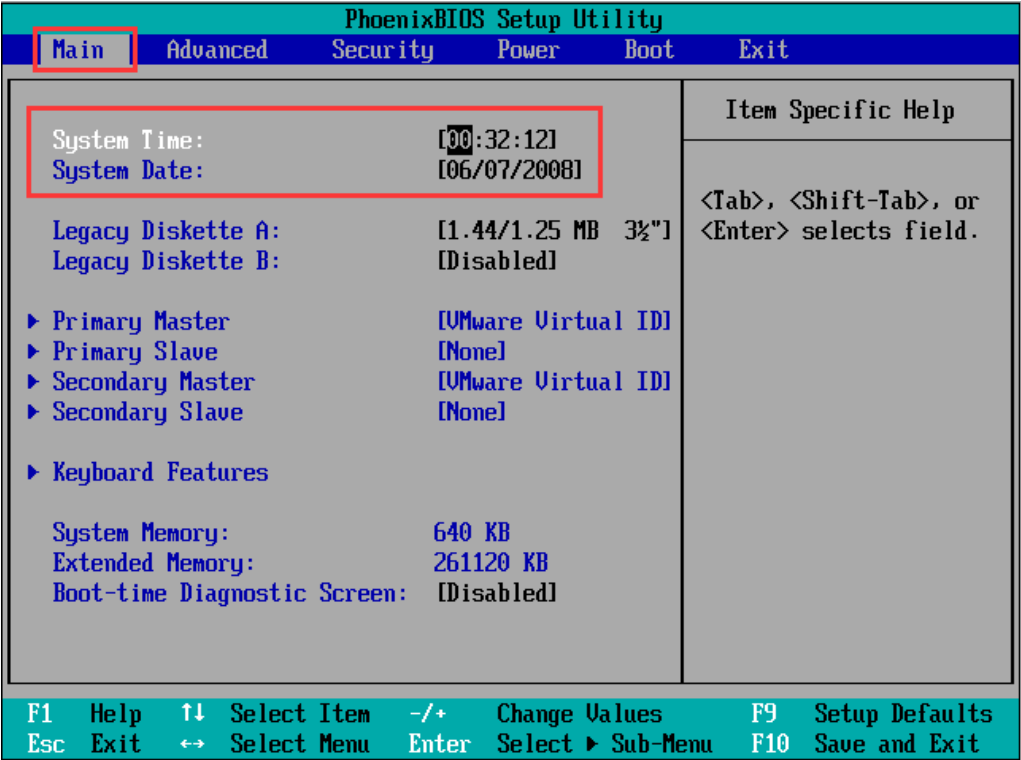
- BIOS 时间同步
- 启用 VT-x 或者 VMX
- 关闭节能模式
- 开启加电自启
- 配置 IPMI 地址（可选）

具体配置举例

进入BIOS的方法根据BIOS厂商自己定义的，通常是在服务器加电启动，到POST界面时，屏幕会提示按DEL、ESC、F10、F11等按键进入BIOS SETUP界面。

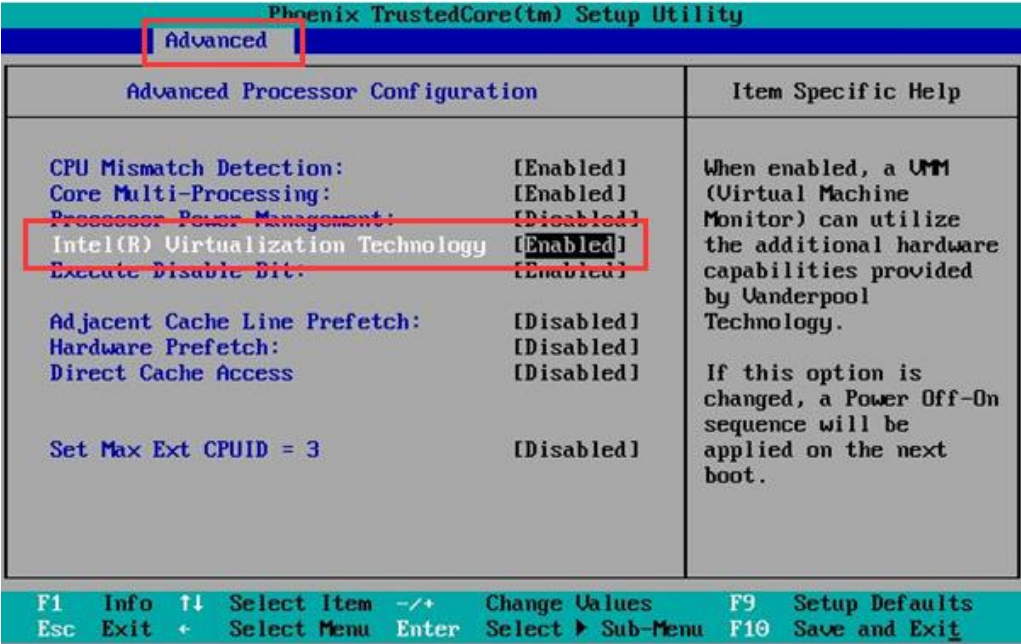
1. BIOS时间同步

超融合平台安装时会读取服务器的BIOS时间作为系统时间，如果系统时间不准确，可能影响部分服务正常运行。因此首先需要修改BIOS时间为当前时间。



2. 启用VT-x

超融合平台运行虚拟机时，要求主机支持Intel VT-x的硬件辅助虚拟化技术。因此除了需要CPU支持VT-x技术外，还需要在BIOS中启用该功能。如果CPU不支持VT-x，或者BIOS中未启用VT-x，则无法成功安装超融合平台。



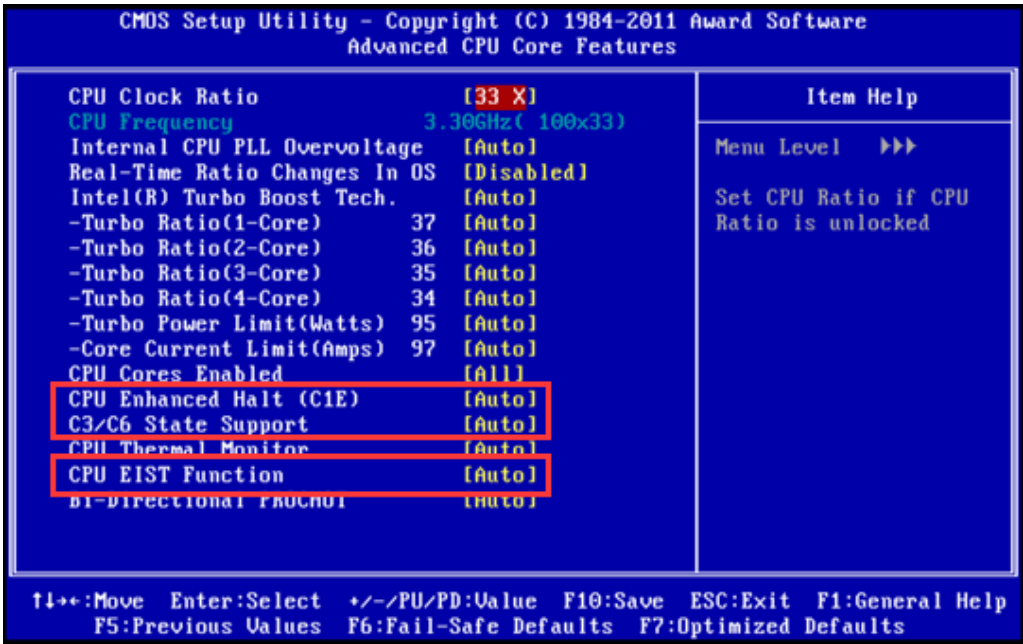
3. 关闭节能模式

关闭CPU节能模式(EIST和C States等选项设置均为Disabled)，根据实际硬件可能名

称不同（如Power Performance等）。

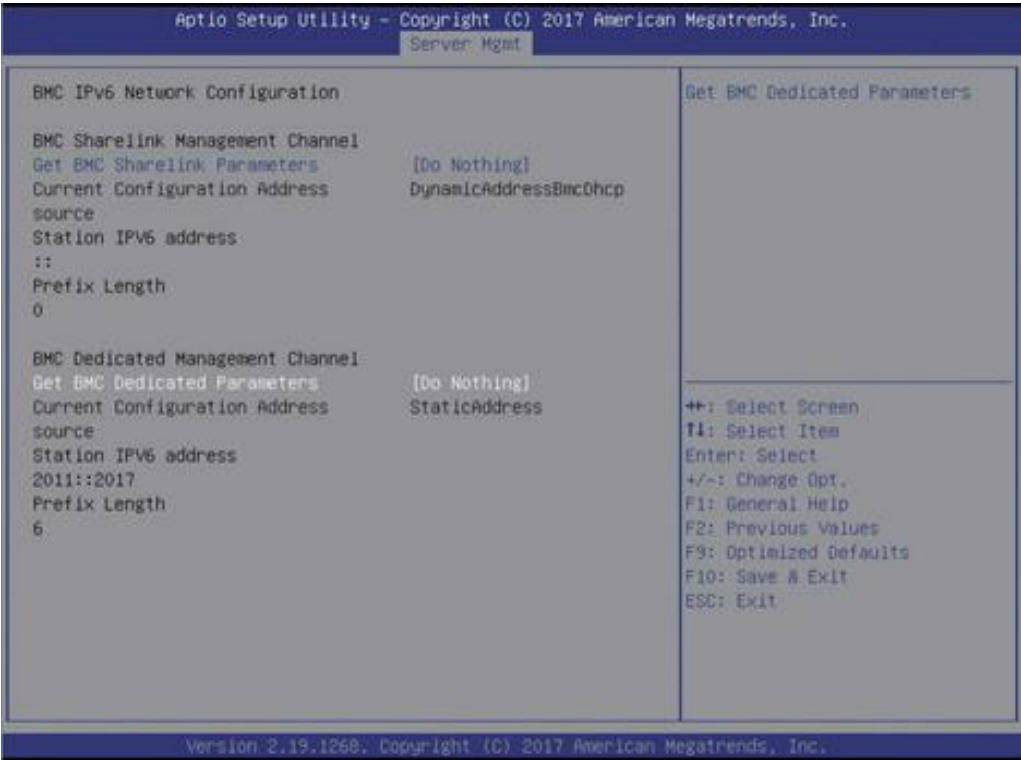
表6 CPU 节能模式

CPU状态	状态解释	状态类型	使用建议
C0	Operating State	CPU 正常工作状态	----
C1	Halt	不同级别、不同深度的 CPU 休眠状态，均建议禁用。	Disable
C1E	Enhanced Halt		Disable
C2	Stop Grant/Clock		Disable
C2E	Extended Stop Grant		Disable
C3	Sleep		Disable
C4	Deeper Sleep		Disable
C4E/C5	Enhanced Deeper Sleep		Disable
C6	Deep Power Down		Disable
EIST	Enhanced Intel SpeedStep Technology	自动调节处理器的电压和频率。	Disable



4. IPMI地址配置

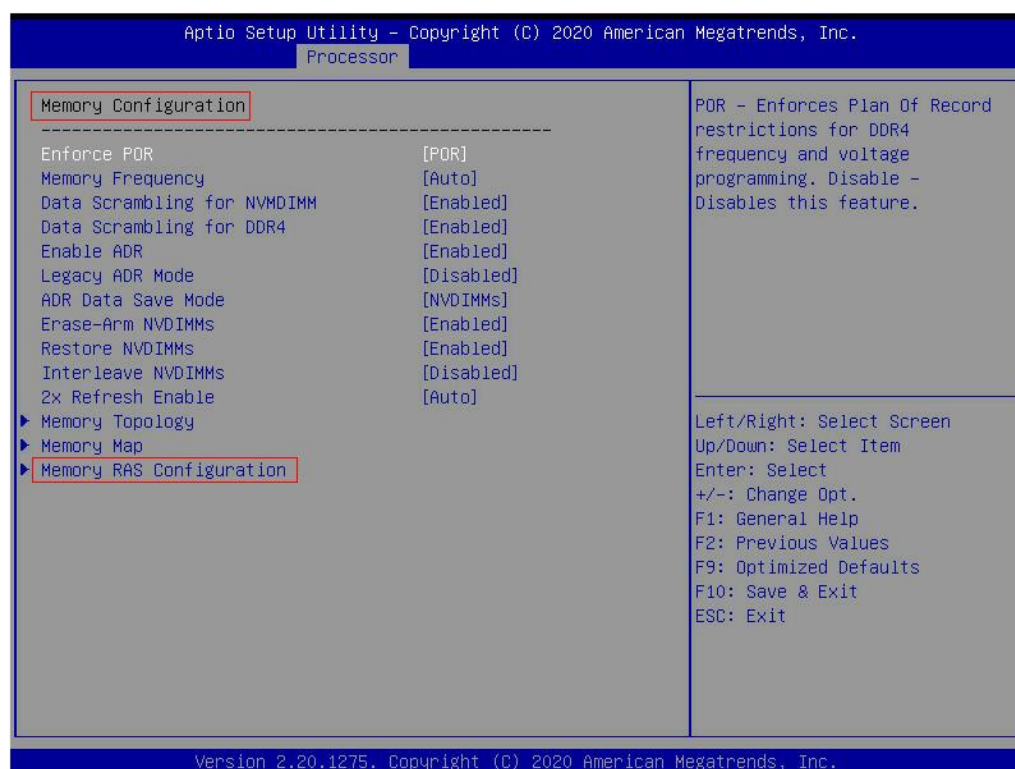
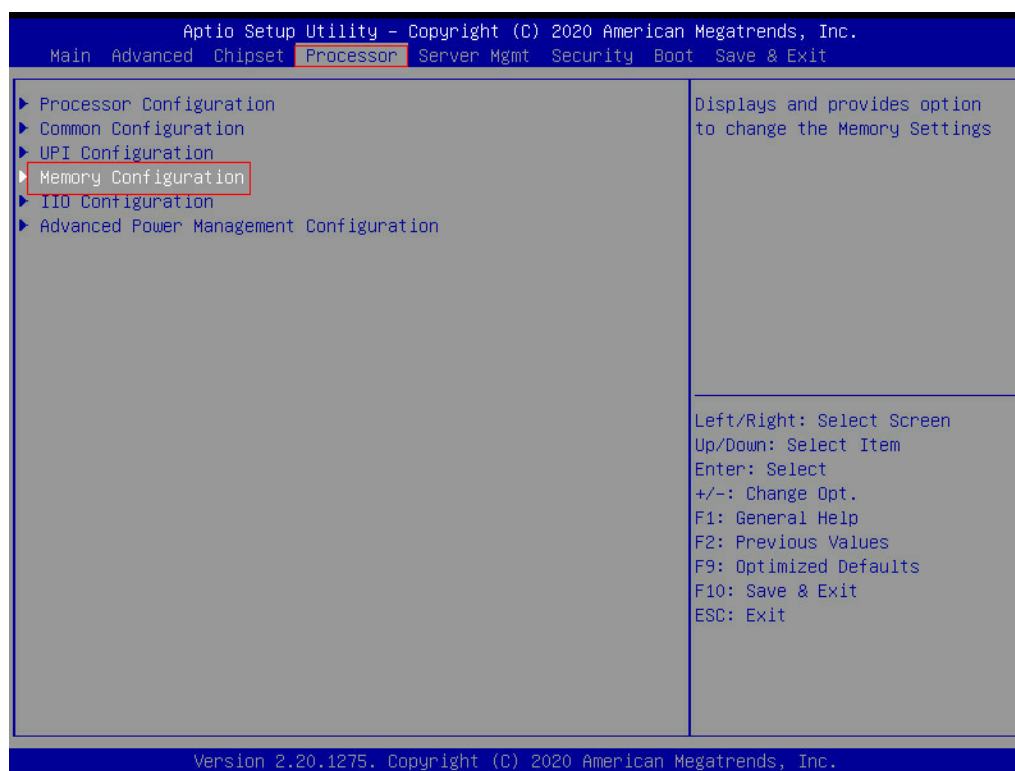
登录到 BIOS 界面，选择“Server Mgmt->BMC Network Configuration->BMC IPv4 Network Configuration/BMC IPv6 Network Configuration”，按 Enter 键，可查看当前 BMC IPv4 和 BMC IPv6 网络参数的配置情况。

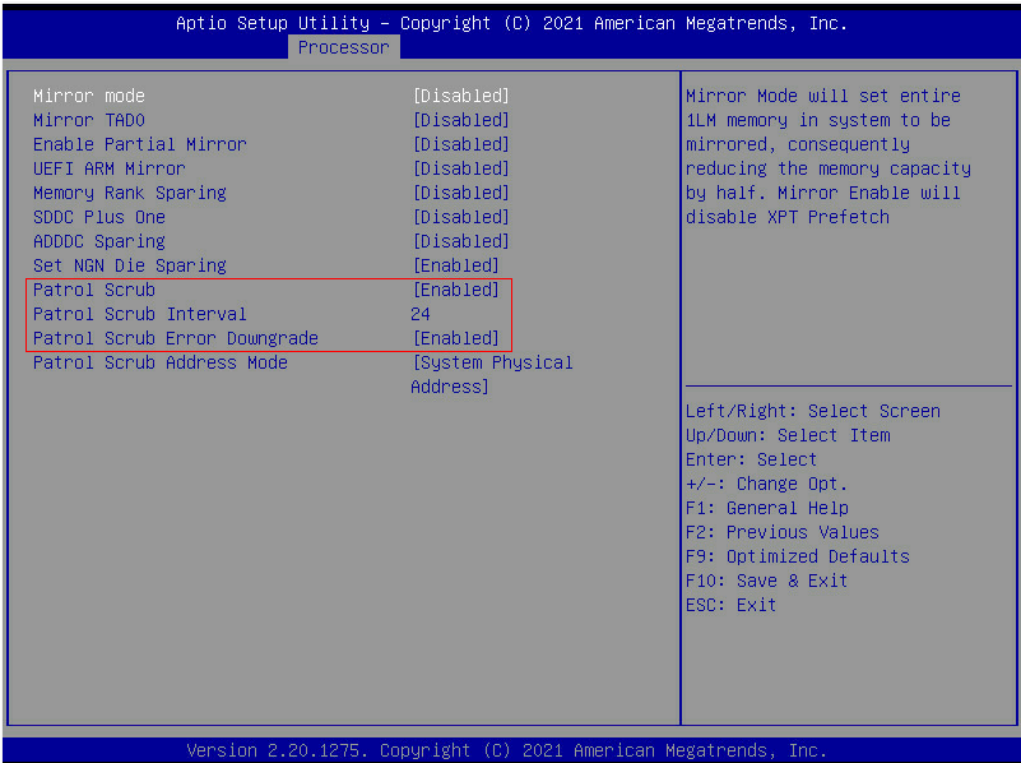


BMC Sharelink 是将IPMI地址复用在网卡第一个接口。BMC Dedicated 是为单独的IPMI接口配置地址。在配置带外管理网络时，对BMC Dedicated进行修改，选择“Manual”人为写入Static地址。

5. 启用内存扫描（内存ECC功能需启用）

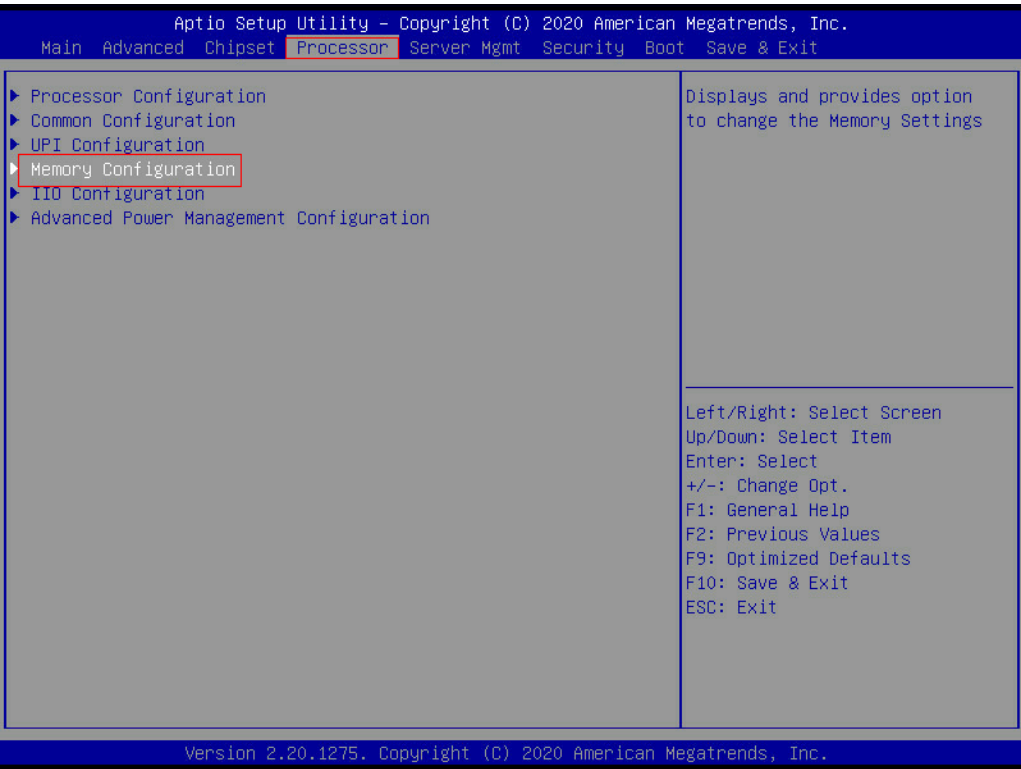
登录到BIOS界面，选择“Processor->Memory Configuration->Memory RAS Configuration”，将Patrol Scrub设置为“Enable”，将Patrol Scrub Intercal设置为“24”。

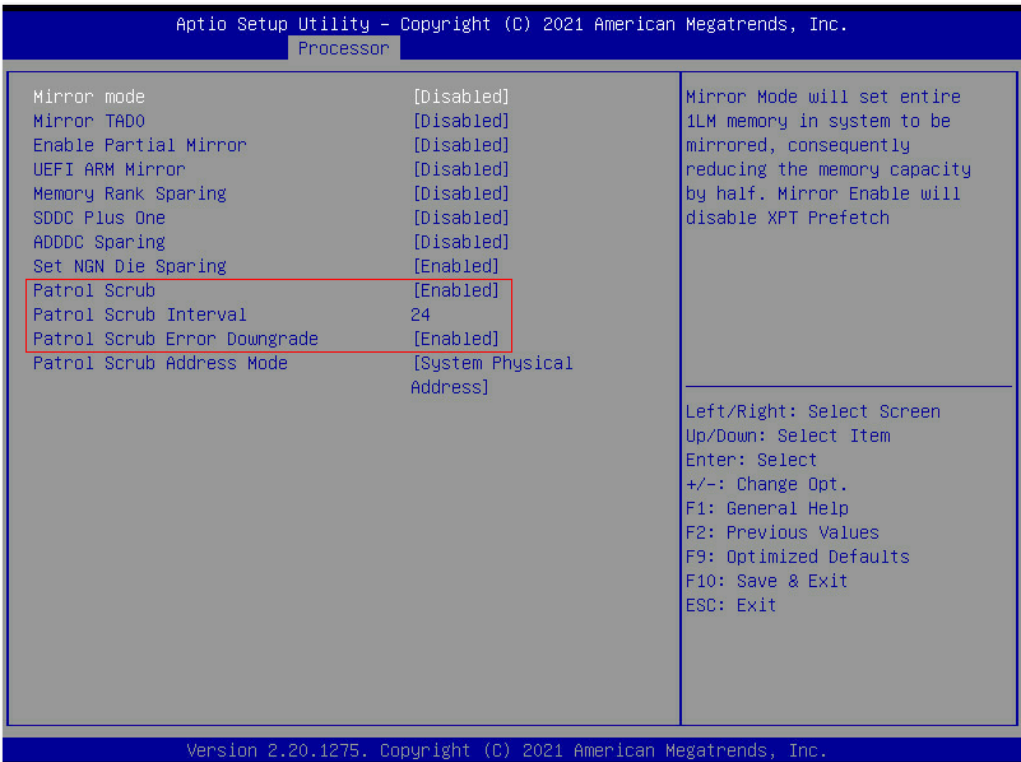
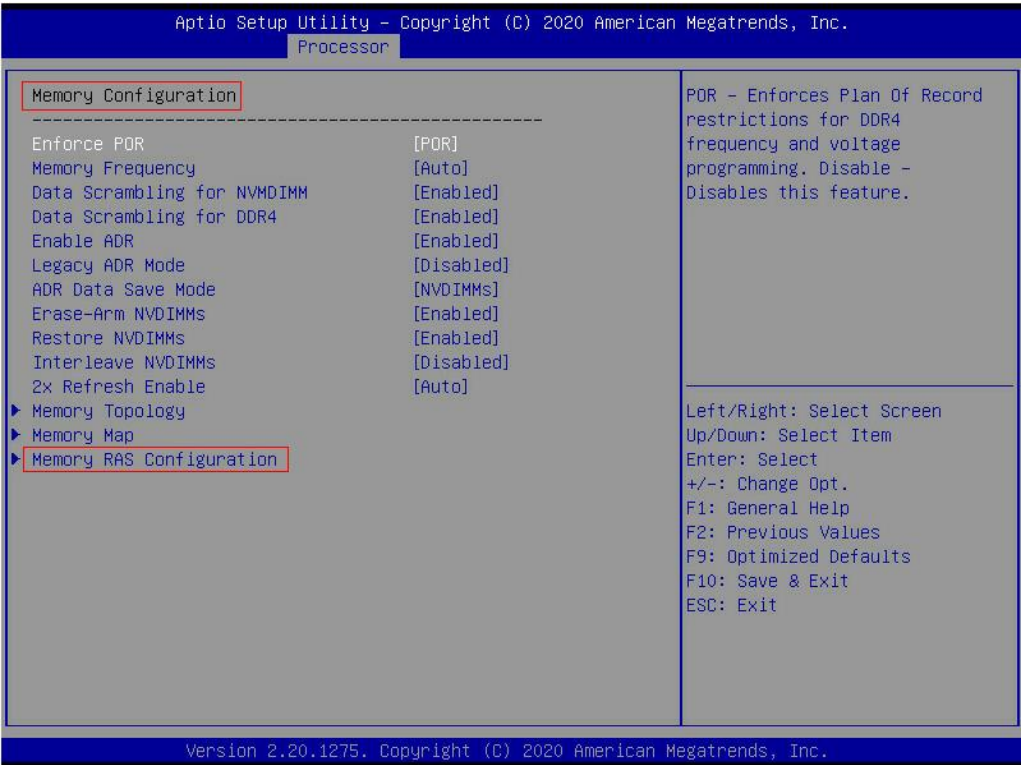




6. 启用内存UE降级（内存ECC功能需启用）

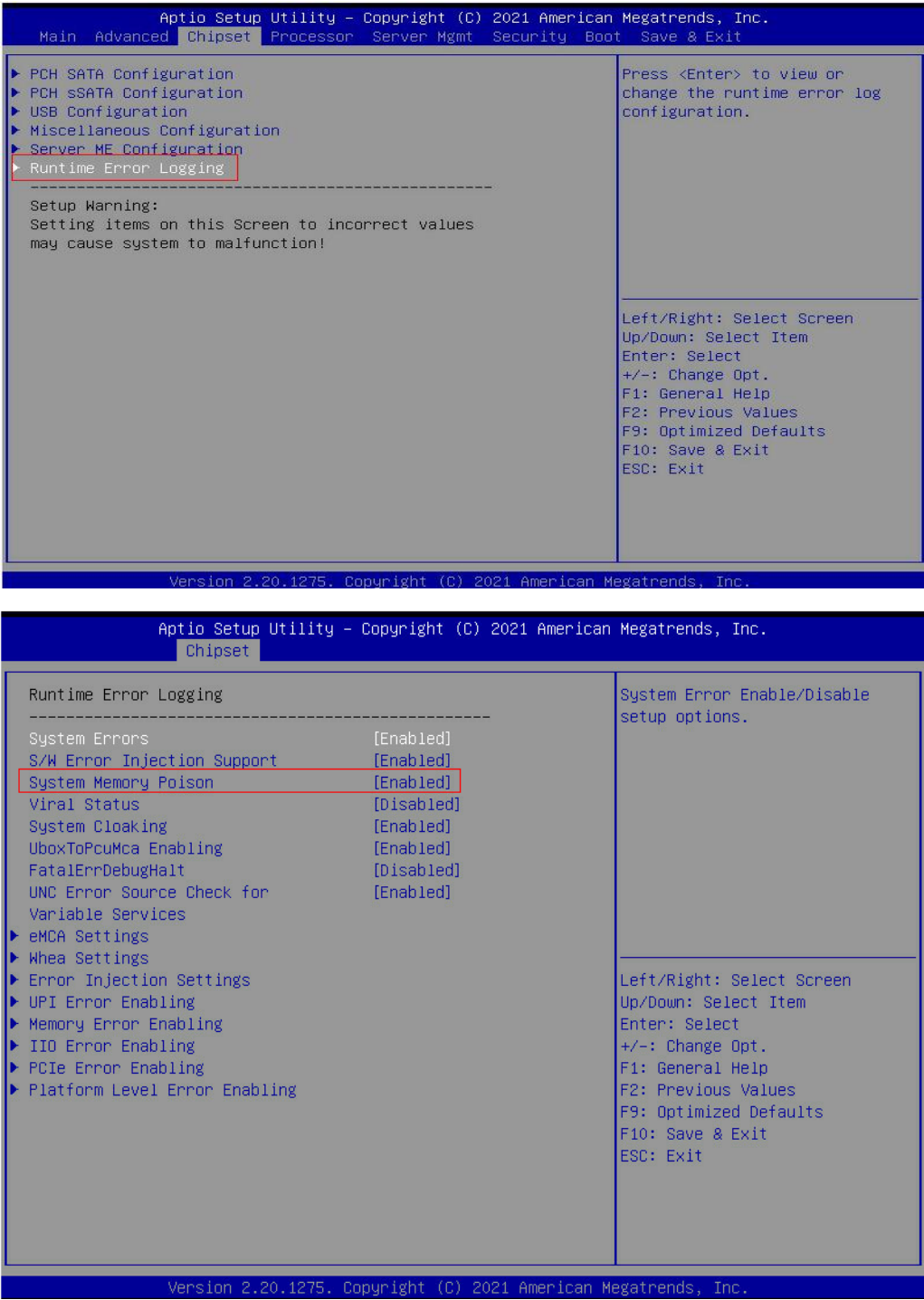
登录到 BIOS 界面，选择 “ Processor->Memory Configuration->Memory RAS Configuration”，将Patrol Scroub Error Downgrage设置为 “Enabled” 。





7. 启用内存隔离（内存ECC功能需启用）

登录到BIOS界面，选择“Chipset->Runtime Error Logging”，将System Memory Poison设置为“Enabled”。



2.4.2.2. ISO 安装

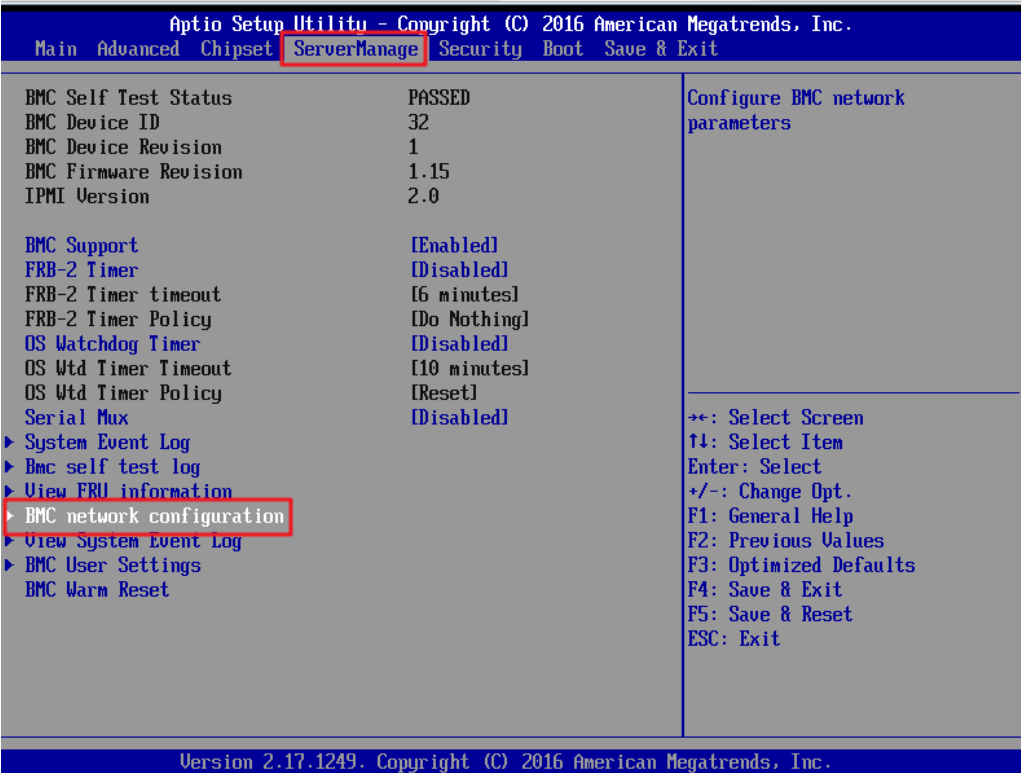
注意事项

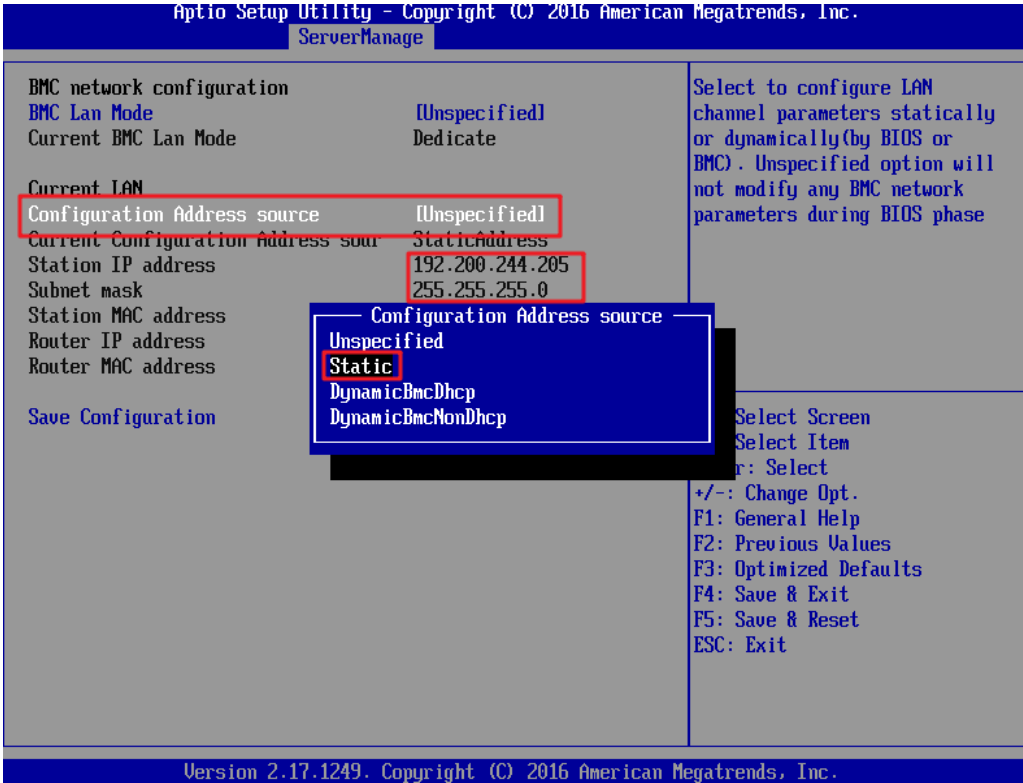
- 1. 此处以浪潮服务器为例进行演示。
- 2. 所需使用的软件：Chrome浏览器。
- 3. 个人PC中需要预先安装java，推荐使用jdk-8u181-windows-x64.exe。

- 4. 交换机及服务器等配置需要满足本手册中“安装前准备”章节中的服务器及交换机配置要求。
- 5. 安装HCI的时候卡在6%不动很长时间需检查磁盘是否离线。
- 6. 插上key服务器就起不来，如有遇到此情况，需要修改BIOS设置中的USB3.0配置，设置为Enable。
- 7. 避免UEFI方式安装，请使用Legacy模式安装（选择不带UEFI的引导盘）。

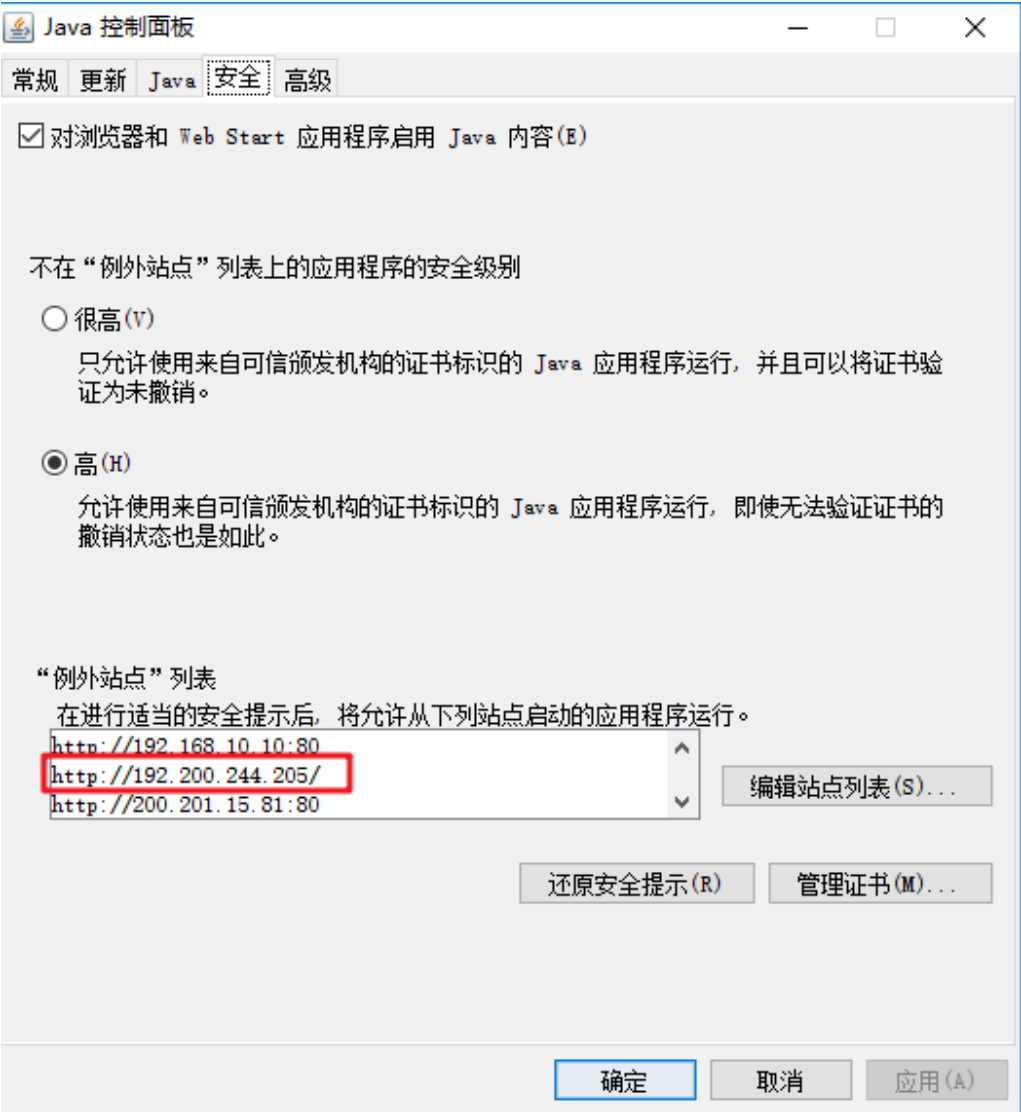
操作步骤

- 1. 在服务器的BIOS中启用IPMI。在[ServerManager/BMC network configuration]中对BMC进行配置。配置静态IP地址，并保存。将设备BMC口（一般在最左侧位置，单独的一个网口，附近有BMC或者mgmt标识）插上网线，并接入网络。





2. 在个人PC中对Java程序进行设置。在[控制面板/程序/Java]的[Java控制面板]中点击[安全]，将[不在“例外站点”列表上的应用程序的安全级别]设置为[高]，并在[例外站点列表]中添加服务器BMC的IP。



3. 在浏览器中输入http://IP，并输入登录账号和密码，进入BMC控制台页面。在控制台页面中点击[远程控制/控制台重定向]。

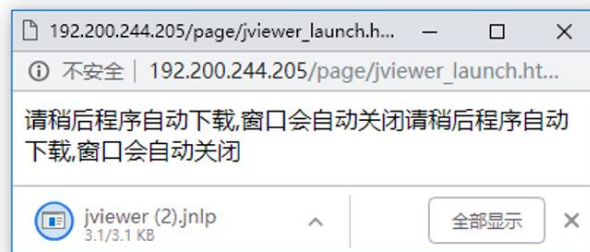


4. 在[控制台重定向]页面中点击Java终端，弹出页面下载jviewer.jnlp。jviewer.jnlp 下载完成之后点击运行会弹出[安全警告]窗口。在弹出的[安全警告]窗口中勾选 [我接受风险并希望运行此应用程序(I).]并点击<运行>。

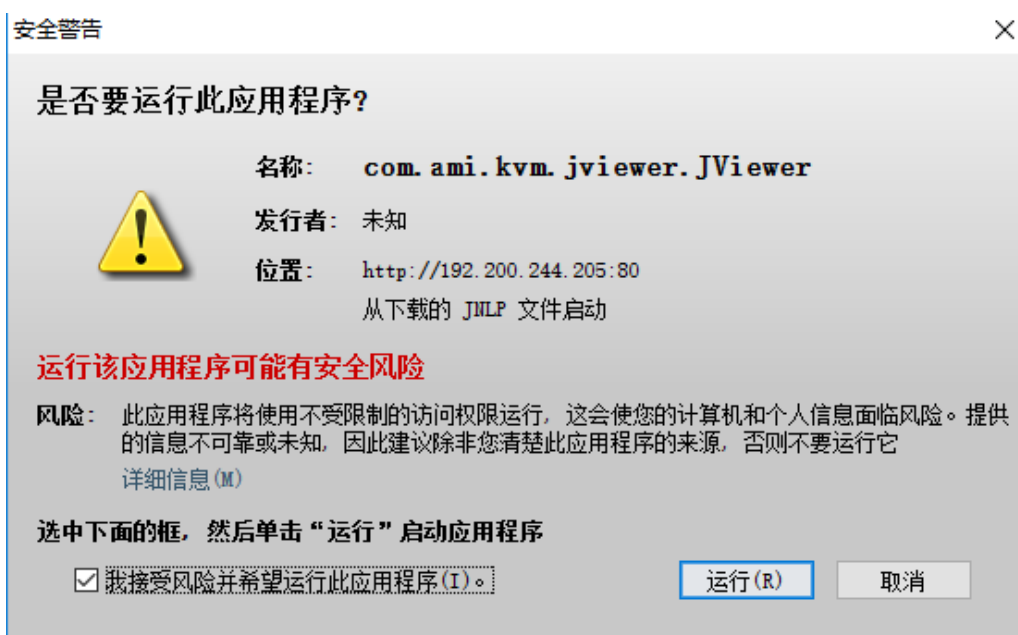
仪表盘 FRU&DMI 服务器健康状况 部件信息 配置 远程控制 自动录像 维护 固件更新 自动

控制台重定向

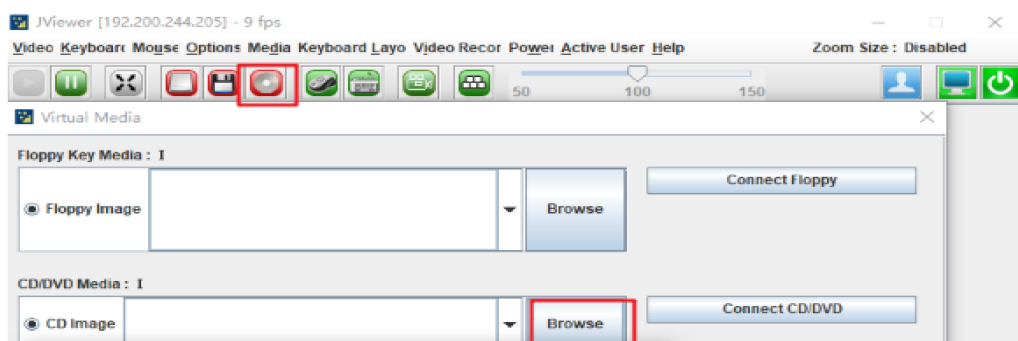
按下按键启动控制台重定向并可以远程管理服务器。

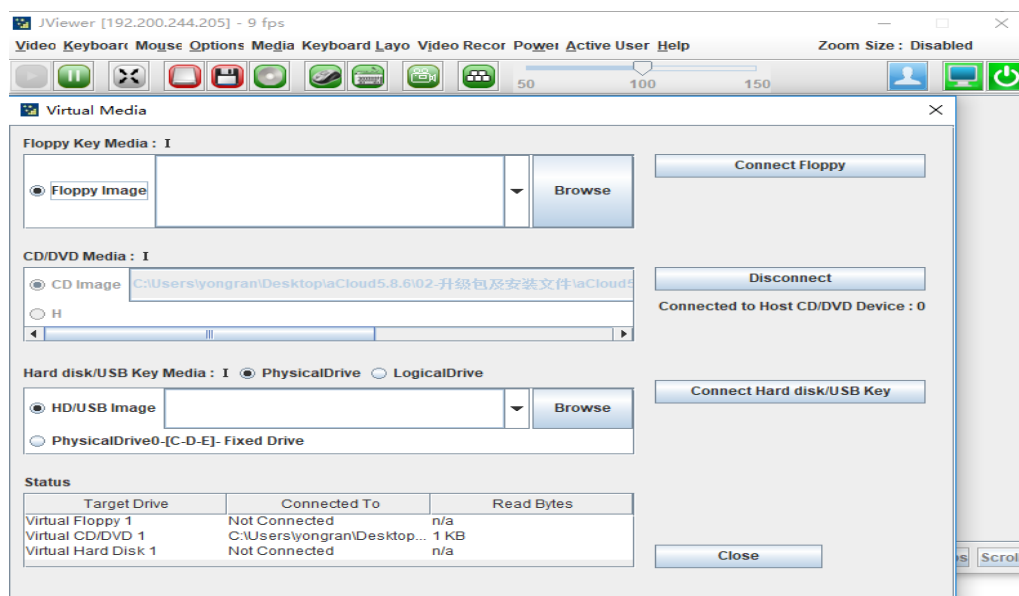


Java终端

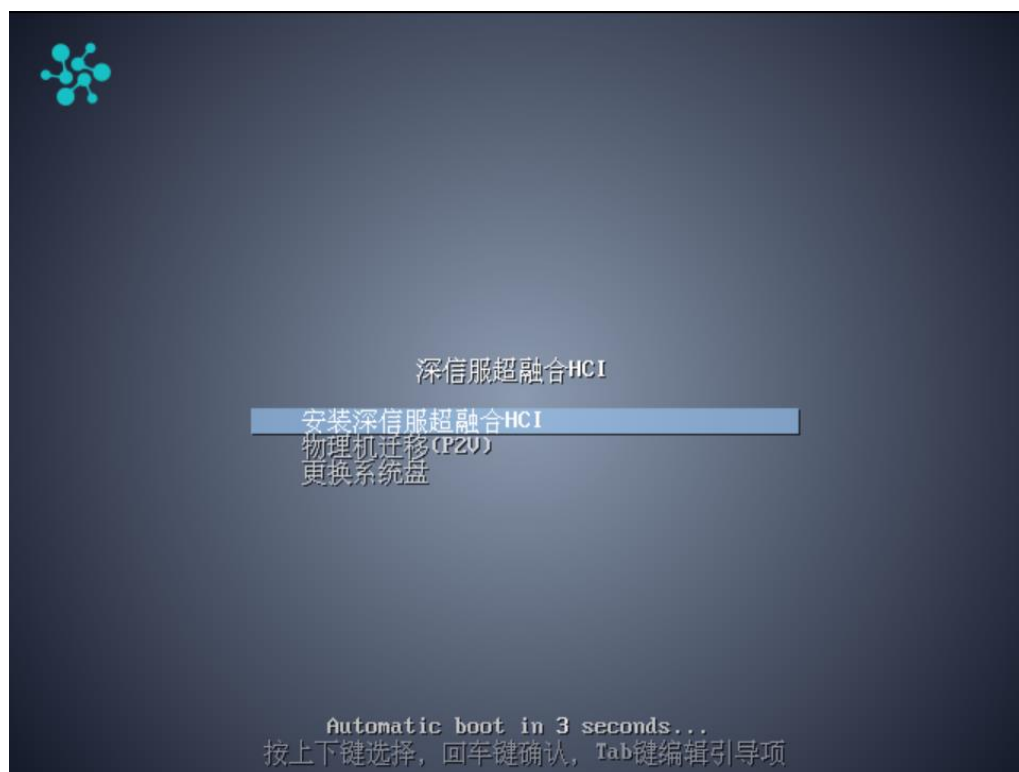


5. [JViewer]窗口中点击<光盘图标>会弹出[virtual Media]窗口。点击[CD/DVD Media:]中的<Browse>, 选择HCI_6.2.0版本的ISO镜像, 并点击<Connect CD/DVD>, 最后点击<Close>退出。再次点击<光盘图标>确认是否挂载成功。





- 重启服务器，按Del/F12进到BIOS，找到BOOT菜单/Boot Option/Enter进入选项，选择CD/DVD为第一启动项；或者按F11进入引导项选择界面，选择CD/DVD进入。
- 进入启动界面，选择[安装深信服超融合（HCI）]，按“ENTER”键，进入安装界面。



8. 选择[格式化安装], 按“ENTER”键, 进入解压安装。



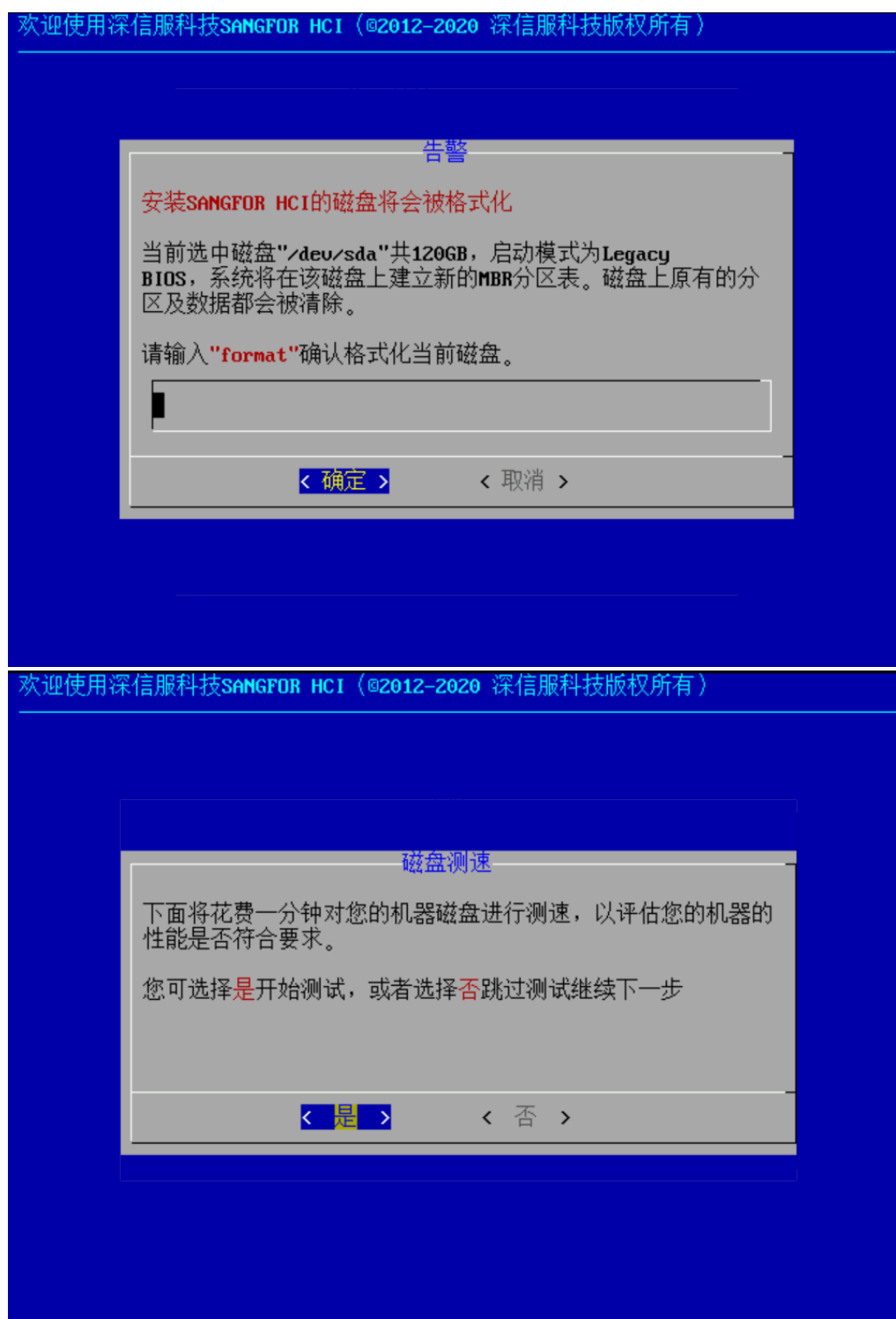
9. 选择安装位置磁盘，如果只有一块硬盘，直接点击<确定>。



⚠ 注意:

所选硬盘容量需要大于 60GB 才允许安装；硬盘大于 2T，建议用 UEFI 模式安装。

10. 选择磁盘后提示需要格式化硬盘数据，在输入框中输入**format**，再点击<确定>开始安装；如果硬盘数据需要保留，请选择<取消>回退到硬盘选择界面。选择磁盘后进行磁盘测速，如果不需要测速可以选择<否>进入下一步。



11. 系统安装完成后，提示配置网卡，选择要配置的网卡，选择<确定>，按“ENTER”键，进入设置界面。

⚠ 注意:

跳过网卡设置会给 eth0 自动设置一个默认 IP: 10.250.0.7; 子网掩码 255.255.255.0; 如果多台设备都没有配置网卡, 则会因默认 IP 一样导致 IP 冲突。



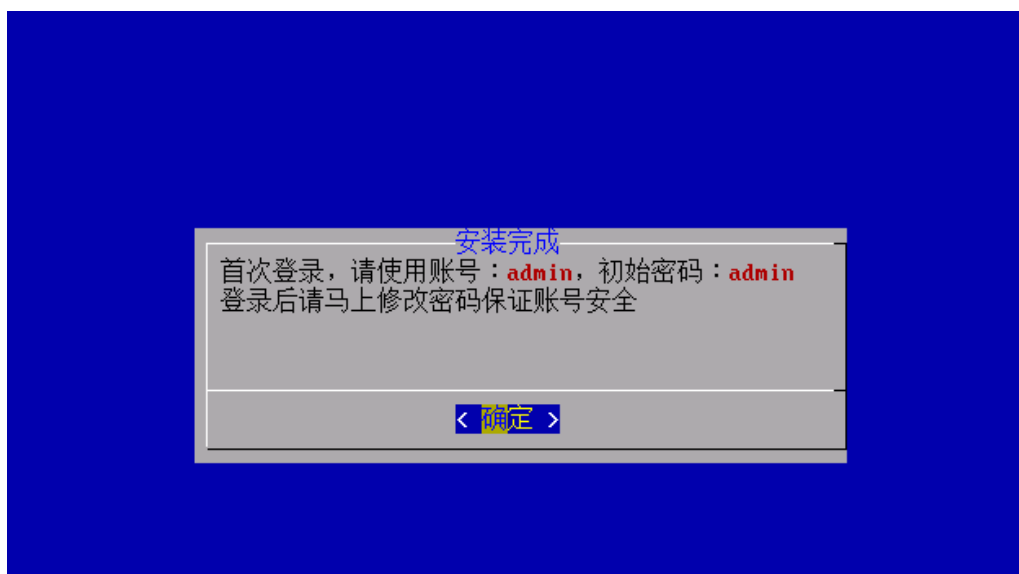
12. 设置网卡IP、子网掩码、网关, 点击<OK>。



⚠ 注意:

默认网关只能设置到一张网卡上; 网关需要与配置 IP 在同一个网段内, 否则会报错。

13. 单张网卡设置好后，提示是否继续设置其他网卡，点击<是>，返回网卡选择界面；点击<否>则安装完成。



14. 安装完成后，点击<Reboot>，重启设备，拔出U盘，安装完毕。



15. 浏览器通过URL地址：<https://配置的IP>，登录HCI的WEB控制台页面。

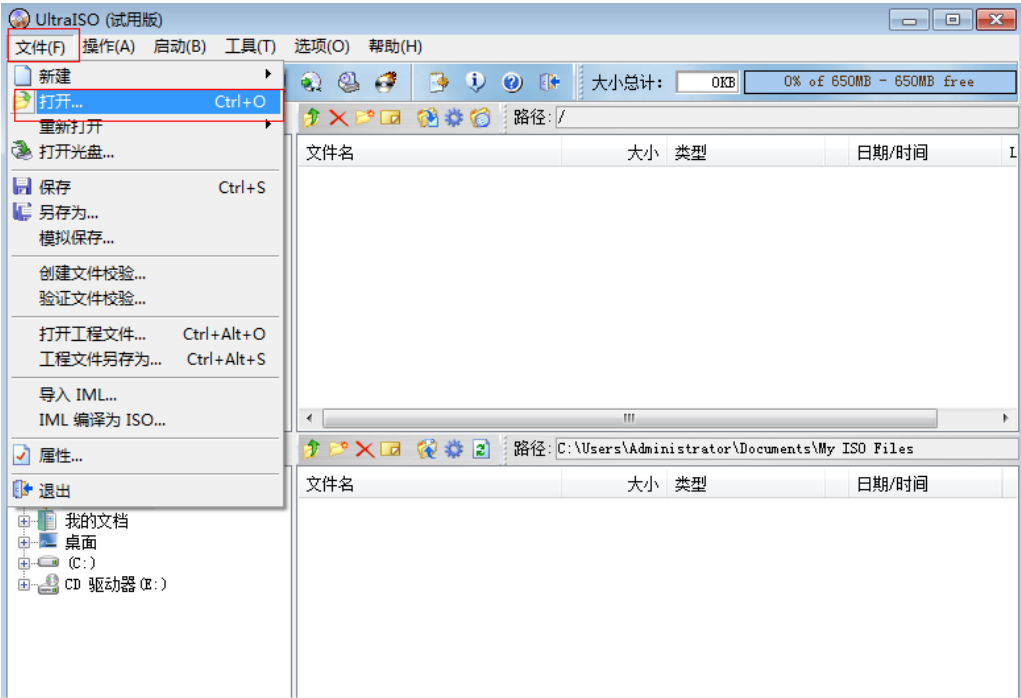
2.4.2.3. U 盘安装

注意事项

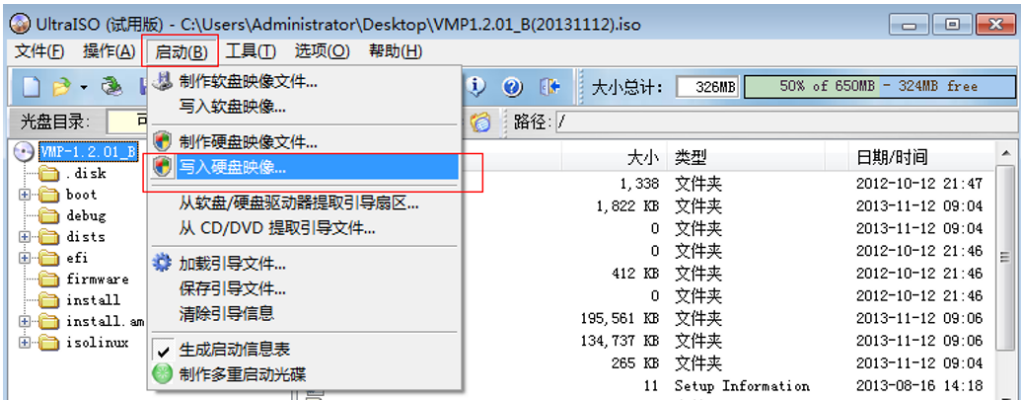
1. UltraISO请尽量使用最新版本。
2. U盘写入格式使用USB-HDD或USB-HDD+都可以，勾选刻录完成后校验。
3. U盘总空间要大于ISO文件。
4. 服务器配置、交换机配置需要满足本手册“[安装前准备](#)”章节中服务器和交换机的配置要求。

操作步骤

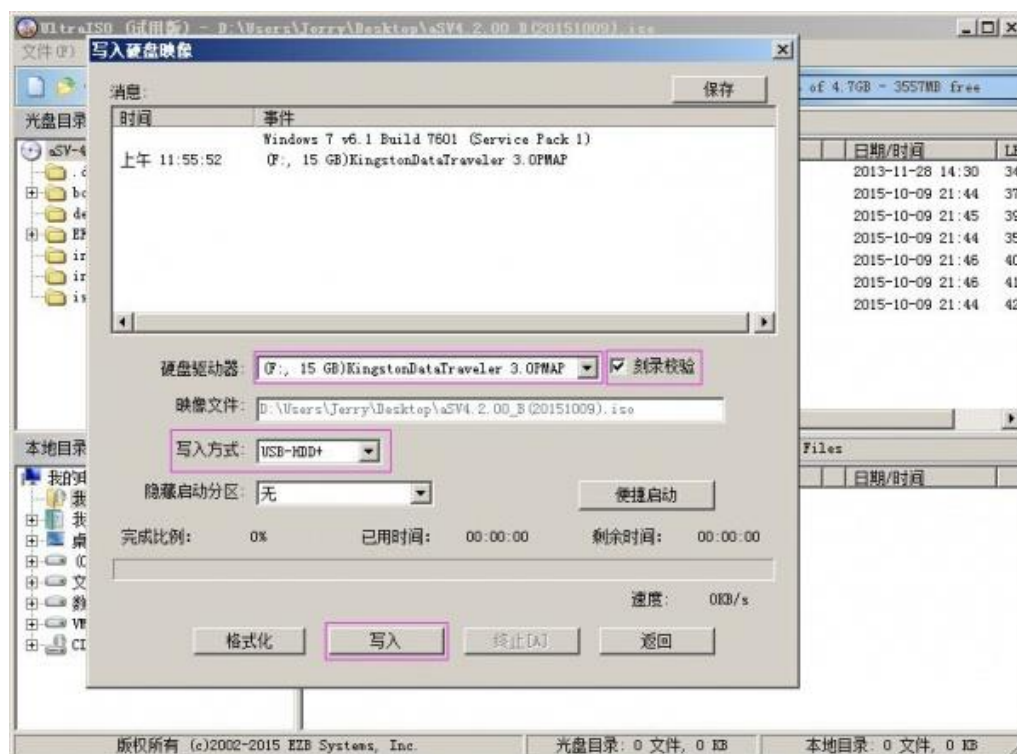
1. 首先在个人PC中插入U盘，然后打开软件UltraISO，选择[打开]，加载待刻录的超融合架构平台 ISO文件。



2. 然后点击 [启动/写入硬盘映像], 点击[写入], 其他默认。完成后关闭刻录软件, 把U盘拔出即可。



3. 写入的目标选择为U盘或光盘, 务必勾选“刻录校验”, 写入方式(通常USB-HDD+)根据服务器支持的USB启动类型决定。



4. 将U盘插到第三方服务器上，在BIOS中设置从U盘启动。
5. 后续HCI虚拟化系统安装过程请参考本手册“[ISO安装](#)”章节中的步骤，具体从步骤7开始。

2.5. 仲裁节点接入

2.5.1. 配置要求

参考“[仲裁节点配置要求](#)”章节。

2.5.2. aServer 一体机

aServer一体机出厂时已预装仲裁节点操作系统，并设置ETH0接口为管理接口，默认IP地址是10.250.0.7/24。使用PC配置同网段IP地址，直连ETH0口，用浏览器打开<https://10.250.0.7/>可以登录仲裁节点一体机的控制台。

默认的管理员账号和密码均为admin，首次登录会提示修改默认密码，使用一个月后强制修改默认密码。

首次登录成功后需要修改默认IP地址，且要求配置的IP地址和网关信息能与HCI集群通信。



2.5.3. 第三方服务器

功能说明

仲裁节点既可以是深信服aServer一体机，也可以采用第三方服务器安装仲裁节点，本章节介绍如何在第三方服务器上安装仲裁节点。

注意事项

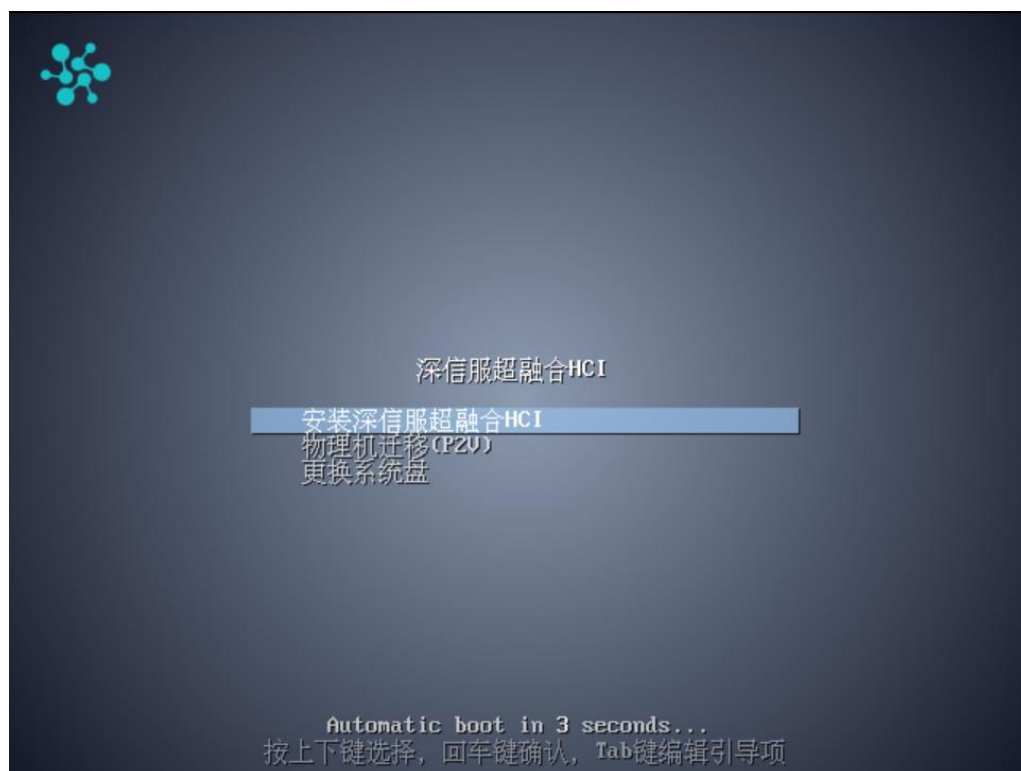
1. 可采用ISO方式安装或者U盘安装，前期的准备工作如U盘刻录、IPMI设置请参考本手册“[ISO安装](#)”章节。
2. 如果后续有集群扩容需求，也可以相应地调整仲裁节点的配置。

前提条件

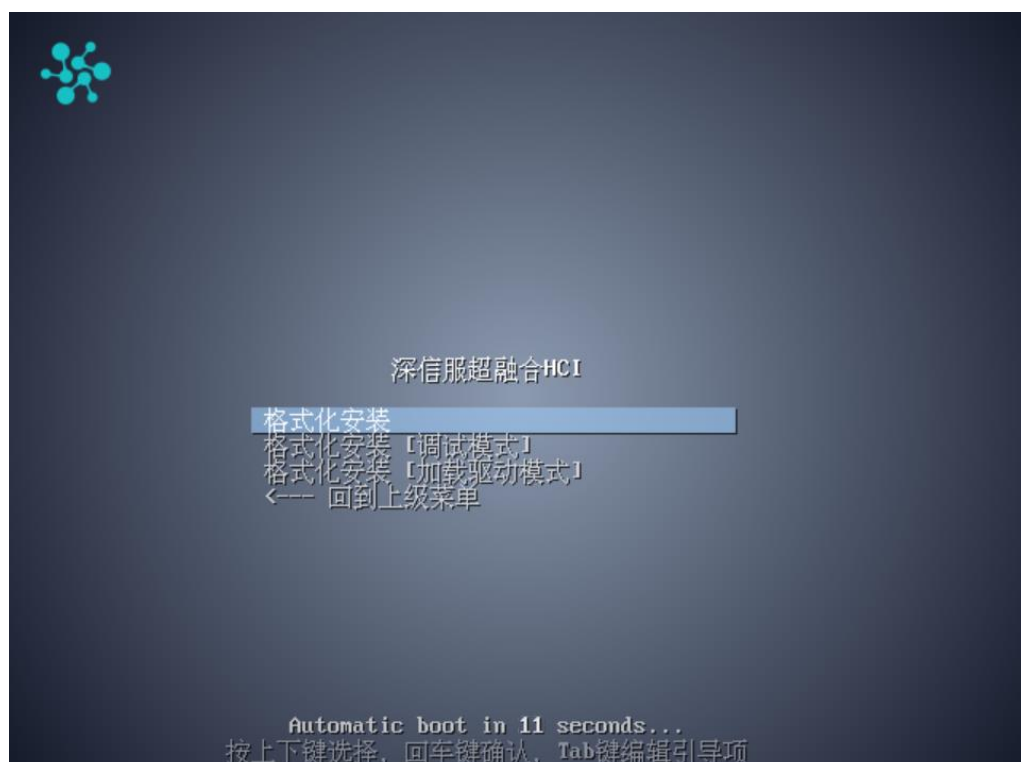
仲裁节点的硬件配置需满足本手册“[仲裁节点配置要求](#)”章节的配置要求

操作步骤

1. 如采用ISO安装，则加载仲裁安装包，选择从IPMI启动。如采用U盘安装，使用仲裁安装包制作好的U盘启动。得到如下页面，选择[安装深信服超融合（HCI）]，按“ENTER”键，进入安装界面。



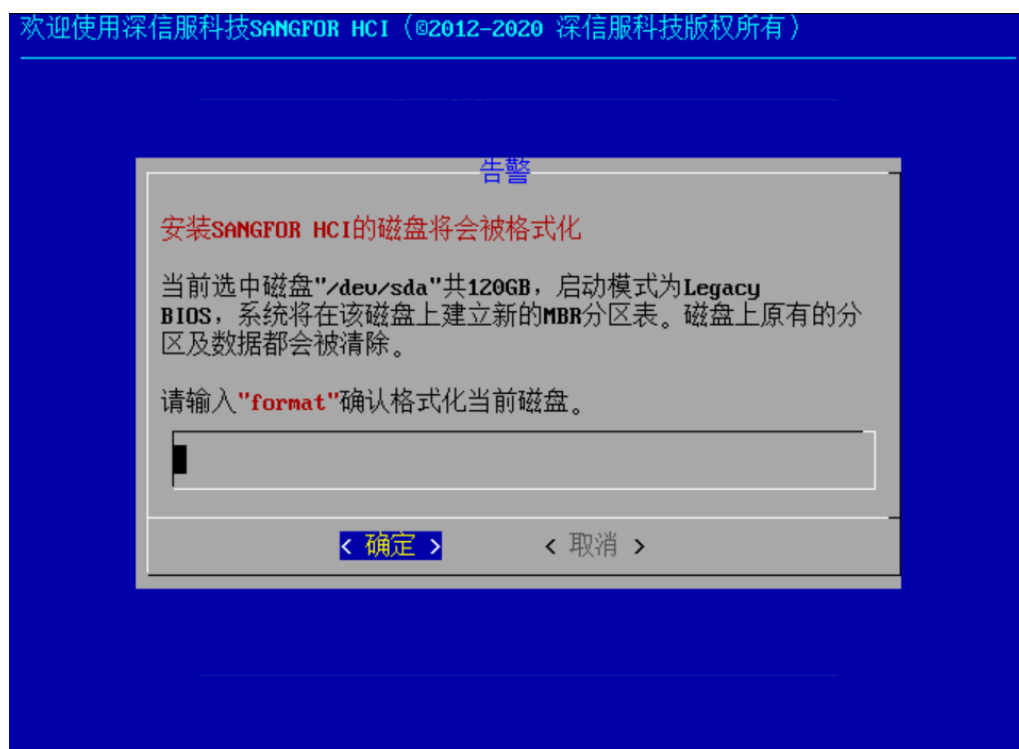
2. 选择[格式化安装], 按“ENTER”键, 进入解压安装。

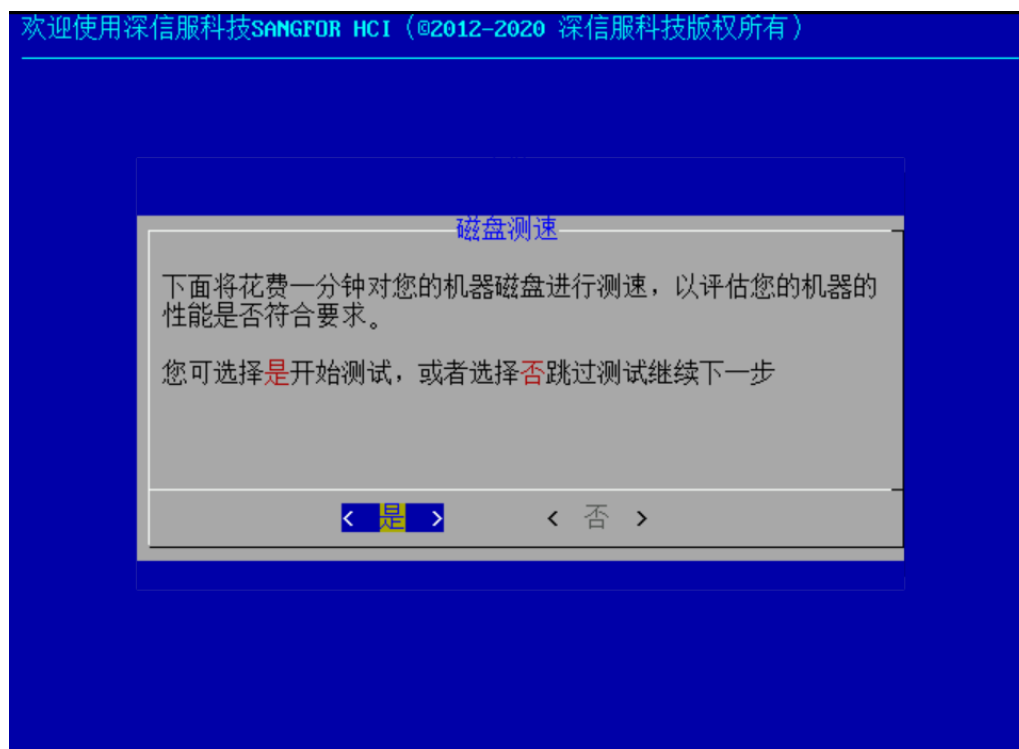


3. 选择安装位置磁盘, 选择后直接点击<确定>。



4. 选择磁盘后提示需要格式化硬盘数据，在输入框中输入**format**，再点击<确定>开始安装；选择磁盘后进行磁盘测速，如果不需要测速可以选择<否>进入下一步。





5. 系统安装完成后，提示配置网卡，选择要配置的网卡，选择<确定>，按“ENTER”键，进入设置界面。



6. 设置网卡IP、子网掩码、网关，点击<确定>。设置时需要确保该地址能与HCI集群正常通信。



7. 单张网卡设置好后，提示是否继续设置其他网卡，点击<是>，返回网卡选择界面；点击<否>则安装完成。



8. 安装完成后，点击<重启>，重启设备，拔出U盘或者移除光盘，安装完毕。



9. 重启完成后，浏览器通过URL地址：<https://配置的IP>，登录仲裁节点的WEB控制台页面。

2.5.4. VMware 平台

功能说明

仲裁节点支持在已有的VMware环境上部署，以虚拟机的形式运行，本章节介绍如何在VMware平台上安装仲裁节点。

注意事项

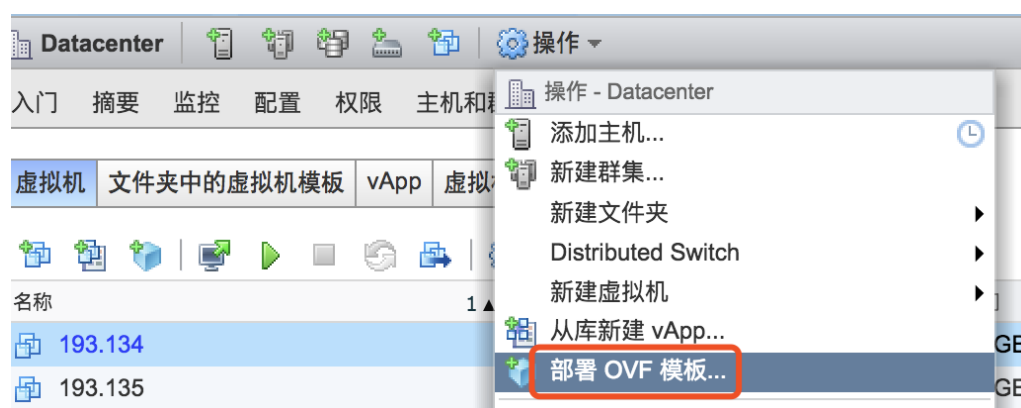
1. 支持VMware部署，暂不支持在HCI环境上部署。
2. 中型部署或大型部署场景不建议使用VMware虚拟化环境部署仲裁节点，仲裁节点硬件配置条件参考本手册“[仲裁节点配置要求](#)”章节。
3. 如果集群后续有扩容需求，需相应的在VMware虚拟化环境中调整仲裁节点的配置以适应扩容后的集群环境。

前提条件

使用的VMware版本必须是vCenter5.5及其以上版本。

操作步骤

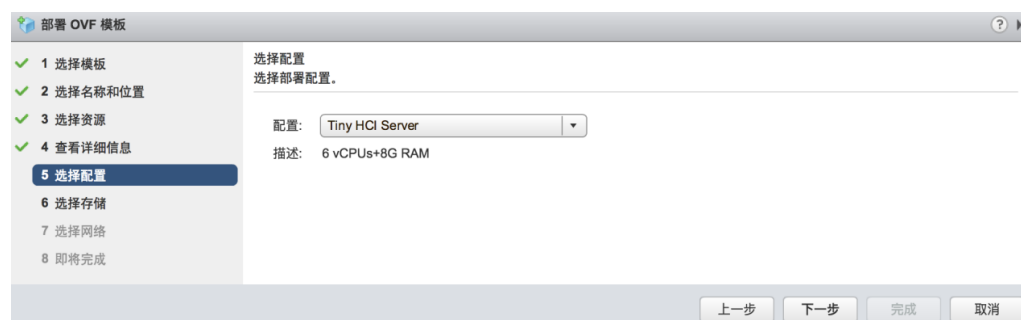
1. 在<操作>中点击[部署OVF模板]。



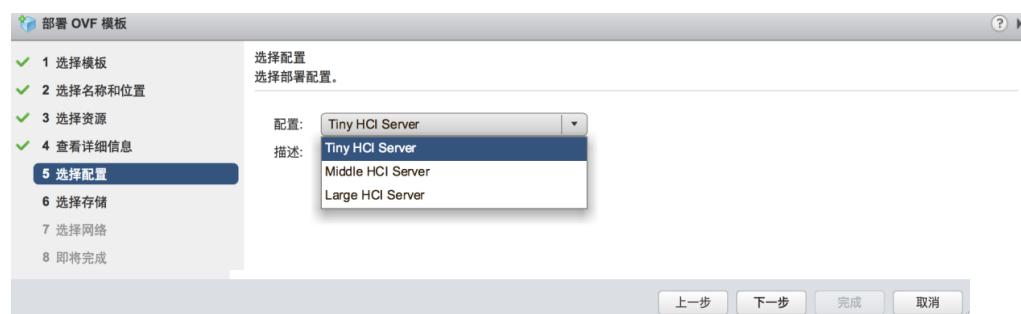
2. 在“本地文件”中，点击<浏览>，选择仲裁节点的OVF文件。



3. 按照默认配置[选择名称和位置]、[选择资源]，进入[选择配置]界面。



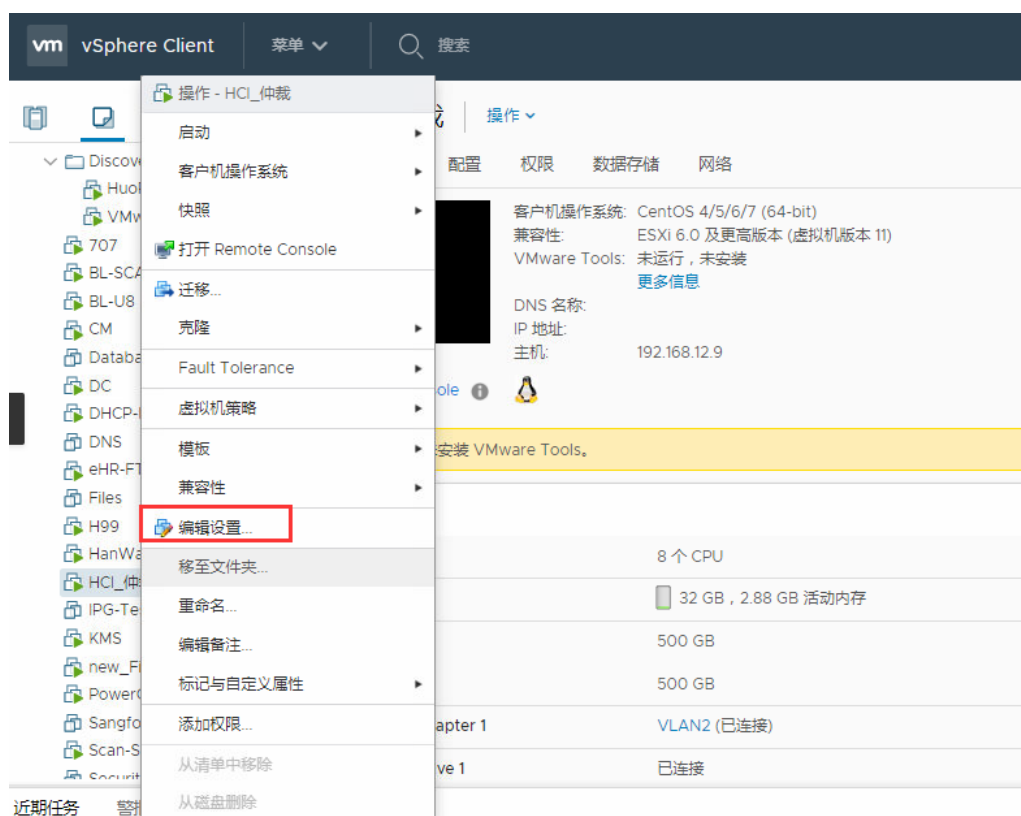
4. 根据集群规模选择合适的参数，可参考本手册“[超融合集群配置要求](#)”章节。
其中Tiny HCI Server表示配置6 vCPUs + 8G RAM，Middle HCI Server表示配置8 vCPUs+16G RAM，Larger HCI Server表示配置10 vCPUs+24G RAM。



5. 选择配置信息后，确认选择的配置，点<完成>，完成仲裁节点的部署。



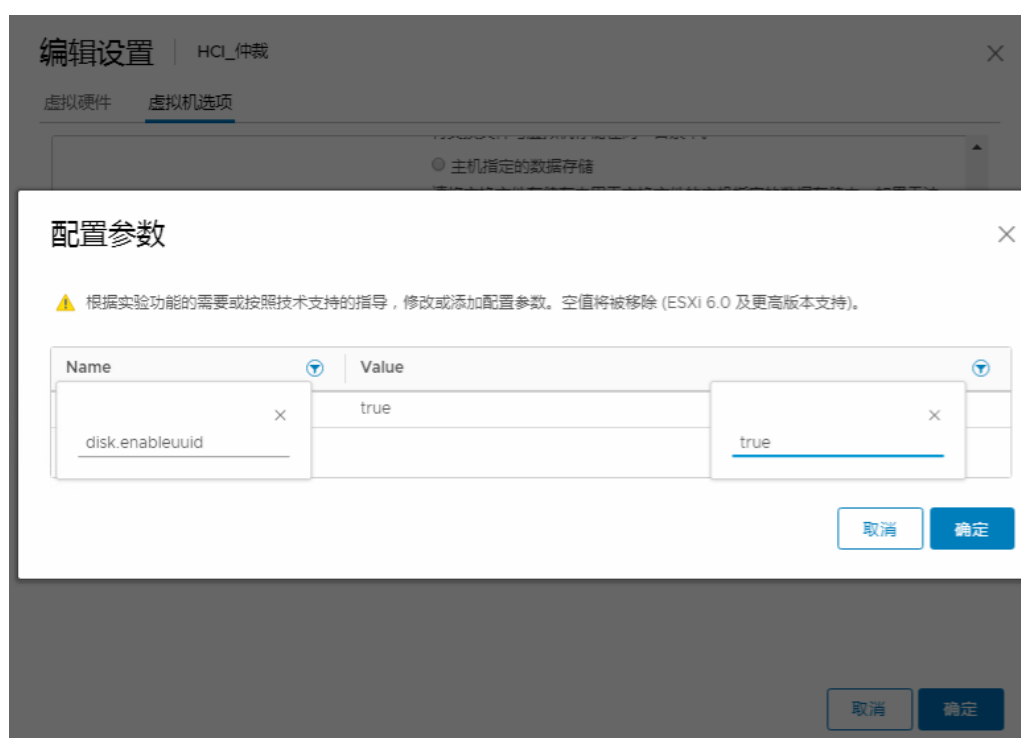
6. 导入虚拟机完成之后，编辑虚拟机设置。



7. 在[虚拟机选项/高级]中找到[配置参数]，点击[编辑配置]。



8. 配置参数写入Name: disk.enableuuid, Value: true, 点击<确定>完成配置。



2.6. 补丁升级

2.6.1. 补丁升级设置

功能说明

在线补丁服务，可定时从在线补丁平台获取最新的补丁资讯，保障设备的稳定性和安全性。

管理网络可以连接互联网的HCI设备，直接访问深信服在线补丁平台更新最新的补丁

资讯。管理网络在内网的HCI设备，如果虚拟机可以访问互联网，可以使用深信服网络代理虚拟机进行补丁更新；如果虚拟机网络无法连接互联网，可以使用第三方网络代理访问在线补丁平台；也可以在内网部署SP补丁服务器进行补丁更新。

注意事项

1. 配置完毕补丁服务必须测试连通性，确保平台可以连接到补丁服务器。
2. 不建议管理网可以直接访问在线补丁服务平台的方式，因为直接将HCI暴露到公网，不利于平台的安全。
3. 使用深信服网络代理虚拟机访问在线补丁平台模式，导入网络代理虚拟机后，请勿修改虚拟机名称（默认名称为：_SangforaOperation_VM_WorkStation_），否则会导致代理服务失效。

前提条件

客户网络需要放通深信服补丁服务器的地址update1.sangfor.net等，确保平台能访问到补丁服务器。

操作步骤

1. 进入[系统管理/补丁升级]界面，点击[补丁设置]页签。
2. 点击[查看在线补丁服务器的地址]确保补丁服务器已在客户网络中放通。放通要求如下表所示。

补丁服务器地址	用途	放通要求
https://cloudbgcop.sangfor.com	云端服务地址	必须放通
http://update1.sangfor.net	在线补丁包平台地址	至少放通一个，建议放通多个
http://update2.sangfor.net		
http://update3.sangfor.net		
http://121.46.26.221		

3. 勾选“开启补丁服务”。
4. 勾选我已阅读并同意[隐私协议]。

☒ 开启补丁服务

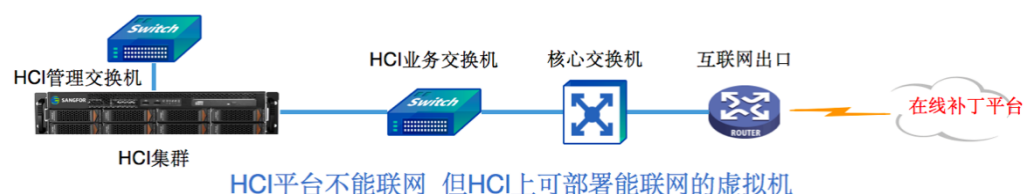
建议开启在线补丁服务，可定时从在线补丁平台获取最新的补丁资讯，保障设备的稳定性和安全性

☒ 我已阅读并同意 [隐私协议](#)

5. 根据HCI部署的场景和网络条件，选择一种合适的在线平台通信方式进行设置。（选择对应场景配置完毕后，直接跳过其他场景到步骤6进行配置）。

场景一：直接访问在线补丁平台。

- 通信方式设置选择[直接访问在线补丁平台]，点击<保存并测试连通性>，确认网络已连通。

**场景二：HCI平台不能联网，但HCI上可以部署能联网的虚拟机。**

- 下载虚拟机模板。
- 在在线补丁平台通信方式设置
- 查看在线补丁平台地址
- [新增虚拟机/导入虚拟机]，其中建议的设置项：开启故障迁移；存储位置使用共享存储；运行位置选择“自动选择”。



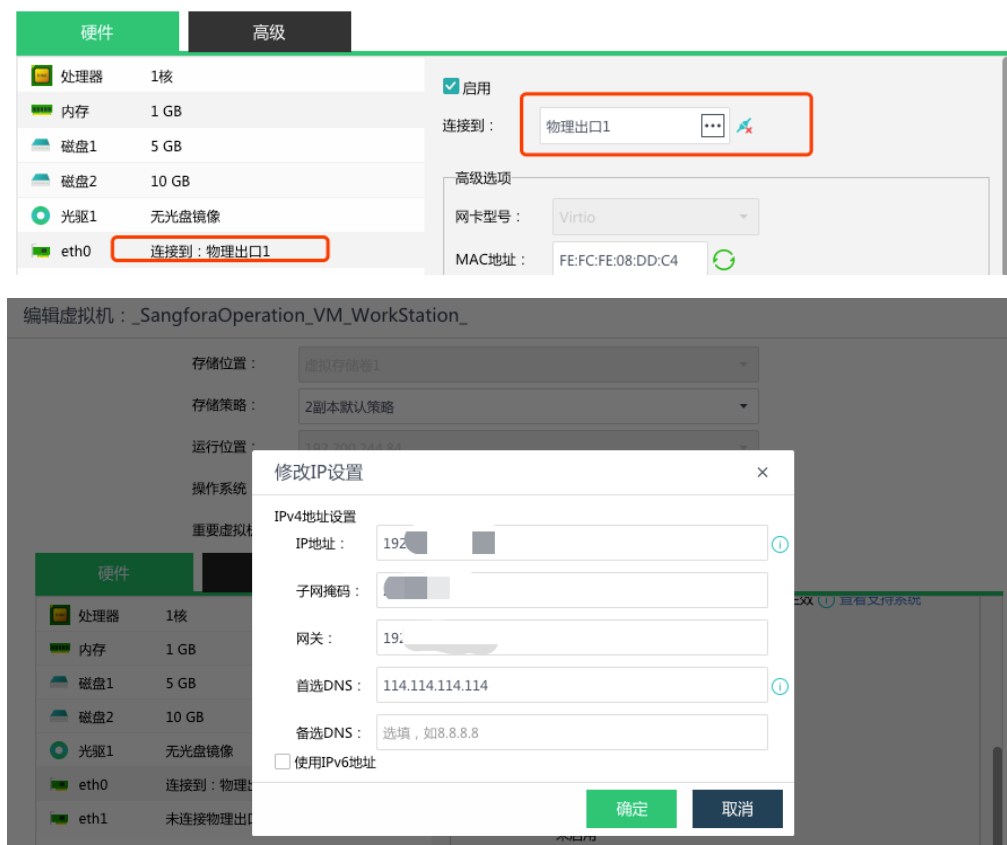
- 编辑虚拟机，查看高级配置，确认配置项：已勾选“开启 HA 功能”；已勾选“主机启动时，自动运行此虚拟机”。

编辑虚拟机：_SangforaOperation_VM_WorkStation_

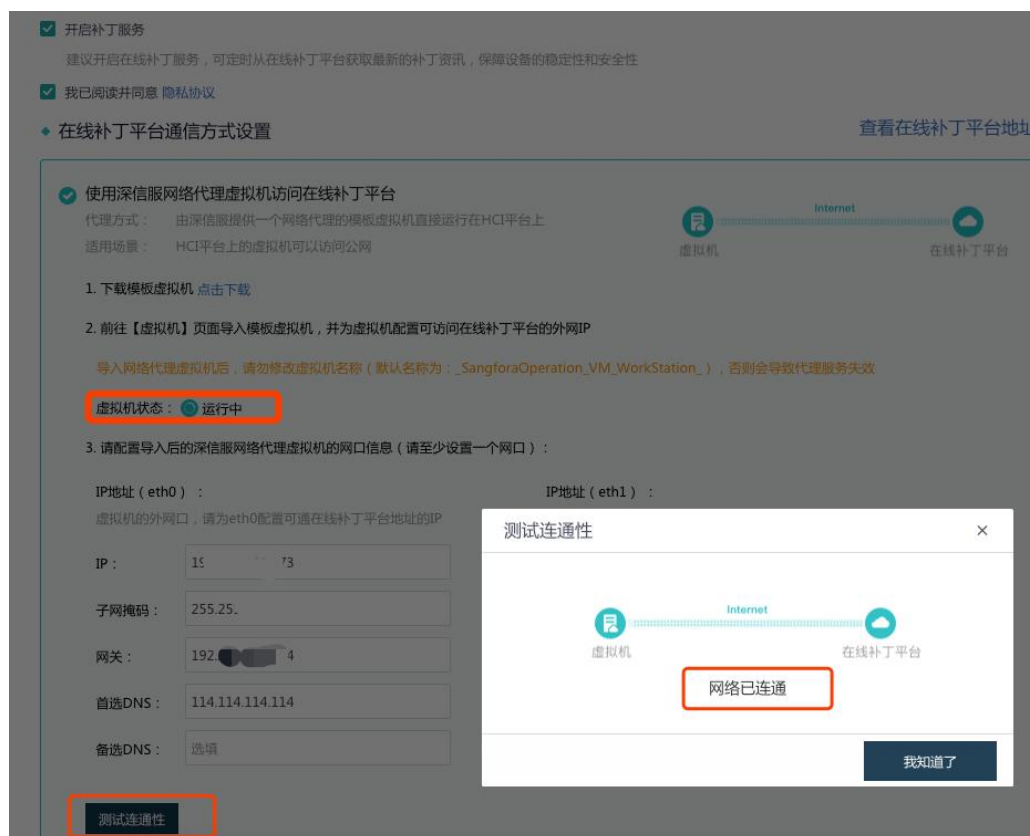
	名称：	_SangforaOperation_VM_WorkStation_
	分组：	默认分组
	标签：	请选择标签
	故障迁移(HA)：	☒ 当虚拟机所在主机出现故障时，自动切换到其它物理主机上运行。配置HA
	存储位置：	虚拟存储卷1
	存储策略：	2副本默认策略
	运行位置：	<自动选择>
	操作系统：	Linux 3.X/2.6 Kernel (64位)
重要虚拟机： ☒ 优先保障该虚拟机的资源使用和故障恢复，重启后生效		

硬件	高级
引导顺序：	1 磁盘1 2 光驱 3 无
生命周期：	☒ 无期限 ☐ 自定义使用到 2020-10-26
hostname：	使用系统默认hostname
其他选项：	☒ 主机启动时，自动运行此虚拟机

- 配置虚拟机 eth0 连接到物理出口，并确保该物理出口可访问外网。在页面修改 IP 设置，将规划好的地址配置给虚拟机，开启虚拟机。



- 如下图，在线补丁平台通信方式设置中，配置 eth0 的 IP、子网掩码、网关（选填）、首选 DNS（选填）、备选 DNS（选填），测试连通性，确保该 IP 可访问在线补丁平台地址。（eth1 是代理虚拟机的内网口，如有 NFV 设备则需要配置 eth1 网口用于连接 NFV 设备，配置方法参考 eth0 口的配置，与 NFV 设备所在网络连通）。



场景三：HCI平台不能联网，但通过第三方代理可进行联网。



HCI平台不能联网 但可 通过第三方代理进行联网

- 网络部署如上图，该场景选择使用第三方代理服务器访问在线补丁平台。



- 点击[<下载第三方代理程序部署指引>](#)，下载的内容为一个压缩包，名为“Proxy_Squid_Deployment_Guidance.rar”，里面包含文档说明以及推荐的代理程序安装包和配置文件等。
- 参考下载的配置指导，在代理服务器上安装和配置第三方代理程序，并确认代理服务器可以访问深信服在线补丁服务器。如下图所示部署 2 个网口，一个可访问到互联网连接到深信服补丁服务器，另一个网口可访问内网的超融合平台。

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr FE:FC:FE:2F:1B:B6
          inet addr:192.200.244.33  Bcast:192.200.244.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfc:feff:fe2f:1bb6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1533230 errors:0 dropped:43718 overruns:0 frame:0
          TX packets:58615 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:338489413 (322.8 MiB)  TX bytes:6926447 (6.6 MiB)

eth1      Link encap:Ethernet  HWaddr FE:FC:FE:B5:C0:EF
          inet addr:10.250.0.20  Bcast:10.250.0.255  Mask:255.255.255.0
          inet6 addr: fe80::fcfc:feff:feb5:c0ef/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:95080 errors:0 dropped:0 overruns:0 frame:0
          TX packets:230 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7877420 (7.5 MiB)  TX bytes:69578 (67.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

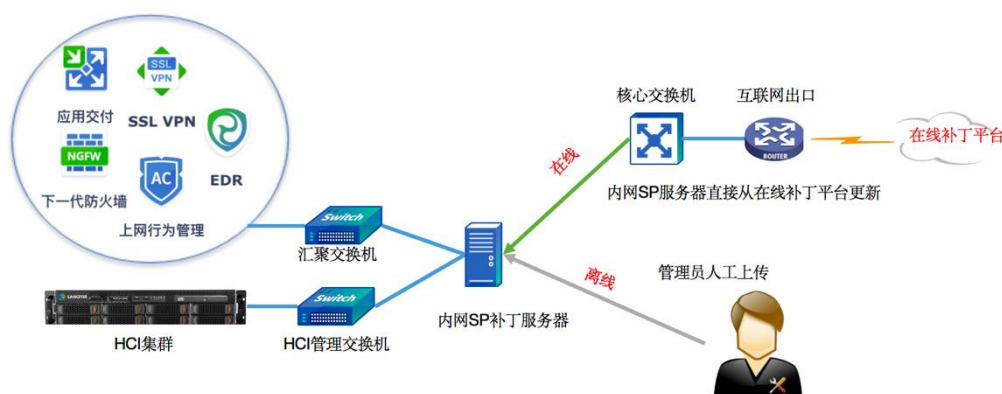
[root@localhost ~]# ping update1.sangfor.net
PING update1.sangfor.net.cdn20.com (113.96.140.206) 56(84) bytes of data.
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=1 ttl=54 time=8.04 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=2 ttl=54 time=8.44 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=3 ttl=54 time=7.52 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=4 ttl=54 time=8.19 ms
64 bytes from 113.96.140.206 (113.96.140.206): icmp_seq=5 ttl=54 time=8.55 ms
^C
--- update1.sangfor.net.cdn20.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 7.521/8.150/8.552/0.361 ms
[root@localhost ~]#
```

- 在 HCI 平台上填入第二步设置的代理的地址（IP+ 端口，示例：10.250.0.20:3128）。以及部署代理服务器过程中设置的代理的认证用户名和密码。
- 其中 IP 地址为代理服务器内网口 IP。
- 端口为代理服务的发布端口，默认为 3128。



- 点击<测试连通性>，确认网络已连通。

场景四：HCI平台不能联网，且本地数据中心已搭建了SP补丁服务器。



客户在数据中心本地部署了内网SP补丁服务器

客户使用了深信服多个产品，且无法联网，此时只需在数据中心中部署1台深信服内网SP补丁服务器，那么在离线更新补丁时，管理员仅需统一将补丁包上传至内网SP补丁服务器上即可，各个产品自行获取补丁包更新，无需管理员逐一登录多个产品平台进行升级。

客户使用了深信服多个产品，只需部署1台深信服内网SP补丁服务器，该服务器可充当在线补丁平台的统一代理进行联网，以及补丁包下载缓存分发至多产品。

- 该场景选择“使用本地搭建的SP补丁服务器”方式。



- 联系深信服技术支持获取离线补丁服务器的 vma 模板。

- 在[虚拟机\新增\导入虚拟机]导入离线补丁服务器的虚拟机。

从本地导入vma文件



① 虚拟机导入后默认使用QXL高性能显卡，如果开机后出现显示的异常，请通过手动切换显卡解决。

文件类型：

虚拟机文件：

分组：

故障迁移(HA)：☒ 当设备所在主机出现故障时，自动切换到其它物理主机上运行。配置HA ①

存储位置：

存储策略：

运行位置：

开始导入

- 导入完毕，点击<转到虚拟机>。点击<编辑>虚拟机。编辑网卡，连接到已经规划好的网络。
- 打开控制台，输入默认的用户名密码，admin/Sangforupdater。登录成功后系统会要求更改默认密码，请配置新密码。

```
CentOS Linux 8 (Core)
Kernel 4.18.0-193.el8.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login: admin
Password:
===== Sangfor offline updater =====

No address in config file, use 'ip address' command to add addresses

'help'      to show command list and help
'config show' to show current config

=====

CHANGING PASSWORD IS REQUIRED !!!

Changing password for user admin.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
Shell>
Shell> [ 126.865580] atkbd serio0: Unknown key pressed (translated set 2, code 0x0 on isa0060/serio0).
[ 126.865616] atkbd serio0: Use 'setkeycodes 00 <keycode>' to make it known.
[ 127.417693] atkbd serio0: Unknown key released (translated set 2, code 0x0 on isa0060/serio0).
[ 127.417736] atkbd serio0: Use 'setkeycodes 00 <keycode>' to make it known.
```

- 使用 `initsrv` 命令修改 IP 地址、掩码、网关、DNS。按 Y 保存配置会自动重启 olu 服务器完成配置。

```

Shell> initsrv
Valid ethernet interfaces:
[1] ens18  UP

Please select interface index[1-1]: 1
Input IP address of ens18, eg. 192.168.1.1/24: 10.250.0.10/24
Input default gateway, eg. 192.168.1.254: 10.250.0.1
Input DNS server, eg. 114.114.114.114: 114.114.114.114

Interface      : ens18
IP address     : 10.250.0.10/24
Default gateway : 10.250.0.1
DNS server     : 114.114.114.114

WARNING: System will reboot. confirm your config? [Y/N]

```

选择可用网口

配置IP地址/掩码

配置网关

配置DNS

确认生效，输入Y，重启服务器

- 确认网卡配置，检查网络的连通性。

```

Shell> ifconfig
ens18: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.250.0.10 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::fcfc:feff:fe2c:6a11 prefixlen 64 scopeid 0x20<link>
    ether fe:fc:fe:2c:6a:11 txqueuelen 1000 (Ethernet)
    RX packets 2792 bytes 171403 (167.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 54 bytes 2668 (2.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 66 bytes 6192 (6.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 66 bytes 6192 (6.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Shell> ping 10.250.0.20
PING 10.250.0.20 (10.250.0.20) 56(84) bytes of data.
64 bytes from 10.250.0.20: icmp_seq=1 ttl=64 time=0.925 ms
64 bytes from 10.250.0.20: icmp_seq=2 ttl=64 time=1.38 ms
64 bytes from 10.250.0.20: icmp_seq=3 ttl=64 time=1.83 ms

```

- 输入命令 `moashell`。弹出二维码，通过深信服口袋助理（MOA）扫描，在口袋助理“小助理”获取密码，输入到命令行。（需要深信服技术支持处理）。

```

Shell>
Shell>
Shell> moashell

```



```

Input password:
2ac8e137

```

- 创建 olu 服务器使用的用户并设置好密码，将 olu 用户的所属组改为 root。

```
[root@localhost ~]# useradd olu
[root@localhost ~]# passwd olu
Changing password for user olu.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
[root@localhost ~]# usermod -g root olu
[root@localhost ~]#
```

- 使用新加的 olu 账号登录补丁服务器，通过 sftp 工具上传 HCI 及 NFV 设备的补丁包到/var/wwwroot 目录，解压后即可在 HCI 补丁列表中查看。

```
[olu@localhost wwwroot]$
[olu@localhost wwwroot]$
[olu@localhost wwwroot]$ pwd
/var/wwwroot
[olu@localhost wwwroot]$
```

- Olu 服务器配置完毕，在 HCI 界面测试 SP 补丁服务器的连通性，填入 SP 补丁服务器的地址，点击<测试连通性>。



- 设置安全组件（aSEC）补丁服务（可选），选择“补丁服务的通信方式与HCI一致”。

◆ 设置安全组件（aSEC）补丁服务（可选）

选择方式：

需要将NFV设备网络连接至管理网的物理出口

- 建议用户填写紧急联系人（非必须）并在页面底部点击<保存>。

◆ 设置紧急联系人（可选）

我们会对紧急联系人的信息进行收集并保密，当平台出现严重高风险问题时，我们会与您主动联系协助解决，保障平台的安全

公司：	选填
联系人：	选填
电话：	选填
邮箱：	选填

保存

2.6.2. 补丁信息获取

功能说明

在[补丁列表]内可以查看到补丁的信息，包括：

- 补丁包名称，如：sp-xxx-xxx。
- 补丁包状态，如：未下载、正在下载、已下载、正在升级、已升级等。
- 补丁包描述，如：该补丁解决了 xxx 问题。
- 补丁包紧急度，如：高、中、低。
- 补丁前置条件，如：无、需关闭虚拟机。
- 补丁升级影响，如：无、网络会中断 xx 秒。
- 补丁发布时间，如：2020-10-20。
- 补丁操作，如：升级、重试。

补丁列表							
补丁名称	状态	描述	紧急度	升级前置条件	升级影响	发布时间	操作
sp-aCloud-5.8.6-5.8.6-8-em	已下载	SCP上手进阶HCI有损补丁包确认升级前测试	高			2020年8月10日	升级
sp-HCI-5.3.00-8-6.1.0_R1-te	已下载	test_sp-HCI-5.3.00-8-6.1.0_R1-test1	高			2020年8月10日	升级
sp-HCI-5.3.00-8-6.1.0_R1-te	已下载	sp-HCI-5.3.00-8-6.1.0_R1-test-20200902	高			2020年8月10日	升级
sp-HCI-5.3.00-8-6.1.0_R1-te	已下载	sp-HCI-5.3.00-8-6.1.0_R1-test-copy.pkg	高			2020年8月10日	升级
sp-aCloud-5.8.6-5.8.6-8-em	已下载	SCP上手进阶HCI有损补丁包确认升级前测试	高			2020年8月2日	升级

注意事项

1. 若平台能联网或通过网络代理虚拟机/第三方代理的方式最终能联网，可访问在线补丁平台地址，可以自动定时获取或者用户点击立即获取平台所需的补丁信息。
2. 若通信方式设置中选择的是“使用本地数据中心搭建的SP补丁服务器”，则是从该补丁服务器上自动定时获取或点击立即获取。

前提条件

无

操作步骤

1. 进入[系统管理/补丁升级]界面，查看[补丁列表]页签。
2. 点击[补丁升级设置]按钮，设置补丁升级的方式。

无感知补丁：

- 补丁升级时，对平台服务及虚拟机完全没有任何影响。
- 补丁升级选项：自动升级、手动升级。自动升级选择后，补丁将在每日 01:00AM - 06:00AM 自动升级。

有感知补丁：

- 补丁升级时，可能会对平台服务或虚拟机产生影响，因此必须由管理员确认补丁造成的影响后，自行选择合适的时间进行手动升级。
- 补丁升级选项：手动升级。

补丁升级设置

无感知补丁

补丁升级时，对平台服务及虚拟机完全没有任何影响

补丁升级选项：☒ 自动升级 ☐ 手动升级

选择后，补丁将在每日01:00AM - 06:00AM自动升级

有感知补丁

补丁升级时，可能会对平台服务或虚拟机产生影响，因此必须由管理员确认补丁造成的影响后，自行选择合适的时间进行手动升级

补丁升级选项：☐ 自动升级 ☒ 手动升级

确定

取消

3. 配置补丁升级选项后点击<确定>。
4. 点击[立即探测补丁]功能，可立即获取平台所需的补丁信息。



2.7. 终端检测响应平台 EDR 安装

功能说明

深信服终端检测响应平台EDR当前作为整体网络安全方案的重要一环，支持对超融合平台的病毒查杀、合规检查等，可对安全事件一键隔离处置以及热点事件IOC全网威胁定位，同时支持防病毒、入侵防御、防火墙隔离、数据信息采集上报等功能。

2.7.1. 安装 EDR 服务器

功能说明

深信服超融合平台HCI支持通过导入EDR虚拟机的形式安装EDR服务器，本章节介绍EDR服务器的安装。

注意事项

1. 目前仅支持使用EDR3.2.33_(20201229)定制版本进行安装。
2. 安装EDR服务器提供了vma格式的系统镜像与ISO格式的安装包两种方式，推荐使用vma进行部署，简便快捷。
3. EDR服务器配置建议如下表所示。

终端数	CPU（单位：核）	内存（单位：G）	硬盘（单位：G）
1-200	2	4	330
201-1000	4	8	330
1001-2000	8	16	330

2.7.1.1. VMA 格式安装

1. 通过admin用户登录HCI控制台，进入[虚拟机]页面，点击<新增/导入虚拟机>，选择vma镜像，确认好存储信息后点击<开始导入>按钮即可创建。

从本地导入虚拟机文件



① 虚拟机导入后默认使用QXL高性能显卡，如果开机后出现显示的异常，请通过手动切换显卡解决。

文件类型：

ova或vma

如需使用vhd、vhdx或者qcow2格式的镜像文件，请选择创建新的虚拟机，并在新建、编辑虚拟机磁盘时选择使用已有磁盘，挂载需要使用的镜像文件。

虚拟机文件：

请选择ova或vma格式文件

分组：

默认分组

故障迁移(HA)：

☒ 当设备所在主机出现故障时，自动切换到其它物理主机上运行。配置HA ①

存储位置：

虚拟存储卷1

存储策略：

2副本默认策略

运行位置：

<自动选择>

操作系统：

默认 ①

开始导入

2. 导入完成后点击EDR服务器虚拟机的[编辑]按钮，根据“[EDR服务器配置建议](#)”配置虚拟机的内存和CPU，默认配置为4核8G。

2.7.1.2. ISO 格式安装

1. 通过admin用户登录HCI控制台，进入[虚拟机]页面，点击<新增/新增虚拟机>，创建EDR服务器虚拟机。
2. 虚拟机配置：
 - 操作系统：CentOS
 - CPU：4 核
 - 内存：8G
 - 磁盘：330G
 - 光驱：选择 EDR 的 ISO 安装包
 - 网口配置需能够连通 HCI 集群内各个主机的管理网络

⚠ 注意:

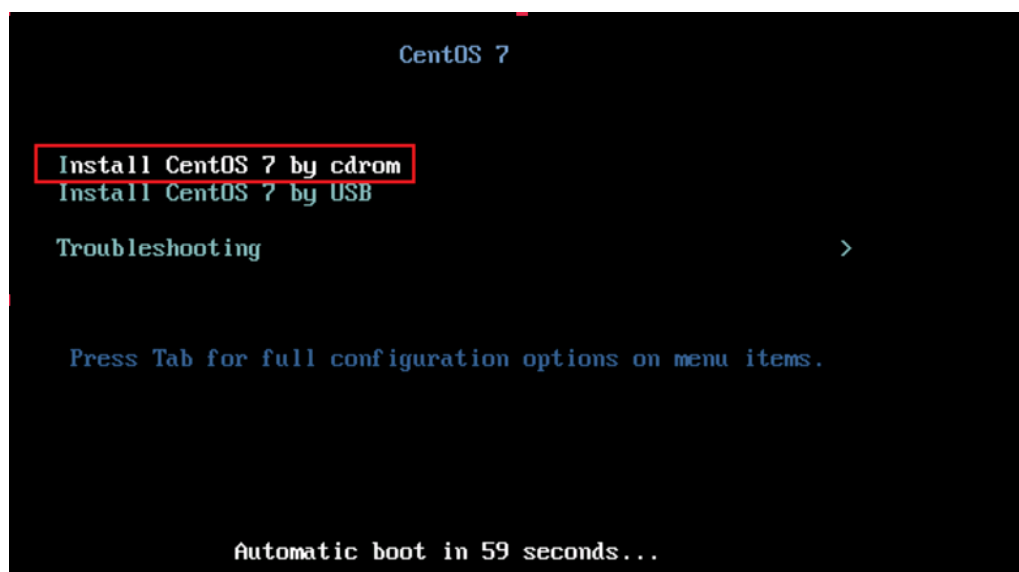
1. CPU 和内存配置参考“[EDR 服务器配置建议](#)”中的配置来选择即可。
2. 存储位置没有特殊要求，按需选择即可，建议优先部署在虚拟存储卷上。



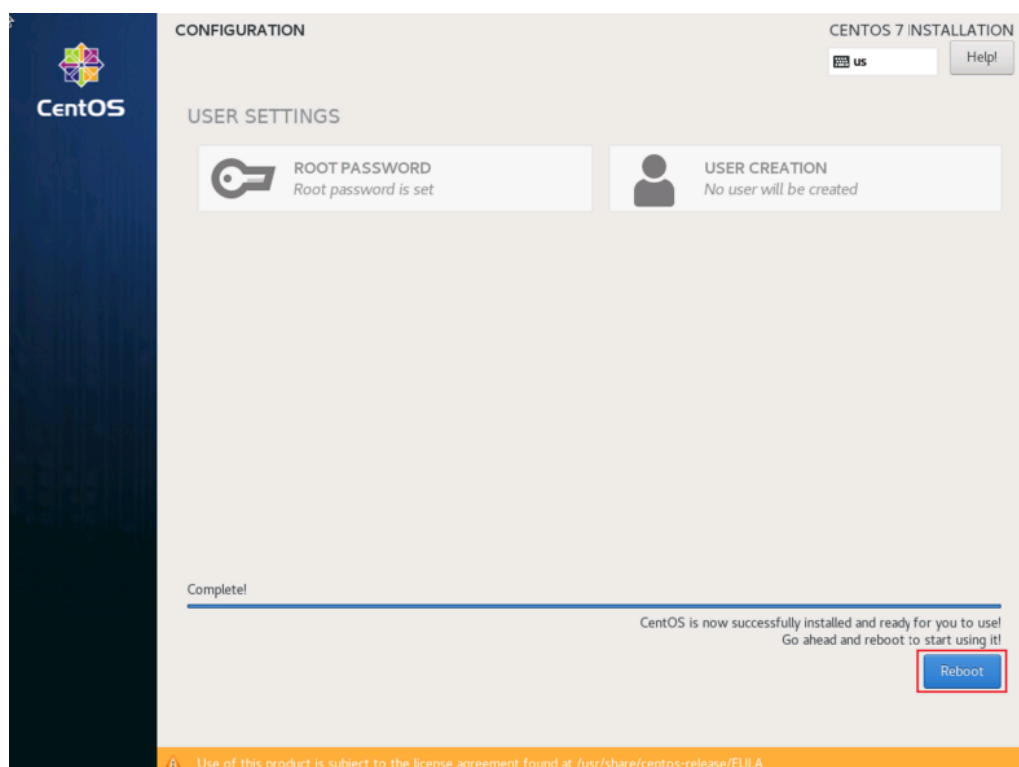
3. 虚拟机创建完成后，开机进行系统安装。点击EDR服务器虚拟机的<安装系统>按钮，进入虚拟机控制台。



4. 等待EDR自动进行安装即可。



5. 安装完成后点击<reboot>重启生效。



2.7.2. EDR 服务器授权

在浏览器输入<https://EDR服务端IP>，登录EDR服务端，默认用户名/密码：admin / admin。点击[系统管理/授权管理]，按照页面操作指引，导入授权文件完成授权。



2.7.3. 安装 EDR 客户端

功能说明

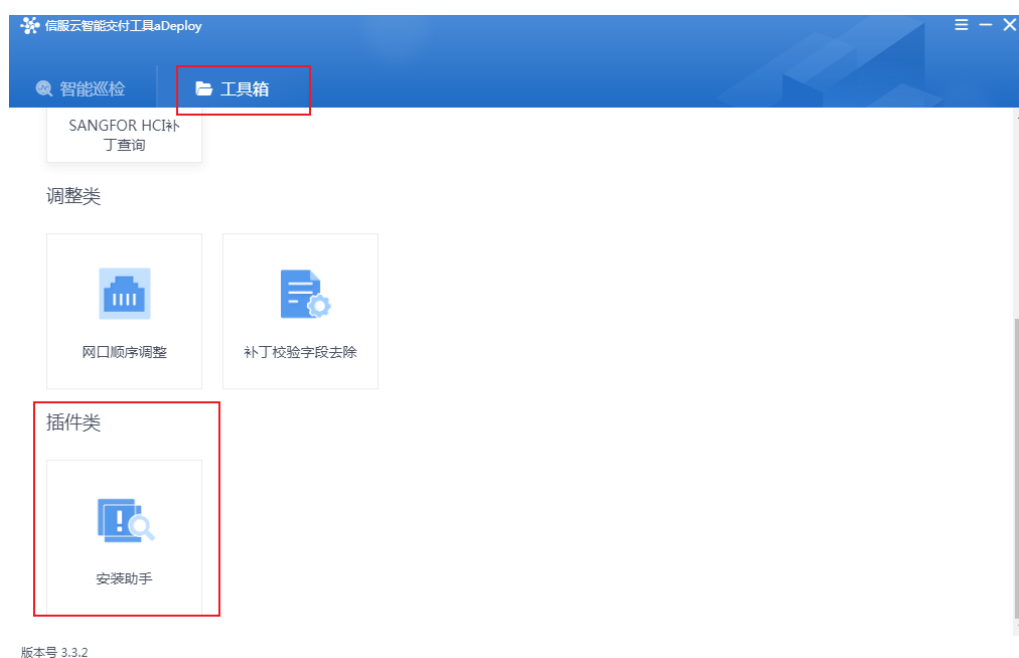
目前仅支持使用aDeploy巡检工具安装EDR客户端。

注意事项

安装EDR客户端时，aDeploy巡检工具会让HCI集群内所有主机都去下载客户端文件，占用部分管理网络的带宽，建议挑选业务空闲时间段进行安装。

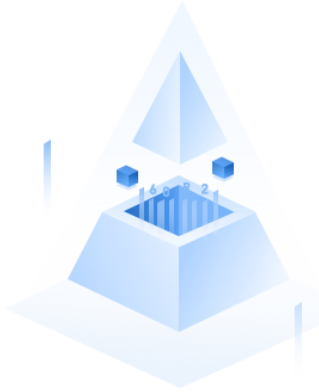
操作步骤

1. 下载并运行aDeploy巡检工具，进入[工具箱]页面，点击<安装助手>。



2. 输入HCI集群IP及登录密码，登入HCI。

 信服云智能交付工具aDeploy



安装助手

用于用于安装插件工具，如使用过程中有疑问，请联系深信服技术支持进行处理。

平台类型：

集群IP：

admin密码：

HTTPS端口：

SSH端口：

3. 输入EDR服务端IP，点击<开始安装>。

 信服云智能交付工具aDeploy

请填写相应信息进行安装操作：

工具名称	所需参数	操作	安装结果
EDR客户端	EDR服务端IP： 200.201.33.233	开始安装	
aOPS agent	运维平台IP地址： 请输入运维平台IP地址 agent版本号： 请输入agent版本号	开始安装	

4. 当安装结果栏出现“安装成功”，即完成了EDR客户端安装。

信服云智能交付工具aDeploy

×

请填写相应信息进行安装操作：

工具名称	所需参数	操作	安装结果
EDR客户端	EDR服务端IP： 200.201.33.233	安装成功	✓ 安装成功
aOPS agent	运维平台IP地址： 请输入运维平台IP地址 agent版本号： 请输入agent版本号	开始安装	

5. EDR客户端安装完成后，登录EDR服务端页面确认客户端是否成功安装。进入[终端管理/终端分组管理]，查看IP地址栏是否有HCI集群的主机IP，若可以看到，即表示客户端安装成功。

终端检测响应平台
Endpoint Detection and Response

首页

终端管理

威胁检测

响应中心

日志报表

系统管理

系统检测到admin账户未重命名或禁用，为了满足合规要求，建议您新增系统、安全、审计管理角色账户后，使用安全管理角色账户对admin默认账户进行重命名或禁用 [去配置>](#)

终端管理

终端分组管理

终端清点

终端发现

策略中心

终端分组

全部终端

本级中心

未分组终端

全部终端 (在线6/总数6)

移动策略

启用Agent

下发消息

刷新

终端类型

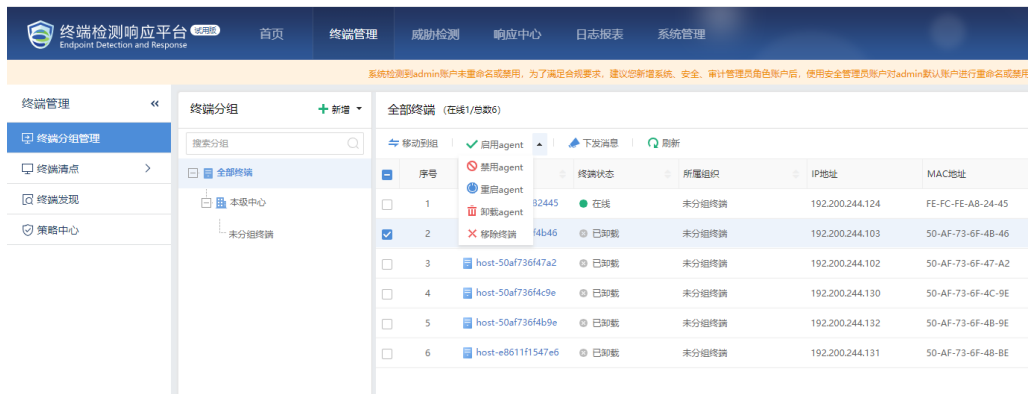
终端状态

终端名称或IP

序号	终端名称	终端状态	所属组织	IP地址	MAC地址	操作系统	系统CPU利用率
1	acmp-fefc...	在线	未分组终端	192.200.244...	FE-FC-FE-A8-24-...	CentOS Li...	25%
2	host-50af...	在线	未分组终端	192.200.244...	50-AF-73-6F-4B-...	x86_64	41%
3	host-50af...	在线	未分组终端	192.200.244...	50-AF-73-6F-47-...	x86_64	46%
4	host-50af...	在线	未分组终端	192.200.244...	50-AF-73-6F-4C-...	x86_64	45%
5	host-50af...	在线	未分组终端	192.200.244...	50-AF-73-6F-4B-...	x86_64	34%
6	host-e861...	在线	未分组终端	192.200.244...	50-AF-73-6F-4B-...	x86_64	26%

2.7.4. EDR 客户端卸载

若需要卸载EDR客户端，则登录服务端页面，进入[终端管理/终端分组管理]，选择对应客户端，点击上方<卸载Agent>按钮即可。



3. HCI 集群初始化

3.1. HCI 集群初始化条件

不管是创建普通集群还是延伸集群，在HCI的集群初始化流程中，授权激活、组建集群、数据通信口配置都是一样的，前提是需要将按照“[安装组网介绍](#)”章节的安装组网要求组网，然后进行集群初始化包括授权激活、组建集群、配置数据通信口，之后再根据实际情况配置虚拟存储，创建普通卷或是延伸卷。

HCI集群初始化有以下条件

1. 需要根据集群内所有主机的CPU颗数购买充足的授权。
2. 单主机不支持虚拟存储；普通集群至少要求集群内需要2台或以上的主机；如果需要虚拟存储的条带化功能或使用虚拟存储多卷功能，则集群内需要3台或以上的主机。
3. 延伸集群至少4主机起步，加上1个仲裁节点。在实际部署中，要确保页面配置的主机位置与实际物理位置一致，否则不能起到机房级别的保护作用。两个故障域机房必须二层打通，仲裁节点链路不需要二层打通，只需要网络可达即可。
4. 如果不使用虚拟存储，使用外置存储作为集群的存储，则需要使用的外置存储支持共享（多台主机同时访问），支持VAAI特性（主要指ats属性），否则无法添加共享存储。
5. 建议生产环境和测试环境独立搭建不同集群。
6. 建议单集群不超过24台主机。
7. 禁止单台主机部署HCI。
8. 序列号检查：序列号有效期如果低于一年，提醒用户及时续约。
9. 一键检测：实施完必须做，排除所有故障风险项。
10. aDeploy巡检工具检测：实施完必须做，排除所有故障风险项。

3.2. 组建集群

3.2.1. 配置集群 IP

用户可以通过集群IP来访问虚拟化平台，以及管理集群资源。在初始部署时，虚拟化系统会从集群主机中选择最早加入的三台物理主机成为控制节点，将第一台主机

设置为“主控”作为平台管理主机并配置集群IP，当该主机故障时，主控可以切换到其他控制节点运行，依然可以继续使用集群IP。

通过进入 [管理/集群配置] 页面，配置集群IP。

集群IP作用是在主机离线后，可以通过集群IP来管理虚拟机资源，通过[系统管理/集群配置]，配置集群IP。

⚠ 注意:

集群 IP 与主机网卡 IP 不能配置为相同 IP，否则会 IP 冲突。



3.2.2. 配置集群时间

操作步骤

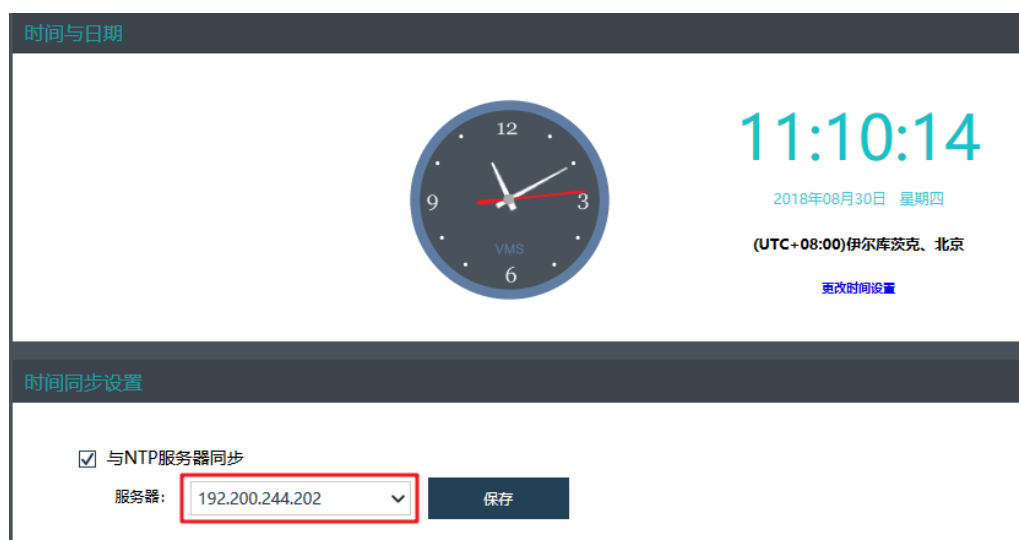
1. 在控制台中点击[系统管理/日期与时间]进入[日期与时间]页面，对比HCI集群时间是否准确。如果时间不准确，点击[更改时间设置]，进入平台时间设置页面。



2. 修改集群时间可以通过点击三角形对时间进行微调，也可以通过获取本地电脑的时间来配置平台的时间。同时也可以修改平台的时区。



3. 如果让平台时间与内部NTP服务器进行同步，只需要勾选“与NTP服务器同步”，同时修改服务器的IP地址保存即可。



3.2.3. 配置告警通知（可选）

操作步骤

1. 进入配置界面：打开控制台，进入[系统管理/告警日志/告警通知]。根据需要勾选“发送到指定邮箱地址”或者“发送到指定手机号码”，设置前需要设置邮件服务器或短信服务器。

管理 > 告警日志

告警日志

告警设置

告警通知

告警通知

☒ 发送到指定邮箱地址

✓ 已配置邮件服务器 修改配置

邮箱地址：

111.111.111.111

一行一个邮箱地址，最多支持设置5个

发送测试邮件

通知内容：

☒ 紧急告警

通知时间：

☐ 实时发送

☒ 定时发送（同一告警事件

15分钟

发送一次

☒ 普通告警

通知时间：

☐ 实时发送

☒ 定时发送（同一告警事件

6小时

发送一次

☒ 发送到指定手机号码

⚠ 当前未配置短信服务器，将导致无法收发短信，请尽快配置。立即配置

手机号码：

请输入接收短信通知的手机号码

一行一个手机号码，最多支持设置10个

发送测试短信

通知内容：

☒ 紧急告警

通知时间：

☐ 实时发送

☒ 定时发送（同一告警事件

15分钟

发送一次

☒ 普通告警

通知时间：

☐ 实时发送

☒ 定时发送（同一告警事件

6小时

发送一次

保存修改

2. 发送到指定邮箱：勾选“发送到指定邮箱地址”，如果没有配置邮件服务器，则点击[立即配置]。如果已经存在配置需要修改配置，点击[修改配置]。并填入邮件服务器的配置信息，点击<确认>保存设置。根据需要填写邮件服务器可送达的邮箱地址，根据需要勾选触发告警通知的条件，点击<保存修改>完成配置。

文档版本 06（2023-02-21）

79

配置邮箱服务器

发件人邮箱:

SMTP服务器地址:

端口:

☐ 服务器要求安全连接 (SSL)

☒ 发送服务器要验证用户名和密码

用户名:

密码:

[确认](#) [取消](#)

管理 > 告警日志

告警日志 告警设置 告警通知

告警通知

☒ 发送到指定邮箱地址 [勾选启用](#)

☒ 已配置邮件服务器 [修改配置](#)

邮箱地址:
 [支持填入多个接受告警信息的邮箱](#)

一行一个邮箱地址，最多支持设置5个 [发送测试邮件](#)

通知内容: ☒ 紧急告警 ☐ 实时发送 ☒ 定期发送 (同一告警事件 15分钟) 发送一次 ☐
☒ 普通告警 ☐ 实时发送 ☒ 定期发送 (同一告警事件 6小时) 发送一次 ☐

通知时间: ☐ 实时发送 ☒ 定期发送 (同一告警事件 6小时) 发送一次 ☐

[触发告警通知的条件设置](#)

☐ 发送到指定手机号码

[当前未配置短信服务器，将导致无法收发短信，请尽快配置。立即配置](#)

手机号码:

一行一个手机号码，最多支持设置10个 [发送测试短信](#)

通知内容: ☒ 紧急告警 ☐ 实时发送 ☒ 定期发送 (同一告警事件 15分钟) 发送一次 ☐
☒ 普通告警 ☐ 实时发送 ☒ 定期发送 (同一告警事件 6小时) 发送一次 ☐

通知时间: ☐ 实时发送 ☒ 定期发送 (同一告警事件 6小时) 发送一次 ☐

[保存修改](#)

3. **发送到指定手机号码：**勾选[发送到指定手机号码]，如果没有配置短信服务器，则点击[立即配置]，如果已经存在配置需要修改配置，点击[修改配置]。填入短信服务器的配置信息，点击<确认>保存设置。在短信服务器配置遇到问题时，可以通过点击[点此下载]按钮下载指导文档。根据需要填写接收短信的手机号码，

根据需要勾选触发告警通知的条件，点击<保存修改>完成配置。

配置短信服务器

工作方式配置

工作方式：

☐ 通过设备内置短信模块发送

☒ 通过安装在外部服务器上的短信模块发送

短信发送程序及指导文档：[点此下载](#)

服务器地址：

192.200.251.222

服务器端口：

8787

服务器配置

短信平台类型

中国移动V3

服务器配置指导文档[点此下载](#)

短信网关服务器地址：

短信网关服务器端口：

7890

企业代码：

业务代码：

SP接入号：

网关编号：

登录账号：

登录口令：

确认口令：

确认

取消

☒ 发送到指定手机号码

勾选启用

当前未配置短信服务器，将导致无法收发短信，请尽快配置。[立即配置](#)

手机号码：

15288888888

15200006666

填写接收告警短信的手机号码

一行一个手机号码，最多支持设置10个

发送测试短信

通知内容：

☒ 紧急告警

通知时间：

☐ 实时发送

☒ 定期发送（同一告警事件

15分钟

发送一次

☒ 普通告警

通知时间：

☐ 实时发送

☒ 定期发送（同一告警事件

6小时

发送一次

填写告警通知的触发条件

保存修改

3.2.4. 添加主机

注意事项

1. 超过24台主机的集群规模，建议将性能较好的硬件作为控制节点的主控。
2. 将两主机扩容到三主机以上，虚拟机必须关机，因为要建立仲裁机制。
3. 三主机以内先添加的主机必须是控制节点且在控制节点池内，其他主机可选是否加入控制节点池。

操作步骤

1. 通过[实体机/物理主机]中点击<添加主机>，新增主机入集群。



2. 选择要添加的主机，输入正确的主机admin认证密码后，主机图标由绿色勾选选中状态，表示允许被添加；点击<完成>，会提示是否重新配置所加主机的防火墙配置，执行主机添加任务。

添加物理主机

×

选择物理主机

[下载SANGFOR HCI \[redacted\]_B Build 20200929软件](#)

(以下是已经安装了SANGFOR HCI的物理主机，默认用户密码均是admin。添加主机自动开启远程主机的ssh端口（22），添加完成后端口启用情况与当前集群保持一致。)

需要认证



192.20[redacted]



2/2

上一步

完成

取消



- 主机添加完成后，在页面能够看到新添加主机。支持卡片和列表模式切换，其中卡片模式支持选择“资源使用率”和“资源负载”两种模式。



3.2.5. 设置控制节点资源池

功能说明

在超融合集群中，主机有控制节点和非控制节点的角色，控制节点可提供集群管理和计算，网络，存储等功能，如虚拟机调度，任务调度等，非控制节点可提供计算，网络，存储等功能，为实现集群管理节点的高可用，设置控制节点资源池，当控制节点故障时可在控制节点资源池内选择别的节点作为控制节点，实现节点高可用切换，保障集群管理功能的正常使用。

注意事项

1. 超过24台主机的集群规模，建议将性能较好的硬件作为主控。
2. 集群最多支持3个控制节点。
3. 主控仅能在控制节点池内切换，控制节点全部故障则无主控

操作步骤

1. 通过[实体机/物理主机]中点击<设置控制节点池>，新增主机入控制节点池。



2. 添加控制节点主机进入控制节点池，并设置其中三台主机为活跃状态。

设置控制节点池

① 当前集群存在延伸集群卷，请将主故障域和备故障域中**所有主机**添加到控制节点池，以满足延伸集群卷下控制节点的高可用。

+ 添加

🗑 移除

⚙ 高级设置

☐	主机IP	状态	所属故障域	控制节点状态	操作
☐	192.168.1.1	● 在线	主故障域	活跃 (主控)	-
☐	192.168.1.2	● 在线	主故障域	活跃	-
☐	192.168.1.3	● 在线	备故障域	活跃	-
☐	192.168.1.4	● 在线	备故障域	备选	设为活跃
☐	192.168.1.5	● 在线	备故障域	备选	设为活跃

添加聚合口 (200.201.202.71)

✔ 选择聚合的网口

2 配置聚合网口

3 确认配置

网口名称:

描述:

IP地址:

使用原eth1的IP

80.251.251.1

子网掩码:255.255.255.0

网关:

聚合网口工作方式:

LACP模式

使用MAC地址进行负载 (Mode: 4)

高级设置

使用MAC地址进行负载 (Mode: 4)

根据IP地址进行负载 (Mode: 4)

根据四层信息进行负载 (Mode: 4)

MTU:1500

MAC地址:fe:fb:fe:3f:77:7b

网口复用:☐ 开启存储通信口复用功能

上一步

下一步

取消

3.3. 管理通信口配置

场景说明

推荐使用聚合网口作为管理通信口，增加带宽的同时可以提升平台的网络稳定性。

注意事项

1. 使用聚合口时，对端交换机需配置对应的端口聚合模式，否则会导致网络不通，无法登录HCI管理界面。
2. 不支持对未插网线的网口进行聚合。
3. 不支持将两个不同角色的网口进行直接聚合，可将一个网口角色取消后再进行聚合。例：无法将eth0（管理口）和eth1（vxlan口）直接聚合，可将vxlan口调整为eth2，此时eth0（管理口）和eth1（无角色）可以聚合。
4. 目前聚合口LACP模式仅支持对接静态LACP协议。
5. 管理通信口禁止使用“根据网口轮询进行负载”。

操作步骤

1. 在HCI控制台中点击[实体机/物理网络]，点击<批量添加聚合口>，选择两个网口，例：eth0和eth1，聚合口工作方式支持选择“静态聚合”和“LACP模式”，优先推荐使用标准链路聚合，选择“根据四层信息进行负载”，如果不支持4层负载，则推荐根据MAC地址进行负载。



2. 在HCI控制台中点击[实体机/网口功能]。在网口角色中点击[管理通信口]，点击<修改配置>进入到配置页面，将管理通信口选择为添加的聚合口。

3.4. 数据通信口配置

注意事项

1. HCI集群部署后，需要为每台主机指定数据通信口。数据通信口要求使用千兆

（或万兆）网口，并使用千兆（或万兆）交换机互联。（只有两台主机时，可以将数据通信口直连）。为了提升数据通信口的接口带宽和冗余，推荐配置聚合口作为数据通信口，此时对端交换机需配置相应的聚合模式。

- 2. 数据通信口默认配置为复用集群管理口，为了获得较高的网络转发性能，建议将管理通信口和数据通信口(VXLAN)设置到不同的网口。
- 3. 不支持将两个不同角色的网口进行直接聚合，可将一个网口角色取消后再进行聚合。例：无法将eth0（管理口）和eth1（vxlan口）直接聚合，可将vxlan口调整为eth2，此时eth0（管理口）和eth1（无角色）可以聚合。
- 4. 目前聚合口LACP模式仅支持对接静态LACP协议。
- 5. 数据通信口禁止使用“根据网口轮询进行负载”。

操作步骤

- 1. 推荐使用聚合网口：在HCI控制台中点击[实体机/物理网络]，点击<批量添加聚合口>，选择两个网口，例：eth2和eth3，聚合口工作方式支持选择“静态聚合”和“LACP模式”，若为标准链路聚合，则推荐选择根据四层信息进行负载，若为交换机不支持四层负载，则推荐根据MAC地址进行负载。

物理主机	物理网络	网口功能	系统盘
刷新	批量添加聚合口	批量添加VLAN子网口	批量编辑网口
主机高级设置			
物理主机	网口名称	VLAN ID	网口功能
192.200.244.201	eth0	-	管理通信口、数据通信口
192.200.244.202	eth1	-	

- 2. 在HCI控制台中点击[实体机/网口功能]。在网口角色中找到数据通信口（VXLAN）点击<修改网口配置>进入到配置页面，可修改数据通信网口。

物理主机	物理网络	网口功能	系统盘
管理通信口	管理数据通信口	修改网口配置	网口规划指引
数据通信口 (vxlan)	数据通信口 (vxlan)	数据通信口 (vxlan)	数据通信口 (vxlan)
业务通信口			
存储通信口			
网络流量控制			
主机名称	网口名称	VLAN ID	网口功能
192.200.244.201	eth1	-	管理通信口、数据通信口
192.200.244.202	eth1	-	
192.200.244.212	eth2	-	
192.200.244.213	eth1	-	
192.200.244.214	eth1	-	

修改配置

刷新

批量修改

主机名称	数据通信口 (vxlan)	数据通信IP	掩码
192.200.244.201	 eth1	10.100.10.15	255.255.255.0
192.200.244.202	 eth1	10.100.10.12	255.255.255.0
192.200.244.212	 eth2	10.100.10.14	255.255.255.0
192.200.244.213	 eth1	10.100.10.11	255.255.255.0
192.200.244.214	 eth1	10.100.10.13	255.255.255.0

☐ 开启网口高性能模式（此操作会将网口的MTU设置为1600，需要在物理交换机上开启巨帧支持，否则会导致网络不通）

确定

取消

3. 在HCI控制台中点击[实体机/网口功能]。在网口角色中找到数据通信口（VXLAN）点击<管理数据通信IP池>进入到配置页面，可修改数据通信IP池。



管理数据通信IP池					
+ 创建 删除 修改数据通信端口 IP池描述/IP范围					
☐	IP池描述	IP范围	分配主机数	剩余可分配IP数	操作
☐	-	10.252.210.1-...	5	5	编辑 删除
10.252.210.1-10.252.210.10					
共1条, 当前1-1条 < 1 > 每页: 20 前往 1 页					

- **创建：**可创建数据通信 IP 池，一个集群内可存在多个数据通信 IP 池，一个主机仅允许加入一个数据通信 IP 池。
 - **删除：**可删除不再使用的数据通信 IP 池。
 - **修改数据通信端口：**可修改数据通信使用的端口号，端口号支持“8472、4789、4790”
4. 点击<创建>进行地址配置。在页面中输入数据通信IP所在的IP池以及子网掩码。IP池的范围必须大于等于主机数量。

编辑数据通信IP池

描述:

选填

数据通信IP:

10.100.10.11-10.100.10.20

掩码:

255.255.255.0

网关:

选填

如需跨三层数据通信，则请填写网关

主机:

系统将从IP池中为每台已选主机自动分配一个通信IP

待选 (0)

主机名称

☒

主机名称

☒

192.200.244.213

☒

192.200.244.202

☒

192.200.244.214

☒

192.200.244.212

☒

192.200.244.201

已选 (5)

清空

主机名称

操作

192.200.244.213

移除

192.200.244.202

移除

192.200.244.201

移除

192.200.244.214

移除

192.200.244.212

移除

确定

取消

- **描述：**描述创建的数据通信 IP 池信息。
 - **数据通信 IP 池：**主机 VXLAN 网络平面使用的 IP 地址，支持单个 IP 设置和范围设置，可多行设置，需保证所以地址为同一网段。
 - **掩码：**数据通信 IP 池中 IP 地址的掩码信息。
 - **网关：**如需跨三层数据通信，需填写三层网关。
 - **主机：**使用数据通信 IP 池中 IP 的主机。
5. 通过勾选[开启网口高性能模式]，会将HCI主机网口的MTU设置为1600字节，这样VXLAN封装的数据发到物理网络时，不会进行分片，能显著提升虚拟网络转发性能；此时对端的物理交换机需启用巨帧（Jumbo Frame）。

3.5. 虚拟存储配置

HCI主机组建为集群后，在[存储/虚拟存储]中点击<创建卷>。因为是首次组建虚拟存储，故而系统会自动提示配置存储私网。



3.5.1. 配置存储通信网络

注意事项

1. 由低版本升级到HCI6.8.0及以上的版本，存储通信网络聚合模式保持原有不变。
2. 全新部署存储通信网络推荐采用标准链路聚合模式部署。
3. 如果存储私网配置了标准链路聚合，暂不支持添加这个网口的静态路由，无链路聚合模式支持配置静态路由。
4. 存储通信口禁止使用“根据网口轮询进行负载”。

操作步骤

1. 在“虚拟存储/创建卷”弹出的提示界面中，点击<立即配置>，为集群各台主机间的存储通信配置部署方式。HCI集群默认使用ETH0作为管理网口和集群通信网口，用于同步HCI配置。存储通信网口用于同步虚拟存储的文件数据。两者建议使用不同的物理网口，标准集群推荐使用[标准链路聚合]方式组建存储通信网络，延伸集群推荐使用[标准链路聚合]方式组建存储通信网络。

部署模式：

- A. **标准链路聚合（推荐）**：通过在主机和交换机上配置网口聚合，可使主机通过虚拟存储网口连接第三方存储或第三方服务器，如使用2台交换机，交换机还需配

置成堆叠/M-LAG模式，网口工作模式建议选择成根据四层信息进行负载。

批量添加聚合口

④ 必须在连接的物理交换机上配置与聚合口工作模式对应的聚合参数，否则可能导致网口聚合后网络不通

添加聚合网口时不可修改IP，您可在添加成功后再进行编辑。所选的物理网口如果是管理通信口或数据通信口，生成的聚合网口将保留原网口的功能和IP配置。

如果选择了被业务通信、iSCSI等功能占用的网口，聚合时会导致其原有功能占用失效；在配置聚合后，请前往相应功能页面重新配置网口，恢复使用。

批量修改

主机名称	主机网口	聚合网口工作方式	IP地址	子网掩码	网关	存储口复用功能
192.200.244.201	eth0, eth5	使用主备模式工作 (M	使用原eth0的IP (192.200.244.201)	255.255.255.0	192.200.244.2...	不支持
192.200.244.202	eth3, eth5	根据四层信息进行负载	-	-	-	不支持
192.200.244.212	eth4, eth6	根据四层信息进行负载	-	-	-	不支持
192.200.244.213	eth3, eth5	根据四层信息进行负载	-	-	-	不支持
192.200.244.214	eth5, eth3	根据四层信息进行负载	-	-	-	不支持

确定

取消

- B. 无链路聚合：将存储数据通信的网络独立出来，对交换机无要求，普通二层交换机即可，也不需要交换机上作任何配置，但当某条链路故障时，会直接导致连接主机上的存储无法使用。
2. 每台主机使用两个网口进行存储通信，通信网口全都接到同一个二层交换机上。主机间存储通信网口会自行进行链路聚合（也需要交换机配置链路聚合）。选择存储通信部署方式后，需要按该部署方式的示意图进行接线，再选择每台主机对应的存储通信网口并配置通信网口地址。
3. 完成存储通信网口IP配置后，存储私网配置完成。

配置虚拟存储通信网络

1 选择虚拟存储通信网络部署模式

2 选择存储通信网口

存储通信网口 (查看当前存储部署方式)

主机名称	主机网口	聚合口IP	连接状态
172.17.1.1	eth2 (1000Mb/s) ,eth3 (1000Mb/s)	10.251.1.1 / 24	连接正常
172.17.1.2	eth2 (1000Mb/s) ,eth3 (1000Mb/s)	10.251.1.2 / 24	连接正常
172.17.1.3	eth2 (1000Mb/s) ,eth3 (1000Mb/s)	10.251.1.3 / 24	连接正常

2/2

上一步

完成

取消

配置虚拟存储通信网络

1 选择虚拟存储通信网络部署模式

2 选择存储通信网口

3 配置探测IP

根据物理主机能否ping通这个IP来判断主机是否被孤立 [详细说明](#)

建议网络连通性探测IP配置成路由器的IP，并保证此IP长期稳定在线。

网络连通性探测IP:

3/3

上一步

完成

取消

3.5.2. 创建卷

虚拟存储卷分为“普通卷”和“延伸卷”，当规划HCI集群为标准集群时，选择“普通卷”；当规划HCI集群为延伸集群时，选择“延伸卷”。

虚拟存储初始化时，无需选择副本数，同一个虚拟存储卷支持以虚拟机为粒度配置副本数，支持2副本和3副本。

集群主机数为三主机或4主机时，如果需要使用3副本，每台主机必须有2个硬盘组。
集群主机数为5主机及其以上时，无硬盘组限制。

192.20.1.1 2.1 TB/7.3 TB

硬盘组1:

硬盘组2:

一个硬盘组可以是SSD和HDD的混合配置，或纯SSD组成。如图，该主机有2个硬盘组。

3.5.2.1. 创建普通卷

注意事项

- 大集群的项目，建议使用多卷，建议每个卷的主机数在12台以内，尽量不要超过16台，例如集群48台主机，建议划分为4个卷，每个卷12来做。
- 不建议使用RAID卷来组建虚拟存储，因为其一般不支持热插拔。RAID应配置为

JBOD直通，如果不支持JBOD，禁用RAID，使用Non-RAID。

操作步骤

1. 配置存储卷类型：点击[存储/虚拟存储]打开虚拟存储页面，然后点击<创建卷>，选择卷类型为“普通卷”。



2. 选择物理主机：选择需要加入存储卷的物理主机。



3. 选择主机中要加入的硬盘。配置硬盘和硬盘组，然后为每个主机的每个磁盘进行详细用途规划。系统会对集群中所有主机的磁盘进行自动检测，默认选择机械磁盘作为数据盘，固态硬盘作为缓存盘。一般建议采用默认配置，也可以自

行修改。如果需要部署磁盘多卷，需要规划预留第二卷组的磁盘。

创建卷

×

选择存储卷类型

选择物理主机

3 选择硬盘

4 配置硬盘组

5 确认配置

请选择加入该卷的硬盘

已选择：固态硬盘8个 机械硬盘0个

快捷选择

✓	硬盘名称		磁盘类型	磁盘大小
✓	192.168.1.10			
✓	vdc	⚠	SSD	240 GB
✓	vdb	⚠	SSD	400 GB
✓	192.168.1.11			
✓	vdb	⚠	SSD	240 GB
✓	vdc	⚠	SSD	400 GB
✓	192.168.1.12			
✓	vdb	⚠	SSD	240 GB
✓	vdc		SSD	400 GB
✓	192.168.1.13			
✓	vdb	⚠	SSD	240 GB

上一步

下一步

取消

创建卷

×

选择存储卷类型

选择物理主机

选择硬盘

4 配置硬盘组

5 确认配置

全部展开

全部收起

配置硬盘组

硬盘组介绍 ⓘ

主机：192.168.1.10

数据盘：2

硬盘组	硬盘名称		硬盘类型	硬盘大小	硬盘用途
硬盘组1	vdb	⚠	SSD	400 GB	数据盘
硬盘组2	vdc	⚠	SSD	240 GB	数据盘

主机：192.168.1.11

数据盘：2

硬盘组	硬盘名称		硬盘类型	硬盘大小	硬盘用途
硬盘组1	vdc	⚠	SSD	400 GB	数据盘
硬盘组2	vdb	⚠	SSD	240 GB	数据盘

上一步

下一步

取消

4. 确认最终信息，成功创建卷。

创建卷

×

✓ 选择存储卷类型

✓ 选择物理主机

✓ 选择硬盘

✓ 配置硬盘组

5 确认配置

请确认普通卷 虚拟存储卷1 的配置信息：

4

2.5 TB

1.15 TB

788 GB

主机数

存储卷裸容量

2副本可用容量

3副本可用容量

存储卷信息：

主机名称	硬盘组数	数据盘数	数据盘裸容量
172.16.1.100	2	2	640 GB
172.16.1.101	2	2	640 GB
172.16.1.102	2	2	640 GB
172.16.1.103	2	2	640 GB

上一步

确定

取消

5. 确认配置：最后显示虚拟存储的配置结果信息，包括最终存储容量、副本数量和磁盘数量。确认配置无误后，需要输入管理员密码，点击<完成>以开始初始化虚拟存储。

3.5.2.2. 创建延伸卷

操作步骤

1. 配置存储卷类型：点击[存储/虚拟存储]打开虚拟存储页面，然后点击<创建卷>，选择卷类型为“延伸卷”。

创建卷

×

1 选择存储卷类型

2 选择物理主机

3 配置故障域

4 选择硬盘

5 配置硬盘组

6 确认配置

存储卷名称：

延伸卷

存储卷类型：

普通卷

延伸卷

数据中心A

数据中心B

延伸卷介绍
延伸卷用于构建双活数据中心，卷内的物理机部署在两个机房并配置成主、备故障域，数据的多份副本则会写入到两个故障域内，实现RPO=0的容灾效果。
配置要求
延伸卷需要配置单独的仲裁物理节点。

下一步

取消

2. 选择物理主机：选择需要加入延伸卷的物理主机，延伸集群需要至少4台主机，分别将2台主机设置在不同的故障域中。

创建卷

✓ 基本信息

2 选择物理主机

3 配置故障域

4 配置硬盘

5 确认配置

选择需要加入该卷的物理主机：

① 延伸集群至少需要4台主机，建议选择偶数台主机，让每个故障域的主机数相同。

已选中4台主机

☒	主机名称	主机IP	固态硬盘总数	机械硬盘总数
☒	192.20.1.101	192.20.1.101	4	0
☒	192.20.1.102	192.20.1.102	4	0
☒	192.20.1.103	192.20.1.103	4	0
☒	192.20.1.104	192.20.1.104	4	0

上一步

下一步

取消

3. 配置故障域：分别将需要的主机加入相应的故障域，本例中有四台主机，则两台主机加入主故障域，两台主机加入备故障域。

创建卷

✓ 基本信息

✓ 选择物理主机

3 配置故障域

4 配置硬盘

5 确认配置

仲裁节点IP： 请添加仲裁节点

添加仲裁节点

待分配主机：

主故障域： 建议以机房名称命名

☐ 192.20.1.101

☐ 192.20.1.102

备故障域： 建议以机房名称命名

☐ 192.20.1.103

☐ 192.20.1.104

上一步

下一步

取消

4. 添加仲裁节点：给主机房和备机房命名后，根据事先安装好的仲裁节点配置仲裁节点IP。按照向导输入密码确认配置仲裁节点，然后确认配置。

创建卷

×

✓ 基本信息

—

✓ 选择物理主机

—

3 配置故障域

—

4 配置硬盘

—

5 确认配置

仲裁节点IP： 请添加仲裁节点

添加仲裁节点

待分配主机：

主故障域： 建议以机房名称命名

①

☐ 192.168.144.254

☐ 192.168.144.255

备故障域： 建议以机房名称命名

①

☐ 192.168.144.254

☐ 192.168.144.255

上一步

下一步

取消

创建卷

×

✓ 基本信息

—

✓ 选择物理主机

—

3 配置故障域

—

4 配置硬盘

—

5 确认配置

仲裁节点IP： 请添加仲裁节点

添加仲裁节点

待分配主机：

添加仲裁节点

×

仲裁节点IP：

用户名：

admin

密码：

.....

确定

取消

上一步

下一步

取消

创建卷

✓ 基本信息

✓ 选择物理主机

3 配置故障域

4 配置硬盘

5 确认配置

仲裁节点IP：

192.168.1.100

添加仲裁节点

待分配主机：

H3

主故障域：

机房1

☐ 192.168.2.4124

☐ 192.168.2.4125

备故障域：

机房2

☐ 192.168.2.4126

☐ 192.168.2.4127

上一步

下一步

取消

5. 确认配置：确认故障域的配置，卷创建后不支持修改主机所在的故障域。

确认配置

⚠ 请确认故障域的配置是否跟主机在两个机房的实际部署一致，卷创建后，不支持修改主机所在的故障域，如果配置不正确，会导致双活功能不正常，例如：有一些数据块2个副本都写到同一个机房。

仲裁节点IP：

192.168.1.100

主故障域：

机房1

192.168.2.4124

192.168.2.4125

备故障域：

机房2

192.168.2.4126

192.168.2.4127

确定

取消

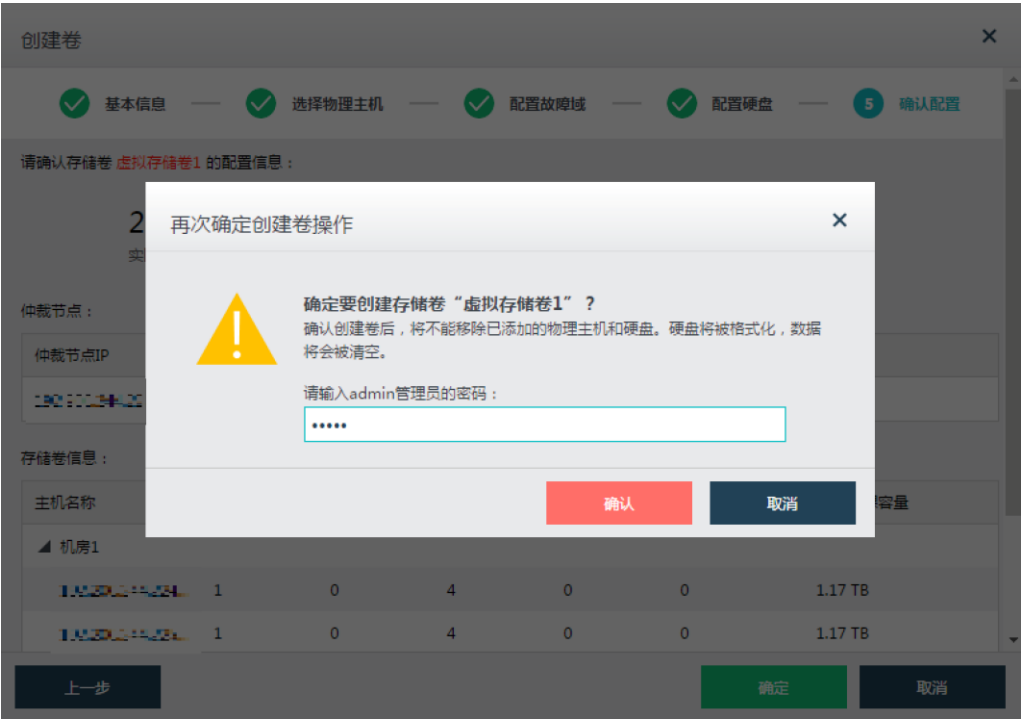
6. 配置硬盘：接下来需要规划磁盘用途。磁盘用途包括数据盘、缓存盘和热备盘。通常用SSD磁盘作为缓存盘，提升虚拟存储的IO性能。系统通常会根据配置自动推荐硬盘用途，默认按照系统推荐的配置即可。

文档版本 06（2023-02-21）

99



7. 确认配置：最后显示虚拟存储的配置结果信息，包括最终存储容量、副本数量和磁盘数量。确认配置无误后，需要输入管理员密码，点击<完成>以开始初始化虚拟存储。



3.6. 终端通信口配置（可选）

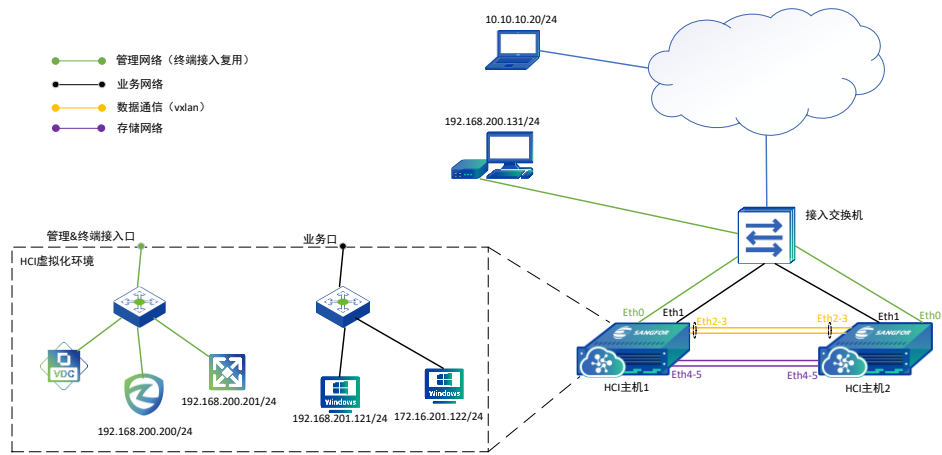
功能说明

适用于VDI场景，平台支持单独为桌面云业务规划终端通信口，用于桌面云客户端与服务器通信。

注意事项

- 1. 终端通信口建议优先选择使用HCI空闲的物理网口，并在HCI平台配置静态路由让终端通信口IP可以和用户终端所在网络（直连接入模式）或者作为代理网关的AD设备通信（AD代理模式）。
- 2. HCI集群仅运行VDI业务的场景下，处于简化部署考虑，可将终端通信口与管理口复用，此时管理口配置应至少为双千兆链路聚合模式。
- 3. 用户内网安全设备需要放通用户终端网络和代理设备（如AD代理网关、atrust代理网关）访问终端与主机通信口TCP&UDP 5500,8888,13500-13999端口通信权限。
- 4. 终端通信口禁止使用“根据网口轮询进行负载”。

拓扑规划



操作步骤

- 1. 推荐使用聚合网口：在HCI控制台中点击[实体机/物理网络]，点击<批量添加聚合口>，选择两个网口，例：eth2和eth3，聚合口工作方式支持选择“静态聚合”和“LACP模式”，若为标准链路聚合，则推荐选择根据四层信息进行负载，若为交换机不支持四层负载，则推荐根据MAC地址进行负载。

物理主机	物理网络	网口功能	系统盘
刷新	批量添加聚合口	批量添加VLAN子网口	批量编辑网口
主机高级设置			
物理主机	网口名称	VLAN ID	网口功能
192.200.244.201	eth0	-	管理通信口、数据通信口
192.200.244.202	eth1	-	

- 2. 在HCI控制台中点击[实体机/网口功能]。在网口角色中找到终端通信口，点击<修改配置>进入到配置页面，可修改终端通信口。



修改配置

刷新 批量修改

主机名称	终端通信口	VLAN ID	终端通信口IP	掩码
200.201.202.71	eth0	-	200.201.202.71	255.255.248.0
200.201.202.72	eth0	-	200.201.202.72	255.255.248.0
200.201.202.73	eth0	-	200.201.202.73	255.255.248.0

确定

取消

3.7. 授权激活

3.7.1. USB KEY 授权

操作步骤

1. 把授权KEY插入到集群的主控上，然后点击进入[系统管理/授权管理]页面。



2. 点击<激活授权>，进入[USB-key授权]页面，导入授权文件。



3. 确定后，即可看到具体授权信息。

3.7.2. vKEY 授权

功能介绍

深信服超融合平台支持免KEY授权，即可以采用vKEY软件授权方式，避免硬件KEY丢失、故障影响集群使用。授权变更场景无需寄回和重新申请USB KEY，变更效率更高。

注意事项

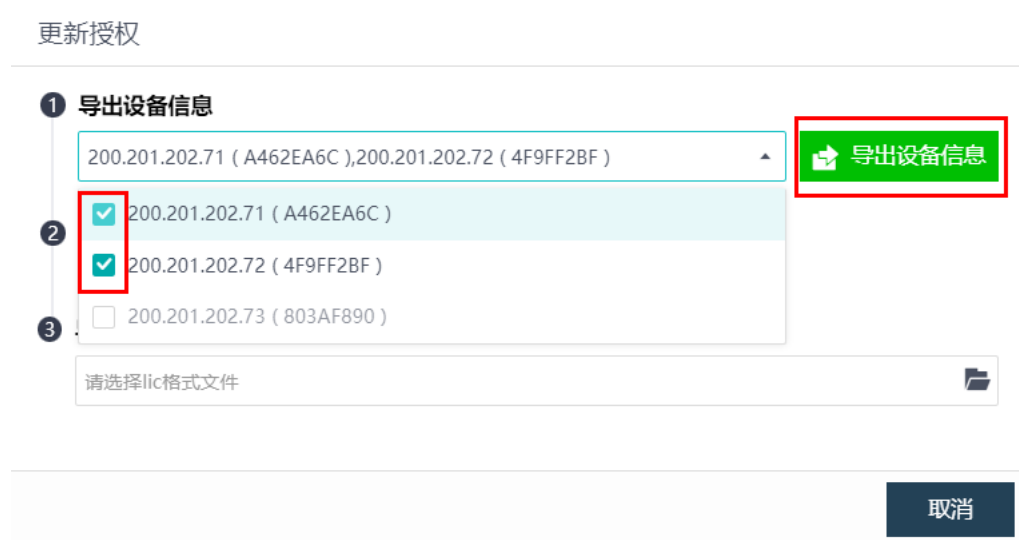
1. 仅HCI6.8.0及其之后的版本支持vKEY授权方式。
2. USB-KEY与vKEY 授权不能同时存在。
3. 对于HCI6.8.0及其之前的版本升级场景，默认使用USB-KEY方式，可在升级之后切换授权方式，且更换时需联系深信服技术支持获取云图账号，并将USB-KEY寄回。
4. 切换授权方式后，原有USB KEY将失效。
5. vKEY授权仅支持离线授权方式，暂不支持在线授权。
6. vKEY授权，导出硬件信息需选择2台主机，若替换其中一台主机时，授权会失效，需要到云图授权中心重新开授权；若两台都替换的场景，HCI授权会失效，但无法在云图授权中心重开授权，需要单独联系深信服云图技术支持开授权。
7. 组建集群后若未导入授权文件，则不允许创建全新虚拟机，仅支持导入SCP虚拟机。

前提条件

1. 已获取深信服云图账号。
2. 已组建好HCI集群，部署流程可参考“[安装流程介绍](#)”章节。

操作步骤

1. 进入[系统管理/授权管理]，点击<激活授权>，进入[离线授权]页面。
2. 选择两台主机导出设备信息。



3. 前往“深信服授权中心”，登录平台导入设备信息，获得授权文件。可点击右上角“帮助信息”，获取授权文件的详细操作指引。



4. 将获取到的授权文件导入平台，完成授权激活。

3.8. 配置 LLDP（可选）

功能描述

深信服HCI支持对接交换机端口的LLDP协议，在界面可以看到对端交换机的网口号、MTU、TTL等信息，方便管理员运维和故障定位。

注意事项

1. 仅支持查看单个物理网口上的LLDP信息，不支持查看聚合口、VLAN子网口上的LLDP信息。
2. 对端交换机trunk口存在多个vlan只能交换机行为决定显示一个vlan。

3. 部分品牌的交换机会转发其他设备的LLDP包（已知信锐交换机会转发），导致获取到的LLDP信息非对端直连端口信息。

前提条件

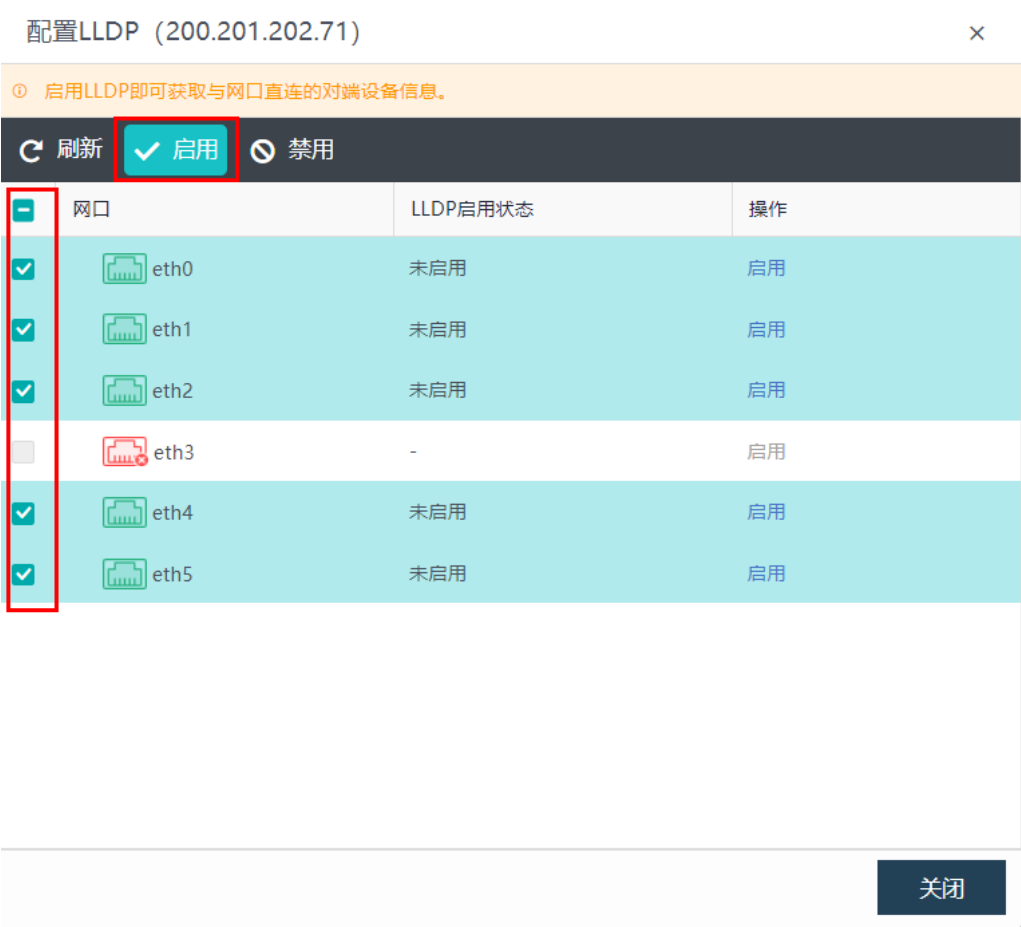
对端交换机已开启LLDP功能。

操作步骤

1. 进入[实体机/物理网络]页面，选择需要查看LLDP的主机，点击<主机高级设置/对单主机配置LLDP>按钮。



2. 选择需要获取对端设备信息的网口，点击<启用>按钮。



3. LLDP启用完成后，回到[物理网络]界面，找到对应的物理网口，点击操作栏的<

查看LLDP>按钮，启用LLDP状态，即可查看到对端交换机网卡传输的LLDP信息。

- 设备 ID：对端端口的 MAC 地址
- 端口 ID：对端端口编号
- TTL：time to live，包的存活时间
- 端口描述：自定义描述信息
- 系统名称：对端交换机名称
- 系统特性：对端交换机模式

LLDP信息

✕

① 检测到存在多个对端设备，目前仅支持显示其中一个设备详情。

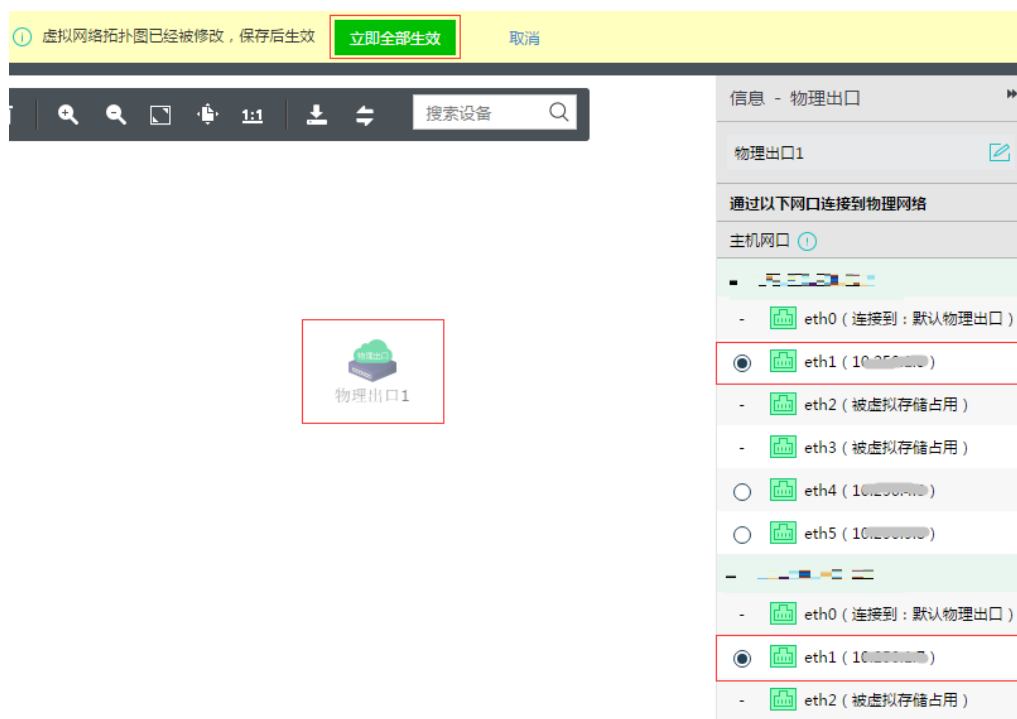
LLDP状态：☒

对端设备信息

设备ID:	1c:3d:2f:d2:7e:50
端口ID:	MultiGE0/0/16
TTL:	120
端口描述:	To_Rack_24
系统名称:	VTT-CORE-SW
系统特性:	BRIDGEROUTER
管理地址:	192.168.1.253
VLAN ID:	150
聚合状态:	未聚合
聚合ID:	0
最大帧长度:	9216
系统描述:	Huawei Switch S5732-H24UM2CCHuawei Versatile Routing Platform SoftwareVRP (R) software Version 5.170 (S5732 V200R019C10SPC500)Copyright (C) 2000-2020 HUAWEI TECH Co. Ltd.

3.9. 物理出口配置

如果是多台主机集群部署，对外作为一个整体来提供服务，虚拟机可能在任意一台主机上运行，因此需要每台主机都指定一个网口连接同一个[物理出口]，同时将主机的对应网口连接到同一个二层交换机上，以保证虚拟网络中的流量能从任一主机发出到达物理网络中。



3.10. 三网合一方案（可选）

功能说明

当服务器的物理网卡不足时，可采用三网合一方案。三网合一方案即管理网络、业务网络、数据通信网络复用一個聚合网口的网络规划方案。

注意事项

1. 如果聚合口使用主备模式，主备模式的聚合对端交换机可以不用配置聚合。
2. 主备模式只支持两网口聚合。
3. 当前聚合模式不支持对两个已有角色的网口直接聚合，需先移动角色到空闲网口再进行聚合。
4. 业务口不支持配置VLAN子接口，业务VLAN只能通过虚拟网络的端口组进行配置。
5. 建议在管理、VXLAN、业务三网复用的情况下设置流量上限设置，以保证网络流量稳定。管理通信口未进行复用的时候不需要配置流量上限。启用限速后，可在[实体机]的主机[详情]页面的[流速趋势]查看管理口、VXLAN口和业务口的流量。
6. 仅推荐在四个万兆网口的环境进行部署。
7. 从老版本热升级完成后，若原有环境已经存在聚合口，聚合口功能操作会失效，

但不影响正常使用，需要重启主机之后才能支持操作。

8. 业务网和VXLAN网复用的场景下，虚拟网络禁止使用任何NFV设备的透明模式。若必须要用透明模式，则使用 VLAN 子接口将业务网络和 VXLAN 网络隔离，并在虚拟网络的物理出口 trunk_all 那里，将 VXLAN 的 VLAN ID 排除在允许范围之内。

前提条件

三网合一的复用网口必须是万兆网口。

操作步骤

1. 在控制台点击[实体机/物理网络]，进入网口配置界面。



2. 由于不支持两个已有角色的网口直接进行聚合，需要先将数据通信口复用到管理通信口上，点击[网口功能/数据通信口（vxlan）/修改配置]将eth1修改为eth0。





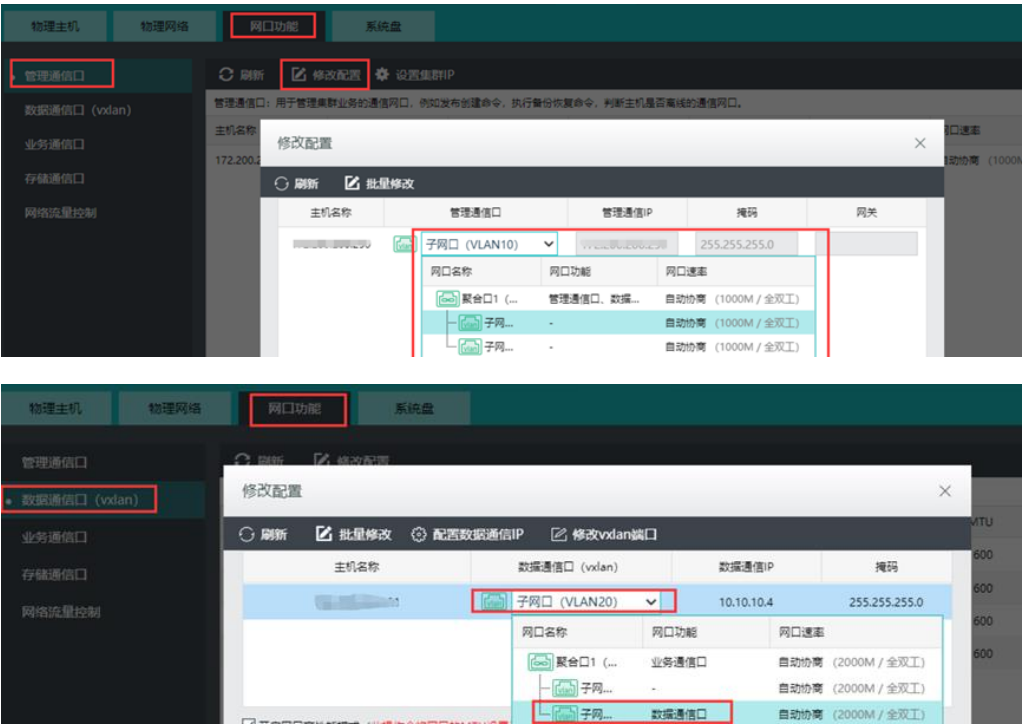
3. 将eth0与eth1进行聚合，点击<批量聚合网口>，选择eth0和eth1，聚合模式推荐根据MAC或IP地址进行负载。



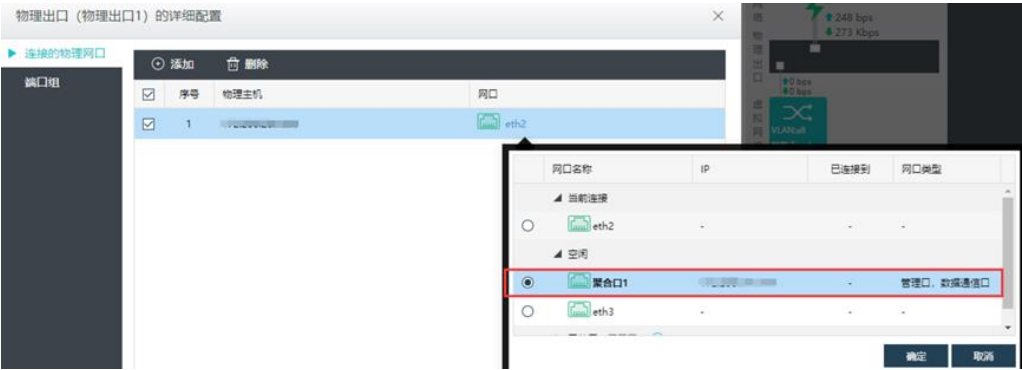
4. 聚合完成后使用VLAN子接口对不同网络平面进行VLAN隔离，点击<批量添加VLAN子网口>，填写对应VLAN，IP地址信息无需填写。



5. VLAN子接口配置完成，将管理通信口和数据通信口切换至对应子接口，点击[网口功能/管理通信口]配置管理通信接口，点击[数据通信口]配置数据通信接口。



6. 点击[虚拟网络/默认物理出口], 修改物理出口为聚合口。



7. 配置完成, 结果如图所示。

物理主机	物理网络	网口功能	系统盘
刷新	批量添加聚合口	批量添加VLAN子网口	批量编辑网口
物理主机	网口名称	VLAN ID	网口功能
192.200.244.211	子网口 (VLAN10)	10	管理通信口
192.200.244.212	子网口 (VLAN20)	20	数据通信口
192.200.244.213	eth0	-	虚拟存储口
192.200.244.231	eth2	-	虚拟存储口
	eth4	-	虚拟存储口
	eth5	-	虚拟存储口

8. 建议在管理、vxlan、业务三网复用的情况下设置流量上限, 以保证网络流量稳定。



3.11. 四网合一方案（可选）

功能说明

当服务器的物理网卡不足时，可采用四网合一方案。四网合一方案即管理网络、业务网络、数据通信网络、存储网络复用一個聚合网口的网络规划方案。该方案提供了网卡级别的冗余保护，单网卡故障不会影响业务。

注意事项

1. 单网口不支持四网合一，最大能支持4个物理网口聚合进行四网合一。
2. 服务器网卡聚合支持主备模式（默认）以及根据IP、MAC地址、网口轮询、四层信息五种负载均衡模式，建议采用按照IP方式进行负载均衡，不推荐主备模式。接入层交换机端口需要配置相应的端口聚合模式。主备模式的聚合对端交换机可以不用配置聚合。
3. 当前聚合模式不支持对两个已有角色的网口直接聚合，需先移动角色到空闲网口再进行聚合。
4. 建议在管理、VXLAN、业务、存储四网合一的情况下设置流量上限限制，以保证网络流量稳定。启用限速后，可在[实体机]的主机[详情]页面的[流速趋势]查看管理口、VXLAN口、业务口和存储口的流量。
5. 当前支持四网合一的网卡类型如下：Mellanox CX4、Mellanox CX6、intel X710、intel X722。
6. 每个网络平面建议配置VLAN进行网络隔离，其中管理、VXLAN、存储配置VLAN子接口，业务口不支持配置VLAN子接口，业务VLAN只能通过虚拟网络的端口组进行配置。
7. 从老版本热升级完成后，若原有环境已经存在聚合口，聚合口功能操作会失效，但不影响正常使用，需要重启主机之后才能支持操作。
8. 旧版本升级上来的设备启用四网合一，intel网卡会中断网络30s（重启DP+交换机STP收敛），mellanox网卡需要重启物理主机后才能生效。

9. 主板需要支持VT-D（三代CPU以后的均支持），新发货一体机在安装系统时会开启。旧版本升级或第三方设备之前未开启VT-D功能，会提示开启后需要重启才能生效。
10. 业务网和VXLAN网复用的场景下，虚拟网络禁止使用任何NFV设备的透明模式。若必须要用透明模式，则使用 VLAN 子接口将业务网络和 VXLAN 网络隔离，并在虚拟网络的物理出口 trunk_all 那里，将 VXLAN 的 VLAN ID 排除在允许范围之内。

前提条件

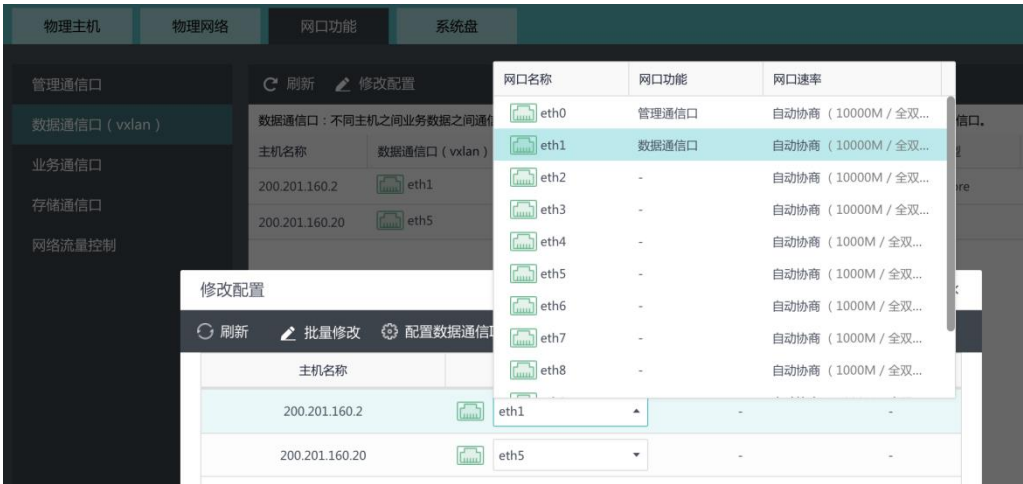
1. 四网合一的复用网口必须是万兆网口，且至少有2个。
2. 每个网络平面建议配置VLAN进行网络隔离，故连接超融合主机的交换机接口需提前配置为Trunk All。并在相关交换机配置好已规划的VLAN。

操作步骤

1. 在控制台点击[实体机/物理网络]，进入网口配置界面。



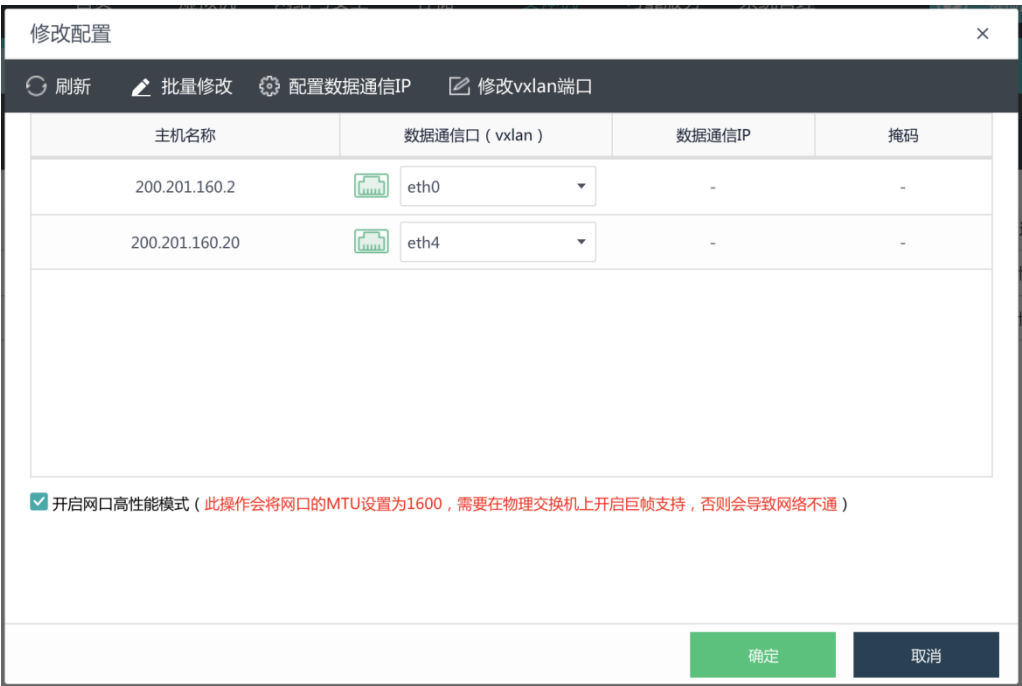
2. 由于不支持两个已有角色的网口直接进行聚合，需要先将数据通信口复用到管理通信口上，点击[网口功能/数据通信口（VXLAN）/修改配置]将数据通信口复用到管理口。



3. 选择“继续使用”。



4. 所有主机网口调整完毕后，点击确定。勾选<开启网口高性能模式>（此操作会将网口的MTU设置为1600，需要在物理交换机上开启巨帧支持，否则会导致网络不通）。



5. 如下图所示，数据通信口已调整到管理口。原数据通信口已无角色，可以进行

聚合。

物理主机	网口名称	VLAN ID	网口功能	描述	IP/掩码	网关	驱动类型	网口速率	启用状态	操作
200.201.160.2	eth0	-	管理通信口、数据通信口	-	200.201.16...	200.201.16...	mlx5_core	自动协商 (100...	✓	编辑
200.201.160.20	eth1	-	-	-	-	-	mlx5_core	自动协商 (100...	✓	编辑
	eth2	-	-	-	-	-	mlx5_core	自动协商 (100...	✓	编辑

6. 将规划好的网口进行聚合，创建聚合口时开启存储复用功能。聚合模式推荐根据MAC或IP地址进行负载。

物理主机	网口名称	VLAN ID	网口功能	描述	IP/掩码	网关	驱动类型	网口速率
200.201.160.2	eth0	-	管理通信口、数据通信口	-	200.201.16...	200.201.16...	mlx5_core	自动协商 (100...
200.201.160.20	eth1	-	-	-	-	-	mlx5_core	自动协商 (100...
	eth2	-	-	-	-	-	mlx5_core	自动协商 (100...
	eth3	-	-	-	-	-	mlx5_core	自动协商 (100...

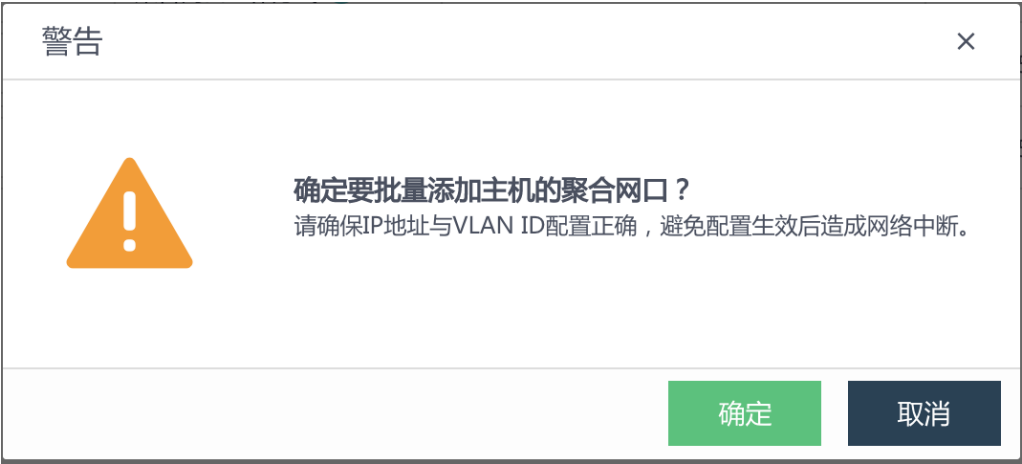
7. 点击<批量添加聚合口>，选择规划的网口；选择聚合网口工作方式，不推荐使用主备模式，网口利用率较差（配置非主备聚合模式后，需要调整连接交换机的聚合方式与平台匹配，否则将无法访问平台）；勾选<存储口复用功能>，点击<确定>。

主机名称	主机网口	聚合网口工作方式	IP地址	子网掩码	网关	存储口复用功能
200.201.160.2	eth0, eth1	使用MAC地址进行负载	使用原eth0的IP (200.201.160.2)	255.255.248.0	200.201.167.2...	✓
200.201.160.20	网口名称	网口功能	网口速率	-	-	不支持
	eth0	管理通信口、数据...	自动协商 (10000M / 全双...			
	eth1	-	自动协商 (10000M / 全双...			

8. 确定启用“存储通信口复用功能”。启用存储通信口复用功能前，需要重启网络服务，将导致“物理主机”和“运行在该物理主机上的虚拟机”网络临时中断几分钟，请谨慎操作。



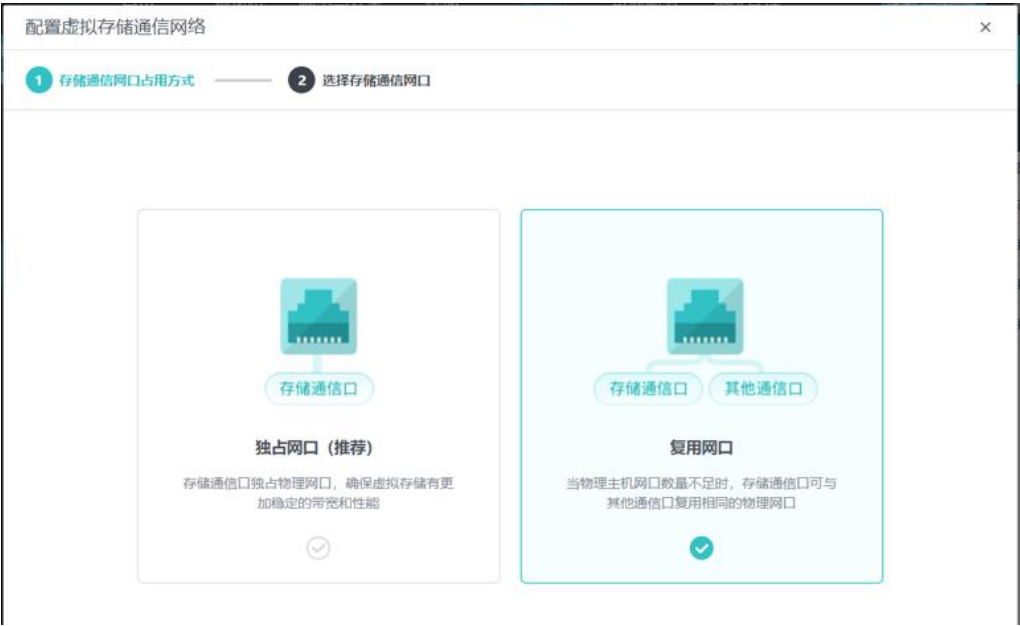
9. 点击<确定>批量添加主机的聚合网口。请确保IP地址与VLAN ID配置正确，避免配置生效后造成网络中断。



10. 如下图，点击<修改配置>，调整存储通讯口。



11. 选择“复用网口”的方式，点击<下一步>，选择前面已启用存储口复用功能的聚合口。填写规划好的VLAN ID和网口IP地址，点击<确定>。



配置虚拟存储通信网络

✓ 存储通信网口占用方式 2 选择存储通信网口

主机名称	主机网口	VLAN ID	网口IP	连接状态
200.201.160.2	子网口 (存储通信口)	101	10.251.251.2 / 24	✓ 连接正常
200.201.160.20	子网口 (存储通信口)	101	10.251.251.1 / 24	✓ 连接正常

12. 点击<修改配置>，调整数据通信网口。



13. 点击<配置数据通信IP>。



14. 填写规划好的IP地址和子网掩码。

配置数据通信IP

为集群中主机的数据通信网口（vxlan）配置IP，让虚拟机能够跨主机通信

配置数据通信IP：

支持配置一个IP池，系统将从IP池中为每台主机分配一个通信IP

192.168.1.1-192.168.1.10

格式说明

子网掩码：

255.255.255.0

确定

取消

15. 点击<确定>后，查看配置的数据通信口IP地址信息。

物理主机	物理网络	网口功能	系统盘				
管理通信口	数据通信口（vxlan）	业务通信口	存储通信口				
网络流量控制							
数据通信口：不同主机之间业务数据之间通信的网口，例如虚拟机与虚拟机之间通信，而且虚拟机所在主机不同，则需要通过数据通信口。							
主机名称	数据通信口（vxlan）	VLAN ID	数据通信IP	掩码	驱动类型	网口速率	MTU
200.201.160.2	聚合口1（eth0，eth1...	-	192.168.1.2	255.255.255.0	-	自动协商（10000M / ...	1500
200.201.160.20	聚合口1（eth4，eth5...	-	192.168.1.3	255.255.255.0	-	自动协商（10000M / ...	1500

16. 批量添加VLAN子接口。

物理主机

物理网络

网口功能

系统盘

刷新

批量添加聚合口

批量添加VLAN子网口

批量编辑网口

主机高级设置

物理主机	网口名称	VLAN ID	网口功能	描述	IP/掩码	网关	驱动类型	网口速率	启用状态	操作
200.201.160.2	聚合口1（eth0，eth1）	-	数据通信口	-	192.168.1.2 ...	-	-	自动协商（100...	✓	编辑 删除
	子网口（管理通信口）	-	管理通信口	-	200.201.160...	200.201.167...	-	自动协商（100...		编辑
200.201.160.20	子网口（存储通信口）	-	存储通信口	-	10.251.251...	-	-	自动协商（100...		

批量添加VLAN子网口

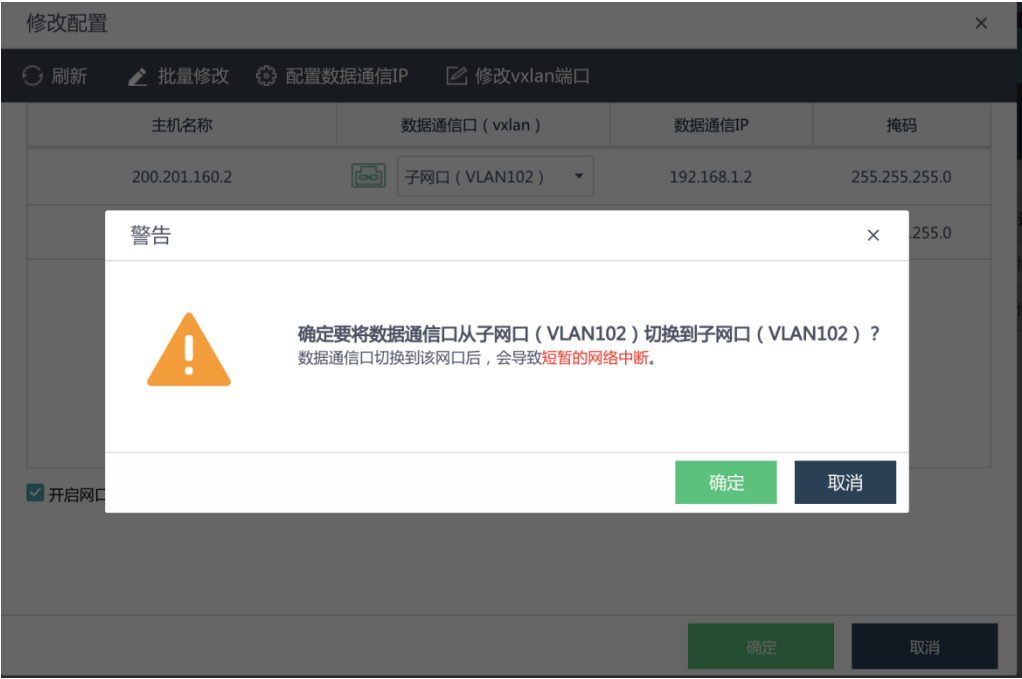
批量修改

主机名称	主机网口	VLAN ID	IP地址	子网掩码	网关
200.201.160.2	聚合口1（eth0，eth1）	102			
200.201.160.20	聚合口1（eth4，eth5）	102			

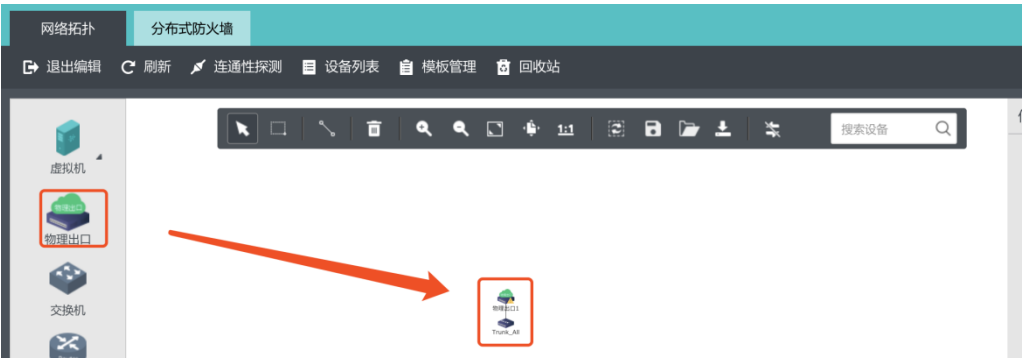
17. 点击<确定>将数据通信口从聚合口切换到子网口。数据通信口切换到该网口后，会导致短暂的网络中断。

文档版本 06（2023-02-21）

118



18. 点击<在网络拓扑图中配置业务口>。在网络拓扑图中添加物理出口，点击<立即生效>。



19. 选择物理出口，点击<连接到主机>。

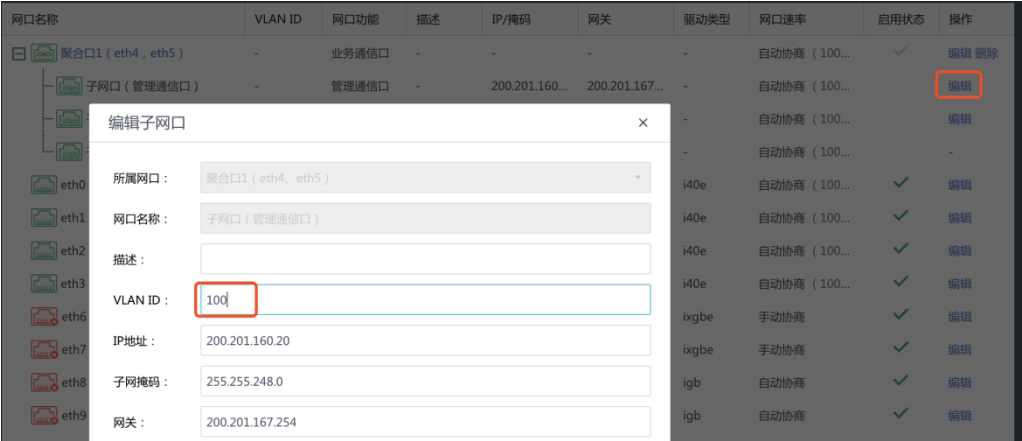


20. 点击<添加>选择网口和主机。



21. 业务网口配置完毕。业务口不支持配置VLAN子接口，业务VLAN只能通过虚拟网络的端口组进行配置。

22. 选择管理网口的子接口，为其配置规划好的VLAN ID。



23. 至此四网合一所有网口配置完毕。



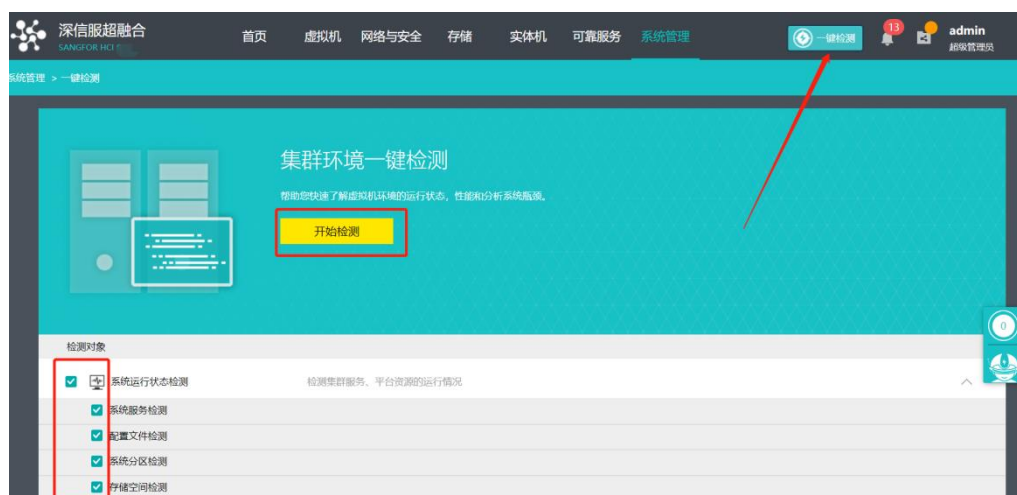
24. 建议在管理、vxlan、业务、存储网口复用的情况下进行带宽/流量上限设置，以保证网络流量稳定。集群创建时建议管理口配置3Gbps；业务口和vxlan配置

5Gbps；存储口配置8Gbps。后续通过观察各个网络平面的流量，再进行优化调整。



3.12. 一键检测集群状态

在平台部署完毕后，需要检查集群中各项配置是否正确。在首页点击<一键检测>。勾选需要检测的对象，点击<开始检测>。确认检测最终得分为100分，若低于100分需按照检测结果建议或联系深信服技术支持进行处理。



3.13. 使用 aDeploy 工具进行检测

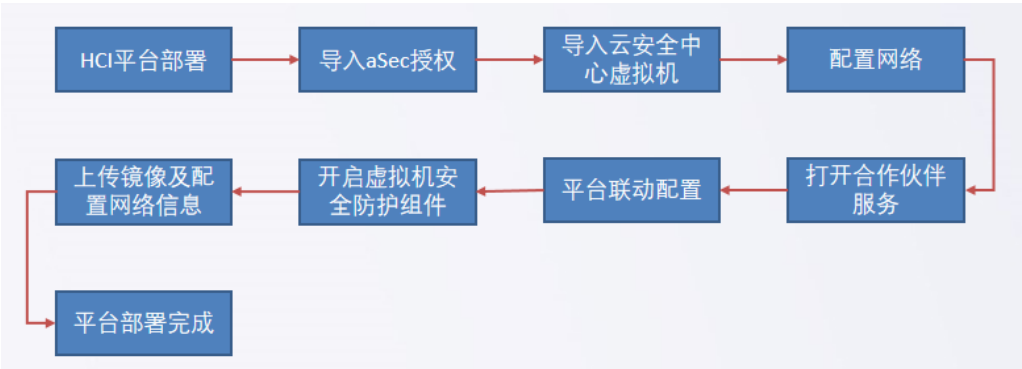
在平台部署完毕后，需要检查当前版本是否有可用的补丁需要升级，请使用aDeploy工具进行检查，并按照检测结果升级对应的补丁包。

aDeploy 工具下载地址：<http://adeploy.sangfor.com:8080/download/aDeploy-server-install.zip>

3.14. 云安全中心安装部署

深信服超融合平台HCI支持通过导入虚拟机的形式部署云安全中心。本章节主要介绍云安全中心的安装部署，包括云安全中心虚拟机aSEC安装和安全防护管理平台部署。

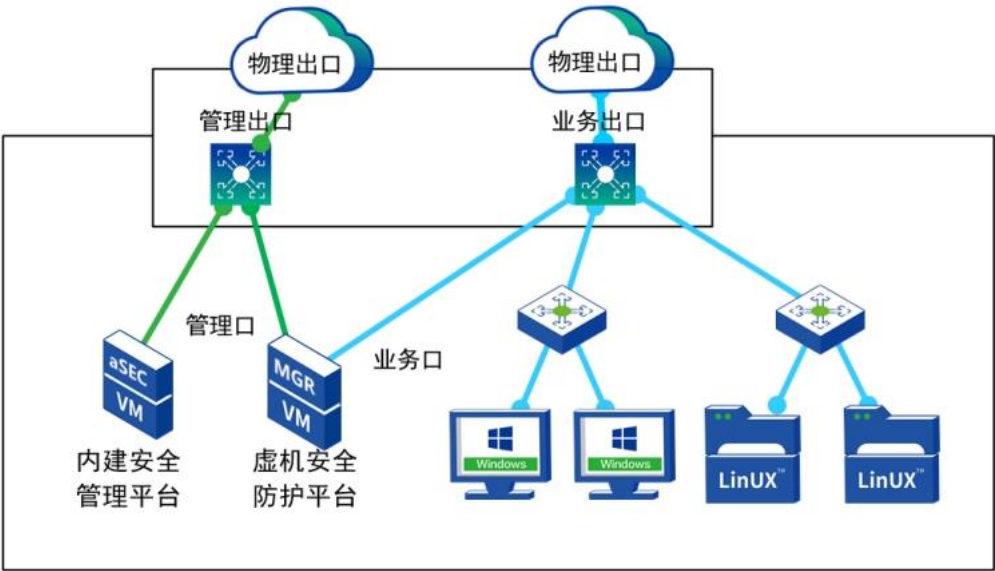
- 云安全中心安装部署流程图如下图所示。



- 云安全中心部署网络拓扑规划如下图所示，云安全中心平台需要和 HCI 的管理网络正常通信（推荐与 HCI 管理网同一网段），主要用于云安全中心平台调用 HCI 的 API 接口执行打快照或创建分布式防火墙等策略；虚拟机安全防护平台的管理口配置连接到物理出口（该物理出口必须桥接 HCI 的管理口，推荐与 HCI 管理网规划成同一网段），虚拟机安全防护平台的业务通信口配置（可选）连接到业务网物理出口，用于连接病毒库、云查服务等安全服务器，实现病毒库的自动更新。

⚠ 注意：

紧急隔离的虚拟机会加入云安全中心网络隔离策略，若虚拟机直连物理出口，则策略不生效。



- 云安全中心推荐配置说明可参考下表。

aSEC虚拟机服务器推荐配置			
接入终端数	CPU	内存	磁盘

1-300（默认规格）	4 核	8G	300G
300-1000	4 核	16G	300G
1000-2000	8 核	32G	300G
安全防护管理平台虚拟机服务器推荐配置			
接入终端数	CPU	内存	磁盘
1-300（默认规格）	2 核	2G	300G
300-1000	2 核	4G	300G
1000-2000	4 核	8G	300G

3.14.1. aSEC 云安全中心安装

注意事项

1. 目前支持HCI6.3.20_P、HCI6.8.0及以上版本，部署云安全中心。
2. 已完成云安全中心授权导入。
3. aSEC密码限制3个月强制修改一次。

操作步骤

1. 进入[虚拟机]页面，点击<新增>，选择<导入虚拟机>。或直接进入[云安全中心]界面，点击<立即部署>按钮。



2. 导入vma文件，选择虚拟机分组、存储位置、存储策略、运行位置。

从本地导入vma文件



① 虚拟机导入后默认使用QXL高性能显卡，如果开机后出现显示的异常，请通过手动切换显卡解决。

文件类型: ova或vma
如需使用vhd、vhdx或者qcow2格式的镜像文件，请选择创建新的虚拟机，并在新建、编辑虚拟机磁盘时选择使用已有磁盘，挂载需要使用的镜像文件。

虚拟机文件: aSEC1.2.0_B(20220730).vma

分组: 默认分组

故障迁移(HA): ☒ 当设备所在主机出现故障时，自动切换到其它物理主机上运行。配置HA ①

存储位置: 虚拟存储卷1

存储策略: 2副本默认策略

运行位置: <自动选择>

开始导入

从本地导入虚拟机文件



虚拟机已成功导入

名称: aSEC

分组: 默认分组

存储位置: 200.201.202.72;200.201.202.71

存储策略: 2副本默认策略

运行位置: <自动选择>

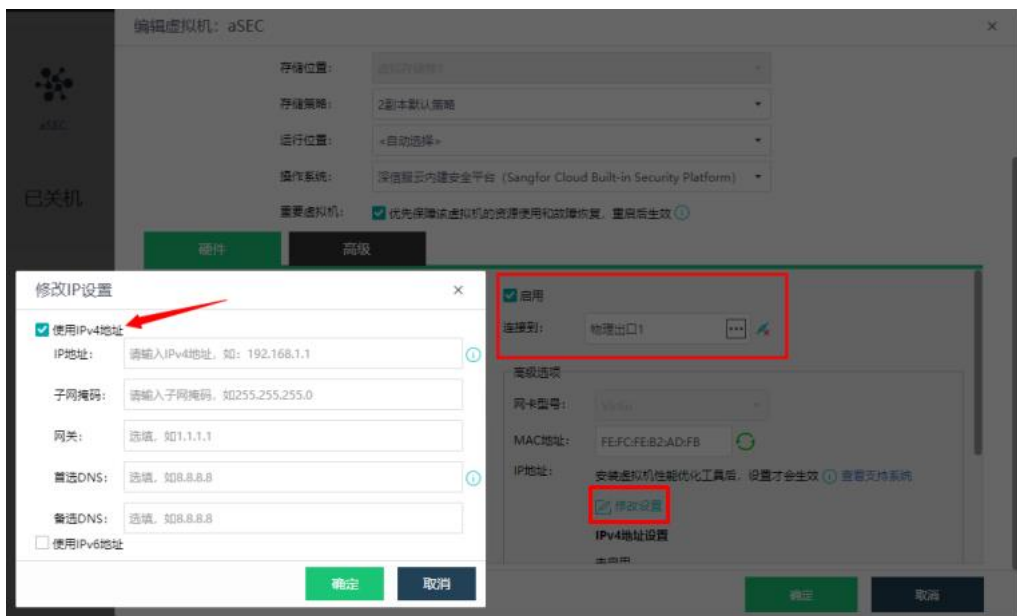
硬件配置: 磁盘 (300 GB), CPU (4 核), 内存 (8 GB), 网卡数 ...

虚拟机网卡未连接交换机，请编辑虚拟机重新配置网卡

关闭

转到虚拟机

3. 导入成功后，进入[编辑虚拟机]界面，进行网卡配置。勾选“启用”，连接到物理出口，点击<修改配置>按钮，选择“使用IPv4地址”，配置aSEC虚拟机IP地址，作为云安全中心管理网络（此处需规划与HCI管理网段能够互通，推荐与HCI管理网同一网段）。



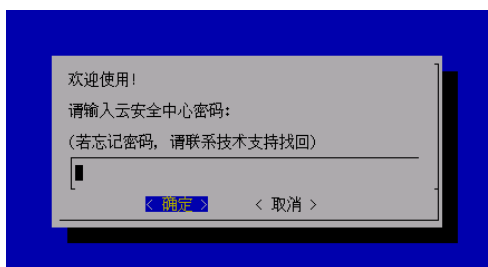
4. 启用合作伙伴服务端口，开启合作伙伴服务，否则将无法访问云安全中心服务。

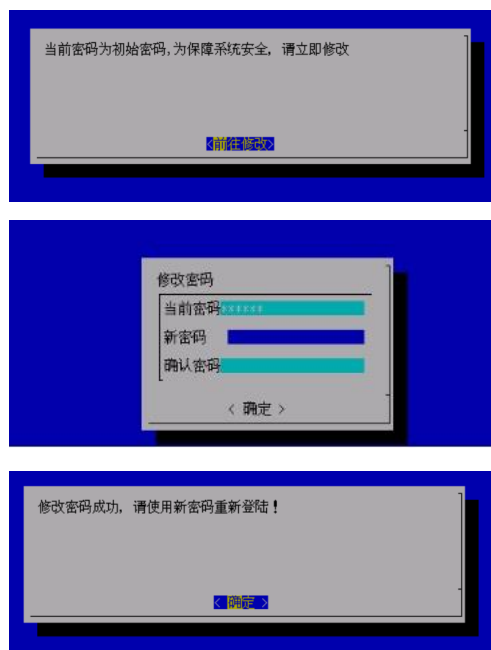


5. 将虚拟机开机，进入虚拟机控制台，进行平台安全联动配置。

步骤1. 输入云安全中心的密码登录。注意：首次登录需要修改密码，默认密码为 Sfcsec@123，密码修改策略如下：

- 长度为 8~64 字符。
- 必须包含大写字母、小写字母、数字和特殊字符 4 项，特殊字符支持 ~`@#%&<>";,;\_^-\$.\*+?=:!{|}~`。
- 不能与用户名相同或者包含用户名。
- 同一字符不能连续出现，如 **aaa**，**11** 等。
- 不能使用 **sangfor/sinfor/dlanrecover** 常用字符（包含大小写）。





⚠ 注意:

如果 10 分钟内未修改或者修改失败, 会提示“内部错误”, 此时为会话超时, 需重新登录后再进行修改。

步骤2. 登录成功后, 点击<平台认证配置>, 进入HCI平台认证页面:

- 集群 IP: 超融合集群 IP。
- 用户名/密码: 超融合超级管理员用户名/密码。

步骤3. 点击<建立认证>, 完成aSEC部署。



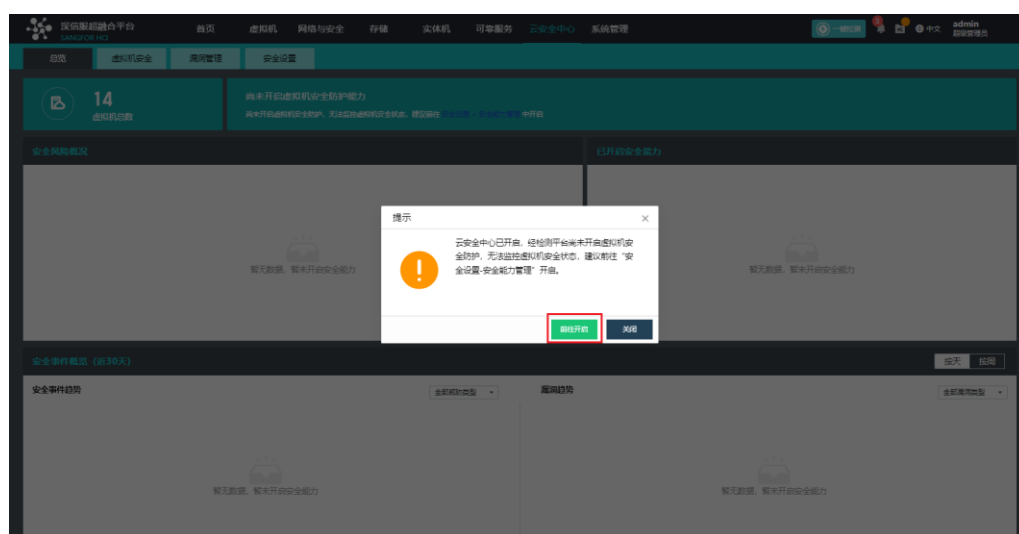
3.14.2. 虚拟机安全防护管理平台安装

前提条件

已完成“[aSEC安装](#)”。

操作步骤

1. 完成aSEC安装后，进入[云安全中心]页面，在弹出的提示页面点击<前往开启>，开启虚拟机安全防护。



2. 进入[安全设置/安全能力管理]页面，点击“虚拟机安全防护”的<开启>按钮。



3. 配置部署EDR_MGR管理平台。

- 基本信息

导入vma虚拟机文件

选择存储位置

运行位置保持默认即可

- 管理口配置：连接到物理出口（该物理出口必须桥接 HCI 的管理口，推荐与 HCI 管理网规划成同一网段）。

- 业务通信口配置（可选）：连接到业务网物理出口，用于连接病毒库、云查服务等安全服务器，且需确保网口可连接至以下服务器：

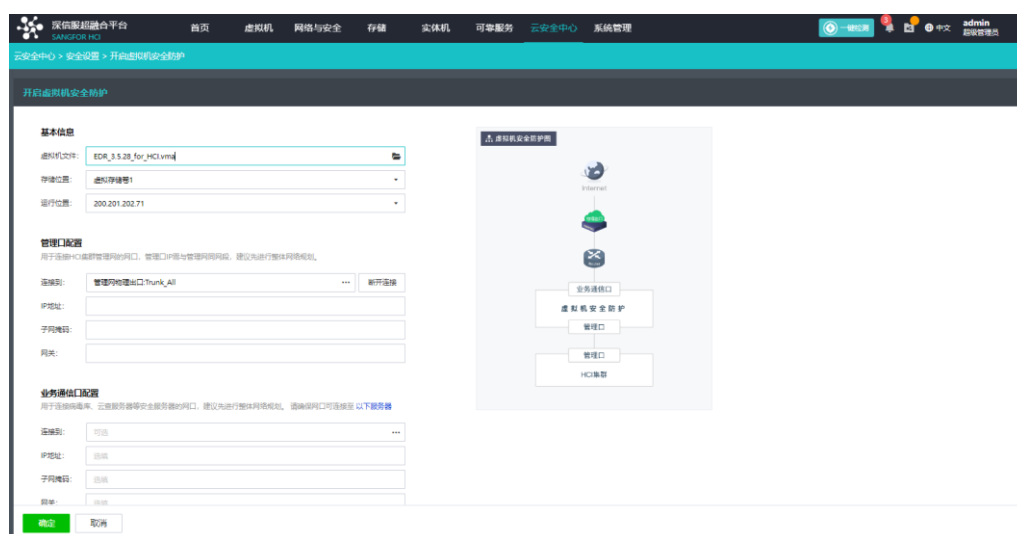
病毒库：<http://download.sangfor.com.cn/download/product/edr>

漏洞补丁：<https://upd.sangfor.com.cn>

云脑：<https://auth.sangfor.com.cn>

云查服务器：<https://analysis.sangfor.com.cn>

云安全计划：<https://clt.sangfor.com.cn>



4. 点击<确定>，开始部署虚拟机安全防护。

正在开启虚拟机安全防护，请稍后...

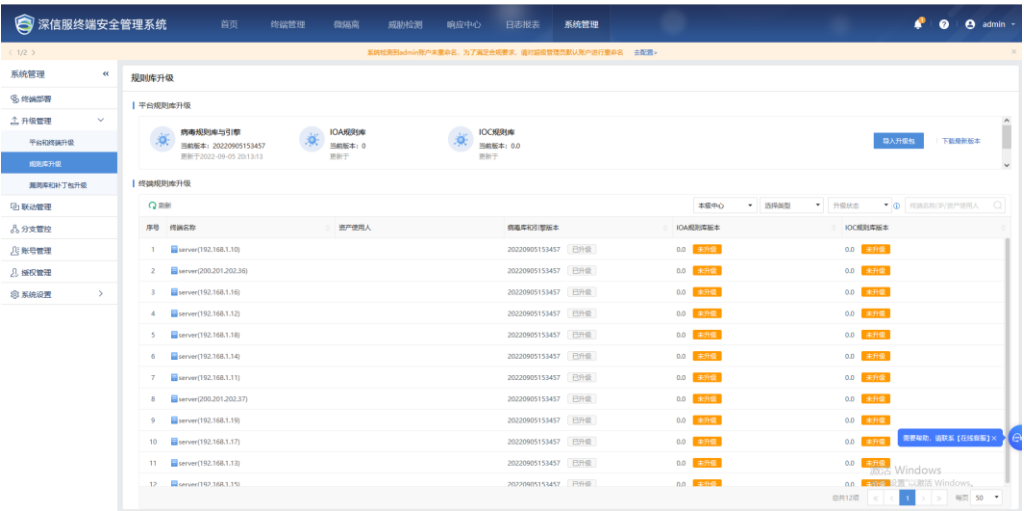
64 %

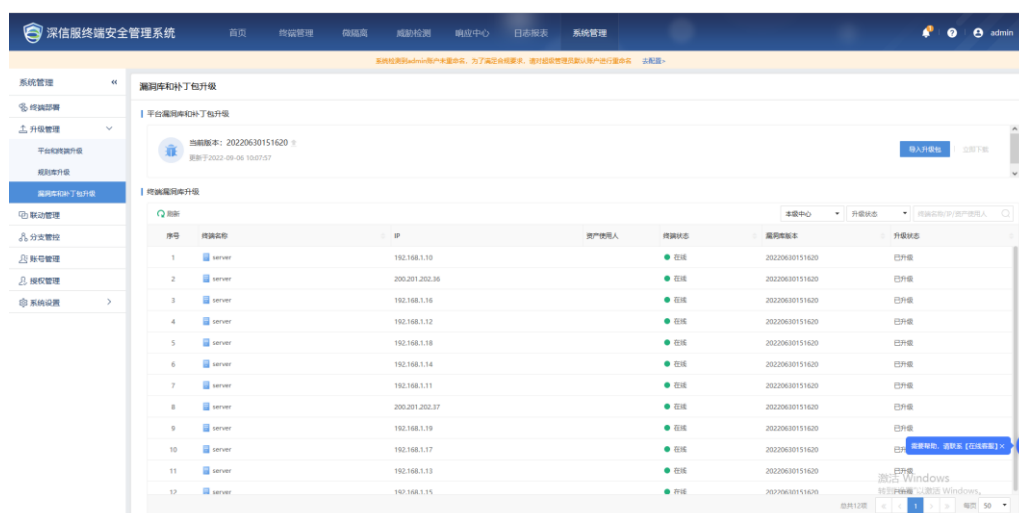
开启虚拟机安全防护将创建虚拟机并部署网络，需要消耗一些时间，请不要关闭此页面！

5. 部署成功后会自动跳转回[安全设置/安全能力管理]页面，并弹出安全配置界面，可查看当前默认安全配置，若需进行其他个性化配置，可参考《[深信服终端安全管理系统EDR用户手册](#)》。



6. 部署完成后, 点击<前往安全防护管理平台>, 进入[系统管理/升级管理/规则库升级]页面, 进行病毒库升级; 进入[系统管理/升级管理/漏洞库和补丁包升级]页面, 进行漏洞库和补丁包升级。





3.14.3. 虚拟机安全组件安装

注意事项

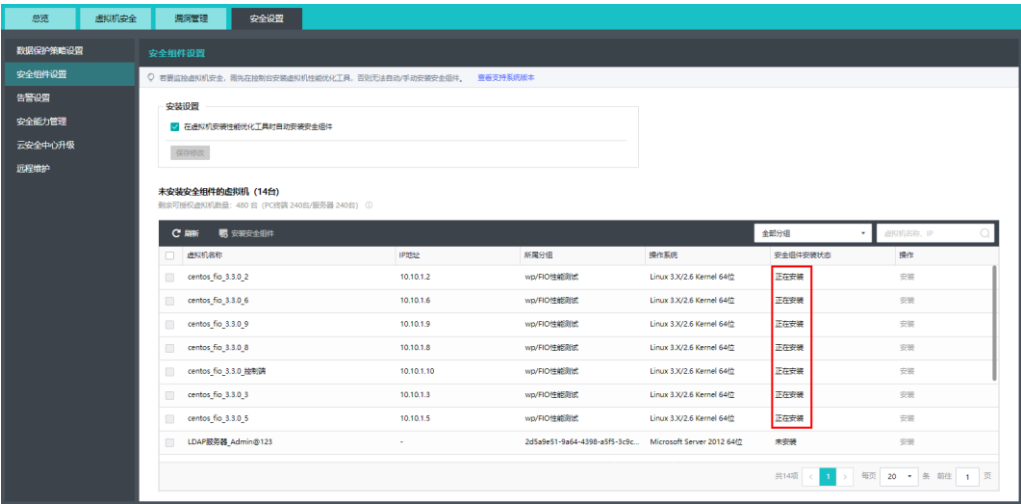
1. 支持对虚拟机自动安装安全组件，但当剩余可授权虚拟机数量不足时，则无法触发自动安装。
2. 虚拟机自动安装安全组件的时间预计在10分钟以内。
3. 不满足兼容性白名单内的操作系统无法安装安全组件。

操作步骤

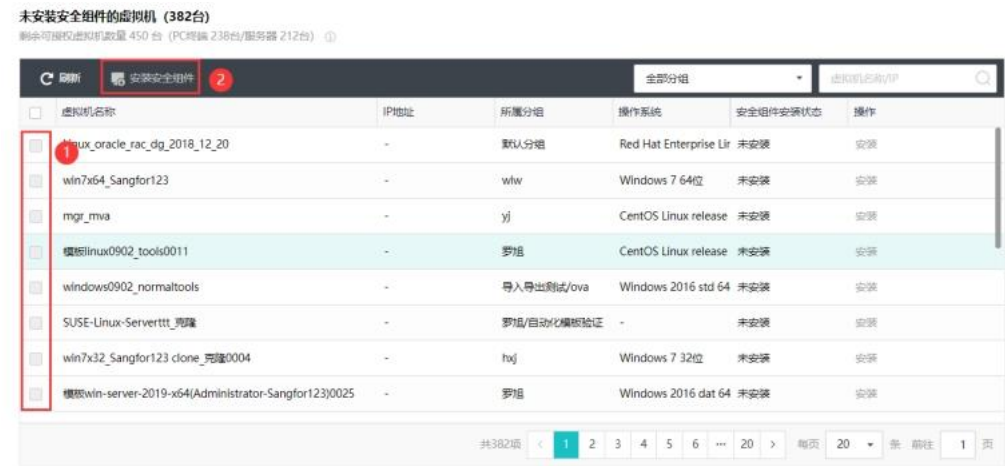
1. 进入[安全设置/安全组件设置]页面，勾选“在虚拟机安装性能优化工具时自动安装安全组件”，勾选后云安全中心模块会自动发现新资产上线，并通过VMtools自动对虚拟机进行安全组件的安装；同时虚拟机安全防护平台也支持通过VMtools自动更新安全组件。操作系统兼容性白名单可点击界面<查看支持操作系统>按钮进行查看。



2. 超融合平台原有虚拟机安全组件安装。
 - 若已勾选自动安装安全组件，则对于已安装性能优化工具且处于开机状态的虚拟机，会自动触发安全组件的安装。



- 若未勾选自动安装安全组件，即客户有业务正在进行中，暂时仅需要对部分虚拟机进行安全防护监控，则可在未安装安全组件的虚拟机列表中，勾选需要安装安全组件的虚拟机后，点击<安装安全组件>按钮，进行批量安装。



4. 平台登录

前提条件

浏览器满足以下条件：Chrome23以上版本、Firefox 18以上版本、IE 10以上版本、Safari 8以上版本。

注意事项

1. 不要在控制台中对虚拟机OS执行过于频繁的数据刷新，如直接在控制台上Linux虚拟机的tcpdump，可能会导致控制台卡住。
2. 两个不同权限用户在同一浏览器登录控制台，会出现互相替换登录信息，导致使用异常。不要使用两个不同权限的用户同时在一个浏览器使用。

操作步骤

1. 打开浏览器，输入https:// HCL_IP 超融合平台集群管理地址，会打开如下页面。



2. 输入HCI超融合平台的用户名密码，如果管理员账号设置了登录限制（IP /MAC / UUID / uKey），需在完全满足限制条件的终端上登录，登录成功后自动进入到控制台页面。



5. 虚拟机配置指导

5.1. 新建虚拟机

5.1.1. 创建全新虚拟机

功能说明

安装全新业务系统时，可采取创建全新虚拟机方式。

注意事项

1. Windows系统磁盘分区列表有MBR、GPT两种，MBR分区列表支持最大2TB，GPT分区列表支持最大128PB。
2. Linux 7在安装时，请选择正确的时区，并检查时间是否正常，Linux 6 在安装时，请勾选UTC，并选择正确的时区。
3. 虚拟机启动时，其时间基准以Host机为准，不支持在运行中修改时间基准。
4. 单个虚拟机核数不超过宿主物理主机核心数，避免vCPU调度会产生竞争问题。
5. 每个虚拟机配置最多16块虚拟磁盘，单盘不超过10T；如果需要更大容量磁盘，建议配置成多个磁盘。
6. Host CPU只有在虚拟机需要使用特殊指令集时开启（如大数据、人工智能等需要AVX指令集）。
7. 重要虚拟机建议开启预先分配存储空间；勾选“标记为重要虚拟机”； 关闭内存回收机制；勾选“使用大页内存”。
8. 64位windows10和2016使用UEFI方式安装失败，没有进入安装界面，进入了UEFI shell界面，可以通过在shell界面输入exit，然后进入boot界面，boot界面选择continue选项，然后按任意键开始安装。
9. 新建虚拟机时，配置的操作系统类型一定要跟实际安装的操作系统类型一致。否则可能导致性能优化工具无法安装。
10. RHEL5.5等Linux系统的磁盘加载顺序跟aSV虚拟机的磁盘加载顺序不同，可能导致虚拟机磁盘顺序变化，虚拟机无法启动或磁盘无法访问等。可以编辑虚拟机选择启动磁盘，并建议Linux虚拟机使用UUID标识磁盘，不要用sda、sdb等名称标识。
11. Linux虚拟机的默认BIOS设置为SANGFOR_LINUX_UEFI，如果导入虚拟机后

系统无法启动，进入UEFI Shell界面，则尝试关机并修改设置为Legacy BIOS重新启动。

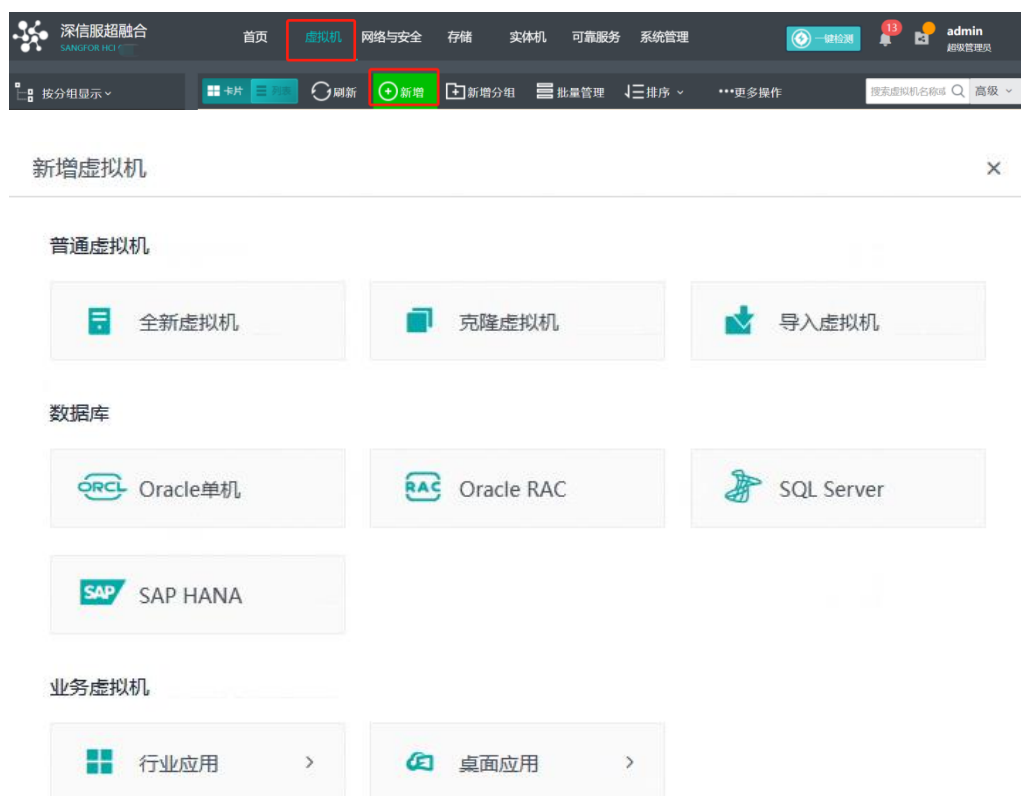
- 虚拟机挂起恢复后，时间还是以前的时间，没有跟现在的主机时间同步，需要手动修改时间。

前提条件

准备并上传ISO格式的操作系统镜像至超融合平台。

操作步骤

- 在[虚拟机/新增]中选择创建全新虚拟机。HCI6.8.0及其之后的版本支持桌面应用向导部署，详情可参考《[深信服桌面云aDesk用户手册](#)》。



- 配置如下信息。



新增虚拟机

名称:

分组: 默认分组

标签: 请选择标签

故障迁移(HA): ☒ 当虚拟机所在主机出现故障时, 自动切换到其它物理主机上运行。配置HA

存储位置: 医疗延伸卷

存储策略: 2副本默认策略

运行位置: <自动选择> 优先在所选位置运行

操作系统: 请选择与实际安装匹配的操作系统...

虚拟机特性: ☐ 重要虚拟机 (优先保障该虚拟机的资源使用和故障恢复) ☐ 高性能虚拟机 (仅关机时允许启用)

硬件 高级

快速配置: 低配 标配 高配

总核数: 8 核

处理器 8核

内存 16 GB

磁盘1 120 GB

虚拟插槽数: 1

每个插槽的核数: 8

确定 取消

- **名称:** 虚拟机的名称。
 - **分组:** 虚拟机分组。
 - **标签:** 可以给虚拟机新增一个标签或者选择已有标签。
 - **故障迁移 (HA):** 当主机发生故障时, 触发共享存储上的虚拟机 HA 切换, 使其从其他主机上恢复运行。
 - **存储位置:** 存储位置是指虚拟机文件的存放位置。
 - **存储策略:** 存储策略是指虚拟机存放的副本数
 - **运行位置:** 运行位置是指定虚拟机运行时使用哪个主机的 CPU 和内存资源, 可以选择自动选择、指定某台主机。当“存储位置”选择为延伸卷时, 还可以指定虚拟机的运行位置为某故障域, 当指定为某故障域时, 可以设置优先在所选位置运行或者必须在所选位置运行。
 - **操作系统:** 请选择和实际系统同一类型。
 - **重要虚拟机:** 勾选后, 优先保证虚拟机的运行和恢复。
 - **高性能虚拟机:** 勾选后, 默认标记为重要虚拟机、使用大页内存、使用 Host CPU 和高性能时钟、磁盘使用预分配方式, 取消勾选后前述启用的功能需手动关闭。
3. 调整虚拟机硬件配置。



- A. **处理器**：为虚拟机分配的vCPU核心数，不超过运行主机的物理CPU总线线程数。
- 总核数=虚拟插槽数*每个插槽的核数。
 - 启用 NUMA 调度：启用可加快内存访问速率，提高虚拟机性能，需重启虚拟机才能生效。若需要透传 NUMA 拓扑给虚拟机，则该虚拟机需安装性能优化工具且配置的 CPU 总核数大于 8 核。启用该功能需要在“系统管理”大于“系统配置”的地方开启 NUMA 调度。
 - Host CPU：默认不开启。使用 Host CPU 后，与虚拟机所在主机 CPU 指令集关联性较强，可能会影响热迁移。
 - 高性能时钟：该选项只对 Windows 生效，启用后可以提高虚拟机数据库性能，开启该选项需要同时开启 Host CPU。
 - 启用 CPU 热添加：需要企业版授权，并且安装虚拟机性能优化工具。
 - 启用 CPU 独占：启用后虚拟机会独占宿主机 vCPU 资源，分配给虚拟机的 CPU 线程将不会再调度给其他虚拟机使用。
 - 限制 CPU 频率：启用可限制虚拟机 vCPU 使用的上限频率，限制范围为 100MHz-1000GHz，当虚拟机运行一周后会显示推荐值到输入框中。



B. 内存：虚拟机的内存分配，不超过单台主机的内存。

- 使用大页内存：对特定应用开启大页内存能提升虚拟机的性能，但开启此选项会导致虚拟机的内存预分配，开启大页内存后，虚拟机的内存回收机制将会被关闭，优先保障内存使用，提高业务性能。
- 启用内存热添加：需要企业版授权，并且安装虚拟机性能优化工具。



C. 磁盘：虚拟机磁盘分配，包括以下4种分配方式。

新磁盘

- 动态分配：根据数据占用情况动态地分配存储空间，在提升性能的同时存储空间使用率也可以提高，最大容量为 16T。
- 精简分配：根据实际数据占用大小，按需分配存储空间，可节省存储空间，最大容量为 63T。
- 预分配：预先分配固定的存储空间，可提升磁盘性能但是会占用较多存储空间，最大容量为 4T。
- 磁盘 IO 限制：该值表示虚拟机可占用的磁盘 IO 上限，可配置读/写速率，读/写次数限制，最大读/写速率限制范围为 128KB/s-102400MB/s，最大读/写次数范围限制为 16-2147483647，当虚拟机运行一周后，会显示推荐值到输入框中。使用 Virtio 磁盘：能够大幅提升虚拟机的磁盘 IO 性能，但是某些版本的操

作系统不支持此功能，可能会导致安装系统时找不到磁盘，建议不要更改默认设置。

- 空间回收：启用后，在删除磁盘上的文件时，将立即释放相应的存储空间，但对于 IDE 磁盘不生效。启用该功能需要操作系统支持 `discard`，windows2012/win8 开始支持 `discard`，linux 的是 4.18 内核开始支持，已测试操作系统如下表所示。

distribution	system version	kernel version	ext3	ext4	xfs	jfs2	btrfs
centos	CentOS 7.9.2009（不支持）	3.10	failed	failed	failed	N/A	N/A
	CentOS 8.0.1905		failed	failed	failed	N/A	N/A
	CentOS 8.1.1911	4.18	pass	pass	pass	N/A	N/A
	CentOS 8.2.2004	4.18	pass	pass	pass	N/A	N/A
	CentOS stream-8		pass	pass	pass	N/A	N/A
	CentOS 8.3.2011	4.18	pass	pass	pass	N/A	N/A
readhat	RHEL 8.0		failed	failed	failed	N/A	N/A
	RHEL 8.1		pass	pass	pass	N/A	N/A
	RHEL 8.2		pass	pass	pass	N/A	N/A
	RHEL 8.3		pass	pass	pass	N/A	N/A
	RHEL 8.4		pass	pass	pass	N/A	N/A
ubuntu	Ubuntu 18.04.6 LTS	4.15	pass	pass	N/A	N/A	N/A
	Ubuntu-18.04.4-desktop	2.6.24	failed	failed	N/A	N/A	N/A
	Ubuntu-16.10-server	4.8.0	failed	failed	N/A	N/A	N/A
	Ubuntu 20.04 LTS	5.4	pass	pass	pass	N/A	N/A
	Ubuntu 21.04		pass	pass	N/A	N/A	N/A

distribution	system version	FAT32	NTFS	HPFS	ReFS
Desktop	Windows7	Failed	Failed	N/A	N/A
	Windows8	Failed	Pass	N/A	N/A
	Windows8.1	Failed	Pass	N/A	N/A
	Windows10	Failed	Pass	N/A	N/A

	Windows10.1909	Failed	Pass	N/A	N/A
	Windows10.2004	Failed	Pass	N/A	N/A
	Windows10.20H2	Failed	Pass	N/A	N/A
	Windows11	Failed	Pass	N/A	N/A
Server	Windows2008R2	Failed	Failed	N/A	N/A
	Windows2012	Failed	Pass	N/A	-
	Windows2012R2	Failed	Pass	N/A	-
	Windows2016	Failed	Pass	N/A	Failed
	Windows2019 build 17763	Failed	Pass	N/A	Failed
	Windows2019	Failed	Pass	N/A	Failed

注意:

1. Windows 虚拟机原有磁盘和扩容磁盘均可启用。
2. Linux 虚拟机，已有磁盘禁止启用，原有虚拟机扩容磁盘，需要执行：`mount -O discard /dev/vdb1 /test`（斜体为自定义）
3. Linux 新建虚拟机，系统盘禁止启用，新建虚拟机的数据盘如果需要启用，在磁盘挂载的时候需要执行：`mount -O discard /dev/vdb1 /test`（斜体为自定义）

- 高级设置：条带数：指同时可以并发读或写的条带数量，这个数量等同于一个虚拟机同时使用的物理硬盘数量。该选项用来设置单台虚拟机的单块磁盘的条带数，建议采用默认设置。

注意:

集群初始化后条带化功能是默认启用的，为了保证最优的 I/O 性能效果，条带数的默认不会超过存储卷中任意一台物理主机上的数据盘个数。从 5.8.6 以下版本升级到 5.8.6 及其以上版本时，升级前所创建的虚拟机默认没有条带化功能，如需使用条带化功能，需将原升级前创建的虚拟机克隆一台出来，使用克隆后的虚拟机即可。

已有磁盘

使用早先创建的虚拟机的磁盘镜像文件，例如 **qcow2** 格式文件。

使用物理磁盘

将物理存储直接挂载给虚拟机使用。

使用虚拟共享盘

选择已有的虚拟共享盘，一般用于部署 Oracle RAC 等需要共享磁盘的应用。

- A. **光驱**：虚拟光驱，用于加载ISO光盘镜像到虚拟机中。
- B. **网卡**：指定虚拟机的网卡连接位置。在高级选项中可以指定网卡型号、MAC地址以及网卡的IP地址。其中：

网卡型号：默认为 **Virtio**。

MAC 地址：设置该网卡的 **MAC 地址**，保持自动获取即可，也可以手动指定。

- **IPv4 设置**：可设置网卡的 **IPv4 地址**，仅支持部分操作系统，支持的操作系统可在平台页面查看，且虚拟机需要安装性能优化工具后才可以生效。设置后需要等待一分钟后才能生效。
- **IPv6 设置**：可设置网卡的 **IPv6 地址**，仅支持部分操作系统，支持的操作系统可在平台页面查看，且虚拟机需要安装性能优化工具后才可以生效。设置后需要等待一分钟后才能生效。

C. **其他硬件和高级配置**：本手册“[虚拟机编辑](#)”章节。

4. 硬件信息选择完成后，选择[光驱1]，点击[加载ISO镜像文件]，点击[直接从本地上传镜像文件]。



进入上传界面，有两种方式，“选择本地镜像文件”和“上传到存储位置”。

- **选择本地镜像文件**：即事先准备好的 **iso 格式镜像**。
 - **上传到存储位置**：存放镜像的存储卷。
5. 选择完本地镜像及目标存储位置后点击<开始上传>。



6. 上传完成后，打开虚拟机控制台安装系统，安装完成后即完成了虚拟机的创建操作。



5.1.2. 虚拟机安装操作系统

5.1.2.1. Windows 系统安装

功能说明

需要为虚拟机安装全新的Windows server2012操作系统。

注意事项

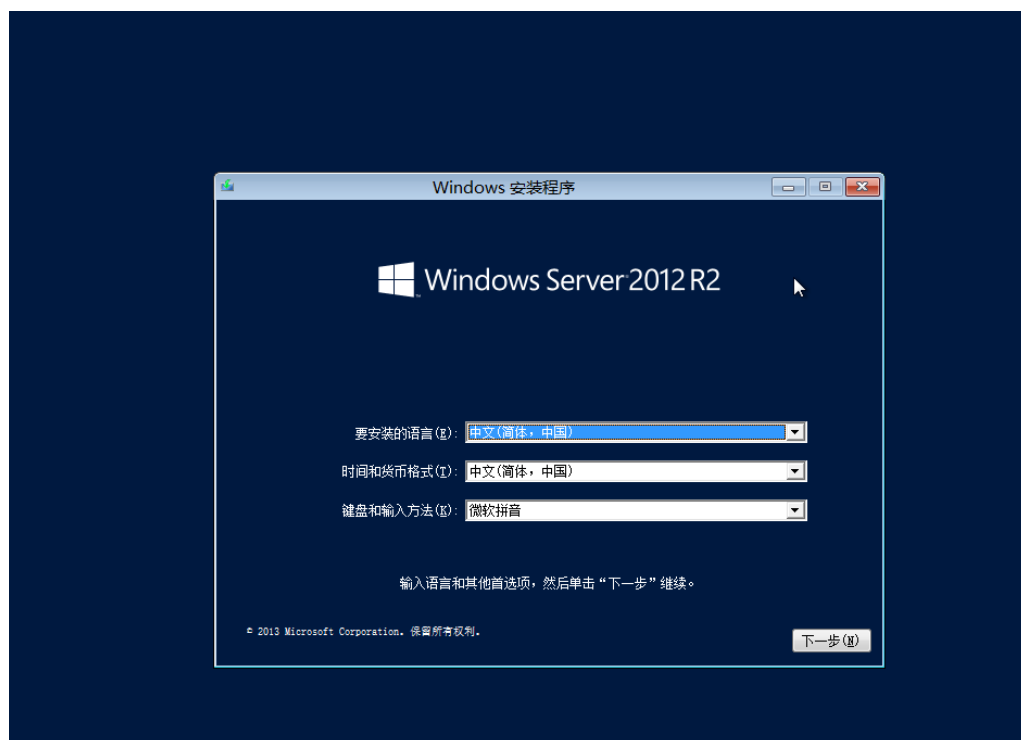
禁止使用外置windows共享目录上的镜像为虚拟机安装操作系统。

前提条件

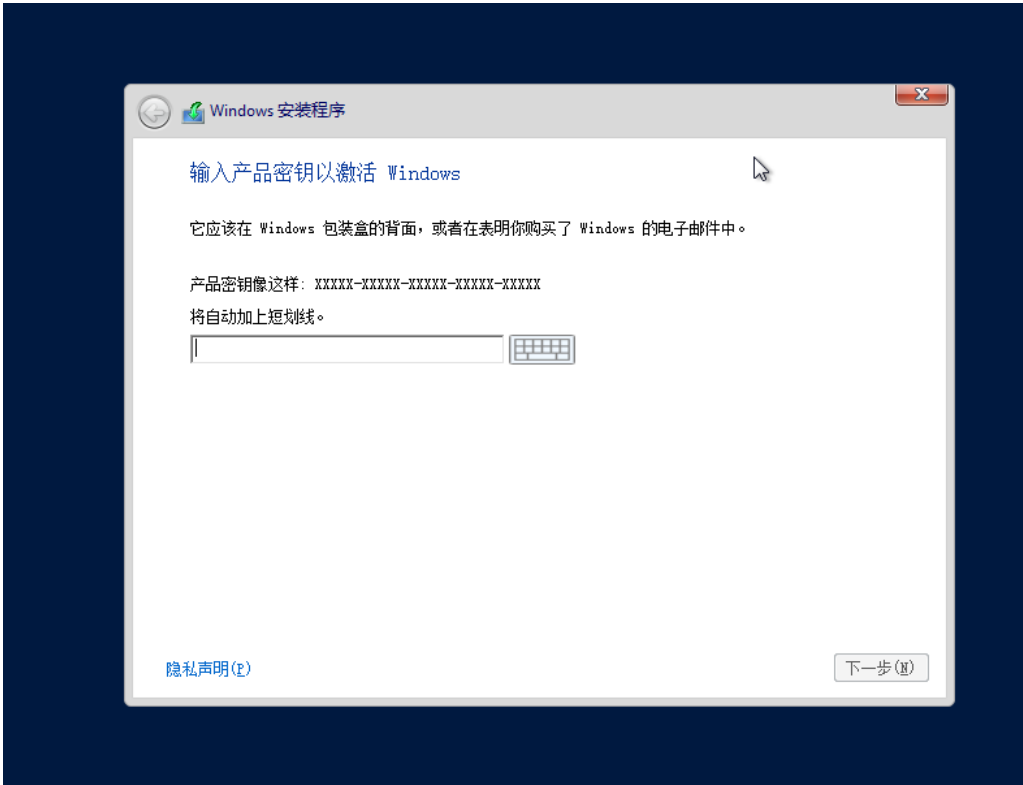
无

操作步骤

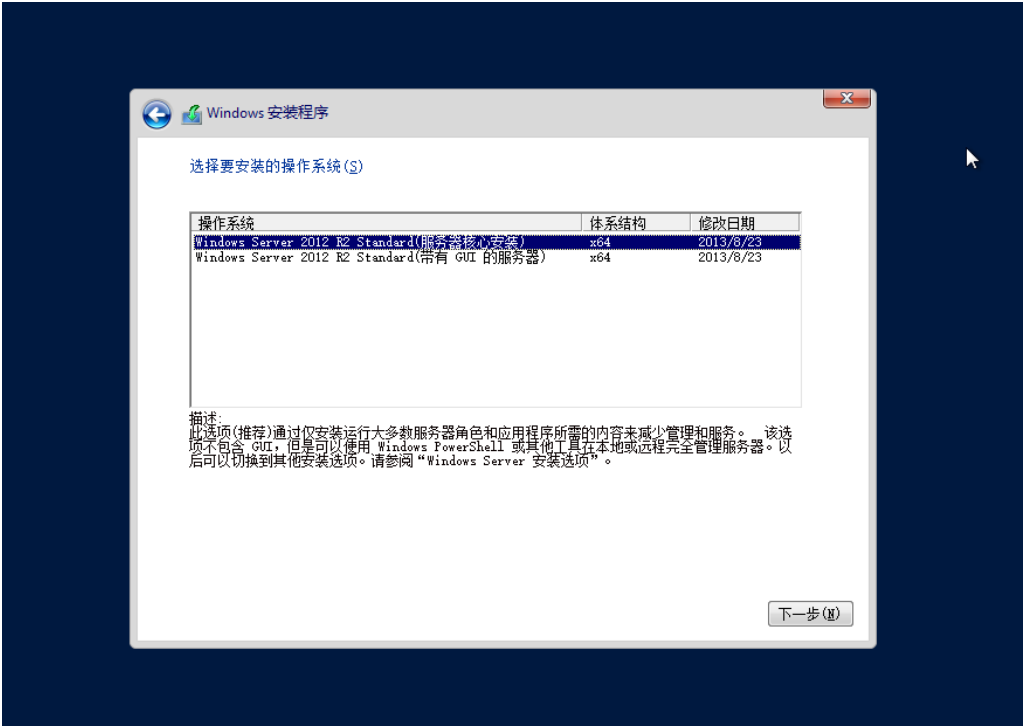
1. 根据“[创建全新虚拟机](#)”章节完成配置进入控制台。



2. 输入语言和其他首选项之后, 点击<下一步>继续, 点击<现在安装>进入安装步骤, 按照提示输入产品密钥。



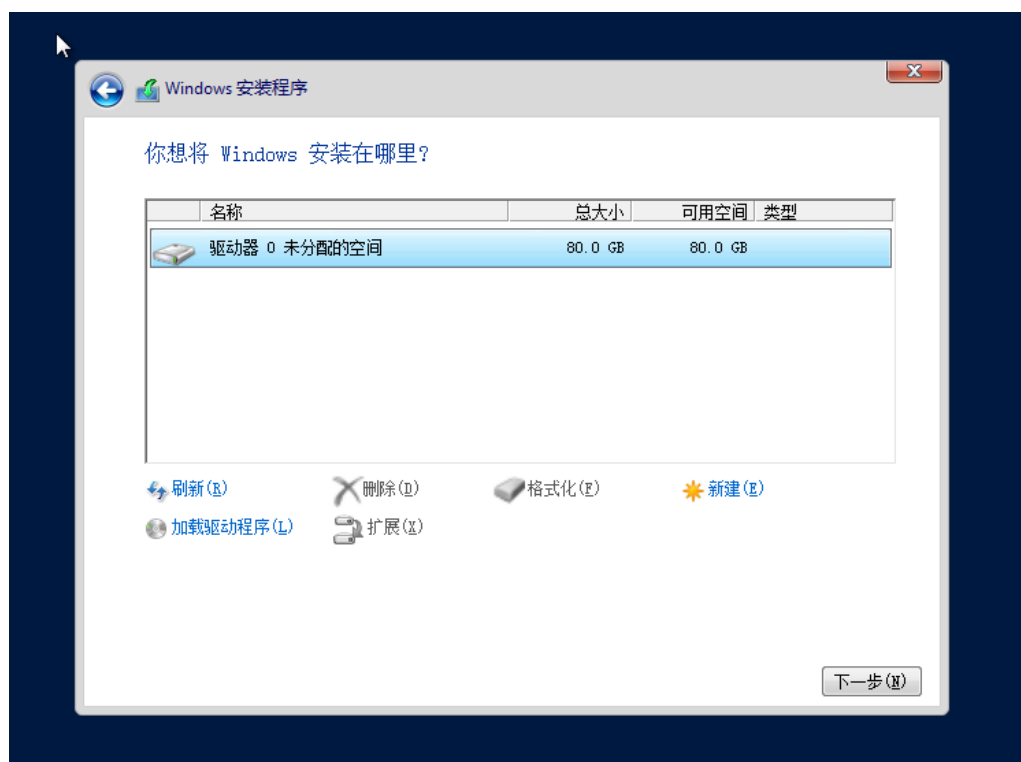
3. 选择需要安装的服务器版本，包括核心安装和带有GUI的安装，核心安装即 windows只有命令行界面，带有GUI的安装即存在桌面，这里选择第二个“带有GUI的服务器”安装。



4. 选择完毕之后点击<下一步>, 选择接受微软许可条款。进入下一步, 选择“自定义安装”。



5. 进入选择安装位置界面，可以看到我们分配的80G系统盘，选中点击<下一步>。



6. 至此Windows系统安装引导完毕，系统进入安装过程，耐心等待安装。



7. 重启开机，设置帐户密码即可进入系统。



8. 安装完成，进入windows界面，安装性能优化工具参考“[安装性能优化工具/Windows操作系统](#)”章节。

5.1.2.2. Linux 系统安装

功能说明

需要为虚拟机安装全新的RHEL 7.3 操作系统。

注意事项

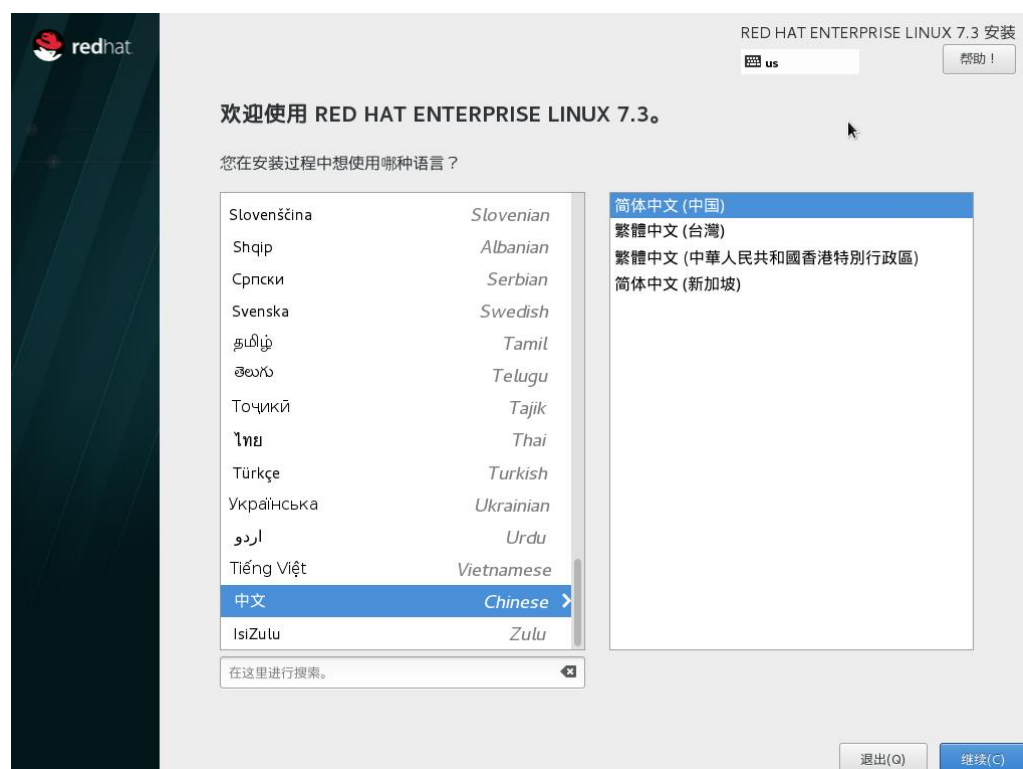
禁止使用外置windows共享目录上的镜像为虚拟机安装操作系统。

前提条件

无

操作步骤

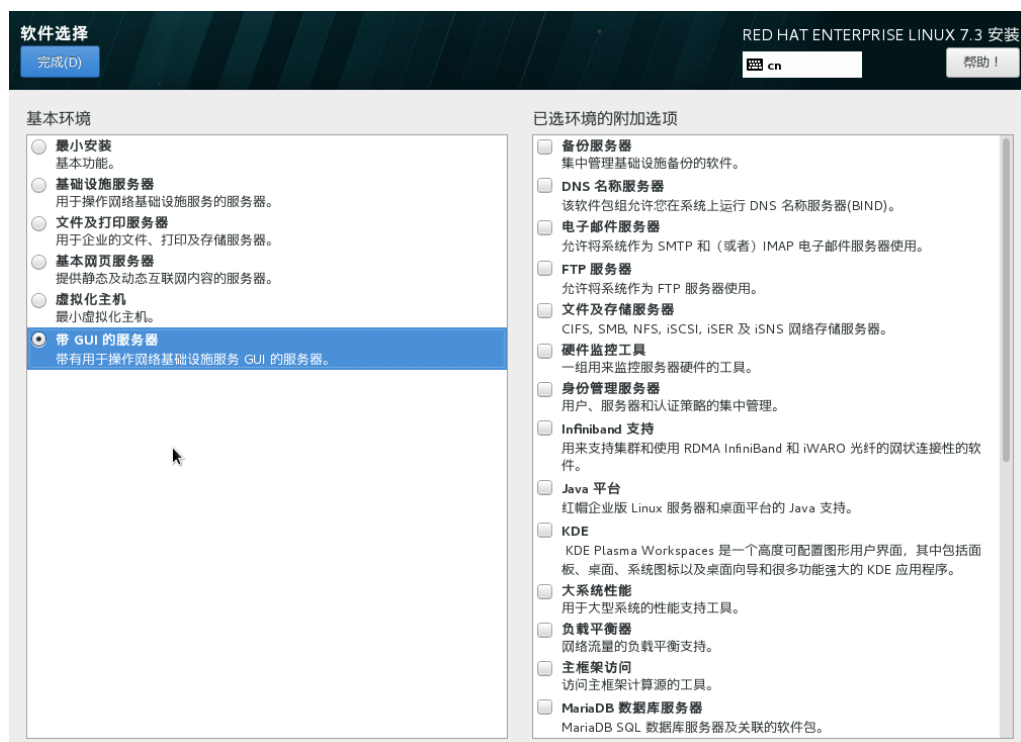
1. 根据“[创建全新虚拟机](#)”章节完成配置进入控制台，在安装界面按下回车开始引导安装，第一个界面选择安装语言（非系统语言），点击<继续>。



2. 进入到安装总览界面，确认安装相关信息是否错误，如果有不一致或需要修改的地方点击对应选项进行修改。



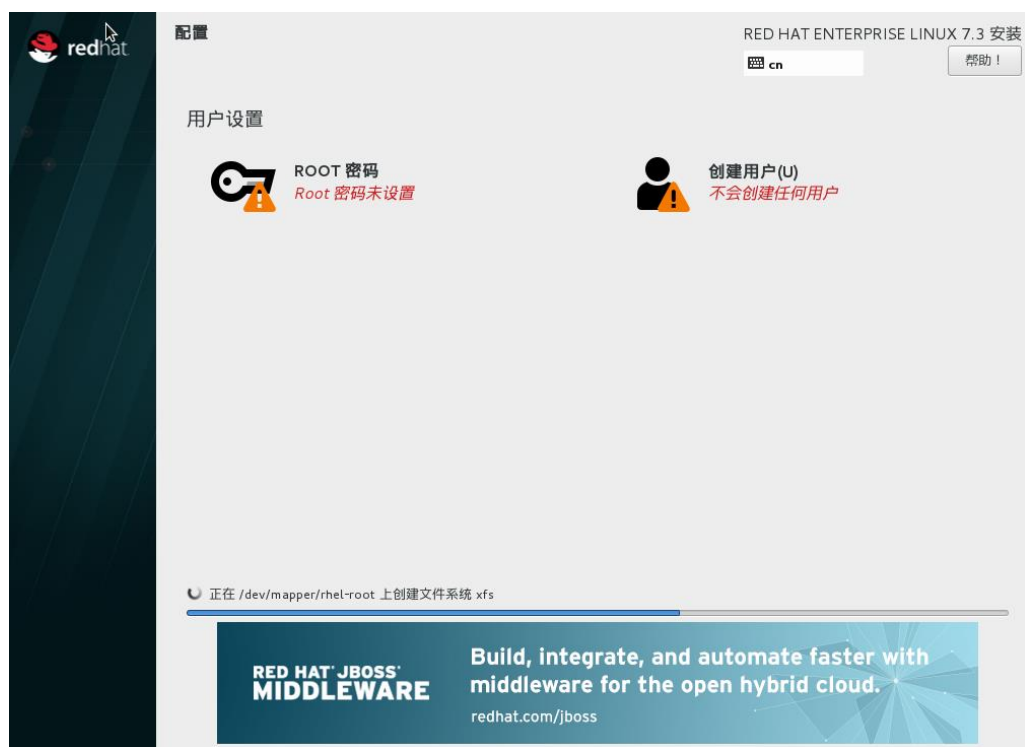
3. 默认软件安装选择的是最小安装，是无GUI界面的，我们可以点击[软件选择]，勾选GUI，也可以根据需要安装其他的软件。选择完毕点击<完成>。



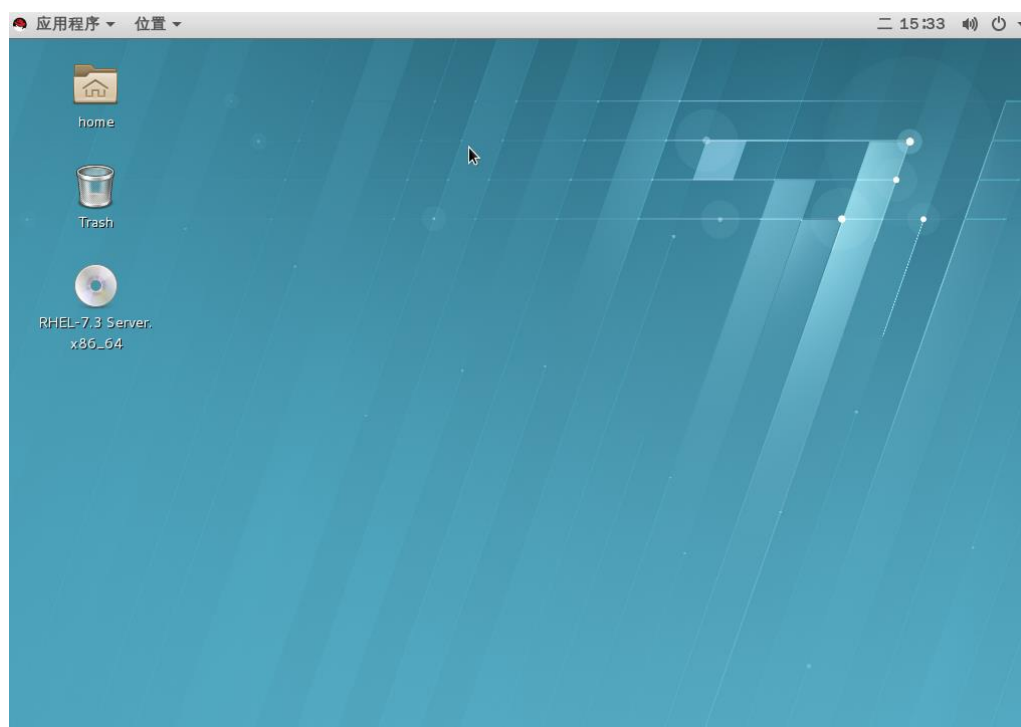
4. 安装位置要手动选择，点击[安装位置]进入到选择安装位置界面，可以看到分配的80G磁盘，选中该磁盘点击<完成>系统即可自动分区，如果有需要手动分区，勾选“我要配置分区”进入到分区界面。



5. 全部配置完毕之后，右下角的<开始安装>变为蓝色，点击即可开始安装。进入到安装界面，系统正在进行软件安装等工作。在此可配置ROOT密码与用户，如果不配置ROOT密码则无法完成安装。



6. 系统安装完成，重启进入系统，完成基础设置即可看到桌面。



7. 安装性能优化工具参考“[安装性能优化工具/Linux操作系统](#)”章节。

5.1.3. 导入 ova/vma/ovf 虚拟机

功能说明

当前已有虚拟化环境，需要将其它虚拟化平台中的虚拟机导出成vma、ova或ovf格式的虚拟机文件，再导入到HCI超融合平台中。

注意事项

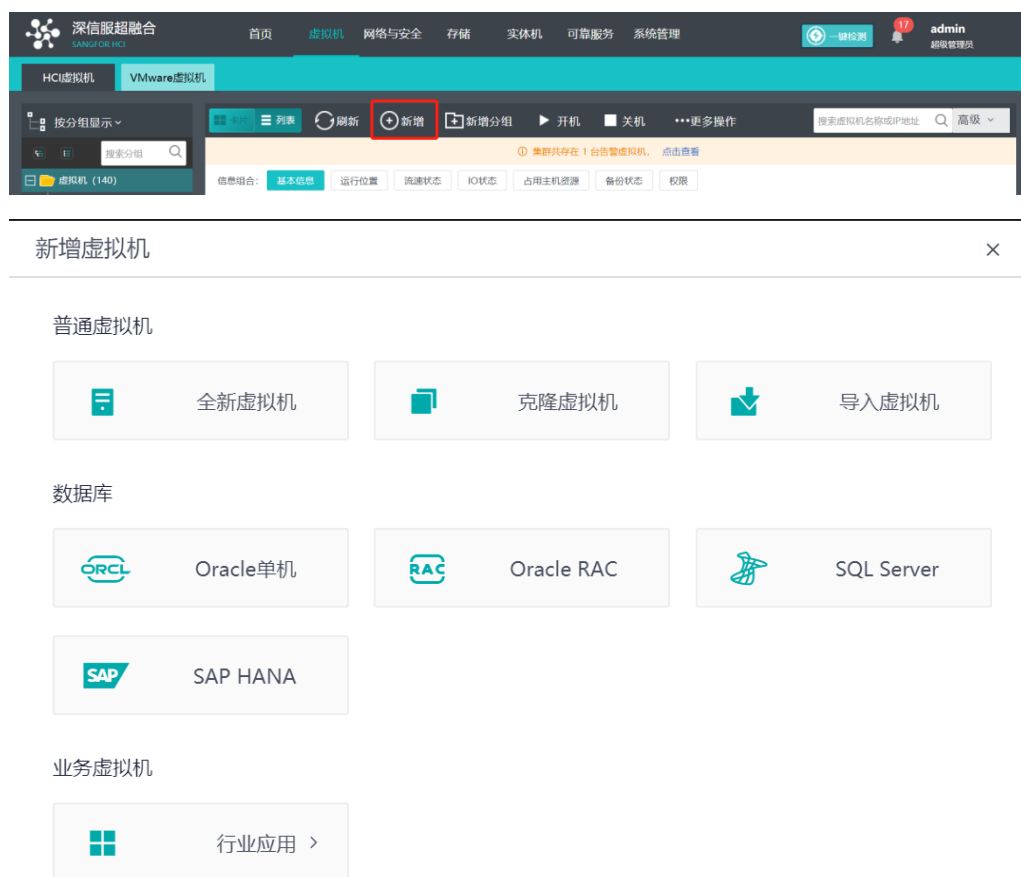
1. 从VMware Workstation中导出的虚拟机，如果名称带有中文，则无法导入到超融合平台，需要先重命名。
2. 不支持VMware网页控制端导出的ova导入超融合平台。
3. 所有的VMware上面导出的虚拟机，在导入到HCI平台之后，都要将VMware Tools卸载掉。

前提条件

vma、ova或ovf格式的虚拟机文件。

操作步骤

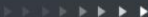
1. 在[虚拟机/新增]中选择<导入虚拟机>。



2. 选择以下信息，选填好以下信息后点击<开始导入>。

- 虚拟机文件：事先准备好的 **vma**、**ova** 或者 **ovf** 格式的虚拟机镜像。
- 分组：即将导入到 **HCI 超融合平台** 的虚拟机分组。
- 故障迁移（**HA**）：当主机发生故障时，触发共享存储上的虚拟机 **HA** 切换，使其从其他主机上恢复运行。
- 存储位置：指虚拟机的配置 **conf** 文件和虚拟磁盘 **qcow2** 文件的存放位置。
- 运行位置：指定虚拟机运行时使用哪个主机的 **CPU** 和内存资源，当“存储位置”选择为延伸卷时，还可以指定虚拟机的运行位置为某故障域，当指定为某故障域时，可以设置优先在所选位置运行或者必须在所选位置运行。
- 操作系统：请选择与导入的虚拟机文件一致的操作系统，以保证虚拟机的正常使用；如无法确定操作系统时，可使用默认。

从本地导入虚拟机文件



文件类型：

ova或vma

虚拟机文件：

请选择ova或vma格式文件

分组：

默认分组

故障迁移(HA)：

☒ 当设备所在主机出现故障时，自动切换到其它物理主机上运行。配置HA ①

存储位置：

虚拟存储卷1

运行位置：

<自动选择>

优先在所选位置运行

操作系统：

默认

开始导入

从本地导入ovf、mf、vmdk文件



文件类型：

ovf、mf、vmdk

虚拟机文件：

请选择ovf、mf、vmdk格式文件

分组：

yqtest

故障迁移(HA)：

☒ 当设备所在主机出现故障时，自动切换到其它物理主机上运行。配置HA ①

存储位置：

虚拟存储卷1

运行位置：

<自动选择>

优先在所选位置运行

操作系统：

默认

开始导入

3. 从本地导入虚拟机文件，导入过程中请勿关闭页面。

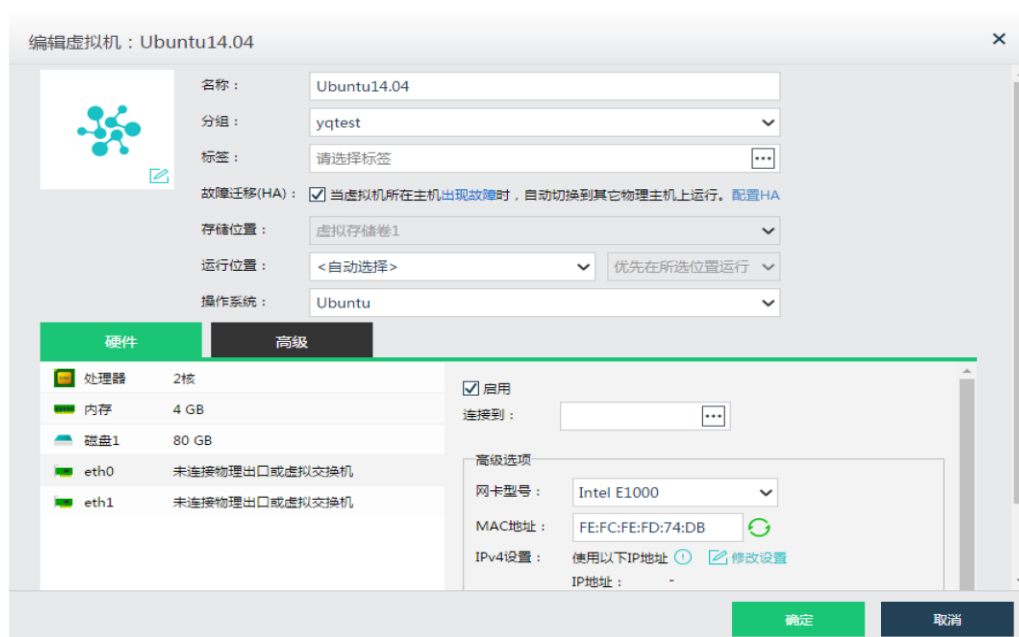


4. 从本地导入虚拟机文件成功，此时的虚拟机网卡未连接交换机，请点击<转到虚拟机>编辑虚拟机重新配置网卡。



5. 转到编辑虚拟机界面，点击[eth0]，选择相应的连接设备，全部编辑完毕后点击

<确定>，此时虚拟机导入操作全部完成。



5.1.4. P2V 迁移

功能说明

将现有物理主机或其他虚拟化平台上的虚拟机的Windows/Linux操作系统及业务数据打包，通过网络克隆到HCI超融合平台上，迁移完成后原业务系统即可在HCI超融合平台上以虚拟机的形态继续运行。迁移过程中对原操作系统不做任何修改。

注意事项

1. 迁移过程中需要保持网络稳定。
2. ISO和exe工具迁移虚拟机时，在超融合上操作都使用admin用户操作。
3. 如果待迁移的机器有个磁盘没有盘符，且分区大小大于HCI集群可用空间，实际占用小于可用空间，迁移时会报HCI空间不足，这时候需要对没有盘符的磁盘加盘符。
4. P2V迁移过程，数据拷贝完成，代理已经收到迁移完成的消息并用已有镜像创建虚拟机的过程中断网（在节点离线的环境下会出现），只是任务日志会失败，实际已经迁移成功。
5. 不支持配置了SR-IOV直通类型网卡的VMware虚拟机备份和迁移到HCI，迁移前需要在VMware/虚拟机查看对应的网卡类型是否满足类型，如果是SR-IOV网卡，可以让客户将VMware上虚拟机的网卡类型改成其他类型再迁移。SR-IOV网卡查看方法如下图所示。



6. winXP迁移到HCI和备份恢复到HCI后，由于winXP没有E1000的网卡驱动，因此网卡不会恢复，可以通过编辑网卡类型为rtl8139网卡来恢复，并且安装完VMtools后，左上角的安装VMtools提示不会消失。
7. 使用ISO包进行P2V迁移，要求物理机内存必须大于等于3G。
8. Oracle RAC虚拟机禁止用P2V方案迁移。
9. 迁移过程中断网了，如果要取消迁移，需源端和目标端分别取消，如果只在目的端取消，会在网络恢复时重新开始迁移，但并不会产生任何影响，再取消一次即可；如果是网络连接正常时，要取消迁移任务在任意端取消迁移任务均可。
10. Windows 操作系统物理服务器超过4块磁盘迁移，需要使用P2V迁移，Linux内核支持Virtio可以直接迁移。
11. Windows 2008 系统不能以UEFI安装，也不能直接迁移过来，会出现黑屏，如需迁移，请先升级到Windows 2008 R2再迁移。
12. P2V迁移时不迁移的磁盘分区，如果该分区默认簇大小是fat16格式，迁移完后分配单元大小为2048字节的分区会被自动格式化，而分配单元大小为4096字节的分区会提示损坏，手动格式化即可。
13. P2V迁移时不迁移的磁盘分区，如果是NTFS格式的分区时，迁移完后也无法自动格式化，迁移完也会提示分区损坏，手动格式化即可。
14. 取消正在进行的关机迁移任务，可以通过重启客户端主机或者在任务列表处取消迁移任务，但是重启客户端取消迁移任务时，迁移名额在15min之内不会释放，因此要等到15min后排队任务才会进入迁移状态。
15. 迁移前需检查客户有无脱机的磁盘。例如：存在磁盘1，2，3，4；磁盘3处于脱机状态，迁移时只允许迁移1，2，4；迁移至目标HCI后，原磁盘4编号前移变成3，迁移过去后导致磁盘4变成脱机状态。
16. 使用converter进行迁移，如果迁移虚拟机分辨率太高（测试2K显示器），则显

示软件配置界面会有问题，可能出现没有<下一步>或者<开始迁移>的按钮，需要调整分辨率。

17. P2V迁移不支持RAID-5卷、Linux LVM卷的优化拷贝，只支持简单卷、动态盘（简单卷）、跨区卷的优化拷贝。
18. P2V在线迁移只支持Windows操作系统，且不支持迁移过程中产生的增量数据。
19. Windows的P2V迁移不管是开机或者关机都不支持迁移外置iSCSI存储的数据。
20. 迁移前需要确保HCI序列号未过期。如果HCI序列号已过期，P2V业务提交过程未校验，迁移到99%后，因为无权限在HCI上新建虚拟机导致迁移业务失败。

前提条件

无

操作步骤

参考《深信服超融合HCI迁移指南》。

5.1.5. 虚拟机克隆

5.1.5.1. 全量克隆

功能说明

通过虚拟机全量克隆，可以创建一台或多台跟原有虚拟机完全一致且独立于原虚拟机的全新虚拟机。

注意事项

1. 克隆出来的虚拟机跟原有虚拟机信息完全一致，克隆完成后的虚拟机网口默认未启用，启用网卡前关闭原虚拟机或修改克隆后虚拟机IP，避免IP冲突。
2. 克隆出来的MAC地址会发生变化，Linux操作系统的虚拟机克隆出来后需要注意配置网络。
3. 避免虚拟机在备份时进行全量克隆。

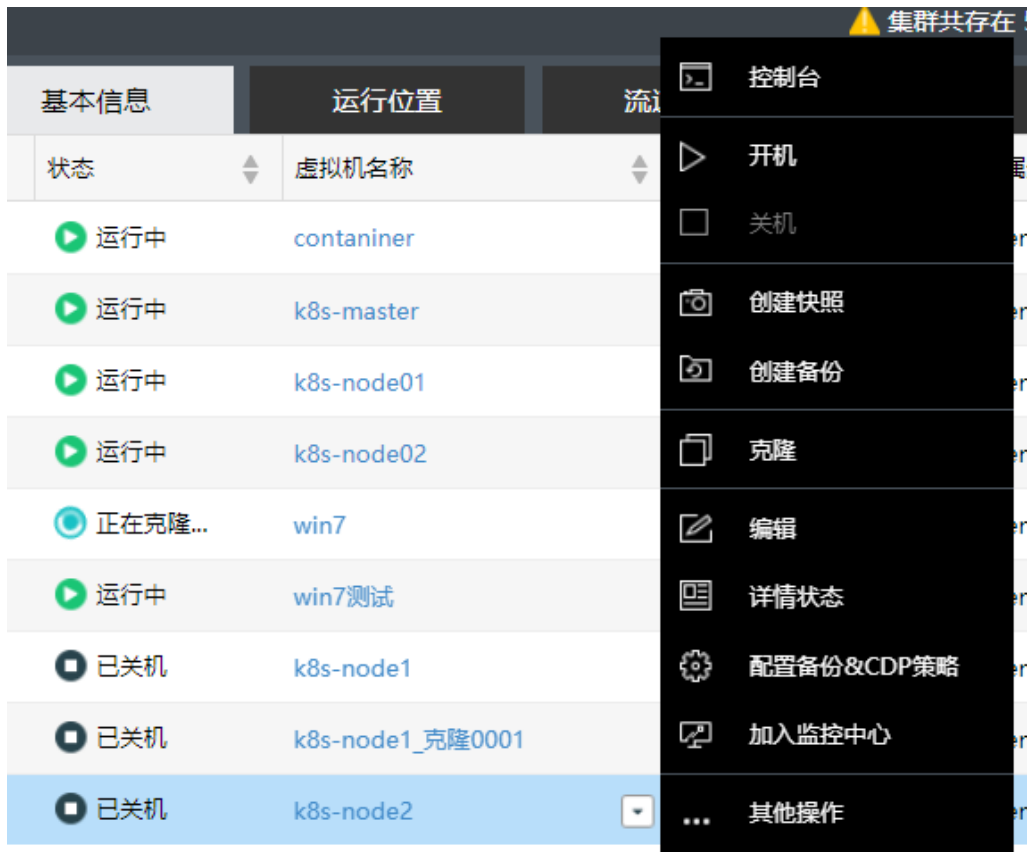
前提条件

在平台任务球处查看，源虚拟机没有其他任务在执行。

操作步骤

1. 在[虚拟机]页面中将鼠标放到需要克隆的虚拟机上，然后点击出现的下拉箭头，

并点击<克隆>。



2. 选择克隆方式为[全量克隆]，自定义虚拟机名称、需要克隆的虚拟机数量、分组、HA、存储位置、存储策略、运行位置等参数。



名称:

k8s-node2_克隆

数量:

1

生成虚拟机名称为: k8s-node2_克隆0001

描述:

分组:

ligen

克隆方式:

快速全量克隆 (推荐)

故障迁移(HA):

快速全量克隆 (推荐)

存储位置:

全量克隆

存储策略:

链接克隆

运行位置:

001 延伸卷

hostname:

<复用虚拟机存储策略: 2副本默认策略>

网络连接:

<自动选择>

优先在所选位置运行

网卡:

选填

查看支持的系统

网络配置:

☐ 启用克隆出来的虚拟机的网卡

网卡:

eth0

连接到:

网络配置

确定

取消

5.1.5.2. 快速全量克隆

功能说明

通过虚拟机快速全量克隆，可以创建一台或多台跟原有虚拟机完全一致且独立于原虚拟机的全新虚拟机。此方式具有虚拟机启动快、数据最终独立、克隆完成后性能完全无影响等特点，是平台推荐的克隆方式。

注意事项

快速全量克隆数据合并过程中无法对虚拟机进行编辑操作。

前提条件

要求源虚拟机和新虚拟机的存储位置均为虚拟存储。

操作步骤

1. 在[虚拟机]页面中将鼠标放到需要克隆的虚拟机上，然后点击出现的下拉箭头，并点击<克隆>。



2. 选择克隆方式为[快速全量克隆]，自定义虚拟机名称、需要克隆的虚拟机数量、分组、HA、存储位置、存储策略、运行位置等参数。



名称:

k8s-node2_克隆

数量:

1

生成虚拟机名称为: k8s-node2_克隆0001

描述:

分组:

ligen

克隆方式:

快速全量克隆 (推荐)

故障迁移(HA):

快速全量克隆 (推荐)

存储位置:

全量克隆

存储策略:

链接克隆

运行位置:

OUT延伸卷

存储策略:

<复用虚拟机存储策略: 2副本默认策略>

运行位置:

<自动选择>

优先在所选位置运行

hostname:

选填

查看支持的系统

网络连接:

☐ 启用克隆出来的虚拟机的网卡

网卡:

eth0

连接到:

网络配置

确定

取消

5.1.5.3. 链接克隆

功能说明

通过虚拟机链接克隆，可以创建一台或多台跟原有虚拟机完全一致且独立于原虚拟机的全新虚拟机。此方式具有1、虚拟机启动快；2、数据非独立，节省存储空间；3、克隆完成后，性能仍会有影响等特点，推荐在功能开发测试等性能不敏感场景使用。

注意事项

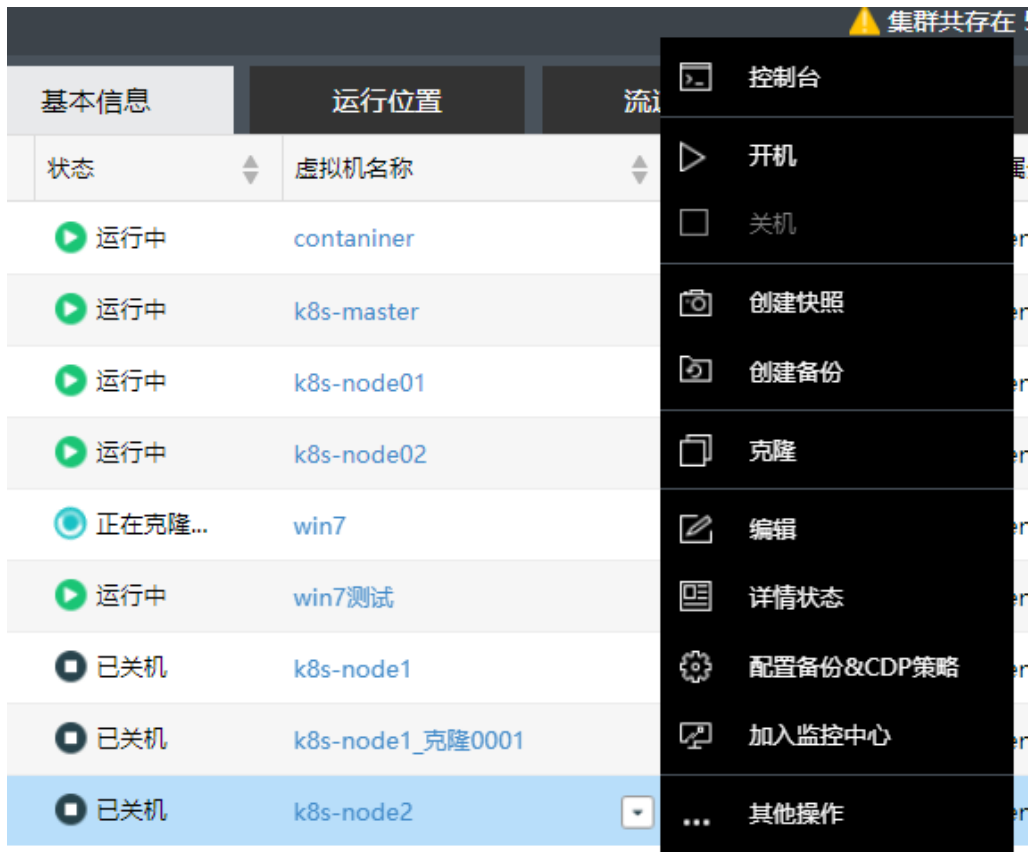
无

前提条件

要求源虚拟机和新虚拟机的存储位置均为虚拟存储。

操作步骤

1. 在[虚拟机]页面中将鼠标放到需要克隆的虚拟机上，然后点击出现的下拉箭头，并点击<克隆>。



2. 选择克隆方式为[链接克隆]，自定义虚拟机名称、需要克隆的虚拟机数量、分组、HA、存储位置、存储策略、运行位置等参数。



名称:

k8s-node2_克隆

数量:

1

生成虚拟机名称为: k8s-node2_克隆0001

描述:

分组:

ligen

克隆方式:

快速全量克隆 (推荐)

故障迁移(HA):

快速全量克隆 (推荐)

存储位置:

全量克隆

存储策略:

链接克隆

运行位置:

001延伸卷

hostname:

<复用虚拟机存储策略: 2副本默认策略>

网络连接:

<自动选择>

优先在所选位置运行

网卡:

选填

查看支持的系统

网络配置:

☐ 启用克隆出来的虚拟机的网卡

网卡:

eth0

连接到:

网络配置

确定

取消

5.1.6. 虚拟机模版部署

功能说明

通过虚拟机模版部署，会派生出跟原有虚拟机完全一致且独立于原虚拟机的全新虚拟机，该模板虚拟机可以被删除，但不能开机，只有转换为普通虚拟机后才可以正常开机使用。

注意事项

1. 进行模版部署操作后，模版虚拟机不能开机，也不可编辑，只有转换为普通虚拟机后才可进行上述操作。
2. 特定属性的虚拟机无法作为模板虚拟机，如配置了CDP策略。
3. 老版本升级到HCI6.8.0版本后，派生虚拟机与模板虚拟机之间保持原有的有链式关系：
 - 模版虚拟机无法被删除，只有当模版虚拟机部署的虚拟机均删除后才能删除该模版。
 - 删除模板和派生虚拟机到回收站，再从回收站还原派生虚拟机会失败。
4. 虚拟机使用独立磁盘，链式磁盘，物理盘，共享盘，USB外设不能转化为模板

虚拟机。

5. 模板虚拟机被删除后VDC的桌面池会受影响无法派生或更新模板。
6. 模板虚拟机在三节点及以上虚拟存储且派生到同一个虚拟存储上，用快速全量派生，其它存储用全量派生。

前提条件

无

操作步骤

1. 在[虚拟机]页面中将鼠标放到需要进行模板部署的虚拟机上，然后点击出现的下拉箭头，并点击<其他操作/模板部署>。



转换模板

×

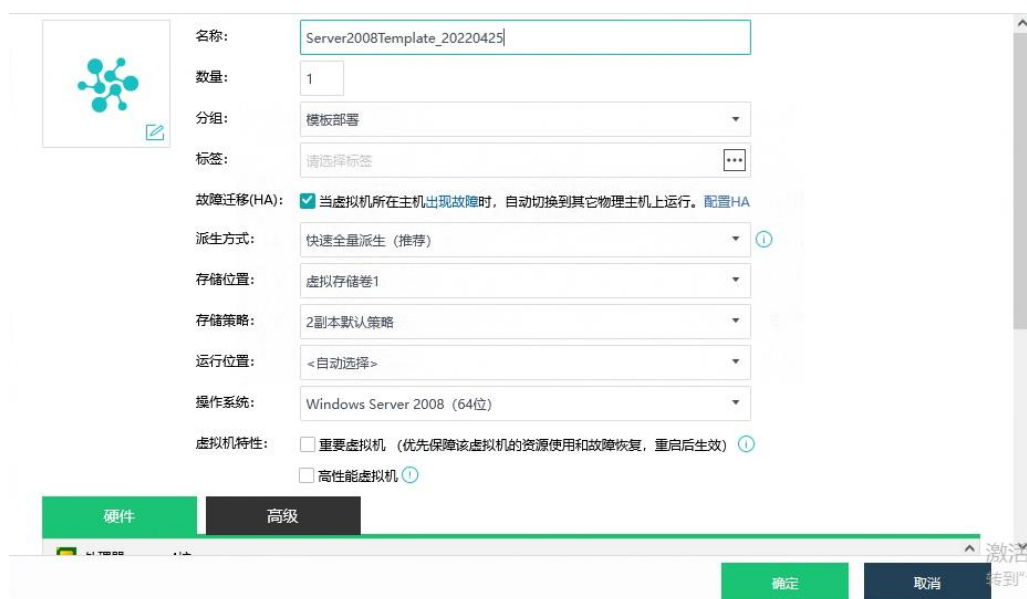


转换后模板将不能开机且不可编辑磁盘相关配置，请确认是否转换为模板？

确定

取消

2. 配置以下信息：配置完上述信息后点击<确定>。更多介绍参考本手册“[创建全新虚拟机](#)”章节。



3. 部署完成后，刷新虚拟机列表，模板虚拟机会展示“模板”的字样。



4. 支持将模板虚拟机转换为普通虚拟机，点击<更多/其他操作/转换为虚拟机>。



5.2. 虚拟机管理

5.2.1. 安装性能优化工具

5.2.1.1. Windows 操作系统

功能说明

所有运行于HCI超融合平台上的虚拟机均建议安装性能优化工具，其包含了驱动和应用程序，一是提供了高性能的半虚拟化接口驱动以提高虚拟机性能，二是将虚拟机信息透传给HCI平台，成功安装后在HCI平台上能查看虚拟机的CPU、内存占用率。

注意事项

1. 安装性能优化工具后需要重启虚拟机，此时如果从控制台对虚拟机强制关闭电源，则可能导致虚拟机蓝屏。因此最好使用虚拟机操作系统的重启功能，切勿使用HCI管理界面的重启电源。
2. Windows操作系统虚拟机安装性能优化工具后，如果因加入域需要执行sysprep等系统初始化操作（会重置网卡驱动），执行完重启虚拟机之前，需要先去掉“使用Virtio磁盘”选项（在虚拟机运行状态页面点击[卸载]），否则虚拟机会蓝屏无法启动。
3. Windows操作系统安装性能优化工具后，不会删除原有网卡，会增加新的FastIO网卡，名称会变化。如果希望将新的FastIO网卡重命名为原来的名称，会提示冲突，需先从注册表删除原来的网卡名称。
4. 未安装性能优化工具时，虚拟机使用IDE总线，总共支持4个磁盘或光驱。如果虚拟机已有4个磁盘，则无法再挂载光驱安装性能优化工具。可以手动复制安装文件进去执行安装，或者临时卸载磁盘并挂载光驱。
5. 提升虚拟机为域控前，需先手动配置网卡的IP再安装VMtools。
6. 目前支持安装性能优化工具的系统如下表所示。

系统类型	Windows	Linux
支持情况	服务器版本：Windows2003SP2 以后 到 Windows2019 个人版：XPsp3 到 win10	内核大于 2.6.25 的

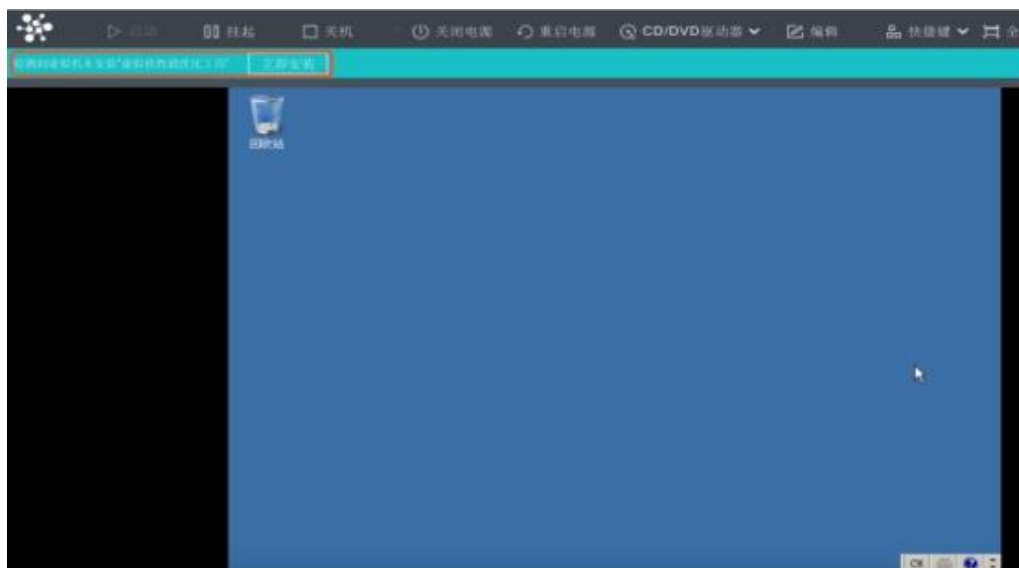
前提条件

虚拟机处于开机状态。

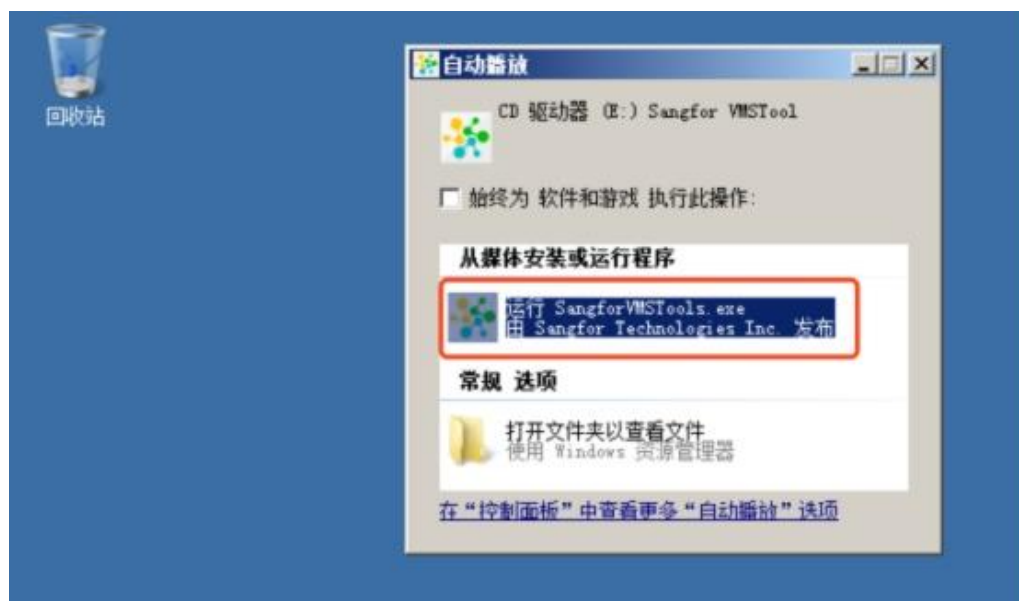
操作步骤

以windows2008为例说明：

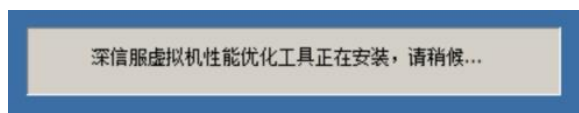
1. 打开刚导入或者新安装完操作系统的虚拟机控制台，会弹出如下提示。



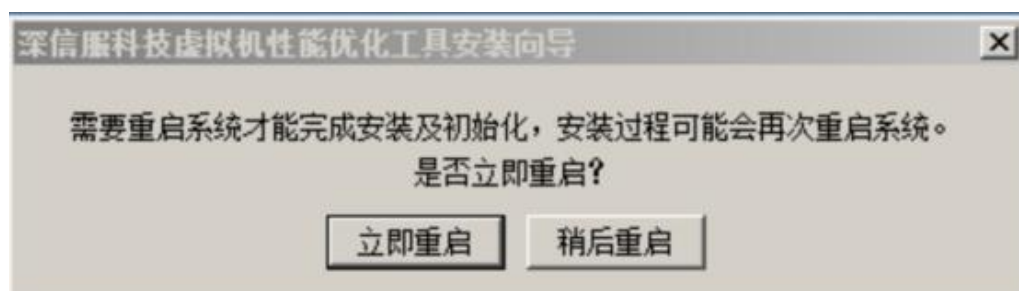
2. 点击<立即安装>，会出现如下页面，然后点击[运行SangforVMSTools.exe]。



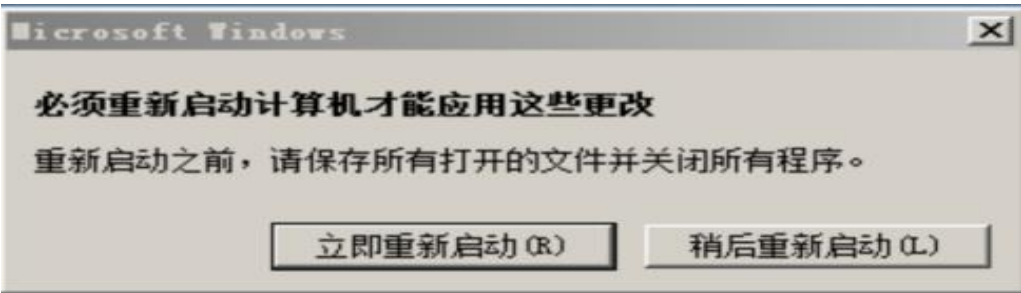
3. 虚拟机桌面会提示“深信服虚拟机性能优化工具正在安装，请稍候…”。



4. 弹出重启提示，如下，点击<立即重启>。



5. 重启后会再次弹出如下提示，点击<立即重新启动>。



6. 将鼠标放到刚安装好性能优化工具的虚拟机上，然后点击出现的下拉箭头，并点击<详情状态>。在[信息]页面可以看到虚拟机性能优化工具已经安装好了。



虚拟机名称:	2008-test
描述:	点击编辑描述信息
分组:	ligen
存储位置:	192.200.244.213;192.200.244.214;192.200.244.211;192.200.244.212
运行位置:	<自动选择>
当前运行主机:	192.200.244.212 (机房1)
调度策略:	-
操作系统:	Microsoft Server 2008 (64位)
虚拟机性能优化工具:	正在运行 重新安装
重要虚拟机:	否
开机自启动:	否
启用内存回收机制:	是 (已回收内存 77.05 MB)
启动顺序:	磁盘1
运行时长:	2天22小时40秒

5.2.1.2. Linux 操作系统

功能说明

所有运行于HCI平台的虚拟机均建议安装性能优化工具。

前提条件

虚拟机处于开机状态。

前提条件

虚拟机添加了虚拟光驱。在编辑虚拟机的页面查看是否有光驱。



操作步骤

以CentOS 6.4为例说明

1. 在控制台界面点击<立即安装>打开刚导入或者新安装完操作系统的虚拟机控制台，控制台弹出如下提示，支持自定义安装路径。



2. 挂载优化工具：创建挂载点，挂载 / dev/sr1，执行install.sh 脚本，安装完毕后，输入yes重启虚拟机。

```
[root@localhost ~]# mkdir /mnt/cdrom
[root@localhost ~]# mount /dev/sr1 /mnt/cdrom/
mount: block device /dev/sr1 is write-protected, mounting read-only
[root@localhost ~]# cd /mnt/cdrom/
[root@localhost cdrom]# ./install.sh
Install virtio success.
Everything is OK. Need to reboot!
reboot now(yes/no)?yes_
```

3. 确认工具是否安装：将鼠标放到刚安装好性能优化工具的虚拟机上，然后点击出现的下拉箭头，并点击<详情状态>。在[信息]页面可以看到虚拟机性能优化工具已经安装好了。

深信服超融合
SANGFOR HCI

首页 虚拟机 网络与安全 存储 实体机 可靠服务 系统管理

一键检测 37 admin 超融合管理员

HCI虚拟机 VMware虚拟机

按分组显示 搜索分组

EDS-ic (3) EDS-lyx (1) KubeManager (3) POC (12) acmp (2) acmp_2020-07-30-14-55- baiwei (12) PaaS (9) VMware (1) 补丁服务器 (1) fanghaorui (6) ligen (15) TenxCloud (0) kubemanager (0) 培训 (10)

列表 刷新 新增 新增分组 开机 关机 更多操作

搜索虚拟机名称或IP地址 高级

集群共存在 1 台告警虚拟机。 点击查看

信息组合: 基本信息 运行位置 流控状态 IO状态 占用主机资源 备份状态 权限

状态	虚拟机名称	IP地址	所属分组	CPU利用率	内存利用率	磁盘利用率
警告	centos-test	-	EDS-ic	1%	6%	1%
运行中	CentOS-7-x86_64-...		anager	4%	6%	1%
运行中	CentOS-7-x86_64-...		anager	3%	6%	1%
运行中	CentOS-7-x86_64-...		anager	3%	6%	1%
运行中	Docker 01_克隆			4%	8%	3%
运行中	MySQL单机_acmp-...			7%	12%	24%
运行中	Sangfor_SCP_6.2.0					
运行中	testthr_acmp-4267			4%	100%	98%
运行中	win2012			0%	21%	8%
运行中	zsg的测试机			17%	30%	44%
运行中	管理集群 master00...			15%	15%	8%

控制台 开机 关机 创建快照 创建备份 克隆 编辑 详情状态 配置备份&CDP策略 加入资源中心

虚拟机名称: CentOS-6.4-i386-minimal

描述: 点击编辑描述信息

分组: 默认组

存储位置: 172.200.200.123;172.200.200.121

运行位置: 172.200.200.123

操作系统: CentOS

虚拟机性能优化工具: 正在运行 重新安装 卸载

重要虚拟机: 否

开机自启动: 否

启用内存回收机制: 是 (已回收内存 223.29 MB)

启动顺序: 磁盘1->光驱

运行时长: 3分46秒

磁盘兼容性驱动: 导入

文档版本 06 (2023-02-21)

142

5.2.2. 卸载性能优化工具

5.2.2.1. Windows 操作系统

功能说明

当由于某些原因（CPU，内存显示不准）时，可能需要卸载性能优化工具重新进行安装。

注意事项

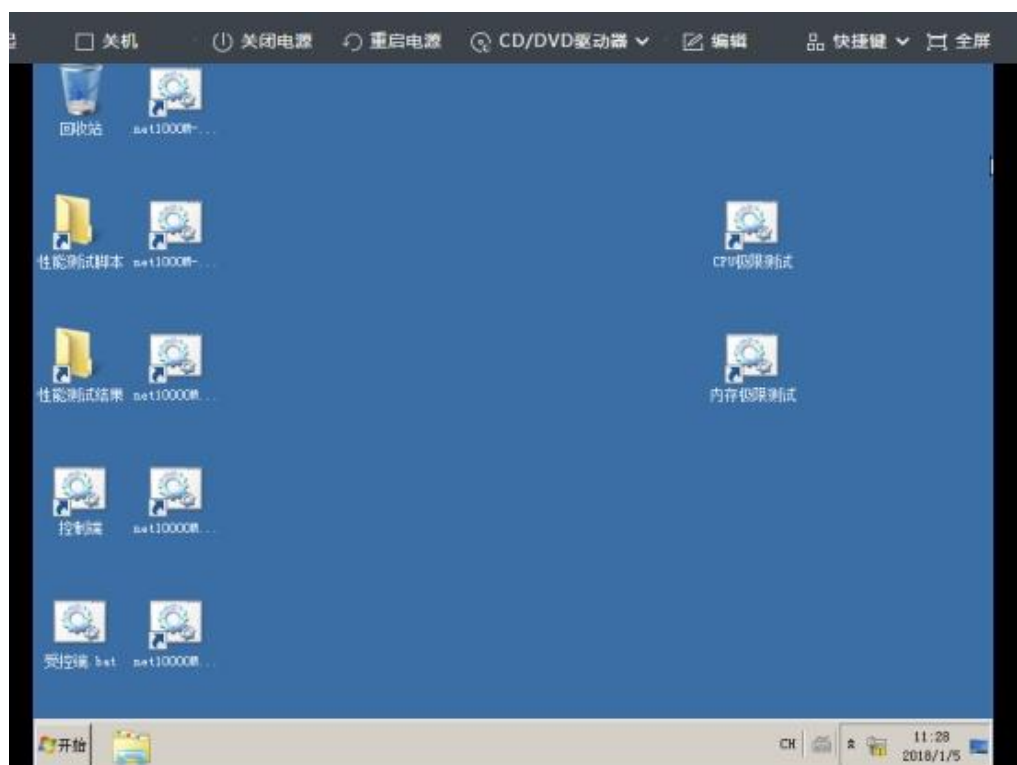
必须要在控制面板中进行卸载，禁止使用第三方工具进行卸载。

前提条件

需要虚拟机的管理员密码。

操作步骤

1. 登录虚拟机的控制台，输入密码进入虚拟机的管理界面。



2. 进入[开始/控制面板/卸载程序]。



3. 找到“深信服虚拟机性能优化工具”点击进行<卸载>。



4. 卸载完成后重启虚拟机。



5.2.2.2. Linux 操作系统

功能说明

当由于某些原因（CPU，内存显示不准）时，可能需要卸载性能优化工具重新进行安装。

注意事项

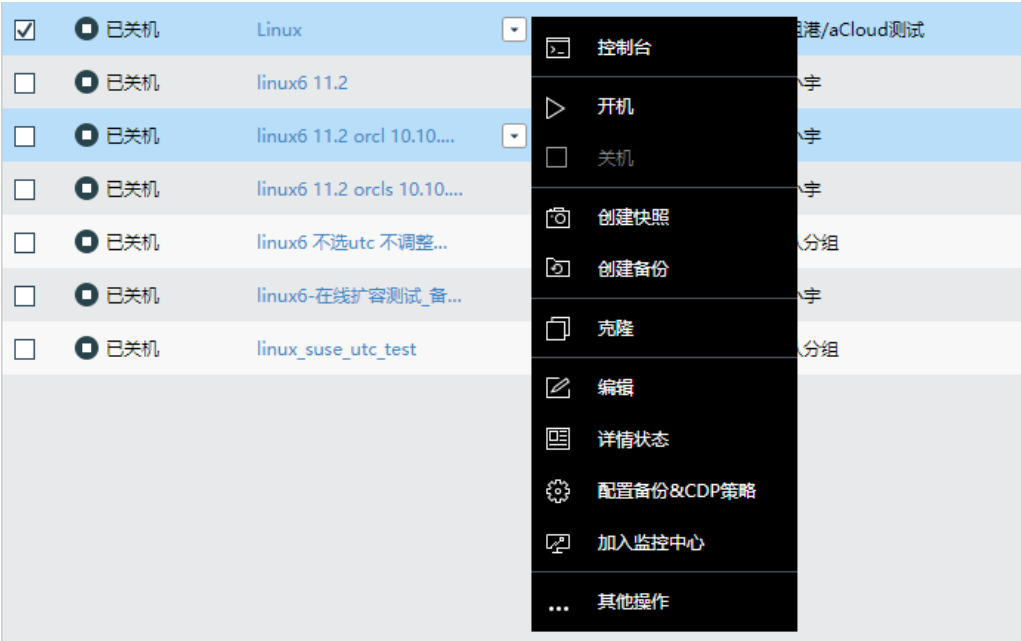
无

前提条件

无

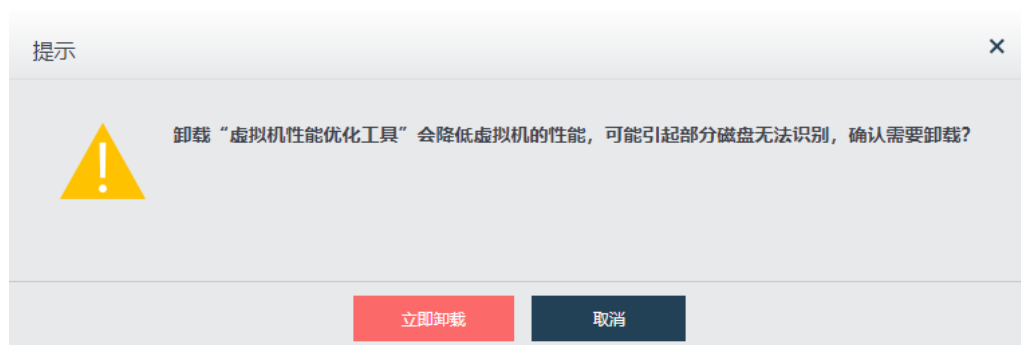
操作步骤

1. 登录HCI控制台，在[虚拟机]页面中找到要卸载性能优化工具的虚拟机，然后进入[详情状态]。



2. 在[信息]栏中，点击[卸载]就可以成功卸载性能优化工具。

虚拟机名称:	Linux
描述:	点击编辑描述信息
分组:	/aCloud测试
存储位置:	192.200.244.214;192.200.244.212
运行位置:	<自动选择>
当前运行主机:	-
调度策略:	-
操作系统:	CentOS
虚拟机性能优化工具:	已安装 重新安装 卸载
重要虚拟机:	否
开机自启动:	否
启用内存回收机制:	是
启动顺序:	磁盘1->光驱
关机时长:	0天



5.2.3. USB 映射

功能说明

已有的一些物理服务器上原本接了USB设备，将这些服务器迁移部署到虚拟化平台上之后，需要把这些USB设备插在虚拟化平台上映射给虚拟机，或者是部署在虚拟化平台上的虚拟机要用到USB设备，需要将插在虚拟化平台的USB设备映射给虚拟机。

注意事项

1. 接入USB前需放通USB设备。
2. 支持跨主机映射，例如将USB设备插在主机A上，虚拟机运行位置在主机A或其他与A在同一集群内的主机时均支持。

3. 虚拟机故障重启、目标端USB设备网络中断等异常情况恢复后自动重映射。
4. USB设备需要在管理页面编辑为准入状态方可映射给虚拟机使用，未编辑准入的USB设备，虚拟机映射USB无法找到该USB设备。

前提条件

USB外设一件。

操作步骤

以U盘为例

1. 任选一个USB口接入设备，如果有组成集群，任意选一台主机接入USB外设。接入USB设备之后界面上会有如下图提示，点击<立即配置>。



2. 选择该U盘需要连接的虚拟机，选好之后点击<确定>。



3. 在步骤2中选中的虚拟机中就可以看到映射的U盘了，如图中的F盘就是所接入的U盘。



4. 如果要修改U盘跟虚拟机的映射，可以在虚拟机编辑页面进行修改。将鼠标放到需要编辑的虚拟机上，然后点击出现的下拉箭头，选择<编辑>。



5. 在[实体机]目录下菜单点击[USB]，即可对USB列表中的USB设备进行单独或批量操作管理，如准入、屏蔽、删除等。支持将USB设备列表及状态导出Excel。



5.2.4. 虚拟机磁盘容量扩容

5.2.4.1. Windows 操作系统

功能说明

扩大已有虚拟机磁盘，新增磁盘请参考本文档“[虚拟机编辑](#)”章节。

注意事项

1. 磁盘分区列表有MBR和GPT两种，其中MBR分区列表支持最大2TB硬盘，GPT分区列表支持最大128PB(1PB=1024TB)。虚拟机磁盘大小请参照最佳实践配置。
2. HCI5.8.7R1及以前版本扩容虚拟机的单块磁盘大小需要关闭虚拟机。
3. HCI5.8.8开始支持开机扩容磁盘。
4. 虚拟机支持在线添加新硬盘。
5. ide磁盘类型不支持磁盘热扩容，需要安装VMtools。
6. 派生虚拟机不支持扩容系统盘。
7. 由于操作系统本身原因，Windows Server 2016 Datacenter版系统盘不支持扩容。
8. 在存储比较小的情况下，创建大存储的动态盘，有可能创建失败。例如：4T的虚拟存储上创建63T的动态盘。
9. 预分配的磁盘扩容的时候，扩容后的磁盘类型为精简分配。例如原本为80G的磁盘扩容到100G，扩的那20G为精简分配。

前提条件

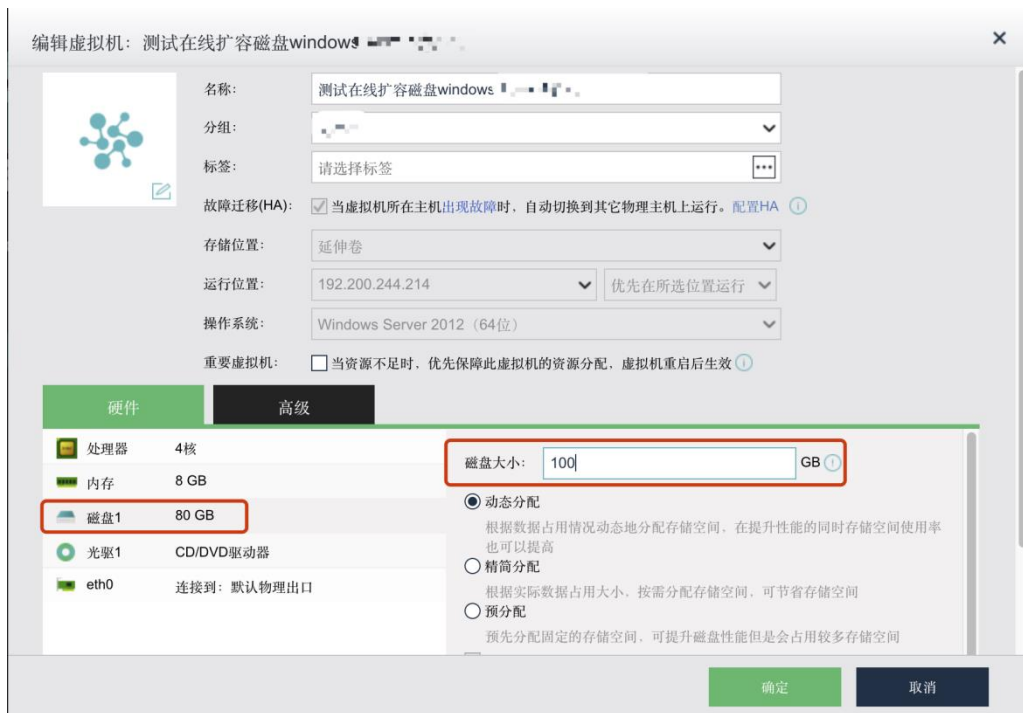
开机扩容需要安装性能优化工具VMtools，且启用Virtio磁盘。

操作步骤

1. 选择编辑：将鼠标放到需要扩容磁盘的虚拟机上，然后点击出现的下拉箭头，选择<编辑>。



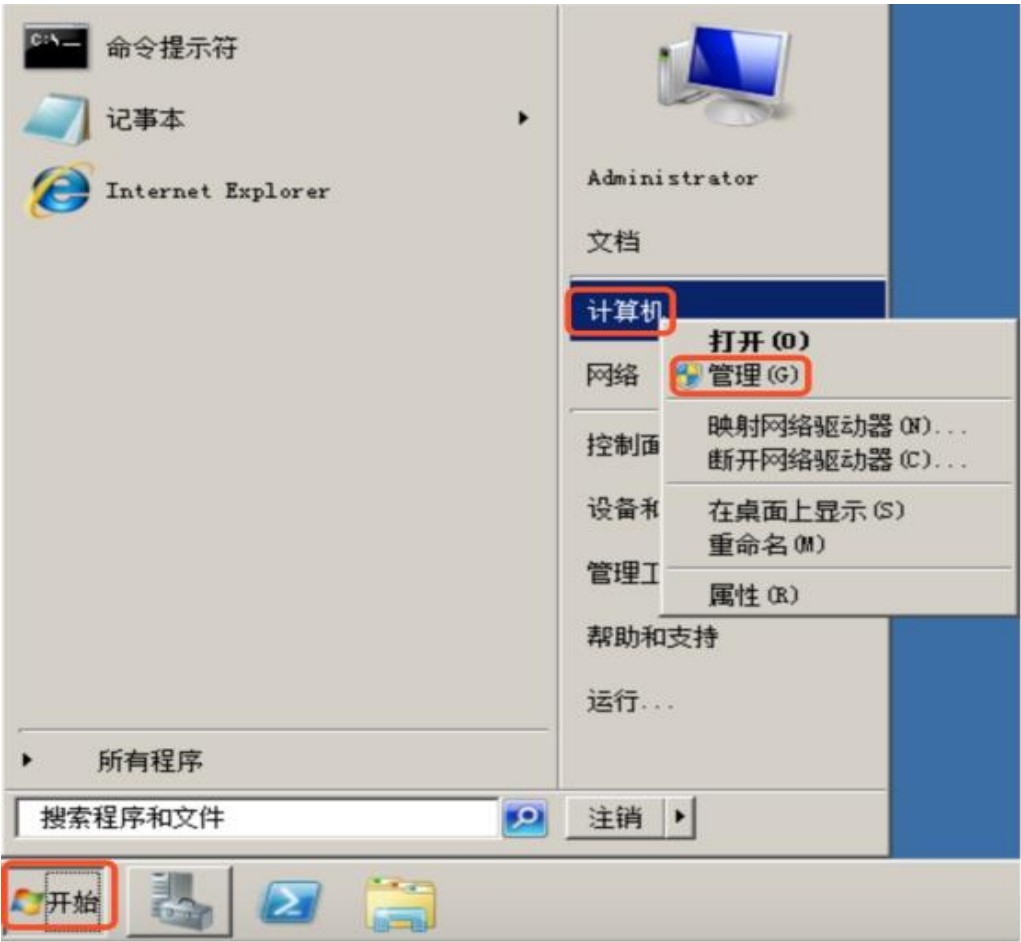
2. 编辑虚拟机磁盘：将磁盘大小调大至需要的大小，本例中磁盘大小从80GB调至100GB，然后点击<确定>。



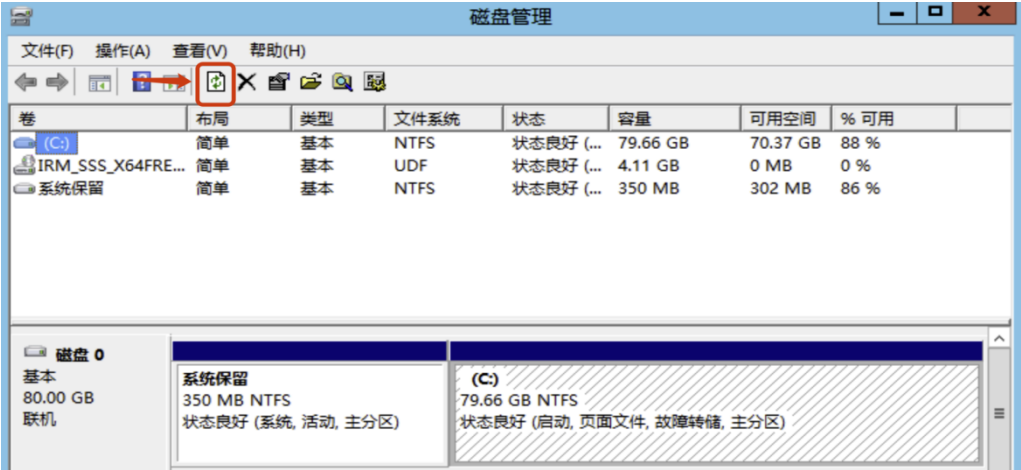
3. 进入虚拟机控制台：将鼠标放到该虚拟机上，然后点击出现的下拉箭头选择<控制台>，打开虚拟机的控制台。



4. 虚拟机磁盘管理：进入<开始/计算机/管理>打开服务管理器，然后点击[磁盘管理]。



5. 刷新磁盘信息：点击磁盘管理工具栏中的刷新按钮，识别到新扩展的空间后，新的空间可以用来新建简单卷，也可以对已有卷做扩展卷操作，以下演示扩展卷。如下图所示。



6. 在需要添加的磁盘上，右键点击，然后点击[扩展卷]，会弹出扩展卷向导，扩展的过程简单，根据系统提示操作，不再赘述。



7. 完成添加：如下图所示，成功完成磁盘扩容操作。



5.2.4.2. Linux 操作系统

功能说明

扩大已有虚拟机磁盘，新增磁盘请参考本文档“[虚拟机编辑](#)”章节。

注意事项

1. 适用于使用了LVM的虚拟机。
2. HCI5.8.7R1及以前版本扩容虚拟机的单块磁盘大小需要关闭虚拟机操作。
3. HCI5.8.8R1虚拟机支持开机扩容磁盘，添加新磁盘。
4. 本手册中虚拟机系统部分，在于演示扩容的一种可行方式，在于演示Linux扩容过程，并非唯一扩容方式，操作者应该完全理解演示中各个命令及参数的意义，并能根据实际需求做相应调整。
5. ide磁盘类型不支持磁盘热扩容，需要安装VMtools。
6. 派生虚拟机不支持扩容系统盘。
7. 在存储比较小的情况下，创建大于存储的动态盘，有可能创建失败。

前提条件

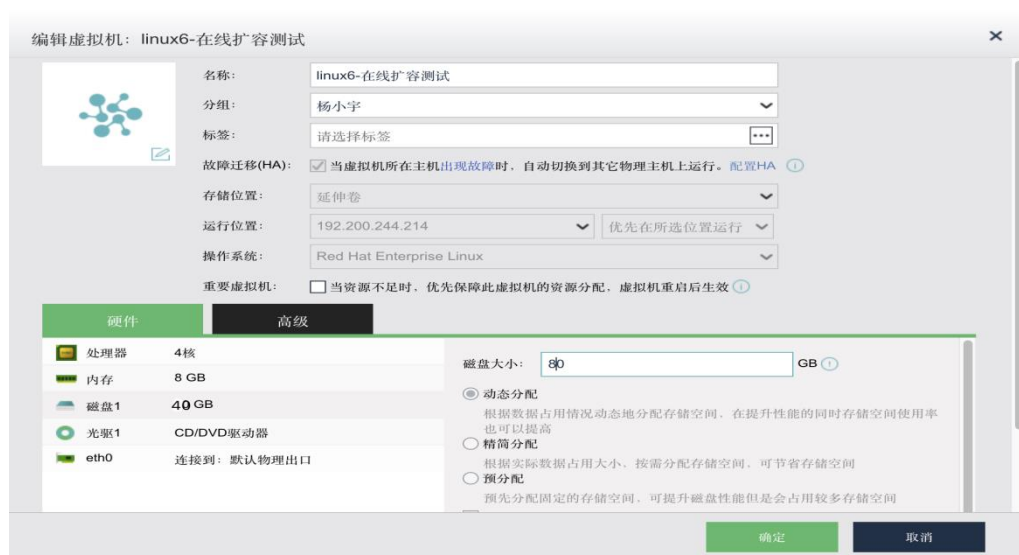
1. 开机扩容需要安装VMtools，且启用Virtio磁盘。
2. 以下用CentOS6.4演示，根目录挂载点扩容。

操作步骤

1. 编辑虚拟机：点击需要扩容磁盘的虚拟机下拉箭头，选择[编辑]。



2. 调整磁盘大小：将磁盘调整到规划的大小，本演示将磁盘从40GB调整为80GB，修改后点击<确定>。如果虚拟机是关闭状态，开启虚拟机，进入控制台。



3. 查看当前信息：通过“lsblk”命令查看扩展后的磁盘信息，磁盘为“/dev/vda”，vg为“VolGroup”，lv为“/dev/VolGroup/lv_root”。


```
[root@localhost ~]# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sr0                                  11:0    1 1024M  0 rom
vda                                  252:0    0   80G  0 disk
├─vda1                              252:1    0  500M  0 part /boot
├─vda2                              252:2    0 39.5G  0 part
└─VolGroup-lv_root (dm-0) 253:0    0 31.7G  0 lvm /
   └─VolGroup-lv_swap (dm-1) 253:1    0  7.8G  0 lvm [SWAP]
```

4. 磁盘分区：通过“fdisk /dev/vda”进入磁盘分区，输入“p”，查看当前分区，目前演示环境中“/dev/vda”磁盘已经有两个主分区，添加一个新的分区号为3，新的分区设备名为“/dev/vda3”，cylinder 起始为83221。

```
[root@localhost ~]# fdisk /dev/vda
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').

Command (m for help): p

Disk /dev/vda: 85.9 GB, 85899345920 bytes
16 heads, 63 sectors/track, 166440 cylinders
Units = cylinders of 1008 * 512 = 516896 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00095052

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1 *          3           1018       512000   83   Linux
Partition 1 does not end on cylinder boundary.
/dev/vda2           1018       83221     41430016   8e   Linux LVM
Partition 2 does not end on cylinder boundary.

Command (m for help):
```

5. 创建新的分区：输入“n”新建分区；输入“p”主分区；输入分区编号；起始cylinders；结束cylinders；再输入“w”保存分区信息并退出fdisk。

```
Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 3
First cylinder (1-166440, default 1): 83221
Last cylinder, +cylinders or +size{K,M,G} (83221-166440, default 166440):
Using default value 166440

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@localhost ~]#
```

6. partx: 修改磁盘分区表后，可以通过“lsblk”命令查看是否识别到分区，如果没有识别到新分区无需重启，用partx命令，内核可以读入新的分区表信息。

```
[root@localhost ~]# partx -a /dev/vda
BLKPG: Device or resource busy
error adding partition 1
BLKPG: Device or resource busy
error adding partition 2
[root@localhost ~]# partx -a /dev/vda3 /dev/vda
[root@localhost ~]#
```

7. 查看磁盘分区是否被识别。


```
[root@localhost ~]# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sr0                                11:0    1 1024M  0 rom
vda                                252:0    0   80G  0 disk
├─vda1                            252:1    0   500M  0 part /boot
├─vda2                            252:2    0  39.5G  0 part
│   └─VolGroup-lv_root (dm-0) 253:0    0  31.7G  0 lvm /
│       └─VolGroup-lv_swap (dm-1) 253:1    0   7.8G  0 lvm [SWAP]
└─vda3                            252:3    0   40G  0 part
```

8. 将新增加的分区转换成pv，添加到vg和lv中；扩展逻辑卷后，使用resize2fs调整分区大小，才能使用已扩展的空间。

```
[root@localhost ~]# pvcreate /dev/vda3
Physical volume "/dev/vda3" successfully created
[root@localhost ~]# vgdisplay | grep "VG Name"
VG Name                VolGroup
[root@localhost ~]# vgextend VolGroup /dev/vda3
Volume group "VolGroup" successfully extended
[root@localhost ~]# lvextend -l +100%FREE /dev/VolGroup/lv_root
Extending logical volume lv_root to 71.68 GiB
Logical volume lv_root successfully resized
[root@localhost ~]# resize2fs /dev/VolGroup/lv_root
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/VolGroup/lv_root is mounted on /; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 5
Performing an on-line resize of /dev/VolGroup/lv_root to 18789376 (4k) blocks.
The filesystem on /dev/VolGroup/lv_root is now 18789376 blocks long.
[root@localhost ~]#
```

9. 查看扩容后的lv大小：通过df命令可以看到该lv扩容后的大小，扩容完成。

```
[root@localhost ~]# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/mapper/VolGroup-lv_root
                          71G       1.8G   66G    3% /
tmpfs                     3.9G         0   3.9G    0% /dev/shm
/dev/vda1                 485M       37M   423M    9% /boot
[root@localhost ~]#
```

5.2.5. 使用物理磁盘（裸磁盘映射）

功能说明

HCI支持添加外置存储，将外置存储上的LUN直接挂载给虚拟机使用。

注意事项

HCI添加外置存储的时，需先点一下“重新发现磁盘”再点击“添加外置存储”发现外置存储。

前提条件

HCI主机上接了FC存储或者iSCSI存储。

操作步骤

以iSCSI存储为例

- 1. 配置HCI主机上用作存储网口的IP地址，使其能够和iSCSI存储服务器能够正常通信。
- 2. 在iSCSI存储上做正确的配置，将相应的卷映射给HCI主机使用。
- 3. 在[存储/其它存储]中点击<iSCSI服务器连接配置>。



- 4. 在弹出的[iSCSI服务器连接配置]页面中点击<添加iSCSI服务器>。会弹出[添加新的iSCSI服务器]窗口。



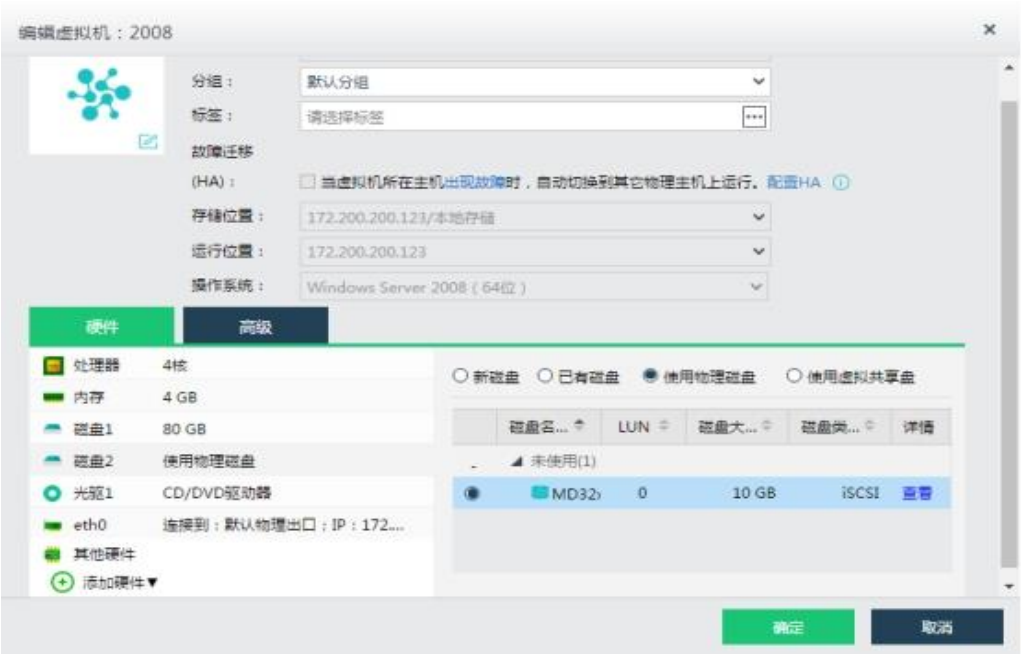
- 5. 输入IP后点击<发现目标>。



6. 然后点击[点击认证]会提示“已认证通过”，然后点击<关闭>即可。



7. 在虚拟机的编辑页面点[添加硬件/磁盘]选择使用物理磁盘，然后选择相应的LUN，点<确定>即可。



5.2.6. 使用 VHD 磁盘

功能说明

需要给虚拟机挂载微软VHD磁盘镜像，挂载后可以读取VHD镜像中的数据。

注意事项

当前VHD镜像只支持导入平台，挂载给虚拟机使用，暂不支持导出为VHD格式。

前提条件

无

操作步骤

1. 进入存储管理页面，将已制作好的VHD镜像上传至指定路径，上传成功后，刷新页面会显示上传成功的镜像。



2. 创建虚拟机，通过选择已有磁盘的方式，选择VHD磁盘。



3. 除了创建虚拟机的时候可以选择挂载已有的VHD磁盘，也可以通过编辑虚拟机，添加磁盘，选择已有磁盘的方式，挂载指定的VHD磁盘。



4. 挂载之后，即可在系统中看到该磁盘，使用磁盘中的数据。

5.2.7. 虚拟机编辑

5.2.7.1. 硬件配置

功能说明

通过编辑虚拟机可以调整虚拟机的相关配置。

注意事项

- 支持开机编辑虚拟机硬件配置，部分操作需在关闭虚拟机的状态下进行。如下信息支持开机编辑操作：
 - 基本信息（除存储位置外）、CPU、内存、光驱、串口、USB、其他硬件。其中，下列项目需要重启虚拟机才能生效：
 - 基本信息：故障迁移、存储策略、运行位置、操作系统；
 - CPU：虚拟插槽数（支持热添加、不支持热删减）、每个插槽的核数、启用 NUMA 调度（支持关闭）、使用 Host CPU、高性能时钟、启用 CPU 热添加；
 - 内存：内存大小（支持热添加、不支持热删减）、使用大页内存、启用内存热添加；

- 磁盘：分配方式（支持热添加、不支持热修改）、使用 Virtio 磁盘（热添加不需重启生效）；
 - 网卡：网卡型号（支持热添加、不支持热修改）、MAC 地址（支持热添加、不支持热修改）、巨帧接收功能（支持热添加、不支持热修改），其他可以支持热修改；
 - 添加硬件：光驱（支持热修改，不支持热添加）、串口（支持热修改，不支持热添加）、网卡（热添加不需重启生效）、IDE 类型磁盘扩容（热添加不需重启生效）；
 - 其他硬件：键盘类型、BIOS 设置、内置显卡。
2. 在虚拟机裸磁盘映射的情况下，不要热插拔映射的磁盘。
 3. HCI上Linux用UEFI模式启动的虚拟机，不能导出ova到VMware中。
 4. 未安装VMtools的Linux虚拟机，编辑网卡型号时，支持选择 Virtio网卡；Windows虚拟机不支持。

前提条件

无

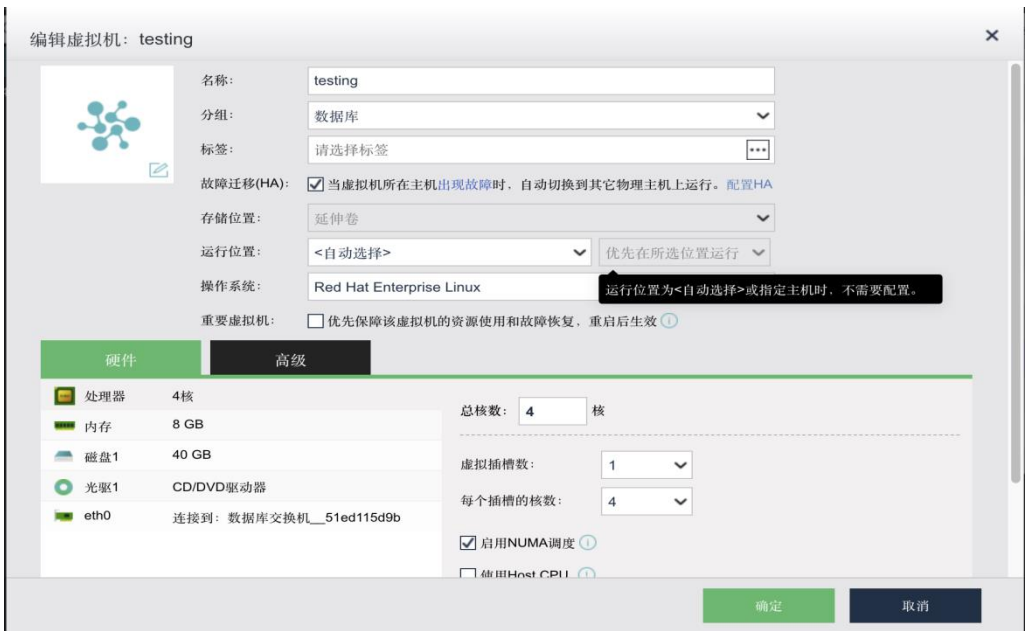
操作步骤

1. 将鼠标放到需要编辑的虚拟机上，然后点击出现的下拉箭头，并点击<编辑>。



2. 在虚拟机编辑页面上可编辑如下信息，更多介绍参考本手册“[创建全新虚拟机](#)”

章节。



3. 编辑完成后，在虚拟机[操作日志]页面会记录详细的变更情况。

深信服超融合平台								
虚拟机 > (CentOS7_RHEL_Client_3.2_root_sangfor)								
状态	行为	开始时间	结束时间	用户名	主机	对象类型	对象	操作
成功	编辑虚拟机	2022-10-20 11:13:14	2022-10-20 11:13:18	admin (172.23.140.25)	200.201.202.71	虚拟机	CentOS7_RHEL_Client_3.2_root_sa...	查看
成功	启动虚拟机	2022-10-18 21:27:32	2022-10-18 21:27:37	admin (200.201.202.43)	200.201.202.71	虚拟机	CentOS7_RHEL_Client_3.2_root_sa...	查看
成功	转换为虚拟机	2022-10-18 21:23:23	2022-10-18 21:23:24	admin (200.201.202.43)	200.201.202.73	模板	CentOS7_RHEL_Client_3.2_root_sa...	查看
成功	编辑虚拟机	2022-10-18 21:12:20	2022-10-18 21:22:44	admin (200.201.202.43)	200.201.202.73	虚拟机	CentOS7_RHEL_Client_3.2_root_sa...	查看
成功	新建虚拟机	2022-10-18 21:12:14	2022-10-18 21:12:14	admin (200.201.202.43)	200.201.202.72	虚拟机	CentOS7_RHEL_Client_3.2_root_sa...	查看

5.2.7.2. 高级配置

功能说明

该任务指导管理员在虚拟机创建时或者创建完成以后配置虚拟机高级选项。

注意事项

支持开机编辑虚拟机高级配置，包括：引导顺序、生命周期、hostname、其他选项、调试选项。其中“调试选项”均不建议用户自行修改。

其中，下列项目需要重启虚拟机才能生效：

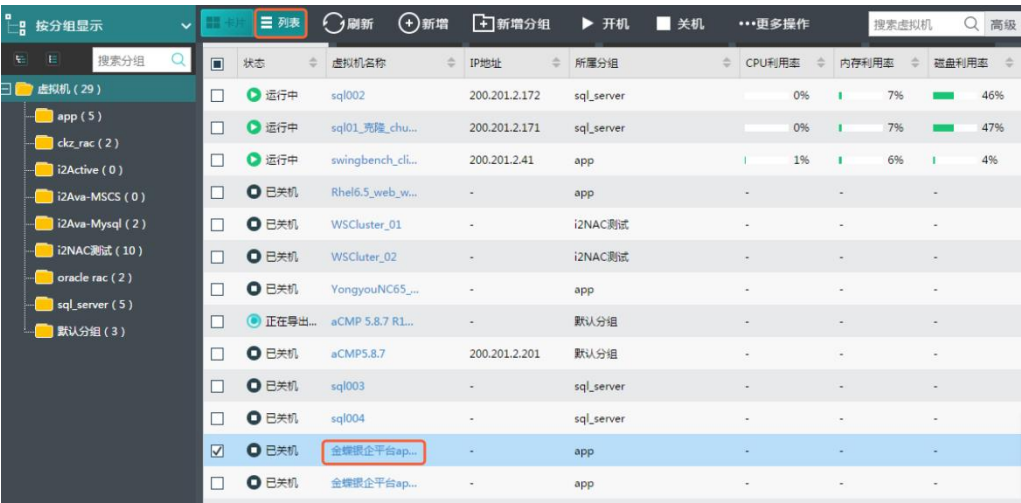
- 引导顺序、禁用 kvmclock、使用 Virtio 磁盘、启用内存回收机制、备份过滤页面文件、禁用 Pause-Loop Exiting、启用 I3-cache、启用磁盘加密。

前提条件

部分功能调整需要虚拟机需要关机。

操作步骤

1. 在[虚拟机]页面虚拟机列表中点击虚拟机名称，进入虚拟机信息页面。



2. 点击<编辑>进入[编辑虚拟机]窗口，再点击[高级]，进入虚拟机高级配置页面。



3. 配置如下信息

- **引导顺序：**虚拟机系统启动顺序。关机时或者创建虚拟机时可编辑该选项。
- **生命周期：**当虚拟机生命周期到期时会有告警，但不影响虚拟机的正常运行，您可以在高级搜索中过滤已过期的虚拟机进行关机或删除，避免虚拟机长期无人使用而浪费资源。

- **hostname：**可以使用系统默认的 **hostname**，也可以在该页面手动指定 **hostname**，但是虚拟机需要安装性能优化工具才能使用这个功能，而且使用之前需要在页面上查看操作系统是否支持，设置后需要等待一分钟左右生效。
 - 主机启动时，自动运行此虚拟机：服务器开机自启动虚拟机。
 - **标记为重要虚拟机：**按照用户虚拟机的内存规格预分配资源，该资源由该虚拟机独享而不会被其他虚拟机抢占争夺，也不会回收内存。
 - **虚拟机异常重启：**当虚拟机无响应（如卡死、蓝屏）时，自动重启，虚拟机重启后生效。默认勾选。
 - **启动 CPU/内存热添加：**开机的虚拟机可以手动添加 **CPU**、内存。注意不同操作系统的支持度不同，操作时先查看系统支持列表，并且该功能需要虚拟机安装 **vmtools** 支持。关机时或者创建虚拟机时可编辑选项；在该选项配置生效以后，在虚拟机开机状态下可热添加内存和 **CPU**，也就是在开机状态下编辑虚拟机，可将 **CPU** 的插槽数和内存大小修改为比原来分配的 **CPU** 插槽数和内存大小高即可。
 - **启用 UUID：**虚拟机的唯一标识符，某些软件需要获取虚拟机 **UUID** 才能正常使用。禁用 **UUID** 后，重新启用时，用户可自主选择使用新 **UUID** 或者沿用原 **UUID**。克隆、模板部署的虚拟机，请根据实际需要决定是否重新生成 **UUID**；注意：**6.X** 之后的版本，**linux** 勾选此项才生效，之前版本则不会生效；该 **UUID** 非加入 **AD** 时使用的 **windows sid**；一般一些特殊的软件授权会用到 **UUID**。
 - **调试选项：**不建议用户自行修改。
4. 编辑完成后，在虚拟机[操作日志]页面会记录详细的变更情况。



状态	行为	开始时间	结束时间	用户名	主机	对象类型	对象	操作
成功	创建虚拟机	2022-10-20 11:13:14	2022-10-20 11:13:18	admin (172.23.140.25)	200.201.202.71	虚拟机	CentOS7_RDS_Client_3.2_root_sa...	查看
成功	启动虚拟机	2022-10-18 21:27:32	2022-10-18 21:27:37	admin (200.201.202.43)	200.201.202.71	虚拟机	CentOS7_RDS_Client_3.2_root_sa...	查看
成功	转换为虚拟机	2022-10-18 21:23:23	2022-10-18 21:23:24	admin (200.201.202.43)	200.201.202.73	模板	CentOS7_RDS_Client_3.2_root_sa...	查看
成功	删除虚拟机	2022-10-18 21:12:20	2022-10-18 21:22:44	admin (200.201.202.43)	200.201.202.73	虚拟机	CentOS7_RDS_Client_3.2_root_sa...	查看
成功	新建虚拟机	2022-10-18 21:12:14	2022-10-18 21:12:14	admin (200.201.202.43)	200.201.202.72	虚拟机	CentOS7_RDS_Client_3.2_root_sa...	查看

5.2.8. 导出虚拟机

功能说明

该任务指导管理员导出ova格式或者vma格式虚拟机镜像文件。

注意事项

HCI 5.2以下版本仅支持导出vma格式；HCI 5.2及以上版本支持导出ova或vma格式

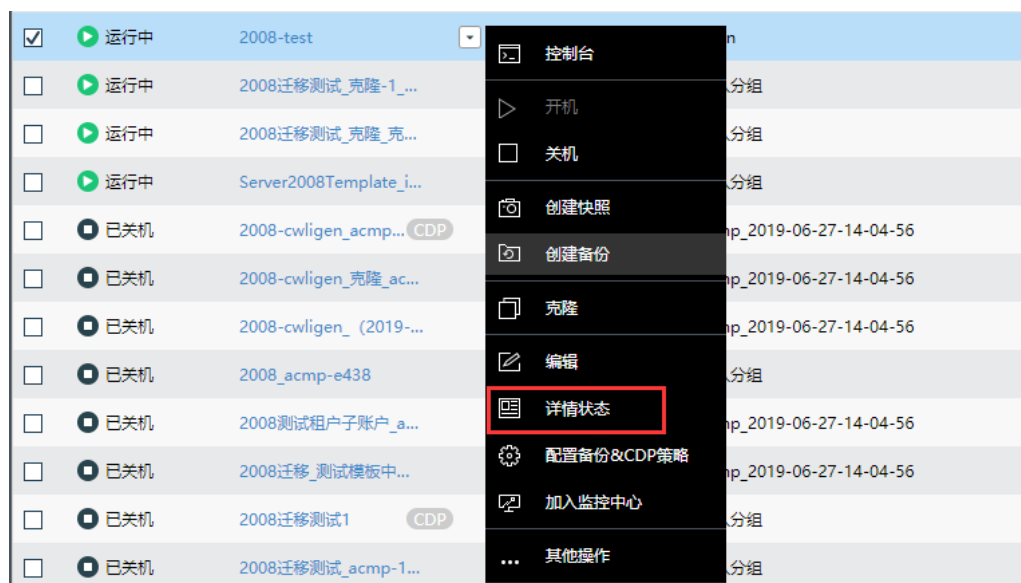
虚拟机文件。

前提条件

虚拟机关机。

操作步骤

1. 在[虚拟机]页面虚拟机列表中点击虚拟机名称，进入虚拟机信息页面。

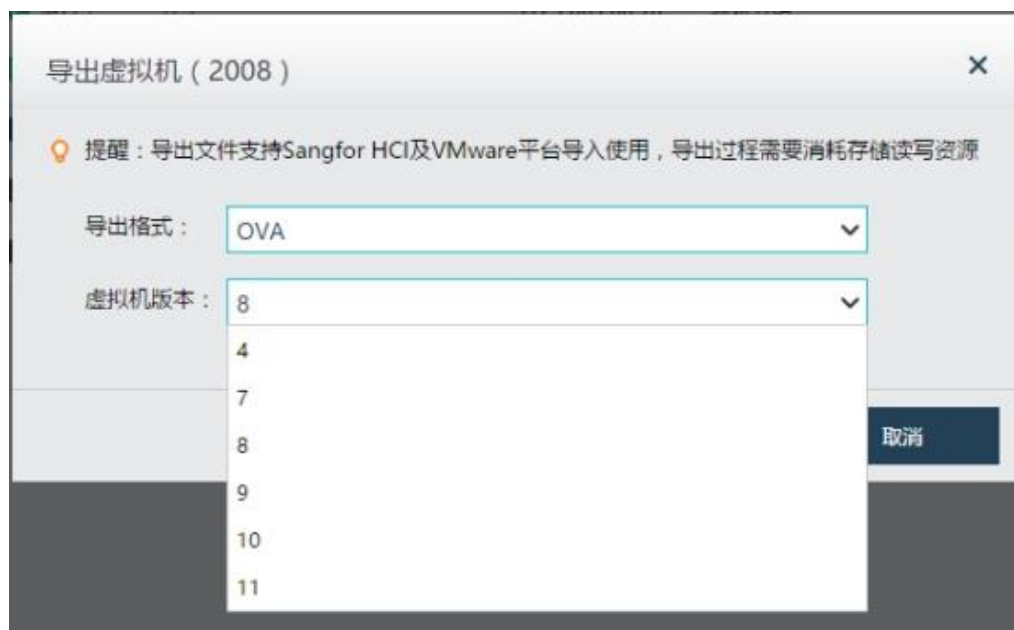


2. 点击<更多操作/导出>，弹出[导出虚拟机]窗口，选择导出的磁盘格式。



⚠ 注意：

导出时如果选择 OVA 格式，需要选择 OVA 格式版本。OVA 不同版本运行的 VMware 版本不同，具体见界面提示选择。



3. 点击<开始导出>，开始导出虚拟机。一段时间后导出完毕。



5.2.9. 虚拟机集群内热迁移（支持批量操作）

功能说明

该任务指导管理员在不关机的情况将虚拟机迁移到集群内其他主机或者存储位置上。

注意事项

1. 支持虚拟机关机状态下进行主机迁移和存储迁移。
2. 支持选择多台虚拟机同时迁移。
3. 批量迁移时：
 - 跨主机：任务允许 2 个并发进行，其余任务排队。
 - 跨主机跨存储：任务允许 1 个并发，其余任务排队。
4. 批量迁移时，待迁移虚拟机的目标存储运行位置必须一致，暂无法每台虚拟机单独设置存储和运行位置。

5. 配置迁移网络之前，保证源端运行节点、目的运行节点的网口必须均配置IP，才能保证迁移网络可用，否则置灰不可选。
6. 批量迁移和迁移存储位置时，默认使用最大带宽链路不做迁移速度限制，不支持设置迁移网络和迁移速度。
7. 虚拟机存储位置为虚拟存储时，才支持配置迁移网络和迁移速度。
8. 超融合平台上已分配显卡、和做了裸磁盘映射的虚拟机不支持热迁移。

前提条件

待迁移的源和目的主机迁移通信网口连通性正常。

操作步骤

1. 在[虚拟机]页面虚拟机列表中勾选待迁移虚拟机选项框。



2. 点击<更多操作/迁移>，进入迁移虚拟机页面。选择迁移方式、目的存储位置、主机位置。

迁移虚拟机

1 选择迁移方式

2 迁移设置

迁移方式:

☐ 只迁移运行位置

将虚拟机迁移到另一台主机上运行

☒ 迁移存储位置和运行位置

将存储位置迁移到另一虚拟存储卷或者其他存储，在迁移存储位置的同时支持将虚拟机迁移到另一主机上运行

下一步

取消

迁移虚拟机

1 选择迁移方式

2 迁移设置

原始位置

存储位置: 医疗延伸卷

存储策略: 2副本默认策略

当前运行主机: 192.200.244.201

目标位置

存储位置: 医疗延伸卷

存储策略: <复用虚拟机存储策略: 2副本>

目的运行主机: 192.200.244.201

✓ 虚拟机的运行位置是虚拟存储卷（医疗延伸卷）的主机，可以达到最佳性能

3. 点击<高级设置>，设置迁移网络、迁移速度、启用压缩传输。

- 迁移网络：此处会自动识别网口带宽，当管理通信口、数据通信口、存储通信口带宽不一致下，优先推荐带宽最高的网口；当网口带宽均一致下，按照数据通信口>存储通信口>管理通信口的规则进行优先推荐。
- 迁移速度：默认为无限制，热迁移前或迁移过程中都可以设置迁移最大速度。
迁移限速值最小值为 **50MB/s**，最大值不能超过当前迁移网络的物理网口带宽值。
- 启用压缩传输：启用后可以提高热迁移速度，但会消耗一定的源主机 CPU 资源（最多消耗 4 线程）。

高级设置

迁移网络：☐ 管理口（1000Mbps）☐ 数据通信口（0Mbps）☒ 存储口（20000Mbps）

迁移速度：☒ 无限制 ☐ 限制最大速度 MB/s

☐ 启用压缩传输

上一步

完成

取消

4. 点击<确定>，虚拟机进入迁移状态，几分钟后虚拟机完成迁移。
5. 支持查看虚拟机迁移记录：进入虚拟机详情中[迁移记录]即可查看迁移记录，点击上方切换按钮，可以按表格或图形切换迁移记录查看页面。



5.2.10. 虚拟机跨集群热迁移（支持批量操作）

功能说明

该任务指导管理员需要在不关机的情况将虚拟机迁移到另一HCI集群内。

注意事项

1. 虚拟机关机状态下也可以进行主机迁移和存储迁移。
2. 跨集群迁移数据需要通过管理网络，注意选择空闲的时间进行迁移。
3. 跨集群迁移源端和目的端的版本必须一致。
4. 源虚拟机在跨集群迁移完成后会关机，并且被删除至回收站中。
5. 支持同时选择多台虚拟机进行跨集群迁移。
6. 批量迁移时，任务允许1个并发进行，其余任务排队。
7. 批量迁移时，待迁移虚拟机的目标存储运行位置必须一致。
8. 在做跨集群迁移的时候，目的端可能会报镜像损坏的错误，因为镜像还没有迁移完成，HCI 30分钟检测一次镜像，检测到这个没有迁移完的镜像会报这个错误。

像损坏了，其实没有坏，只是跨集群迁移比较慢，还没有迁移完。

9. 超融合平台上已分配显卡、做了裸磁盘映射的虚拟机不支持热迁移。

前提条件

待迁移的源和目的主机迁移网口连通性正常，并在端口管理中开启虚拟机迁移服务。

操作步骤

1. 选择待迁移虚拟机：在[虚拟机]页面虚拟机列表中点击待迁移虚拟机名称，进入虚拟机信息页面，勾选一台或多台待迁移的虚拟机；点击<更多操作/迁移到其他集群>，进入迁移虚拟机页面。



2. 填写目标集群信息：输入目的集群IP、超级管理员用户名、密码，点击<下一步>。

迁移虚拟机 (Server2008Template_20220425-模板) 到其他集群 ×

1 目标集群

2 配置迁移位置

3 配置网卡

迁移方式:

☒ 迁移到其他集群

通过热迁移方式，将虚拟机迁移到其他集群

☐ 迁移到其他集群，并保留原集群的虚拟机

保留原集群虚拟机，通过虚拟机克隆方式在其他集群上创建新的虚拟机

集群IP:

200.201.202.30

超级管理员:

admin

密码:

下一步

取消

3. 选择目标集群的存储位置、存储策略、运行位置，点击<高级设置>，设置迁移网络、迁移速度、启用压缩传输。
- 迁移网络：此处会自动识别网口带宽，当管理通信口、数据通信口、存储通信口带宽均一致下，按照数据通信口>存储通信口>管理通信口的规则进行优先推荐。
 - 迁移速度：默认为无限制，热迁移前或迁移过程中都可以设置迁移最大速度。
迁移限速值最小值为 **50MB/s**，最大值不能超过当前迁移网络的物理网口带宽值。
 - 启用压缩传输：启用后可以提高热迁移速度，但会消耗一定源主机 CPU 资源（最多消耗 4 线程）。

迁移虚拟机 (Server2008Template_20220425-7[REDACTED] 到其他集群 ×

1 目标集群

2 配置迁移位置

3 配置网卡

源集群 (200.201.202.80)

存储位置: 虚拟存储卷1

存储策略: 2副本默认策略

运行位置: 200.201.202.71

...

目标集群 (200.201.202.30)

存储位置: 虚拟存储卷1

存储策略: 2副本默认策略

运行位置: 200.201.202.21

☒ 迁移完成后, 自动启动虚拟机 (目标集群)

高级设置

迁移网络: ☒ 管理口 (1000Mbps) ☐ 数据通信口 (0Mbps) ? ☐ 存储口 (0Mbps)

迁移速度: ☒ 无限制 ☐ 限制最大速度

MB/s

☒ 启用压缩传输 ?

💡 虚拟机将会迁移到目标集群的默认分组, 热迁移完成后源集群虚拟机将会自动关机

上一步

下一步

取消

6. 点击<下一步>, 配置网卡信息。

迁移虚拟机 (Server2008Template_20220425-7[REDACTED] 到其他集群 ×

1 目标集群

2 配置迁移位置

3 配置网卡

eth0 连接到: 管理网物理出口

☒ 启用

连接到: 管理网物理出口 ...

网卡原配置:

高级选项

网卡型号: virtio

MAC地址: FE:FC:FE:90:13:64 ↻

上一步

确定

取消

4. 点击<确定>并选择<继续迁移>, 虚拟机进入跨集群热迁移阶段, 一段时间后热迁移完成。



5.2.11. 虚拟机快照

功能说明

指导管理员给开机或者关机状态下的虚拟机创建快照，常用于虚拟机补丁升级、软件更新等操作后需要对原有数据进行恢复的场景。

注意事项

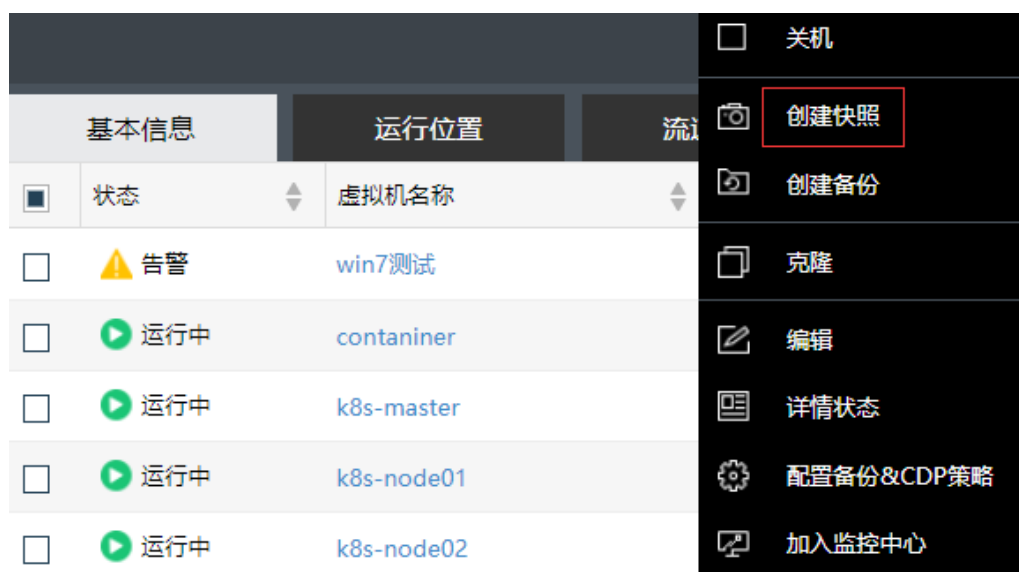
1. 虚拟机快照不作为备份手段，仅用于虚拟机补丁升级、软件更新等高危操作前的虚拟机保护。
2. 三主机及其以上集群，使用aSAN虚拟存储时，默认采用存储快照（基于存储的ROW技术）对虚拟机打快照；当虚拟机在老版本平台打过快照时，可以选择“继续保持使用虚拟磁盘快照”或“切换为存储快照”。当切换至存储快照时，需要清除已创建的虚拟磁盘快照。
3. 使用外置存储时，采用虚拟磁盘快照（基于qemu的ROW技术）对虚拟机打快照。
4. 两主机集群，使用aSAN虚拟存储时，默认采用虚拟磁盘快照，无法使用存储快照；当扩容至三主机时可以切换至存储快照（前提是需要清除已创建的虚拟磁盘快照）。
5. 存储快照支持的最大快照个数为48个。
6. 虚拟机快照会中断业务，中断时间 $\leq 1s$ 。

前提条件

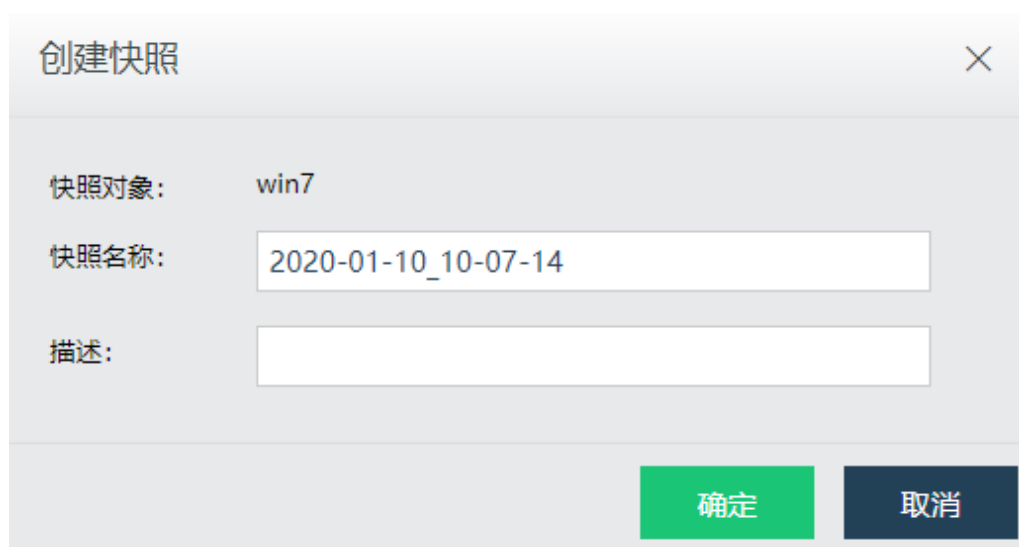
无

操作步骤

1. 在[虚拟机]页面虚拟机列表中点击虚拟机对应的三角标识，点击<创建快照>。



2. 自定义快照名称、描述信息或者保持默认名称。



3. 点击<确定>，完成快照创建。
4. 在虚拟机详情页中可以查看已创建的快照信息。



5. 点击快照照相机图标，可进行快照删除、克隆以及虚拟机快照恢复的操作。



6. 当虚拟机处于开机运行状态，利用快照进行恢复时，恢复后的虚拟机默认会关机，可以勾选恢复完成后自动开启虚拟机，此时虚拟机恢复完后将自动开机。



5.2.12. 一致性组快照

功能说明

将Oracle-RAC的虚拟机或一个业务的多个虚拟机加入到一致性组中，以实现对整个组虚拟机执行一致性快照，确保多个虚拟机的快照数据是同一时刻生成的，保证利用快照恢复后业务正常可用。

注意事项

1. 虚拟机加入到一致性组之前打的快照不允许回滚，但可以利用快照克隆虚拟机。
2. 一致性组快照只针对虚拟存储上的虚拟磁盘、共享盘打快照，不在虚拟存储的磁盘，不会生成快照数据。
3. 一致性组快照对磁盘数量有限制，一致性组内虚拟机磁盘数量总和不允许超过64个。

前提条件

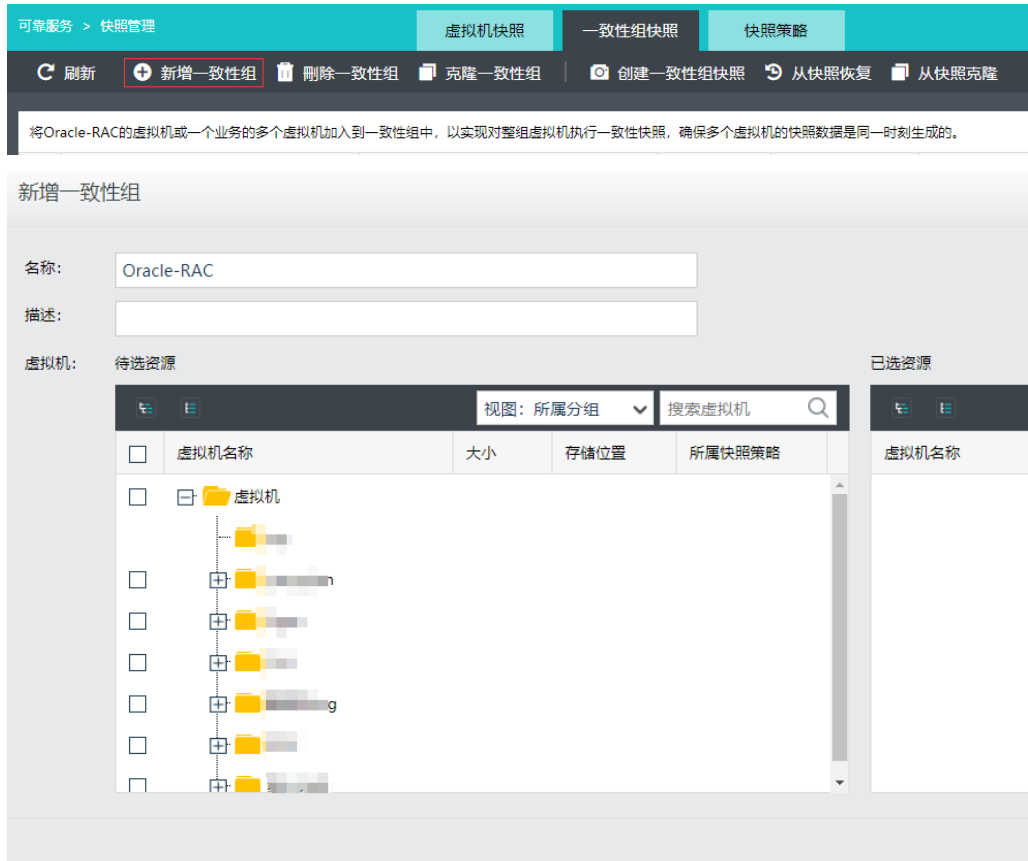
无

操作步骤

1. 点击[可靠服务/快照管理]，进入一致性组快照。



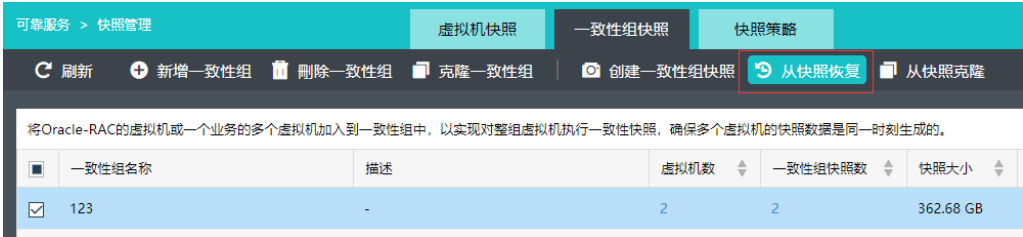
2. 新增一致性组，选择相互关联的虚拟机，加入到一致性组中；虚拟机加入一致性组后，可以对一致性组进行克隆，保证了虚拟机克隆之后的数据一致性。



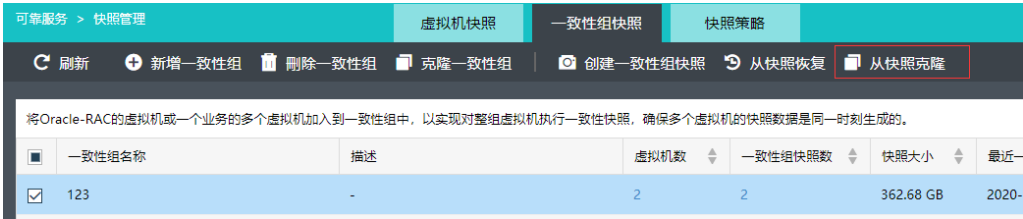
3. 勾选需要打快照的一致性组，点击<创建一致性组快照>，即可针对一致性组内所有的虚拟机进行快照。



4. 当需要使用快照对一致性组内的虚拟机进行恢复时，选择需要恢复的一致性组，点击<从快照恢复>，即可对虚拟机进行恢复。



5. 此外，还可以利用一致性组快照进行虚拟机克隆。



5.2.13. 快照策略

功能说明

支持通过为业务虚拟机创建定时快照策略实现自动创建快照，如按小时、天、周等频率对虚拟机进行快照，并支持配置快照保留策略，超过保留范围的快照将自动删除，释放存储空间。

通过设置快照策略，可以实现对虚拟机进行定期的保护，在虚拟机出现逻辑性错误，比如中毒，可以利用快照进行回滚，恢复虚拟机，降低损失。

注意事项

1. 快照策略分为手动、智能两种模式，默认为智能模式。若需切换快照策略模式，切换模式前，请先删除原模式下的全部快照策略，否则无法切换。
2. 持续性执行存储快照操作会对虚拟机性能有一定影响，时间段外的快照将进行合并，以节省大量空间，至少保留最近5个快照文件，最多保留7个快照。

3. 若选择的虚拟机或一致性组已经存在快照策略，则将会从原策略移除，加入到当前策略中。

前提条件

快照策略中，每天打快照的数量存在一定的限制：

- 混合卷： $vm_num = (0.6(host_num - 3)4 + 12) * (\text{单块 ssd 容量} * 0.5 * \text{ssd 磁盘个数} / 480G)$ ，注意：如果存储容量异构（不相等）时，以最小的存储容量为准。
- 全闪卷：2048

操作步骤

1. 点击[可靠服务/快照策略]，进入快照策略管理界面。



2. 快照策略分为手动、智能两种模式，支持两种模式之间进行切换。

- 手动模式：支持指定每周、每天创建快照的具体时间或快照时间间隔。
- 智能模式：可自动估算出系统的快照安全阈值，确保快照不会对业务造成明显的影响；支持指定每周、每天自动创建快照。

在[快照策略]页面。点击<切换至智能模式>，即可进行模式切换。



3. 点击<新增快照策略>，根据虚拟机业务类型创建快照策略，选择需要进行定时快照的虚拟机或者一致性组。



4. 根据实际需求设置快照的频率

- 手动模式下：可以按周、天、小时进行快照；也可以设置快照的保留方式，以节约存储空间。



- 智能模式下：可以指定每周、每天自动创建快照。



5. 填写基本信息后，进行确认，完成快照策略的创建。

新增快照策略

✓ 选择快照虚拟机

✓ 配置快照频率

✓ 填写基本信息

4 完成

名称:

win7虚拟机快照策略

描述:

-

快照频率:

按天快照 (每天00:00)

是否为一致性组:

否

5.2.14. vGPU 管理

功能说明

- 用户本来使用传统物理架构，现在想对业务进行虚拟化改造，上 HCI，原本有少数业务比如 GIS 是需要显卡支持的，现在需要一起虚拟化改造，因此需要虚拟化平台支持配置显卡。
- 用户有大规模的需要显卡支持的应用，在 GPU 资源的使用会遇到闲置浪费、分配不灵活的情况，希望能做到 GPU 使用灵活、按需分配、资源共享。
- 平台的显卡资源在分配、使用、调整的时候，需要做到可视化，方便管理者更好地管理显卡资源。

注意事项

1. 使用vGPU需获取NVIDIA的授权。
2. 使用vGPU的虚拟机必须安装和HCI平台对应版本的英伟达显卡驱动，可前往“[深信服社区 - 自助服务 - 软件下载 - 超融合 HCI](#)”获取显卡驱动。
3. HCI的vGPU授权分为两种：vWS和vCS，vWS用于专业图形和计算场景，vCS用于面向计算常见进行优化，如人工智能、深度学习、科研场景等。
4. vCS不支持Windows虚拟机，最小切割粒度为4GB，最大为32GB。
5. 不是所有显卡都支持vGPU的，支持vGPU的显卡才能使用vGPU，不支持的可以使用直通模式。
6. 支持将2张显卡直通给一台虚拟机，其中T4、2080Ti最大可支持8张。
7. vGPU场景下，显卡兼容性可查询“[信服云兼容性平台](#)”。
8. 直通场景下，需使用英伟达公版驱动，显卡版本和驱动下载参考下列链接：
<https://www.nvidia.cn/Download/index.aspx?lang=cn>。

前提条件

1. 显卡服务器+显卡，两台显卡服务器组成集群使用，或者一台显卡服务器和一台普通服务器组成集群，需要至少一张显卡。可以用深信服购买的显卡，也可以使用用户原有的显卡。
2. 服务器有2D和3D服务器区分，原本的一体机是不能插显卡的，插显卡需要专门的显卡服务器。

操作步骤

HCI环境部署。硬件方面，在服务器上插上显卡，注意显卡的供电线要接上，显卡才会工作（显卡的功率大，有专门的供电线）；软件方面，在服务器上安装HCI系统软件时或者是已有集群在插上显卡之后，平台检测硬件有显卡的时候，界面会自动显示是否需要开启IOMMU的选项，选择开启（开启之后需要重启主机才生效）。



5.2.14.1. 部署英伟达授权服务器

功能说明

部署英伟达vGPU授权服务器，为3D vGPU虚拟机提供授权。使用vGPU，需要授予英伟达的授权序列号，否则vGPU的性能发挥不出来。授权服务器是一个虚拟机模板，装在HCI平台作为一个虚拟机使用，把申请来的vGPU测试序列号填在授权服务器上，再把授权服务器的IP填在需要使用vGPU的虚拟机的显卡驱动上，虚拟机才可以正常使用vGPU。

注意事项

授权服务器需要与使用vGPU的业务虚拟机通信。

前提条件

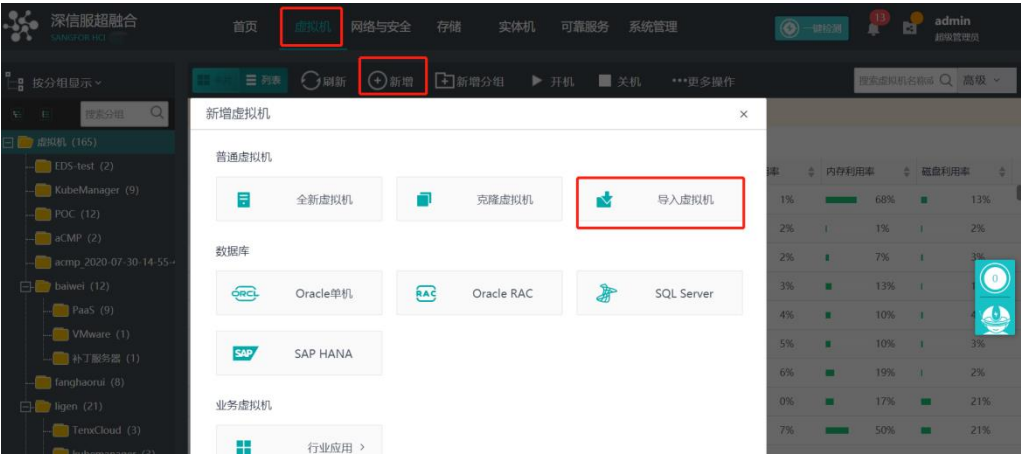
下载授权服务器镜像

表7 授权服务器下载

文件名称	3D 授权服务器-HCI-1.1.0.vma
下载地址	深信服社区 - 自助服务 - 软件下载 - 超融合 HCI：vGPU 授权服务器和驱动
MD5值	2CCA7CF803AF4F14B6F554187E07FA9C

操作步骤

1. 登录HCI控制台，点击[虚拟机/新增/导入虚拟机]，选择NVIDIA授权服务器vma镜像进行导入。



2. 进入导入虚拟机的页面，会弹出一个从本地导入虚拟机文件的页面，首先在虚拟机文件选项在弹出的文件选择页面选择下载的授权服务器镜像文件，然后在分组选项中选择一下分组，最后选择<开始导入>。

从本地导入vma文件

① 虚拟机导入后默认使用QXL高性能显卡，如果开机后出现显示的异常，请通过手动切换显卡解决。

文件类型: ova或vma

虚拟机文件: 3D授权服务器-HCI-1.1.0.vma

分组: 默认分组

故障迁移(HA): ☒ 当设备所在主机出现故障时，自动切换到其它物理主机上运行。配置HA ⓘ

存储位置: 虚拟存储卷1

存储策略: 2副本默认策略

运行位置: <自动选择>

开始导入

3. 点击<开始导入>后，页面显示如下，等待导入完成。

从本地导入vma文件

正在上传文件[3D授权服务器-HCI-1.1.0.vma]，请不要关闭此页面

正在计算文件大小...

0%

取消上传

4. 导入成功后点击“转到虚拟机”进行编辑，编辑网卡设置，修改IP地址。



5. 编辑完成，进入控制台界面后登入，如下界面输入dls_system回车。

```
Warning: Access to this system is restricted to authorized personnel only. All activity on this system is monitored and audited. Unauthorized access will be prosecuted to the fullest extent of the law.
nls-si-0 login:
```

6. 执行/etc/adminscripts/set-static-ip-cli.sh，设置静态IP，示例如下图所示。

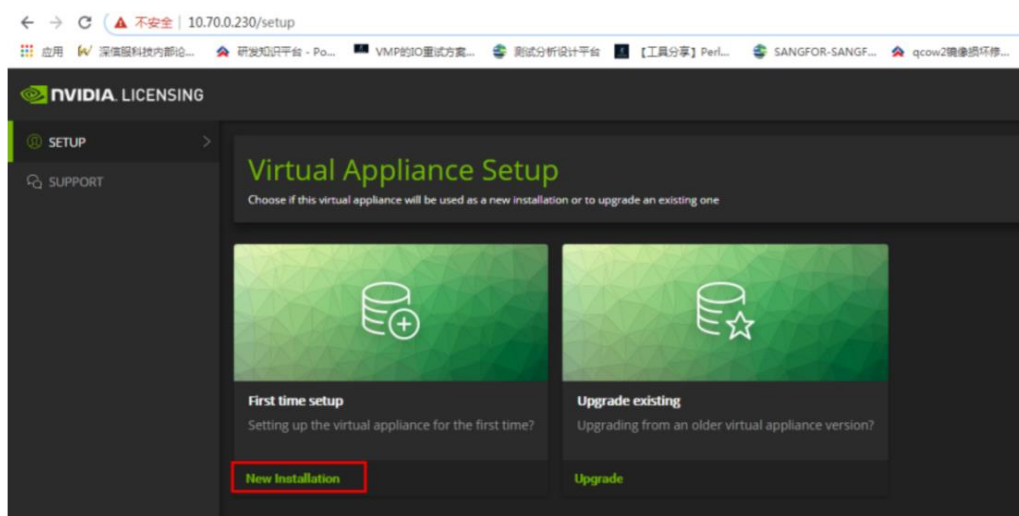
```
dls_system@nls-si-0:~$ /etc/adminscripts/set-static-ip-cli.sh
Enter 4 for IPV4 and 6 for IPV6 IP Opearation : 4
New IP Address: 10.70.0.230
Gateway (Default : 10.70.255.254) : 10.70.255.254
DNS Server One (Default : 199.200.0.100): 199.200.0.100
DNS server two (Default : ):
Netmask Prefix (CIDR Notation e.g 24 for 255.255.255.0, 28 for 255.255.255.240) (Default : 16): 16
```

7. 执行ip addr show确认IP生效。

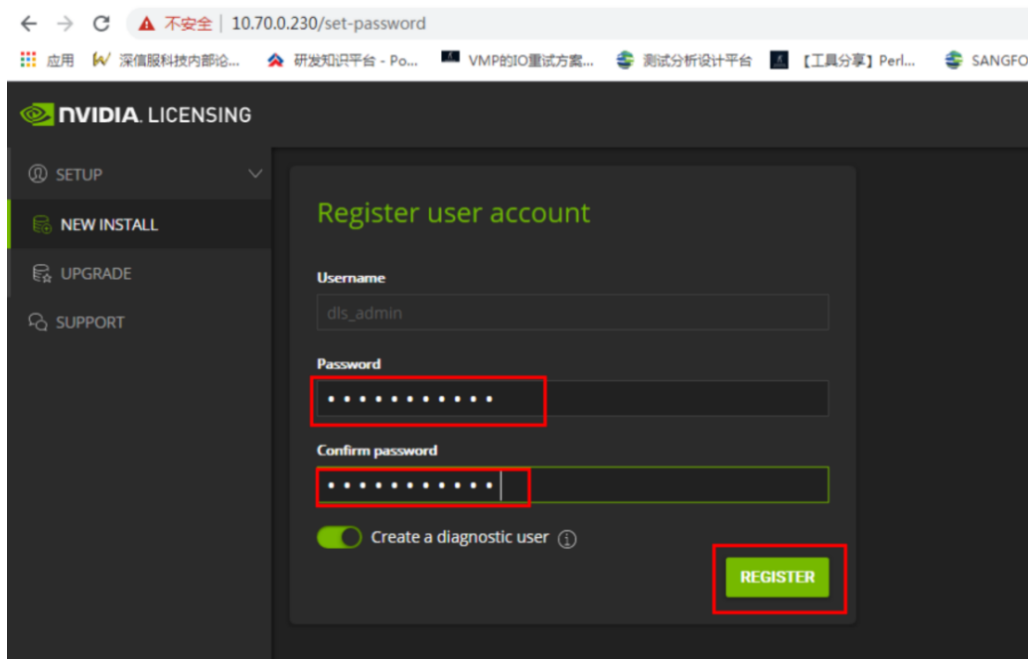
```
dls_system@nls-si-0:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether fe:fc:fe:16:c3:57 brd ff:ff:ff:ff:ff:ff
    inet 10.70.0.230/16 brd 10.70.255.255 scope global noprefixroute enp0s18
        valid_lft forever preferred_lft forever
    inet6 fe80::b841:67cb:5519:74cc/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

8. 浏览器输入设置的IP（如上则直接输入10.70.0.230）访问授权服务器web页面，

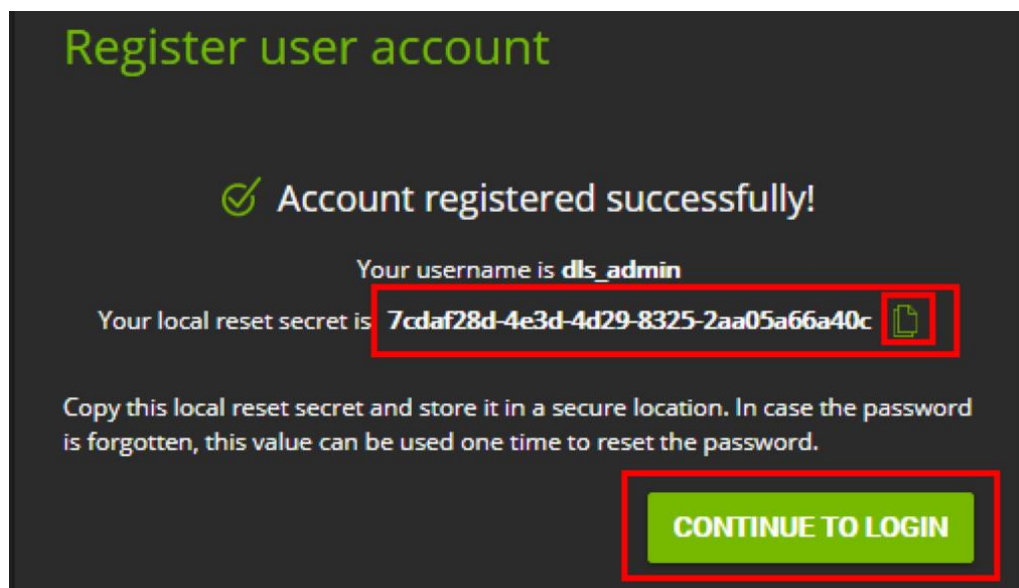
选择"New Installation"。



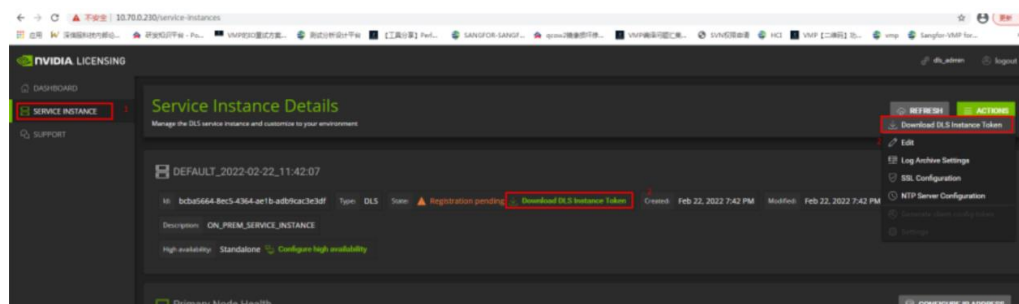
9. 输入要设置的密码，点击<REGISTER>注册账户。



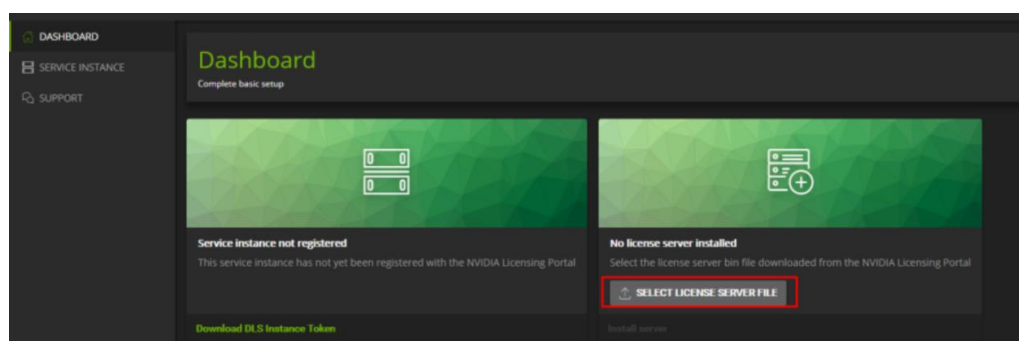
10. 保存图中字符串至本地文件，此字符串可用于重置密码。点击<CONTINUE TO LOGIN>。



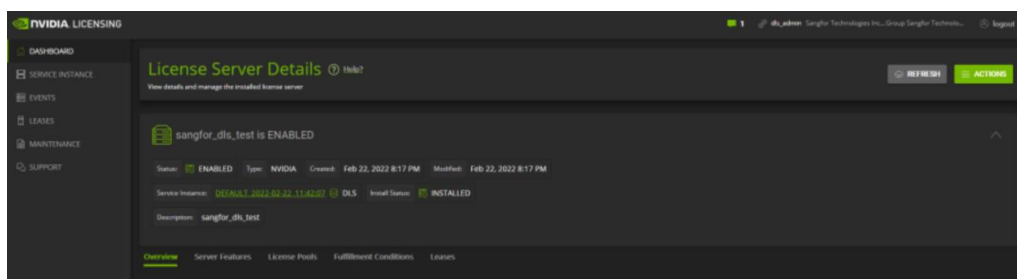
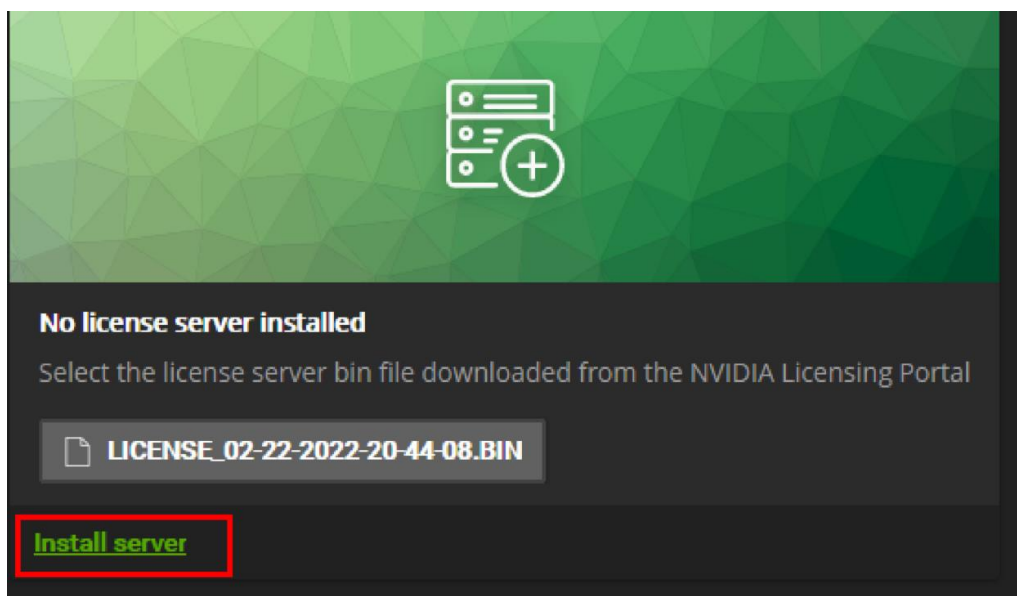
11. 选择 "SERVICE INSTANCE", 点击 <Download DLS Instance Token>, 下载 DLS实例Token文件, 若需测试授权则将该文件传递给深信服技术服务获取授权文件。



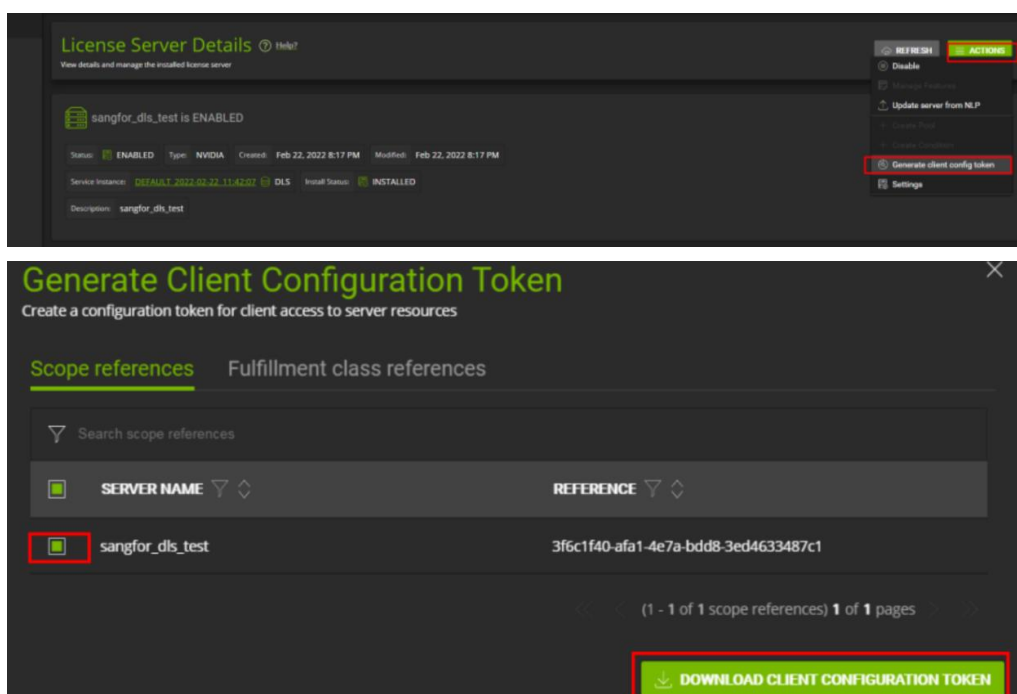
12. 获取到授权文件后, 点击<SELECT LICENSE SERVER FILE>, 将文件上传。



13. 点击 “Install server”, 配置授权服务。



14. 下载client config token，用于给GPU虚拟机授权。



5.2.14.2. 显卡管理

功能说明

服务器显卡核心可以配置为直通模式或者自动以及手动指定切分类型，默认由系统自动配置切分类型。支持将显卡切分为Q系列或C系列的vGPU：

Q系列适用于需要Quadro技术的性能和功能的创意和技术专业人员的虚拟工作站；

C系列适用于计算密集型服务器工作，诸如人工智能（AI），深度学习，或高性能计算（HPC）。

注意事项

1. 对于直通显卡，会默认为直通模式，对于支持vGPU的显卡，会默认为自动模式，可以根据测试需要调整切分模式。
2. 支持将2张显卡直通给一台虚拟机，其中T4、2080Ti最大可支持8张，不支持将多个vGPU分配给一台虚拟机。
3. 支持使用的是10.2、13.2的vGPU版本，相关软件的兼容性列表可前往英伟达官网查询。全新安装或者升级到HCI6.8.0，都需要重新导入GRID驱动，并重启主机后生效。
4. 超融合平台上已分配显卡的虚拟机不支持热迁移。
5. vGPU场景下，显卡的显存资源是分配且独占的，显卡的计算资源会依据调度器进行调度，该版本支持三种调度器：Best Effort（抢占）、Equal Share（等分）、Fixed Share（固定配比）

Best Effort（抢占）：当多虚拟机运行在该显卡时，会根据工作负载情况抢占算力资源；

Equal Share（等分）：当多虚拟机运行在该显卡时会均分算力资源；

Fixed Share（固定配比）：当多虚拟机运行在该显卡时，会一句虚拟机所配置的显存比例分配算力资源。
6. 单台服务器禁止使用两个不同型号的显卡，同集群不同主机可以支持不同型号的GPU。
7. 当A、B两张显卡插在紧邻着的两个PCI插槽，并且B显卡存在核心损坏时，显卡B的核心会被识别为显卡A的，请及时更换损坏显卡。

前提条件

调整显卡切分模式时，占用该显卡资源的虚拟机需要关机。

操作步骤

1. 点击[实体机/显卡管理]，在[显卡管理]窗口中可查看各显卡核心实时分配状态和驱动版本信息。



2. 点击目标显卡右侧的<编辑>按钮，可对显卡进行编辑：
 - ① 待编辑的显卡名称
 - ② 显卡的使用方式：可以选择直通或切分，当使用方式选择“切分”，若显卡有多个核心，则支持按不同核心进行显存大小的切分
 - ③ 选择是否启用显存ECC：开启可以提高GPU的运行稳定性
 - ④ 选择切分的方式，可以切分为Q系列或C系列的vGPU
 - ⑤ 选择GPU计算调度器

编辑显卡

① 已被虚拟机使用的核心不支持修改

显卡：

NVIDIA Tesla T4

1

☒ 核心 1 使用方式：

☐ 直通

☒ 切分

2

显存ECC：

☐ 启用

3

切分方式：

16 块 T4-1Q/1B (可运行1Q/1B授权，显存为 1 GB 的虚

4

调度器：

☒ Best Effort

☐ Equal Share

☐ Fixed Share

5

确定

取消

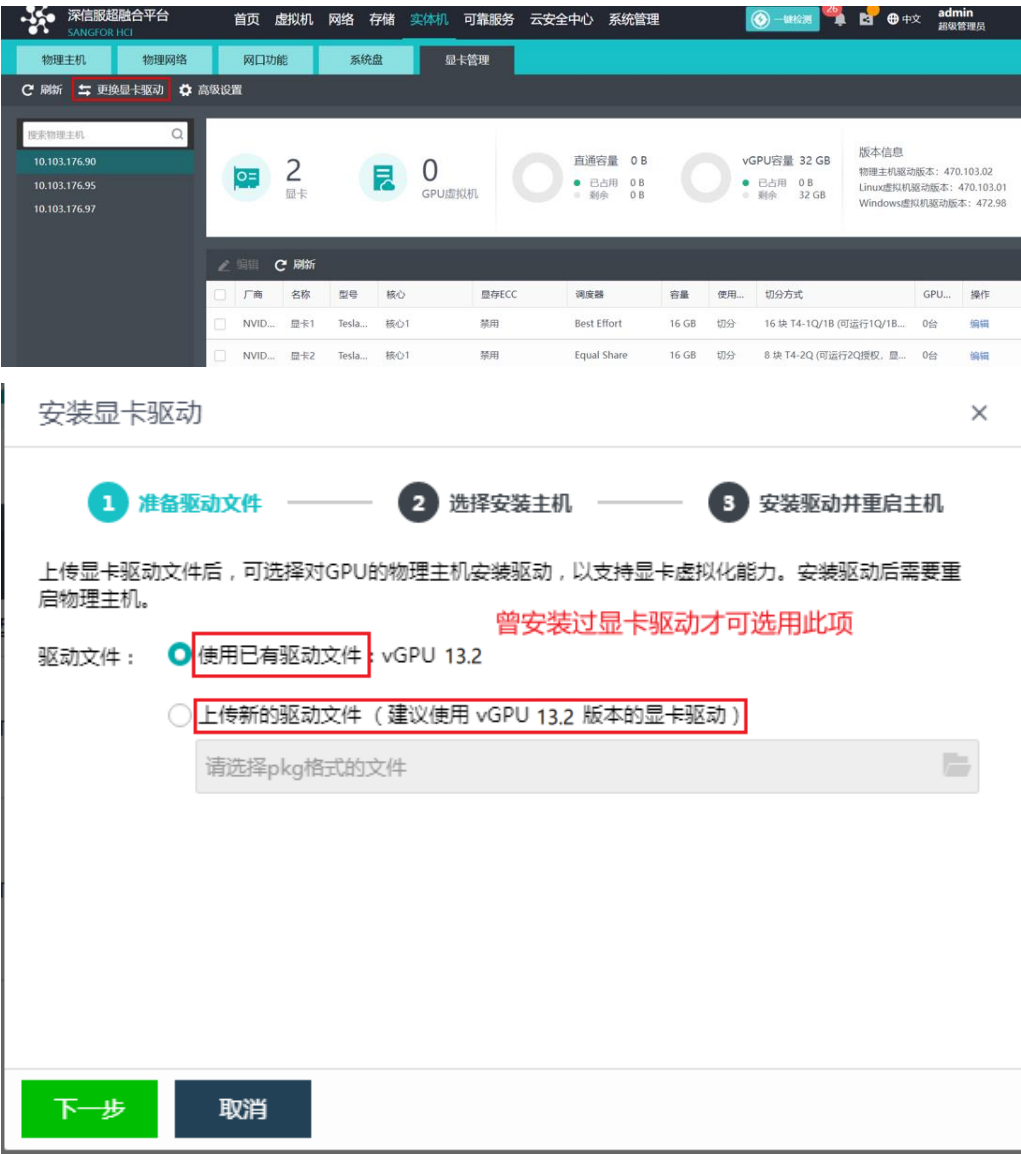
3. 点击<确认>，可以在界面看到显卡的配置信息。



4. 点击<更换服务器驱动>，导入GRID驱动。

注意：

若为 vGPU（HCI6.2.30）用户，升级至 HCI6.8.0 场景，均需要重新导入 GRID 驱动（当前支持 10.2、13.2 版本），且重启主机后生效，因此建议在完成升级后，先导入 vGPU 驱动，再重启主机。



5. 等待上传驱动文件。



6. 选择需要安装驱动的主机，并等待分发驱动文件。





7. 点击“进入单主机维护模式”后，重启电源，使驱动生效。



5.2.14.3. 虚拟机添加显卡

功能说明

给虚拟机添加显卡硬件转变为3D虚拟机，提升对图像处理要求高的场景的支持能力。

注意事项

1. 开机状态的虚拟机添加完显卡后，重启生效。
2. 3D虚拟机桌面只有windows10和windows2016可以通过虚拟机控制台查看，其他Windows操作系统版本暂时不支持在虚拟机控制台查看，因此装显卡驱动时需通过客户端或者远程桌面接入到虚拟机系统。Linux系统的3D虚拟机桌面支持控制台查看。

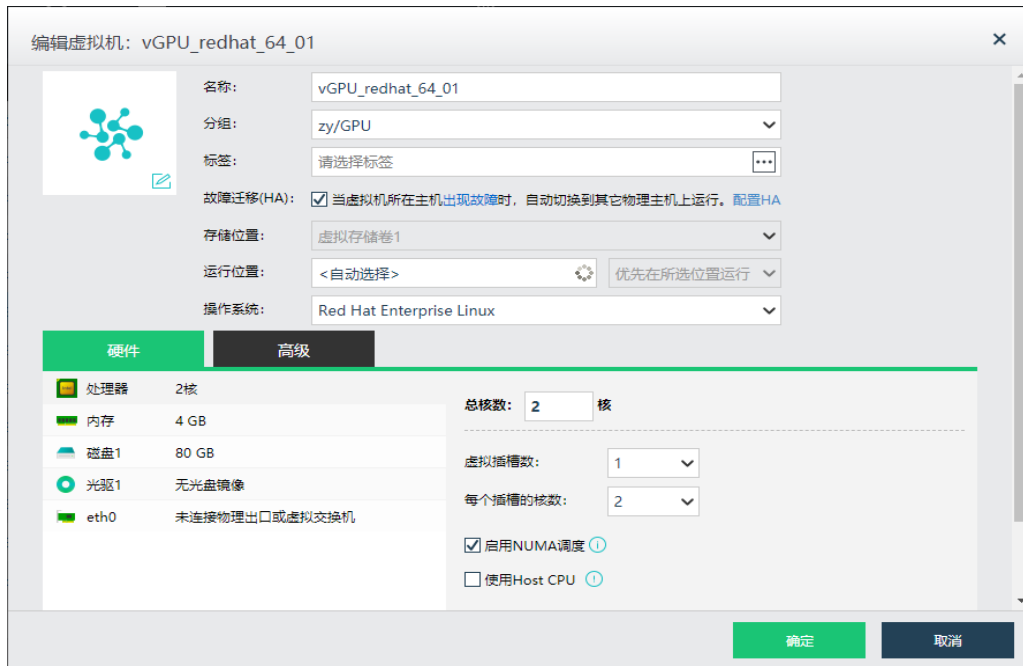
前提条件

直通类型显卡需要平台有锁定为直通模式的显卡核心才能使用。

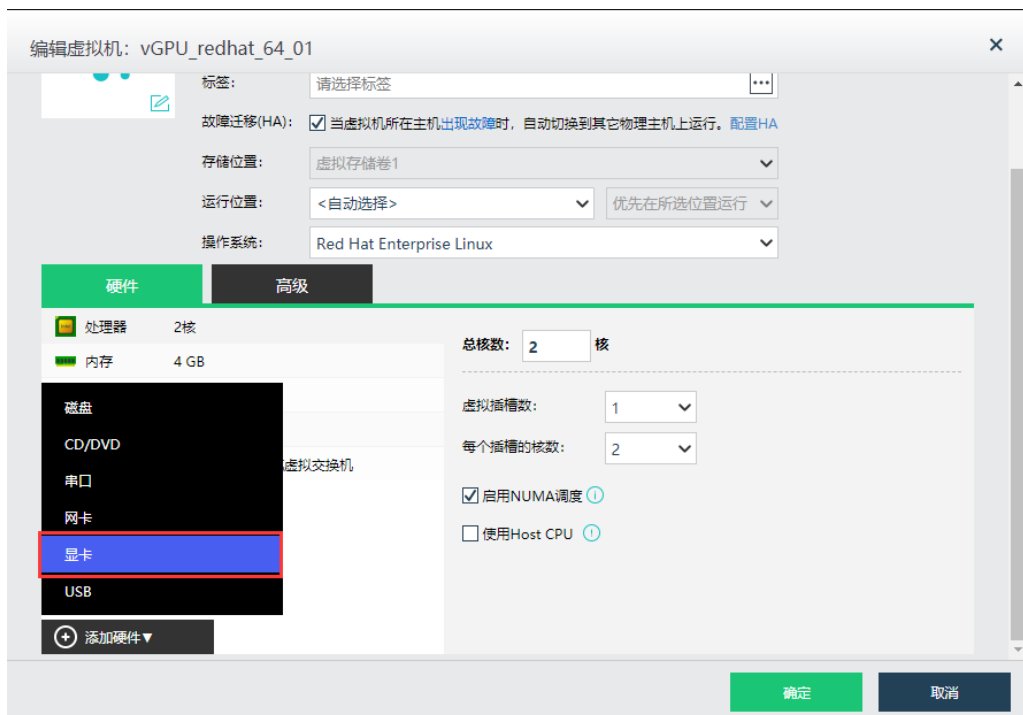
操作步骤

1. 选择要配置的虚拟机，进入编辑虚拟机页面。





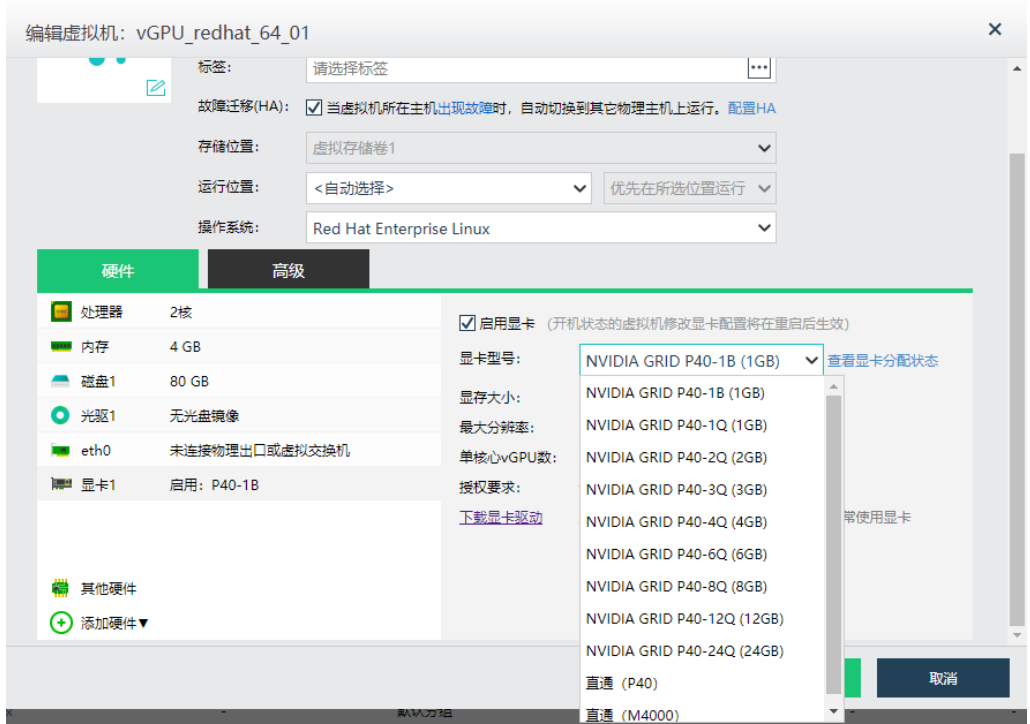
2. 添加硬件中，选择显卡。



3. 选择要配置显卡的型号，然后点击<确定>。

- ① 为虚拟机添加显卡。
- ② 显卡选择直通或者切分模式。
- ③ 当主机上有多显卡时，选择显卡型号。
- ④ 选择已为显卡设置好的切分方式。
- ⑤ 显示该切分方式下的显存容量。

- ⑥ 选择调度器，当多块同型号的显卡存在不同调度器策略时，虚拟机会依照调度器策略来选择显卡。



5.2.14.4. Windows 虚拟机安装显卡驱动及授权

功能说明

给虚拟机配置vGPU后，需要对虚拟机安装显卡驱动虚拟机才可正常使用。

注意事项

无

前提条件

如果GPU显卡硬件兼容，则Windows系统兼容性以英伟达官网为准。

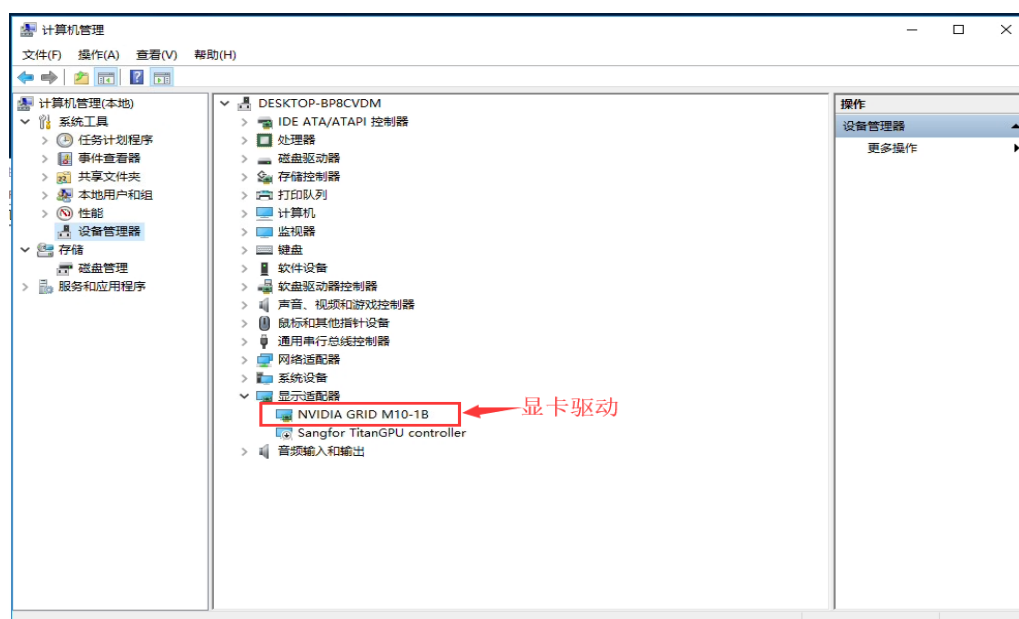
操作步骤

1. 给Windows虚拟机配置相应的IP地址、子网掩码和网关等信息。
2. 给模板虚拟机安装对应版本的显卡驱动，运行安装程序，一路选择默认安装即可。安装之后，重启虚拟机。

名称	修改日期
3D授权服务器-HCI-1.1.0.vma	2022/8/30 11:15
3D授权服务器-VMP-1.1.0.vma	2022/8/30 11:20
472.98_grid_server2012R2_64bit_international	2022/8/29 15:44
472.98_grid_win10_win11_server2016_server2019_server2022_64bit_international	2022/8/29 15:45
dls_instance_token_08-30-2022-21-01-28.tok	2022/8/31 10:50
NVIDIA-Linux-x86_64-470.103.01-grid.run	2022/8/29 15:46
vGPU授权服务器 (nls1.1.0) 搭建和使用教程	2022/8/30 10:42
新建文本文档	2022/8/31 10:50

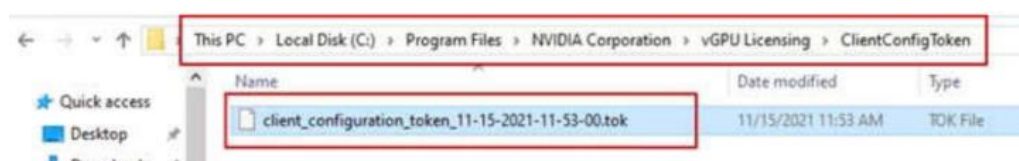


3. 在设备管理器中可查看驱动是否安装成功，如下图所示。

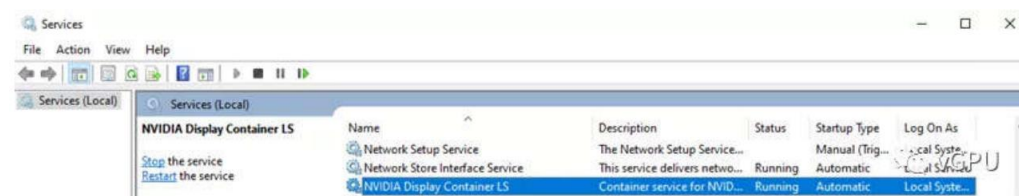


4. 按照“[部署英伟达授权服务器](#)”章节操作，将获取到的客户端授权文件（.tok文件）复制到

C:\Program Files\NVIDIA Corporation\vgpu\licensing\ClientConfigToken



5. 重启NvDisplayContainer服务。



6. 查看License状态。

C:\ProgramFiles\NVIDIA Corporation\NVSMI\nvidia-smi.exe -q



5.2.14.5. Linux 虚拟机安装显卡驱动及授权

功能说明

给虚拟机配置vGPU后，需要对虚拟机安装显卡驱动虚拟机才可正常使用。

注意事项

无

前提条件

如果GPU显卡硬件兼容，则Linux系统兼容性以英伟达官网为准。

操作步骤

1. 给Linux虚拟机配置相应的IP地址、子网掩码和网关等信息。
2. 禁用nouveau驱动。nouveau是一个开源的NVIDIA驱动，可能对后续驱动安装造成干扰。禁用方法如下。

- CentOS_7 或 RedHat7 环境。在 /usr/lib/modprobe.d/dist-blacklist.conf 或 /lib/modprobe.d/dist-blacklist.conf 中添加。

```
blacklist nouveau
options nouveau modeset=0
```

- Ubuntu16.04 环境。创建文件 /etc/modprobe.d/blacklist.conf 且内容如下。

```
blacklist nouveau
options nouveau modeset=0
```

执行命令：\$ sudo update-initramfs -u

- 执行 dracut --force，执行完毕，重启虚拟机。

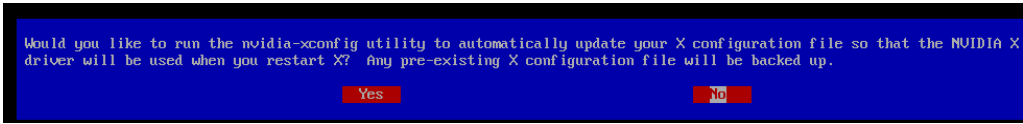
```
dracut --force
reboot
```

- 使用命令 lsmod | grep nouveau 若无输出则证明禁用成功。
3. 关闭X window。可以使用命令：“init 3” 实现。（方法不唯一）
 4. 安装驱动。
 - 拷贝正确版本的 vGPU 驱动 runfile 文件到系统。例如：在 CentOS 中对应的驱动文件为：NVIDIA-Linux-x86_64-390.75-grid.run 下文中，以该文件为例进行讲解。
 - 以超级用户修改文件权限，并执行。注意执行时需要加入以下参数。
- ```
sudo chmod +x NVIDIA-Linux-x86_64-390.75-grid.run
./NVIDIA-Linux-x86_64-390.75-grid.run -Z --no-opengl-files
```
- 安装开始时，会显示蓝色的对话框。按提示进行安装即可，所有的选项都选择默认项。具体过程如下图所示。



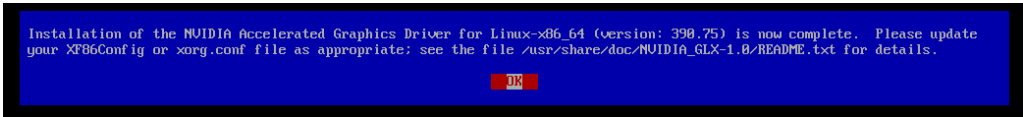
Install NVIDIA's 32-bit compatibility libraries?

- 是否安装：Yes。



Would you like to run the nvidia-xconfig utility to automatically update your X configuration file so that the NVIDIA X driver will be used when you restart X? Any pre-existing X configuration file will be backed up.

- 是否自动升级 X 配置文件，NO。

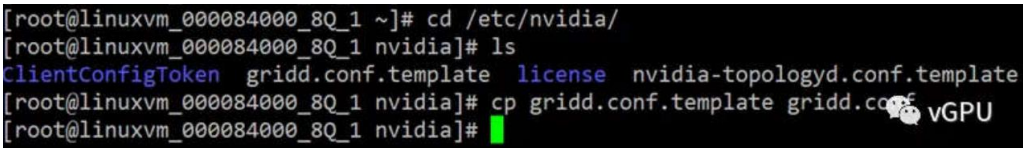


Installation of the NVIDIA Accelerated Graphics Driver for Linux-x86\_64 (version: 390.75) is now complete. Please update your XF86Config or xorg.conf file as appropriate; see the file /usr/share/doc/NVIDIA\_GLX-1.0/README.txt for details.

- 安装完成。

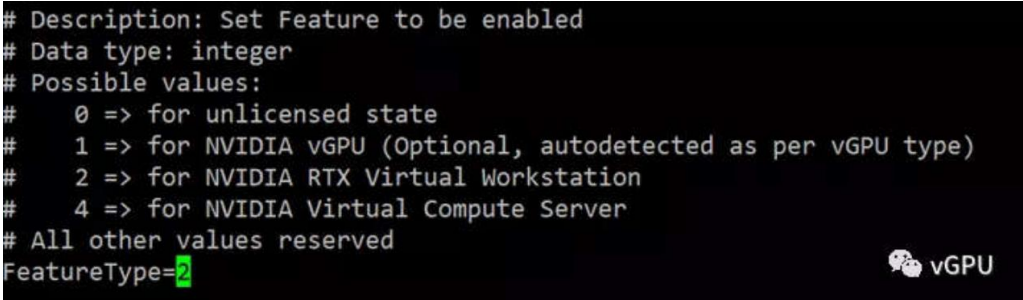
## 5. 获取授权。

- 按照“[部署英伟达授权服务器](#)”章节操作，下载客户端授权文件（.tok 文件）。
- cd /etc/nvidia 进入 nvidia 目录，复制 gridd.conf.template 为 gridd.conf



```
[root@linuxvm_000084000_8Q_1 ~]# cd /etc/nvidia/
[root@linuxvm_000084000_8Q_1 nvidia]# ls
ClientConfigToken gridd.conf.template license nvidia-topologyd.conf.template
[root@linuxvm_000084000_8Q_1 nvidia]# cp gridd.conf.template gridd.conf
[root@linuxvm_000084000_8Q_1 nvidia]#
```

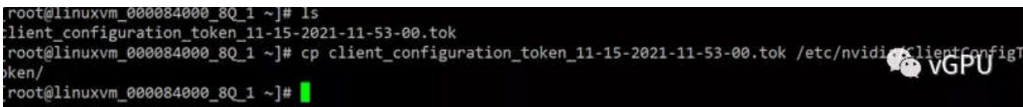
- 编辑 gridd.conf，只需设置 FeatureType 的值为要请求的 vGPU License 类型编号，不要设置其中的 ServerAddress。



```
Description: Set Feature to be enabled
Data type: integer
Possible values:
0 => for unlicensed state
1 => for NVIDIA vGPU (Optional, autodetected as per vGPU type)
2 => for NVIDIA RTX Virtual Workstation
4 => for NVIDIA Virtual Compute Server
All other values reserved
FeatureType=2
```

- 然后将下载到的 Token 文件复制到/etc/nvidia/ClientConfigToken 目录中，例如：

```
cp client_configuration_token_11-15-2021-11-53-00.tok
/etc/nvidia/ClientConfigToken/
```



```
root@linuxvm_000084000_8Q_1 ~]# ls
client_configuration_token_11-15-2021-11-53-00.tok
root@linuxvm_000084000_8Q_1 ~]# cp client_configuration_token_11-15-2021-11-53-00.tok /etc/nvidia/ClientConfigToken/
root@linuxvm_000084000_8Q_1 ~]#
```

- systemctl restart nvidia-gridd 重启 nvidia-gridd 服务，应看到 vGPU 授权成功。

```
[root@linuxvm_000084000_8Q_1 ~]# systemctl restart nvidia-gridd.service
[root@linuxvm_000084000_8Q_1 ~]# systemctl status nvidia-gridd.service
● nvidia-gridd.service - NVIDIA Grid Daemon
 Loaded: loaded (/usr/lib/systemd/system/nvidia-gridd.service; enabled; vendor preset: disabled)
 Active: active (running) since Mon 2021-11-15 12:40:40 CST; 8s ago
 Process: 26582 ExecStopPost=/bin/rm -rf /var/run/nvidia-gridd (code=exited, status=0/SUCCESS)
 Process: 26583 ExecStart=/usr/bin/nvidia-gridd (code=exited, status=0/SUCCESS)
 Main PID: 26585 (nvidia-gridd)
 Tasks: 4 (limit: 49632)
 Memory: 1.5M
 CGroup: /system.slice/nvidia-gridd.service
 └─26585 /usr/bin/nvidia-gridd

Nov 15 12:40:40 linuxvm_000084000_8Q_1 systemd[1]: Stopped NVIDIA Grid Daemon.
Nov 15 12:40:40 linuxvm_000084000_8Q_1 systemd[1]: Starting NVIDIA Grid Daemon...
Nov 15 12:40:40 linuxvm_000084000_8Q_1 nvidia-gridd[26585]: Started (26585)
Nov 15 12:40:40 linuxvm_000084000_8Q_1 systemd[1]: Started NVIDIA Grid Daemon.
Nov 15 12:40:40 linuxvm_000084000_8Q_1 nvidia-gridd[26585]: Configuration parameter { ServerAddress } not set
Nov 15 12:40:40 linuxvm_000084000_8Q_1 nvidia-gridd[26585]: vGPU Software package (0)
Nov 15 12:40:40 linuxvm_000084000_8Q_1 nvidia-gridd[26585]: Ignore service provider and node-locked licensing
Nov 15 12:40:40 linuxvm_000084000_8Q_1 nvidia-gridd[26585]: NLS initialized
Nov 15 12:40:40 linuxvm_000084000_8Q_1 nvidia-gridd[26585]: Acquiring license. (Info: api.cls.licensing.nvidia.)
Nov 15 12:40:48 linuxvm_000084000_8Q_1 nvidia-gridd[26585]: License acquired successfully. (Info: api.cls.licensing.nvidia.)
lines 1-21/21 (END)
```

- 也可以用 NVIDIA-smi -q 查询授权状态：

```
[root@linuxvm_000084000_8Q_1 ~]# nvidia-smi -q |grep -i status
License Status : Licensed (Expiry: 2021-11-16 4:59:24 GMT+0800)
[root@linuxvm_000084000_8Q_1 ~]#
```

5.2.14.6. 虚拟机修改显卡

功能说明

给虚拟机修改显卡硬件，以便灵活调整显卡的使用。

注意事项

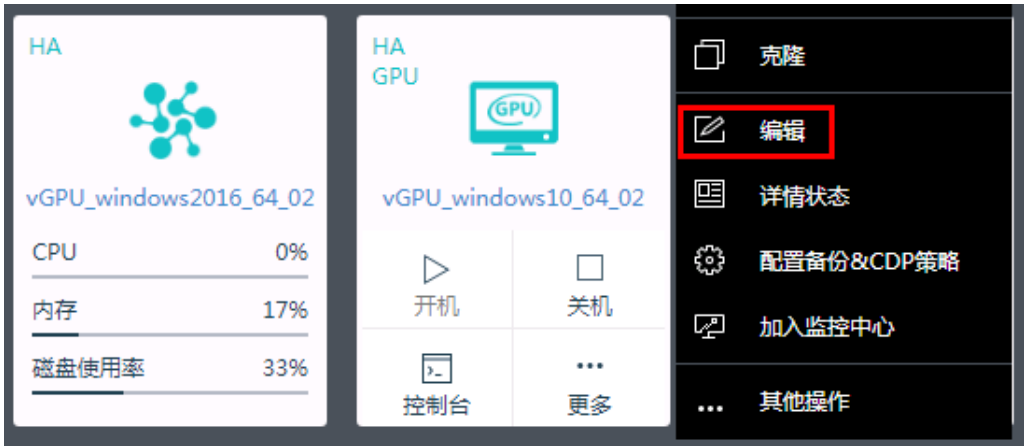
开机状态下修改显卡类型后，虚拟机重启生效。

前提条件

无

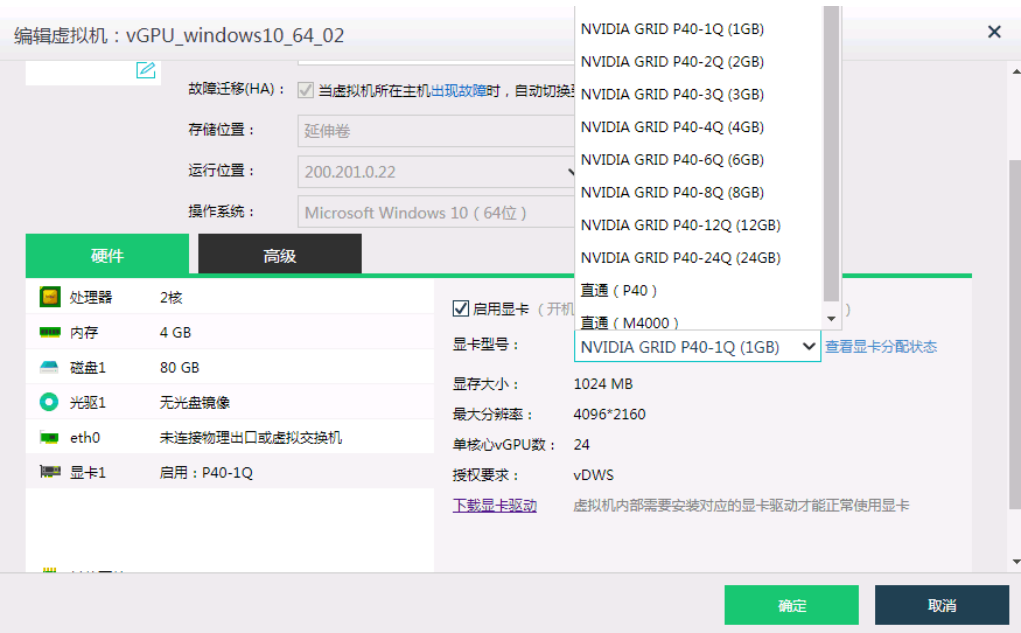
操作步骤

1. 点击[虚拟机]进入虚拟机关联界面，找到要修改显卡类型的虚拟机，点击<更多/编辑>。





2. 点击原有显卡，修改显卡型号到需要型号，确定即可。



## 5.2.15. 导出虚拟机报表

### 功能说明

导出虚拟机的配置信息为Excel文件。

### 注意事项

无

### 前提条件

无

### 操作步骤

通过[虚拟机/更多操作/导出虚拟机配置报表]可导出HCI平台所有虚拟机配置信息。





## 5.2.16. 虚拟机 Qos 上限限制

### 5.2.16.1. CPU 频率限制

#### 功能说明

该任务指导管理员限制异常虚拟机对资源的大量消耗，保障其他正常虚拟机有充足的资源可使用，在开机状态下也支持设置，当虚拟机运行一周后会生成推荐值显示在输入框中，CPU频率限制值范围为100MHz-1000GHz。

#### 注意事项

1. 虚拟机CPU频率如果限制的过低，比如100MHz，可能会出现虚拟机报表数据更新不及时和虚拟机内部重启的风险。
2. 安装了vmtools的windows虚拟机，可能会出现虚拟机设置了CPU限制，但是操作系统内的CPU使用率以及虚拟机报表显示的CPU利用率没有降下来，需要在平台后台查看虚拟机的CPU使用率。

#### 前提条件

无

#### 操作步骤

1. 在[虚拟机]页面勾选需要操作的虚拟机，点击[更多操作/编辑]进入虚拟机编辑页面。



2. 点击[处理器]进入到处理器信息界面，勾选[限制CPU频率]，设置限制值并点击[确定]。



### 5.2.16.2. 磁盘 I/O 频率限制

#### 功能说明

该任务指导管理员限制非重要虚拟机对资源的使用上限，保障重要虚拟机有充足的

资源可使用，在开机状态下也支持设置，可对磁盘的最大读/写速率和最大读/写次数进行限制，当虚拟机运行一周后会生成推荐值显示在输入框中，其中最大读/写速率限制范围为128KB/s-102400MB/s，最大读/写次数范围限制为16-2147483647。

## 注意事项

虚拟机系统的IO如果限制太低，如128KB/s，可能会出现虚拟机内部重启的风险。

## 前提条件

无

## 操作步骤

1. 在[虚拟机]页面勾选需要操作的虚拟机，点击[更多操作/编辑]进入虚拟机编辑页面。



2. 点击[磁盘]进入到磁盘信息界面，勾选[磁盘IO限制]，设置限制值并点击[确定]。



### 5.2.16.3. 网卡流量限制

#### 功能说明

业务高压访问场景下需要借助QoS功能对非重要虚拟机的网卡流量进行限制，以保证核心业务的正常运行。深信服HCI支持对单张网卡进行上/下行QoS设置，限制虚拟机网络带宽。

#### 注意事项

1. 虚拟机网卡发送流量限制范围：1000Kbps-20000Mbps；
2. 接收流量限制范围：1000Kbps-20000Mbps。

#### 前提条件

无

#### 操作步骤

1. 在[虚拟机]页面勾选需要操作的虚拟机，点击[更多/编辑]进入虚拟机编辑页面。



2. 点击需要限制流量的网卡，进入到网卡信息界面，流量限制勾选“启用”，设置发送流量、接收流量限制值并点击<确定>。



## 5.2.17. 多国语言键盘支持

### 功能说明

该任务指导管理员切换多国语言键盘输入方式，可支持德语，法语，西班牙语、意大利等键盘输入，默认使用美式英文键盘。

### 注意事项

1. 虚拟机键盘类型只支持在关机状态下编辑。

### 前提条件

无

### 操作步骤

1. 在[虚拟机]页面勾选需要操作的虚拟机，点击[更多操作/编辑]进入虚拟机编辑页面。



2. 下拉找到并点击[其他硬件]进入硬件信息页面设置虚拟机键盘类型。



### 5.3. 查看虚拟机运行状态

#### 功能说明

该任务指导管理员查看虚拟机基本运行状态。

注意事项

无

前提条件

无

操作步骤

1. 在[虚拟机]页面虚拟机列表中点击虚拟机名称，进入虚拟机信息页面。



2. 在[运行状态]栏中查看虚拟机CPU、内存、磁盘容量使用率。



3. 查看包速率趋势、流速趋势、CPU趋势、内存趋势、IO次数趋势、IO速率趋势。



4. 在[基本信息与硬件配置]中查看虚拟机基本信息以及硬件配置信息。

| ■ 基本信息与硬件配置 |                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------|
| 虚拟机名称：      | 2008                                                                                                           |
| 描述：         | <a href="#">点击编辑描述信息</a>  |
| 分组：         | 默认组                                                                                                            |
| 存储位置：       | 172.200.200.123;172.200.200.121                                                                                |
| 运行位置：       | 172.200.200.121                                                                                                |
| 操作系统：       | Microsoft Server 2008 ( 64位 )                                                                                  |
| 虚拟机性能优化工具：  | 已安装 <a href="#">重新安装</a>                                                                                       |
| 重要虚拟机：      | 否                                                                                                              |
| 开机自启动：      | 否                                                                                                              |
| 启用内存回收机制：   | 是                                                                                                              |
| 启动顺序：       | 磁盘1->光驱                                                                                                        |
| 关机时长：       | 2天                                                                                                             |





## 5.4. 删除虚拟机

### 功能说明

该任务指导管理员删除虚拟机。

### 注意事项

共享磁盘不会随虚拟机删除而删除，如需删除，请到[存储/虚拟存储/虚拟共享盘]中手工删除，参考本手册“[删除虚拟共享盘](#)”章节。

### 前提条件

虚拟机关机。

### 操作步骤

1. 在[虚拟机]页面虚拟机列表中移动鼠标到虚拟机名称上，点击下拉框按钮，选择<其他操作/删除>，进入删除虚拟机确认页面。



2. 点击<确认>，完成虚拟机删除。

**警告：**

删除后的虚拟机可以在回收站内恢复，防止误删除。管理员可以通过[管理/回收站]打开回收站。

## 6. 虚拟网络配置指导

### 6.1. 创建物理出口

#### 6.1.1. 物理出口相关概念

**物理出口：**物理出口用来连通虚拟网络和物理网络，对用户呈现为服务器物理网口。

“物理出口”对内可以通过端口组连接虚拟路由器、虚拟网络设备，对外通过主机的物理网口连接交换机与外部网络互通。

**端口组：**通过划分“端口组”，将虚拟网络连接到“物理出口”的网口进行分组，通常将具有相同网络属性（如相同的VLAN）的网口集合划分到同一个组。虚拟网络中的设备或虚拟机可以通过端口组连接到“物理出口”。

#### 6.1.2. 新建物理出口及端口组（多网段）

##### 功能说明

该任务指导管理员创建多网段端口组的物理出口，此种端口组允许虚拟机接入多个网段。

##### 注意事项

1. 多网段标签端口组关联的物理网口的对端必须配置为trunk，交换机端口的pvid为物理出口关联端口组设置的pvid VLAN。此种类型的端口组允许用户使用多个业务网段。
2. 物理出口支持单网口、链路聚合的双网口、链路聚合的四网口。链路聚合需要在实体机详情的物理网络中进行配置，交换机的端口也需要配置相应的链路聚合模式。
3. 同一个端口组的pvid与交换机保持一致。

##### 前提条件

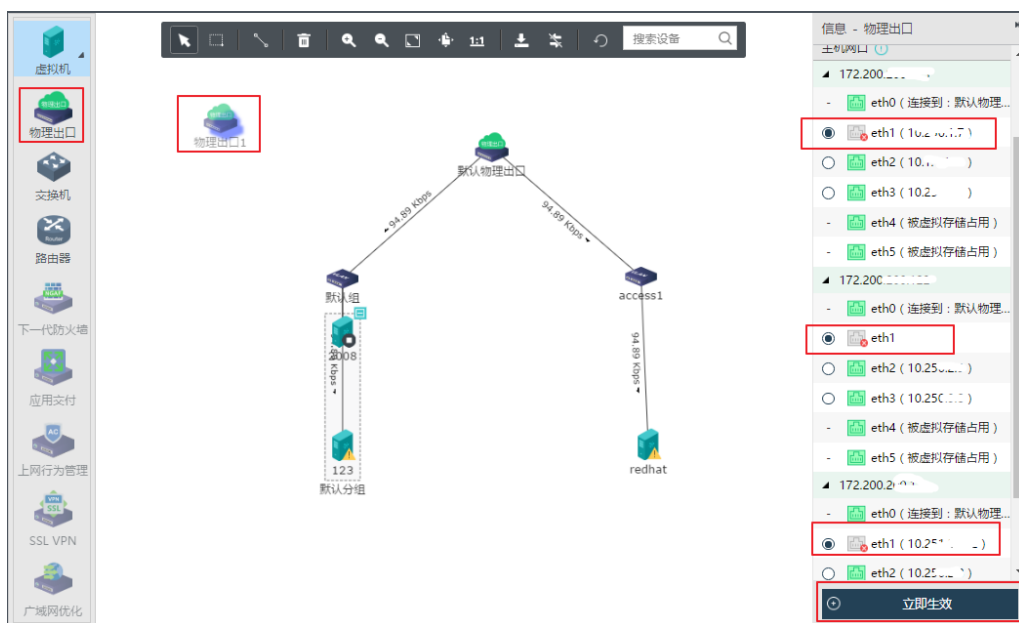
已经按照注意事项完成交换机配置。

##### 操作步骤

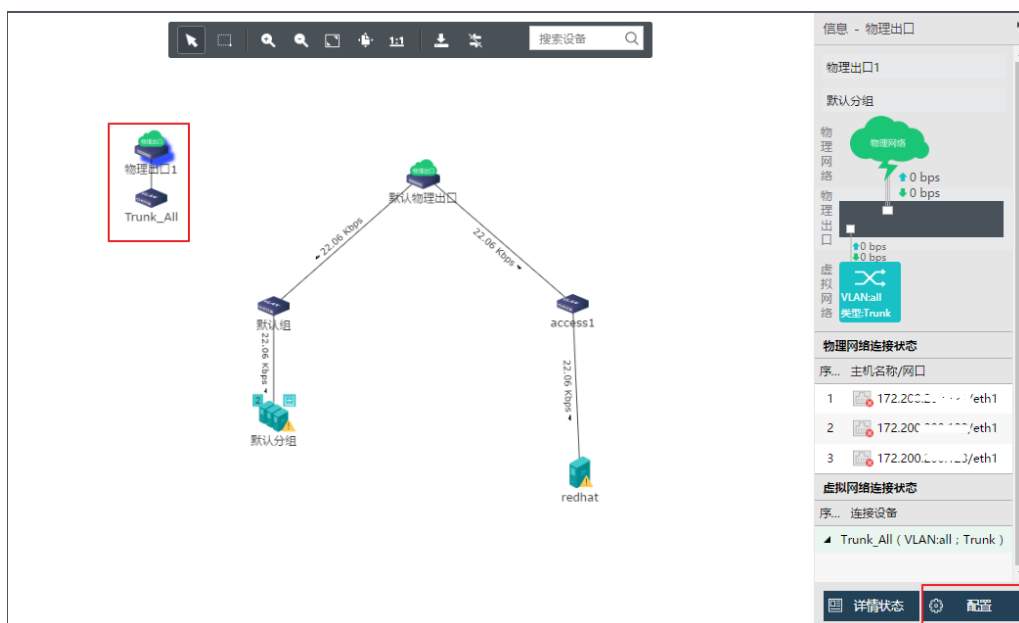
1. 在[网络与安全/网络拓扑]页面中点击<编辑拓扑>，网络拓扑进入编辑状态。



2. 在左侧网络设备中拖动物理出口至网络拓扑中，并接着在右侧服务器中选择相应的物理出口。



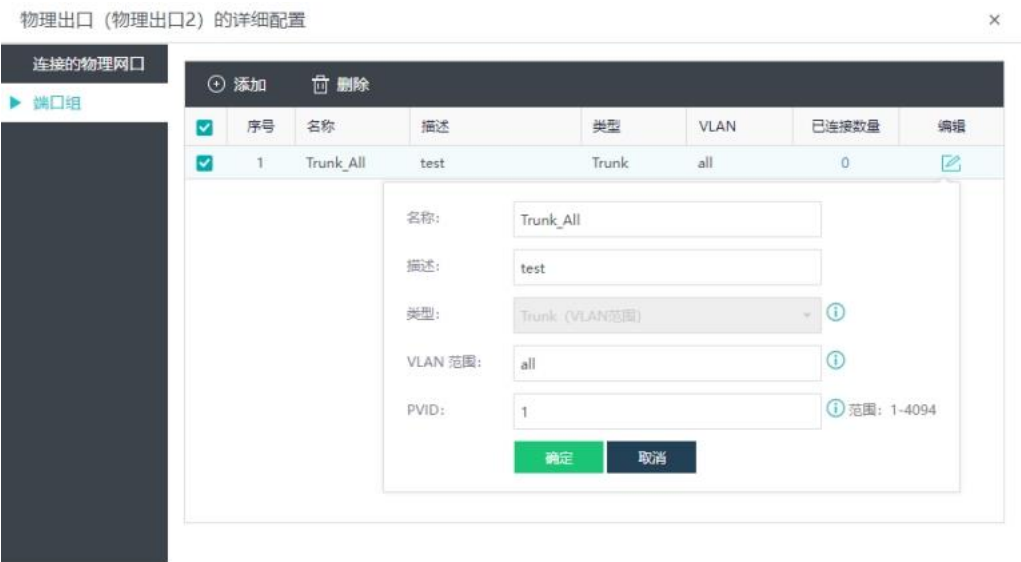
3. 点击<立即生效>，并点击左上角<退出编辑>，完成物理出口创建。
4. 选择已创建的物理出口，选择<配置>，进入[物理出口编辑]页面。



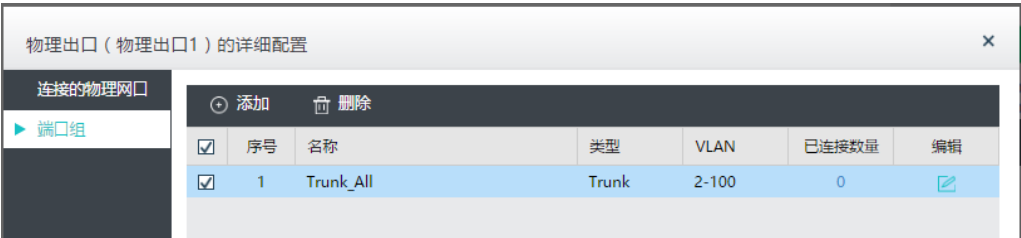
5. 选择[端口组], 点击编辑图标。（也可以自行添加一个trunk类型的端口组）



6. 配置端口组名称、描述、VLAN范围和pvid VLAN，点击<确定>保存配置。



7. 创建物理端口确认。



6.1.3. 新建物理出口及端口组（单网段）

功能说明

该任务指导管理员创建单网段端口组的物理出口。

注意事项

- 1. 非多网段标签端口组的物理出口关联的服务器网口对端的交换机必须配置为 access，交换机端口允许通过的VLAN为物理出口关联端口组设置的pvid VLAN。此种类型的端口组只允许用户使用一个业务网口段。
- 2. 物理出口支持单网口和链路聚合。链路聚合需要在实体机的物理网络中进行配置，交换机的端口也需要配置相应的链路聚合模式。

## ⚠ 注意:

同一个物理出口的端口组的 pvid 与交换机保持一致。

## 前提条件

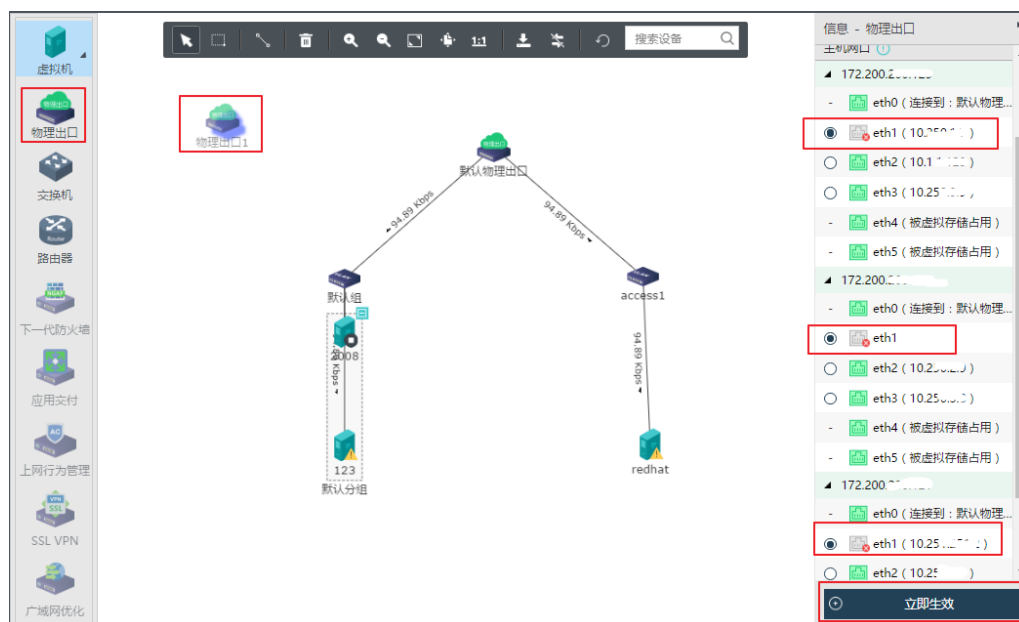
已经按照注意事项完成交换机配置。

## 操作步骤

1. 在[网络与安全/网络拓扑]页面中点击<编辑拓扑>，网络拓扑进入编辑状态。



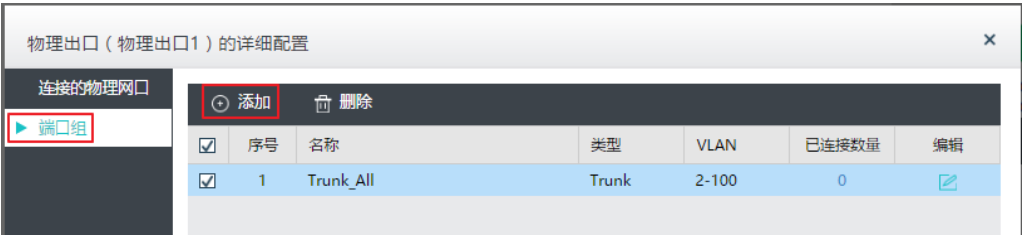
2. 在左侧网络设备中拖动物理出口至网络拓扑中，并接着在右侧服务器中选择相应的物理出口。



3. 点击<立即生效>，并点击左上角<退出编辑>，完成物理出口创建。
4. 选择已创建的物理出口，选择<配置端口组>，进入[物理出口编辑]页面。



5. 选择[端口组]，点击<添加>。



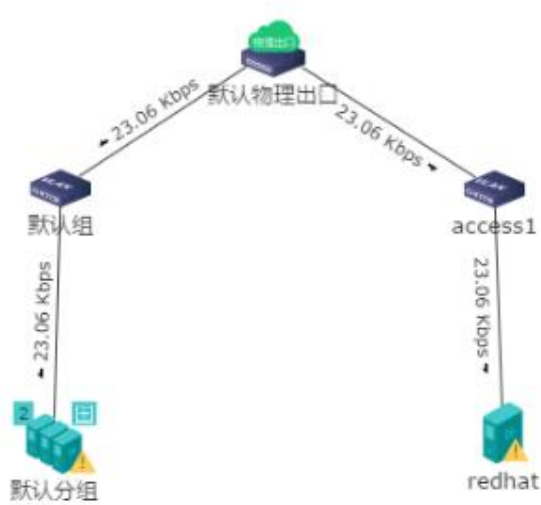
6. 配置端口组名称、描述，类型选择access，pvid VLAN，点击<确定>保存配置。



7. 创建物理端口确认。



### 6.1.4. 物理出口典型拓扑



#### 配置说明

虚拟机直连物理出口，通过不同的端口组连接不同的业务网段。

## 6.2. 创建虚拟网络设备

### 6.2.1. 虚拟路由器创建

#### 功能说明

该任务指导管理员创建虚拟路由器。

虚拟路由器支持以下功能：

- 三层网口、VLAN子接口（支持IPv4和IPv6）
- 静态路由（支持IPv4和IPv6）
- 源地址转换（SNAT）、目的地址转换（DNAT）（仅支持IPv4）



- 策略路由（支持IPv4和IPv6）
- 访问控制
- DHCPv4和DHCPv6
- DNS代理
- 高可用HA
- 指定运行位置

## 注意事项

1. 路由器可以直连物理出口端口组。
2. 路由器连接二层虚拟机交换机，才能连接虚拟机。
3. 路由器与路由器、防火墙等其他三层设备对接时中间需要连接二层交换机。
4. 单个虚拟路由器运行在单个主机上，可以通过故障HA实现冗余。

## 前提条件

无

## 操作步骤

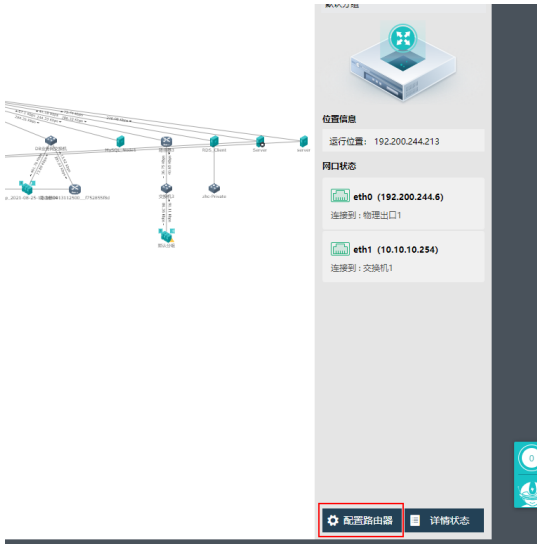
1. 在[网络与安全/网络拓扑]页面中点击<编辑拓扑>，网络拓扑进入编辑状态。



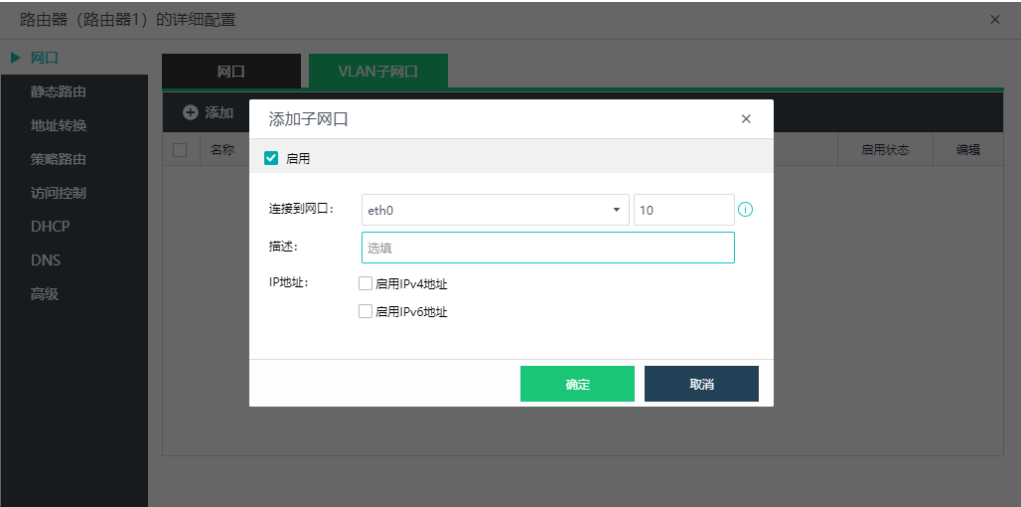
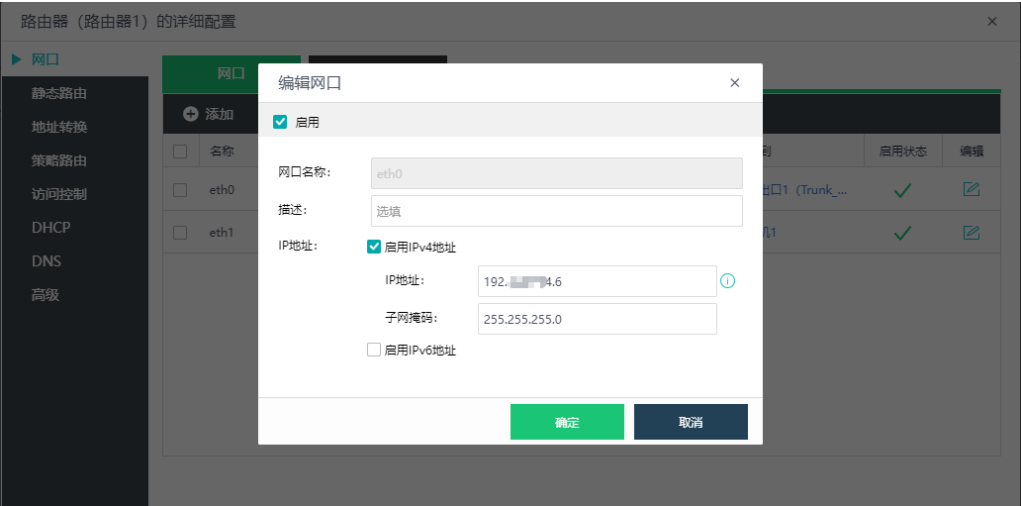
2. 在左侧网络设备中拖动虚拟路由器至网络拓扑中，点击<立即生效>。



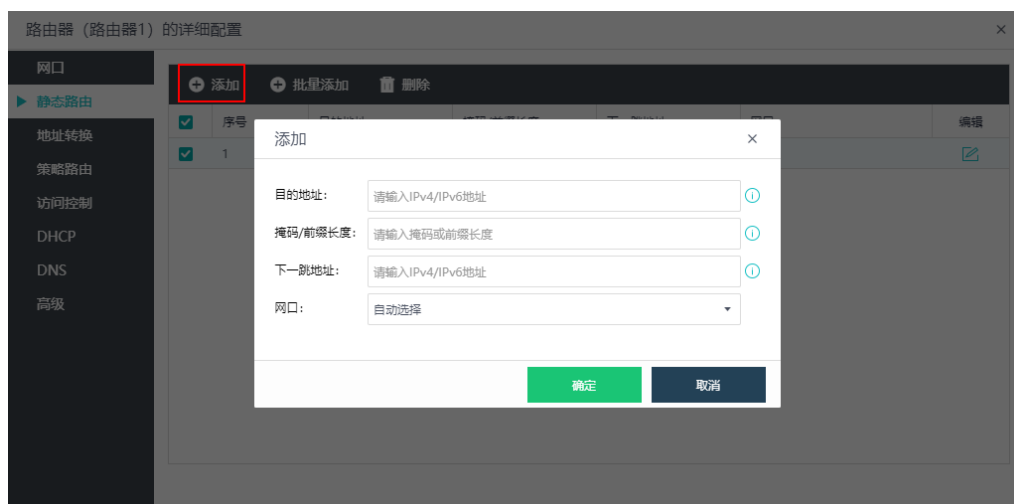
3. 点击<配置路由器>，进入虚拟路由器的配置界面。



4. 在<网口>标签页下点击<添加>配置网口和VLAN子接口，网口地址支持配置IPv4和IPv6地址



5. 在<静态路由>标签页下点击<添加>配置静态路由，静态路由支持IPv4和IPv6



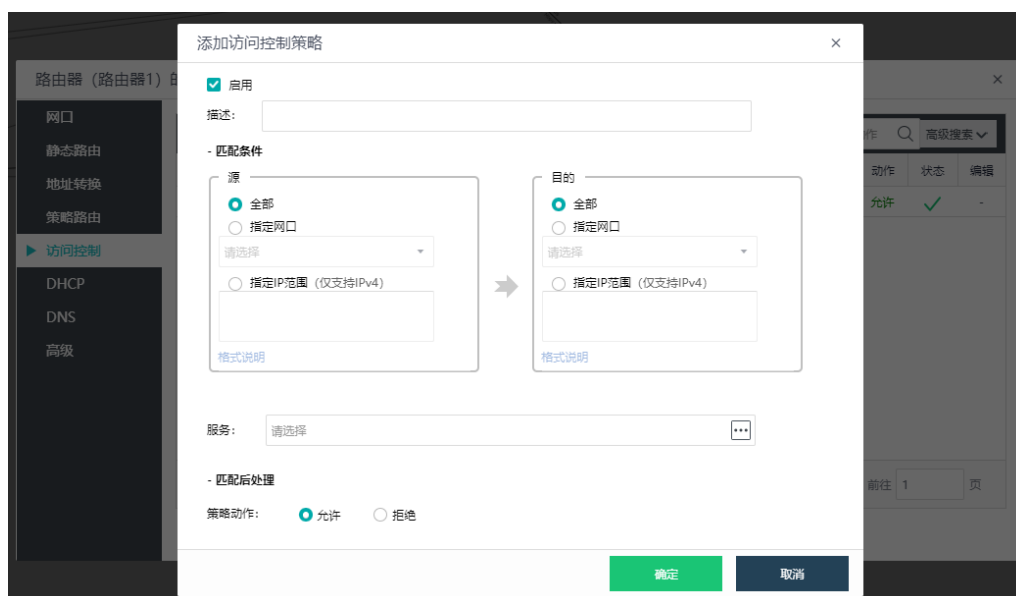
6. 在<地址转换/源地址转换(SNAT)> 标签页下点击<添加>配置源地址转换，在<地址转换/目的地址转换(DNAT)>标签页下点击<添加>配置目的地址转换。源地址转换和目的地址转换仅支持IPv4地址。



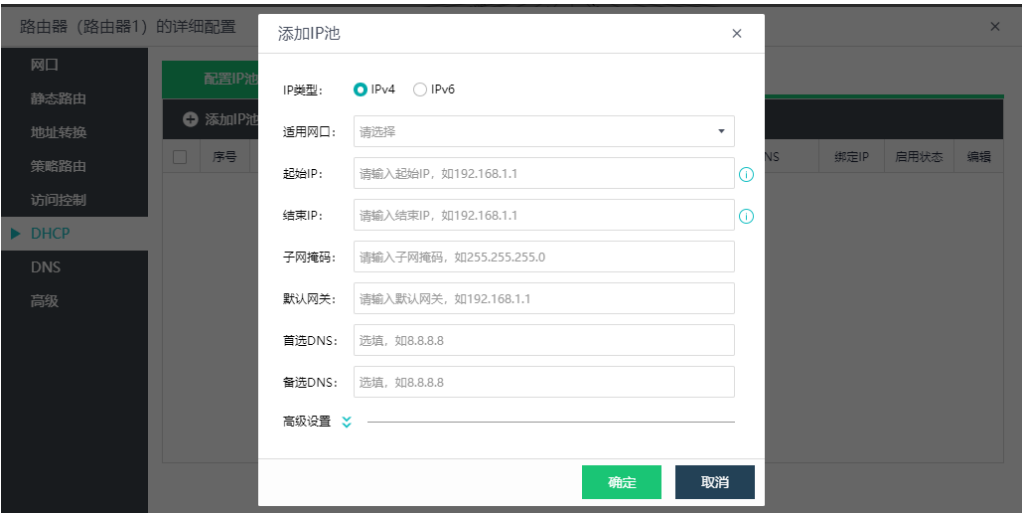
7. 在<策略路由>标签页下点击<添加>，配置策略路由，策略路由支持IPv4和IPv6。



8. 在<访问控制>标签下，点击<添加>配置访问控制策略



9. 在<DHCP/配置IP池>标签下，点击<添加IP池>，配置DHCP IP池的地址范围（支持IPv4和IPv6），在<DHCP/DHCPv4>可以查看当前已分配的IPv4地址信息，在<DHCP/DHCPv6>可以查看当前已分配的IPv6地址信息。



10. 在<DNS>标签页下，勾选“DNS代理”并点击“修改”配置首选DNS和备选DNS。



11. 在<高级>标签页下，可配置虚拟路由器的HA和运行位置





- **高可用：**路由器 HA，当本节点的路由器故障之后会在其他节点上面重新拉起路由器，避免路由器所在主机故障之后出现网络无法恢复的问题。
- **路由器运行位置：**系统会根据配置自动选择路由器的运行位置，但在某些特殊场景下，您也可以手动指定运行位置。

### 6.2.2. 分布式虚拟机交换机创建

#### 功能说明

该任务指导管理员创建分布式虚拟交换机。

分布式虚拟交换机支持广播风暴抑制，可设置流速阈值，包速阈值。

#### 注意事项

1. 分布式虚拟交换机都是二层交换机。
2. 通常与虚拟路由器等三层设备直连。

#### 前提条件

无

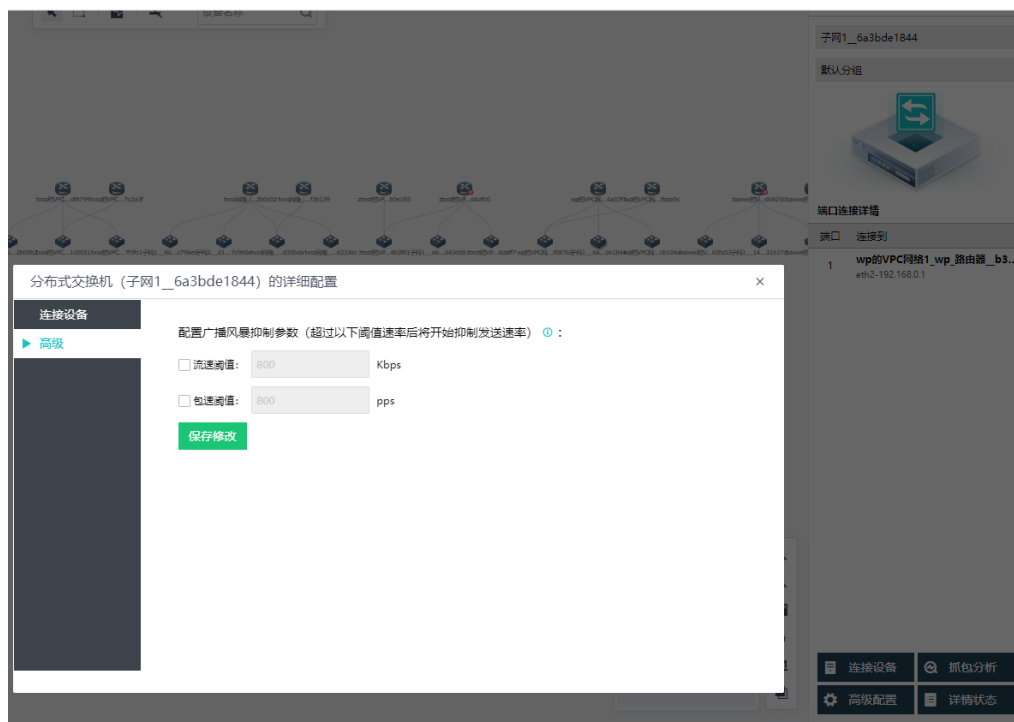
#### 操作步骤

1. 在[网络与安全/网络拓扑]页面中点击<编辑拓扑>，网络拓扑进入编辑状态。



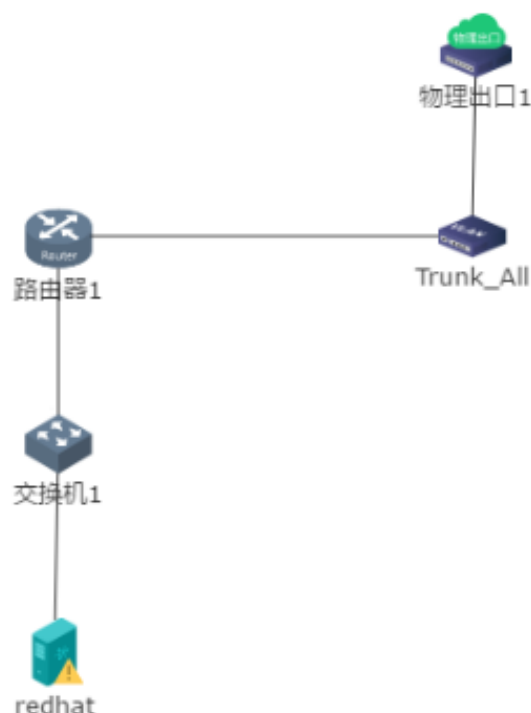
2. 在左侧网络设备中拖动虚拟交换机至网络拓扑中，点击<立即生效>，并点击左上角<退出编辑>完成虚拟交换机创建。

3. 点击虚拟交换机，在右边选择框出点击[高级配置/高级]可进行广播风暴抑制参数配置，并点击<保存修改>。



- **流速阈值：**当交换机出现广播风暴的时候，可以限制交换机转发网络流速，或者断开某些网口以阻断风暴。
- **包速阈值：**当交换机出现广播风暴的时候，可以限制交换机转发发包速率，或者断开某些网口以阻断风暴。

### 6.2.3. 虚拟交换机路由器典型拓扑



#### 配置说明

1. 交换机作为二层设备，连接虚拟机和路由器，路由配置业务网络IP与外部业务网关进行对接。
2. 路由器上配置路由以及NAT策略使内部虚拟机与外部互通。

### 6.2.4. 其他 NFV 设备创建

#### 功能说明

该任务指导管理员创建NFV设备（以上网行为管理vAC示例）。

#### 注意事项

NFV设备包含深信服公司下一代防火墙vAF、应用交付vAD、上网行为管理vAC、SSL VPN、广域网优化vWOC，它们的创建方式类似。

#### 前提条件

1. 已经获得vAC授权。



2. 已经上传深信服NFV相关的vAC模板。

## 操作步骤

1. 在[网络与安全/网络拓扑]页面中点击<编辑拓扑>，网络拓扑进入编辑状态。



2. 在左侧网络设备中拖动虚拟上网行为管理vAC至网络拓扑中，点击<立即生效>，并点击左上角<退出编辑>完成vAC创建。
3. 选择<授权>，对设备进行授权配置（不要超过购买授权数）。



4. 授权后设备自动开机后，即可登录web进行管理。



## 6.3. 配置流量镜像

### 功能说明

运维场景下需要将业务虚拟机的网络流量镜像至安全审计设备以实现流量筛选和监控。深信服HCI支持将虚拟机/网络设备的网卡流量复制转发至超融合出口，如需镜像至外部设备，需在中间交换机配置流量镜像。

### 注意事项

1. 一条镜像规则源对象最多可选1024个网口。
2. 目的对象仅能选择1个虚拟机网口或网络设备网口。
3. 一个虚拟机/网络设备网口、物理主机业务口如果作为源对象，只能属于一条流量镜像策略；如果作为目的对象，可以属于多条流量镜像策略。
4. 不支持物理网络到虚拟网络的镜像功能。

5. 随着规则数越多，业务流量时延越大，吞吐越小，建议配置在100条规则以内。
6. 被流量镜像引用后的虚拟机支持集群内迁移，迁移后流量镜像仍然生效。
7. 支持为流量镜像单独配置物理出口。将虚拟网络流量镜像给外部设备场景下，镜像流量占用业务通信口；集群内跨主机镜像时，镜像流量占用数据通信口；为避免镜像流量与业务口或数据通信口抢占带宽，高负载场景下建议规划单独物理网卡进行流量镜像转发。
8. 镜像到物理业务口时，必须配置VLAN，且VLAN必须和物理出口连接的物理交换机（trunk口）上允许的VLAN一致，同时镜像流量不能包含该VLAN的流量。
9. 镜像规则使用物理出口连接的业务口时，当物理出口连接的业务口修改后，流量镜像规则中对应的物理业务口也随之变更。
10. 仅连通域场景下支持跨资源池镜像。
11. 即使被DFW拦截的流量，和被QoS限制的流量，都会被流量镜像捕捉转发。
12. 多网合一网口为镜像源端时，仅捕捉业务流量。

## 前提条件

无

## 操作步骤

1. 进入[网络与安全/流量镜像]页面，点击<新增>按钮，配置流量镜像策略。



1. 平台支持配置3种流量镜像策略：虚拟网络内部流量镜像、虚拟网络流量镜像至物理网络、物理网口间流量镜像。

- 指定镜像源：

虚拟网络内部流量镜像：指定虚拟机/网络设备网口；

虚拟网络流量镜像至物理网络：指定虚拟机/网络设备网口；

物理网口间流量镜像：指定物理主机业务口。

- 指定镜像目的：

虚拟网络内部流量镜像：指定虚拟机/网络设备网口；

虚拟网络流量镜像至物理网络：指定物理主机业务口；

物理网口间流量镜像：指定物理主机业务口。

- VLAN ID:

虚拟网络内部流量镜像：无需填写；

虚拟网络流量镜像至物理网络：指定镜像报文所携带的VLAN ID；

物理网口间流量镜像：指定镜像报文所携带的VLAN ID。

- 采样率：源对象流量被镜像的比例，默认 100%，表示流量被完全镜像。
- 流量方向：需要镜像的源对象流量方向。

输入/输出表示同时镜像源对象接收和发出的流量；

仅输入表示仅镜像源对象接收的流量；

仅输出表示仅镜像源对象发出的流量。

- 策略状态：勾选“启用”，则策略生效。

新增流量镜像策略×

① 支持虚拟网络内部流量镜像、虚拟网络流量镜像至物理网络、物理网口间流量镜像三种策略。[配置指引](#)

名称：

指定镜像源：

请选择

...

指定镜像目的：

请选择

...

VLAN ID：

采样率 ①：

100

%

流量方向 ①：

☒ 输入/输出

☐ 仅输入

☐ 仅输出

策略状态：

☒ 启用

确定

取消

2. 策略配置完成后，即可在目的端设备上监控到源端的网络流量。

## 6.4. 配置分布式防火墙

### 功能说明

该任务指导管理员创建分布式防火墙。

### 注意事项

1. 分布式防火墙是针对4层以下的防护。

- 2. 当HCI被SCP纳管但未创建连通域时，分布式防火墙原有策略保持不变，但不显示。
- 3. 当HCI被SCP纳管并创建连通域时，分布式防火墙功能不可用。
- 4. 当HCI从低版本升级到670版本时，原有分布式防火墙策略会放在默认策略中。

前提条件

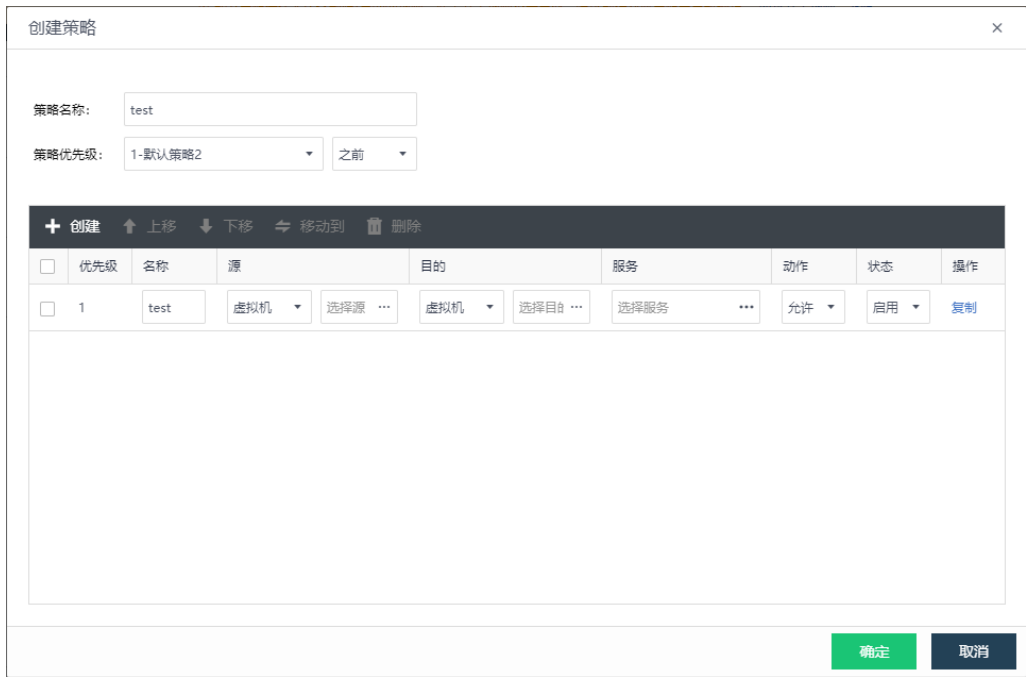
已购买aNet授权。

操作步骤

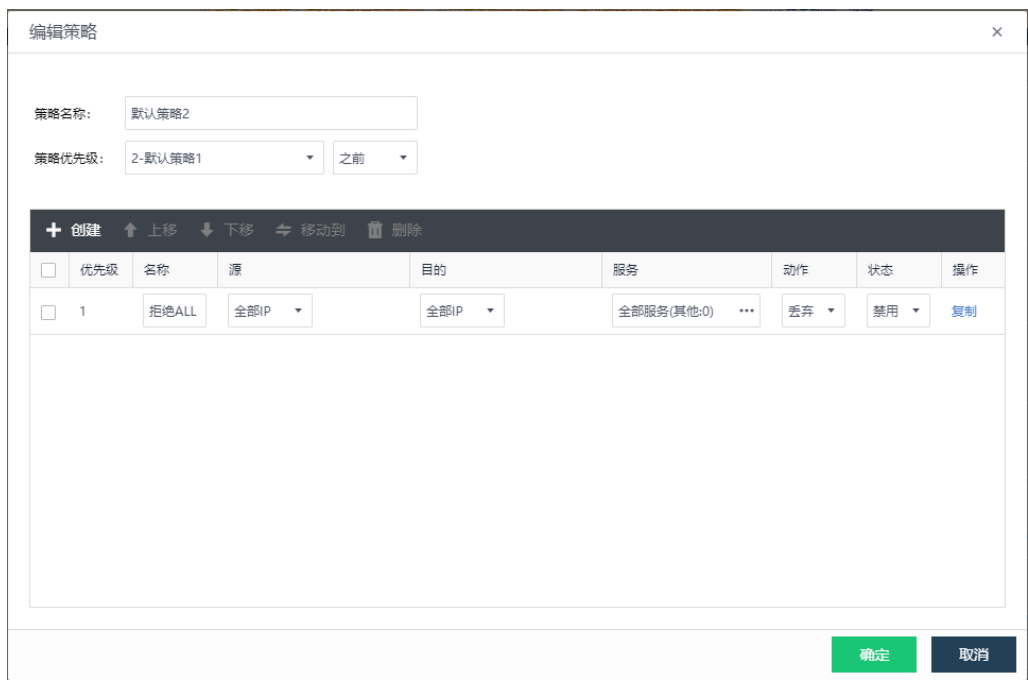
- 1. 点击[网络与安全/分布式防火墙]，进入防火墙配置界面状态，点击<创建>，进入[创建策略]页面。



- 2. 配置策略名称和优先级，配置规则的源和目的IP或者虚拟机，选择服务或自定义服务协议和端口，选择策略中规则动作，并启用该规则，点击<确定>完成配置。



- 3. 选择策略中规则动作，并启用该规则，点击<确定>完成配置。



- 策略名称：定义防火墙策略的名称。
- 策略优先级：定义所创建的策略在所有策略中的优先级顺序。
- 优先级：定义策略中规则的优先级，数值越低优先级越高。

## 6.5. 网络可视化

### 功能说明

网络可视化（aNI，Advanced Network Insight）实现虚拟机访问关系自动采集梳理，新增资产自动添加展示，及时同步资产情况。从业务的角度提供直观、清晰的虚拟机间的访问关系拓扑图和访问详情，便于优化策略配置、发现业务访问风险、减少风险端口暴露。

### 注意事项

- 单主机访问关系记录数超出规格限制，会导致超负荷的虚拟机随机丢包，访问关系数据丢失。规格要求如下：

| 规格 | 核数 | 内存    | 存储    | 适用虚拟机总数 |
|----|----|-------|-------|---------|
| 小型 | 8  | 16GB  | 500GB | 100     |
| 中型 | 32 | 64GB  | 1T    | 1000    |
| 大型 | 64 | 128GB | 1.5T  | 3000    |

- 暂不支持采集虚拟路由器/虚拟交换机之间的流量、NFV的流量。

3. 暂不支持IPv6流量信息采集。
4. HCI对虚拟机进行IP变更操作时，流量可视化服务更新将会延迟，一条流最晚更新时间为5min。
5. 网络可视化授权集成在aNET中，无需单独开通授权。
6. aNI虚拟机密码限制3个月强制修改一次。
7. 界面暂不支持展开超过100台虚拟机的分组。
8. 只采集经过DFW的流量（670的DFW默认是开启的），不经过DFW的流量无法采集上报。（虚拟路由器、虚拟交换机之间的流量、NFV均不采集）

## 前提条件

无

## 操作步骤

1. 进入[网络安全/网络可视化]页面，点击<配置指引>按钮，可参照指引完成网络可视化部署。



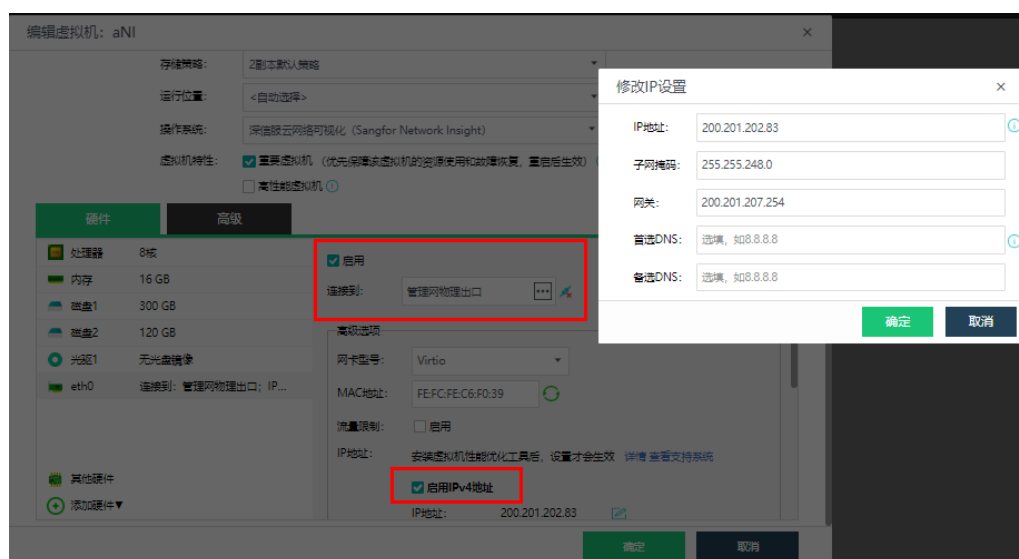
2. 点击<立即部署>按钮，进入导入虚拟机页面，按向导提示，导入访问关系虚拟机aNI的vma文件，选择虚拟机分组、存储位置、存储策略、运行位置。

### ⚠ 注意:

虚拟机导入后，请查看下图所示向导，根据现有虚拟机数量，按照小型、中型、大型规格，编辑模板虚拟机的参数，其中存储容量主要用于存储平台上 30 天内存在访问关系的虚拟机的全部流数据。



3. 导入成功后，进入[编辑虚拟机]界面，进行网卡配置。勾选“启用”，连接到物理出口，点击<修改配置>按钮，选择“使用IPv4地址”，配置aNI虚拟机IP地址，作为“网络可视化”管理网络（此处需规划与HCI管理网段能够互通，推荐与HCI管理网同一网段）。



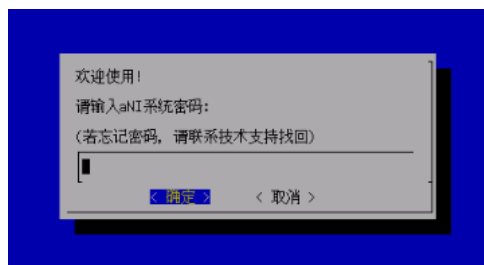
4. 启用合作伙伴服务端口，开启合作伙伴服务，否则将无法访问网络可视化服务。



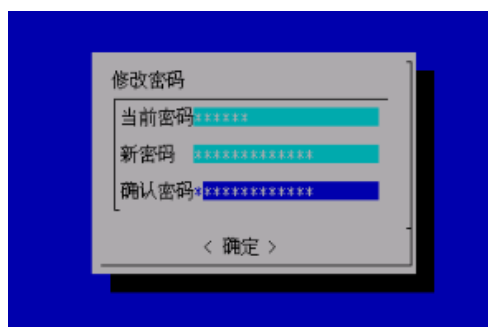
3. 将虚拟机开机，进入虚拟机控制台，进行平台认证配置。

步骤1. 输入云安全中心的密码登录。**注意：**首次登录需要修改密码，仅有5次试错密码的机会，若5次均输入错误，则账号会被锁定5min，5min后才可再次输入。默认密码为Sfcsec@123，密码修改策略如下：

- 密码长度应为 8-64 个字符且不能包含用户名；
- 密码必须包含大、小写字母，数字，特殊字符 4 种类型字符。



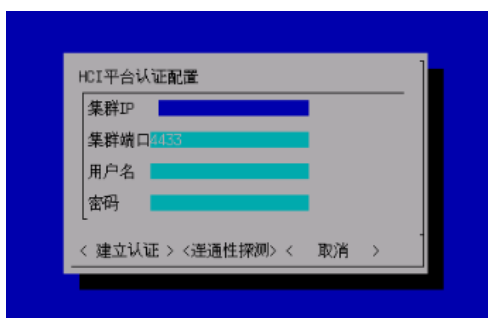




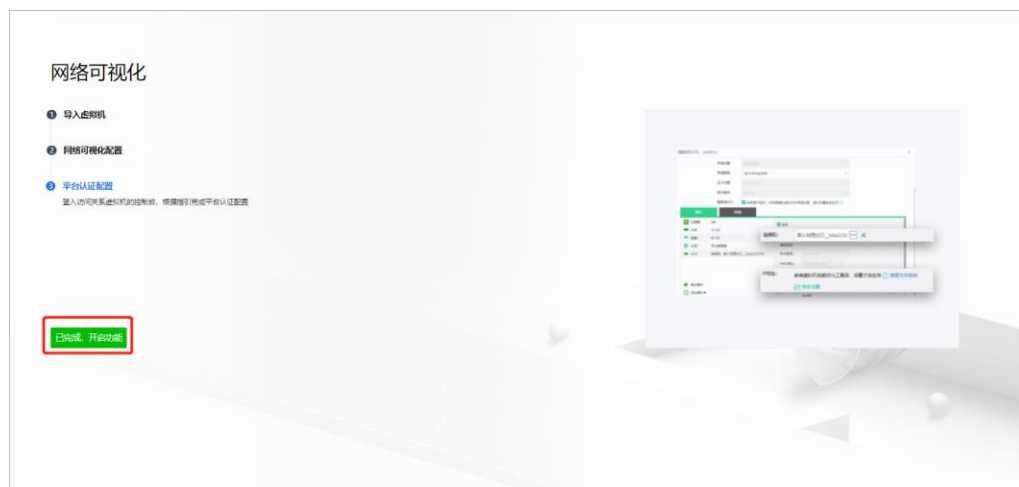
步骤2. 修改后需要重新登录，选择“平台认证配置”，平台类型配置选择“HCI”。



步骤3. 输入集群IP、用户名、密码，完成平台认证配置。



4. 平台认证配置成功后，重新进入[网络可视化]页面，点击<已完成，开启功能>按钮，进入网络可视化页面。

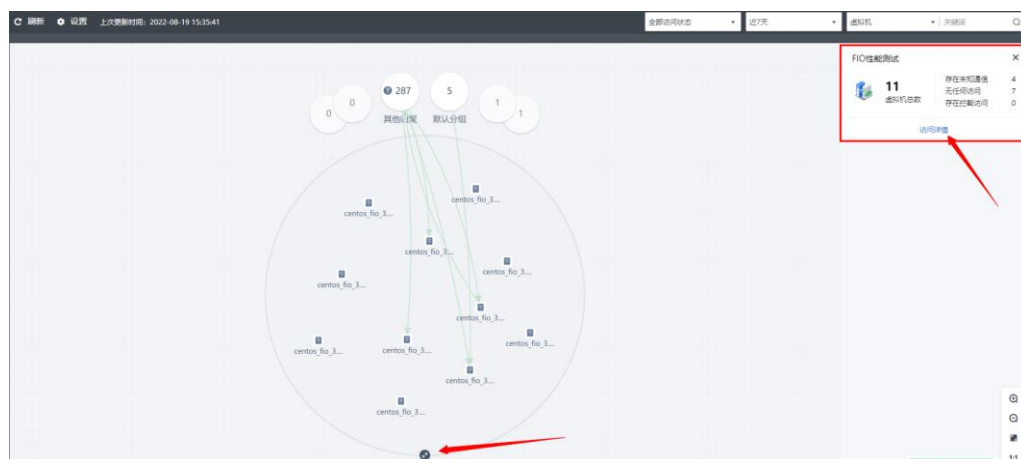


5. 在可视化页面可以看到平台上所有虚拟机的访问情况。右上角高级筛选，支持按照不同条件进行界面筛选。同时支持按照虚拟机、虚拟机分组的维度进行搜索，快速定位所需查看的虚拟机或分组。
- 访问状态筛选：全部访问状态、被策略允许、被策略丢弃、无策略匹配。
  - 时间筛选：近 30 天、近 7 天、近 3 天、今天。



6. 选择分组，进入虚拟机分组展示页面，右上角卡片展示当前分组内虚拟机访问关系信息，包括虚拟机总数、存在位置通信、无任何访问、存在拦截访问。点击缩小按钮，将收起返回初始界面。





7. 点击<访问详情>按钮，进入详情页面，点击操作栏<查看详情>，可获取每一条记录的详情信息，包括防火墙策略五元组信息：源对象、源IP、目的对象、目的IP、服务。

| 最近访问时间              | 虚拟设备名称               | IP              | 源和目的IP       | 操作                   |
|---------------------|----------------------|-----------------|--------------|----------------------|
| 2022/08/19 15:46:01 | centos_fio_3.3.0_控制面 | 200.201.202.101 | 192.168.1.11 | <a href="#">查看详情</a> |
| 2022/08/19 15:37:11 | centos_fio_3.3.0_2   | 192.168.1.11    | 192.168.1.12 | <a href="#">查看详情</a> |
| 2022/08/19 15:37:11 | centos_fio_3.3.0_4   | 192.168.1.11    | 192.168.1.12 | <a href="#">查看详情</a> |
| 2022/08/15 15:54:28 | centos_fio_3.3.0_1   | 200.201.202.40  |              | <a href="#">查看详情</a> |

8. 点击<查看策略>按钮，将会跳转到[分布式防火墙]页面，可对访问策略进行增删改查等操作。

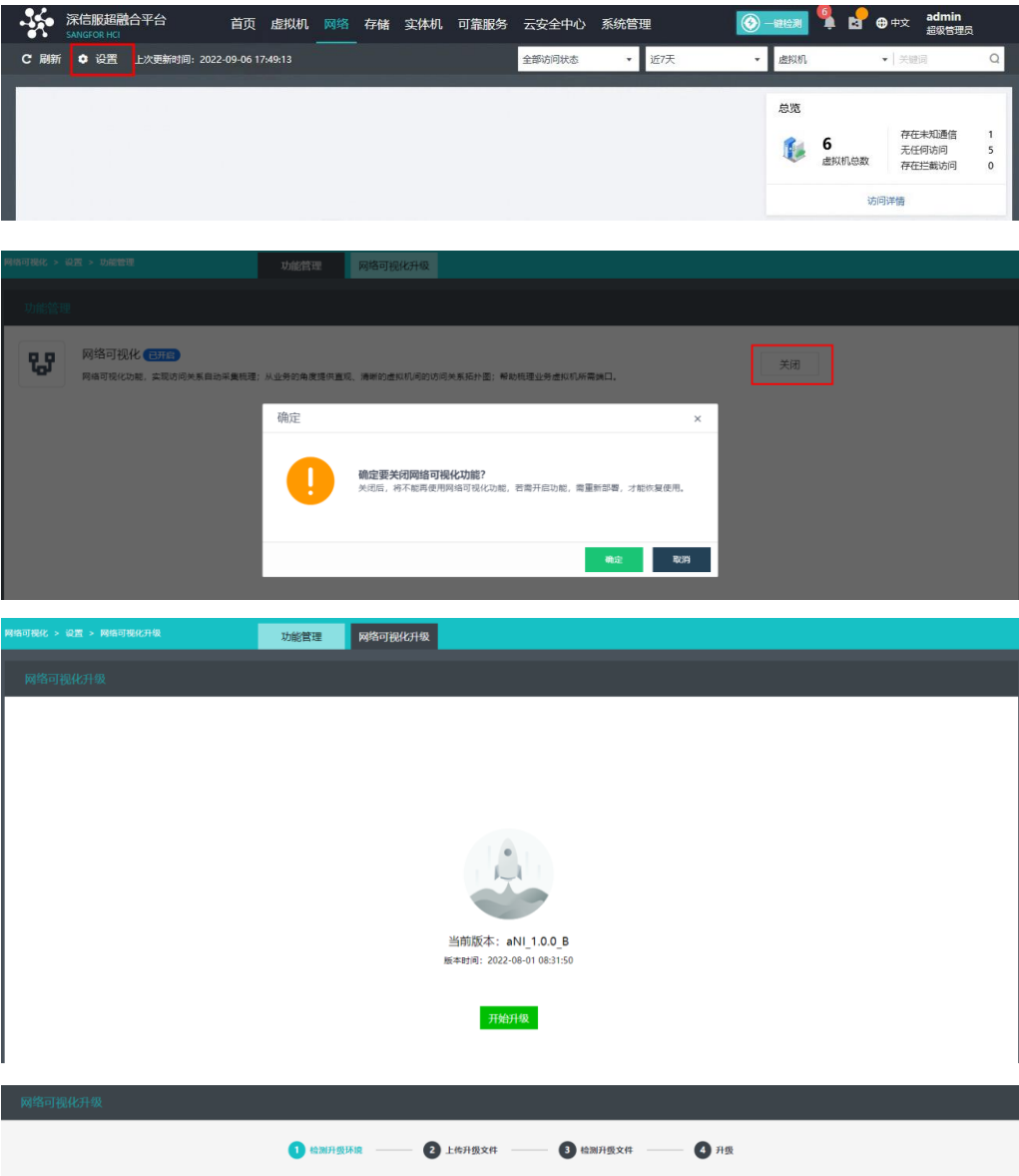
| 最近访问时间              | 访问方向 | 源IP              | 目的对象                 | 目的IP            | 服务            | 动作 | 访问次数 | 操作                   |
|---------------------|------|------------------|----------------------|-----------------|---------------|----|------|----------------------|
| 2022/08/19 15:47:24 | 被访问  |                  | centos_fio_3.3.0_控制面 | 200.201.202.101 | ms-sql(TCP... | 允许 | 335  | <a href="#">查看详情</a> |
| 2022/08/19 15:47:11 | 被访问  |                  | centos_fio_3.3.0_2   | 200.201.202.101 | oika(TCP:445) | 允许 | 312  | <a href="#">查看详情</a> |
| 2022/08/19 15:47:11 | 被访问  |                  | centos_fio_3.3.0_4   | 200.201.202.101 | ms-sql(TCP... | 允许 | 540  | <a href="#">查看详情</a> |
| 2022/08/15 15:54:28 | 被访问  |                  | centos_fio_3.3.0_1   | 200.201.202.101 | oika(TCP:445) | 允许 | 500  | <a href="#">查看详情</a> |
| 2022/08/19 15:46:01 | 被访问  | 200.201.29.20    | centos_fio_3.3.0_控制面 | 200.201.202.101 | ms-sql(TCP... | 允许 | 116  | <a href="#">查看详情</a> |
| 2022/08/19 15:46:00 | 被访问  | 200.201.29.20    | centos_fio_3.3.0_2   | 200.201.202.101 | oika(TCP:445) | 允许 | 116  | <a href="#">查看详情</a> |
| 2022/08/19 15:40:31 | 被访问  | 200.201.186.1... | centos_fio_3.3.0_4   | 200.201.202.101 | ms-sql(TCP... | 允许 | 287  | <a href="#">查看详情</a> |

9. 平台也支持对网络可视化服务进行相关设置操作，点击<设置>按钮，支持对该服务进行开启、关闭、升级等设置。



**注意：**

网络可视化服务关闭后，将不能再使用该功能，若需开启功能，需重新部署，才能恢复使用。



## 6.6. 管理 NFV 设备（支持批量操作）

### 功能说明

NFV的开机，关机，关闭电源，迁移，删除操作，支持多台设备同时操作。

### 注意事项

1. vAF虚拟机的名字包含“服务器”字样，单点登录会被vAF拦截，被识别成sql注入。vAF虚拟机名称不要有“服务器”字样，修改成其他的名称。
2. 同时打开vSSL VPN和vAF单点登录控制台，相互影响，导致无法单点登录，如需同时打开，请使用不同浏览器打开vAF和SSL VPN进行单点登录。
3. 不要在一个广播域部署多台使用透明模式的vAF，会导致MAC地址冲突。

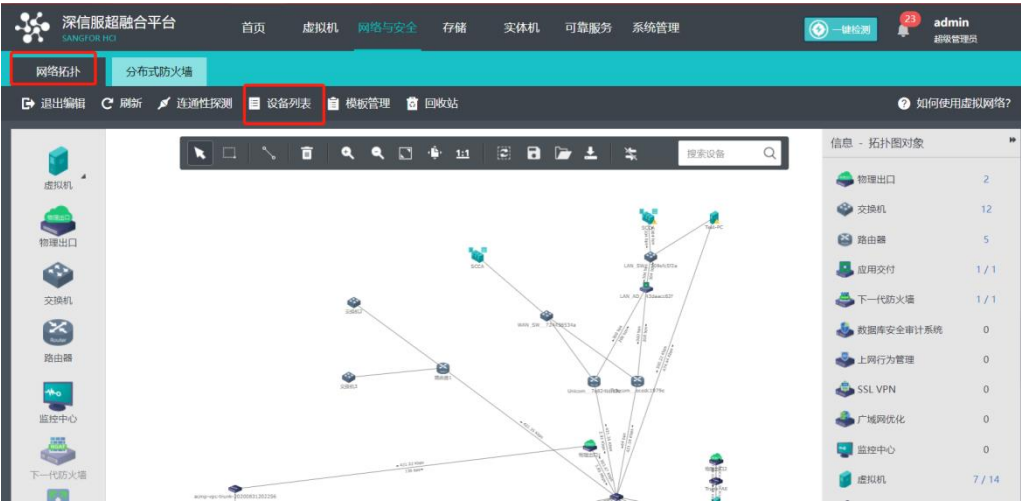
- 4. 东西向流量尽量不要经过vAF。原因是东西向流量会比较大，vAF的性能比物理AF要低很多，一旦遇到性能瓶颈会导致网络变慢。东西向流量也没必要做7层清洗，使用aNET的分布式防火墙就可以满足需求。vAF推荐部署在南北向流量的出口。
- 5. 集群部署完成后，如果有用NFV（比如vAD，vAF之类的）不建议修改主机中的“网络转发消耗的cpu核数”和“网络转发消耗的内存”，如果修改有可能导致网络中断，此时必须手动将所有虚拟网络设备的网线删掉重连才能恢复。
- 6. 不支持对NFV进行克隆部署，需要从“网络拓扑”新加部署。

前提条件

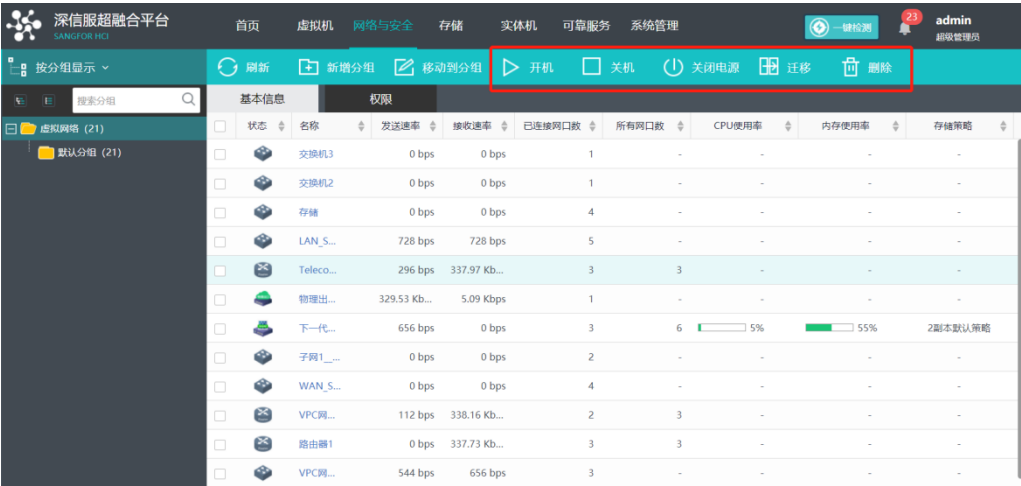
无

操作步骤

- 1. 在[网络拓扑]页面中点击<设备列表>，进入虚拟网络设备管理页面。



- 2. 勾选一个或多个需要管理的NFV设备，再点击需要的操作。





## 7. 存储配置指导

### 7.1. 查看存储状态

#### 功能说明

可以通过查看存储状态来判断所有存储的状态、使用率、实时状况、性能状况、告警日志及任务执行状态。

#### 注意事项

无

#### 前提条件

无

#### 操作步骤

1. 在[存储/总览]可以查看到总览页面，在[存储状态]这项可以看到所有存储的运行状态，如有异常可以直接在页面的数字点进去定位到异常存储。



2. 在[虚拟存储状态]这项，可以看到虚拟存储当前的总容量、已用容量和剩余容量。选择相应的时间范围，查看该时间段内的IO次数趋势、IO速度趋势、IO时延趋势以及主机命中率。

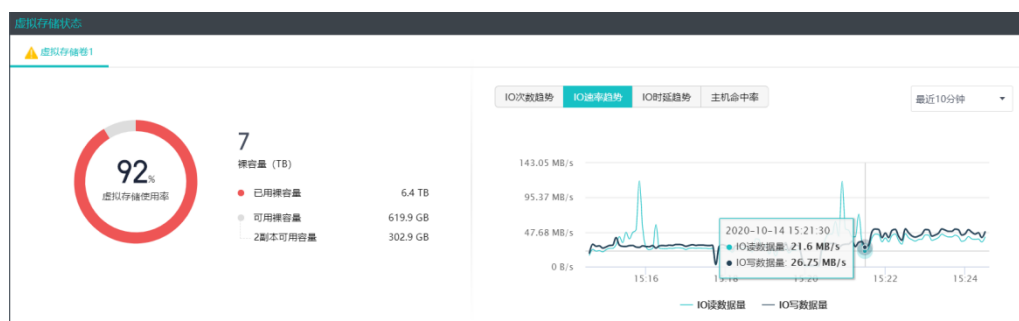


3. [IO次数趋势]展示的是虚拟存储每秒发生读和写的次数，对应于业界术语IOPS

值，展示的是虚拟存储的并发IO次数趋势，反映了虚拟存储的随机IO能力。



4. [IO速率趋势]展示的是虚拟存储每秒读写的字节数，即每秒读 xxx MB，写 xx MB，展示的是虚拟存储的并发IO吞吐趋势，通过IO速率趋势可以反映了虚拟存储的顺序IO能力。

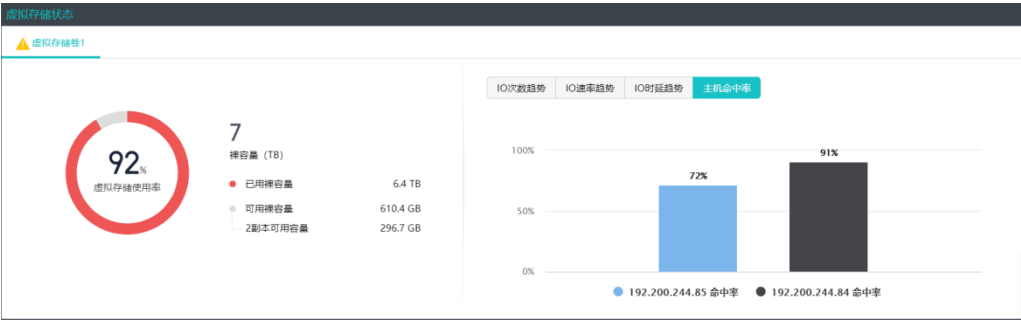


5. [IO时延趋势]展示的是虚拟存储平均每次读和写需要的时间，通过IO时延趋势可以看出存储的IO负载，如果IO时延增大，那说明IO请求已经在排队了，性能开始不够。通常平均IO延时低于30ms表示负载很轻，低于60ms处于正常水平。



6. [主机命中率]展示的主机开机以来的平均缓存命中率，通过柱状图可以形象地对比不同主机命中率的差别。





7. 在[其他存储实时状态]这项可以看到其他存储的总容量、容量使用率、IO读速率、IO写速率以及存储在该存储上的虚拟机数量和正在运行的虚拟机数量。

| 存储名称                | 状态 | 类型      | 总容量     | 容量使用率 | IO读速率 | IO写速率     | 虚拟机总数... | 正在运行的虚拟机... |
|---------------------|----|---------|---------|-------|-------|-----------|----------|-------------|
| 192.200.244.84/本地存储 | 正常 | 本地存储    | 1.7 TB  | 1%    | 0 B/s | 0 B/s     | 0        | 0           |
| seeding_stor        | 正常 | 本地存储    | 464 GB  | 6%    | 0 B/s | 174.1 B/s | 0        | 0           |
| test                | 离线 | iSCSI存储 | 0 bytes | -     | 0 B/s | 0 B/s     | 0        | 0           |

8. 在[未读告警日志]这项可以查看HCI的告警信息，在[任务执行状态]可以查看HCI集群当前执行的任务。这两项可以分别从页面上点进去查看。

| 告警对象 | 时间 | 内容 |
|------|----|----|
| 空    |    |    |

查看历史告警

| 对象名称            | 状态   | 动作   | 所属卷    | 进度  |
|-----------------|------|------|--------|-----|
| 192.200.244.202 | 正在执行 | 数据同步 | 虚拟存储卷1 | 58% |

查看全部任务

| 级别 | 时间                  | 对象类型 | 告警对象 | 事件     | 描述                                             | 操作   |
|----|---------------------|------|------|--------|------------------------------------------------|------|
| 紧急 | 2020-10-19 15:28:16 | 存储   | 123  | 存储离线告警 | 主机<192.200.244.84>的存储<123>离线, 请检查存储设备或网络连接是否异常 | 手动确认 |
| 紧急 | 2020-10-19 15:23:52 | 存储   | 123  | 存储离线告警 | 主机<192.200.244.84>的存储<123>离线, 请检查存储设备或网络连接是否异常 | 手动确认 |
| 紧急 | 2020-10-19 15:21:21 | 存储   | 123  | 存储离线告警 | 主机<192.200.244.84>的存储<123>离线, 请检查存储设备或网络连接是否异常 | 手动确认 |
| 紧急 | 2020-10-19 15:14:24 | 存储   | 123  | 存储离线告警 | 主机<192.200.244.84>的存储<123>离线, 请检查存储设备或网络连接是否异常 | 手动确认 |

| 对象名称          | 状态 | 动作   | 所属卷    | 进度   | 速率 | 剩余时间 | 开始时间                | 结束时间                | 操作 |
|---------------|----|------|--------|------|----|------|---------------------|---------------------|----|
| 200.201.10.21 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 17:05:02 | 2018-12-05 17:06:06 | 查看 |
| 200.201.10.21 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 17:01:06 | 2018-12-05 17:02:06 | 查看 |
| 200.201.10.21 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 16:52:10 | 2018-12-05 16:53:01 | 查看 |
| 200.201.10.22 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 16:50:08 | 2018-12-05 16:51:06 | 查看 |
| 200.201.10.27 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 16:50:08 | 2018-12-05 16:51:06 | 查看 |
| 200.201.10.21 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 16:50:05 | 2018-12-05 16:51:06 | 查看 |
| 200.201.10.21 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 16:49:29 | 2018-12-05 16:50:06 | 查看 |
| 200.201.10.22 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 14:48:57 | 2018-12-05 14:50:00 | 查看 |
| 200.201.10.22 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 14:47:59 | 2018-12-05 14:49:00 | 查看 |
| 200.201.10.22 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 14:46:59 | 2018-12-05 14:47:57 | 查看 |
| 200.201.10.22 | 完成 | 数据同步 | 虚拟存储卷1 | 100% | -  | -    | 2018-12-05 14:46:26 | 2018-12-05 14:47:00 | 查看 |

7.2. 虚拟存储配置指导

7.2.1. 查看虚拟存储状态

功能说明

主要是可以通过查看存储的IO读写等操作，来判断存储的繁忙程度。

注意事项

无

前提条件

无

操作步骤

1. 在[存储/虚拟存储/存储卷]中选择要查看的存储，点击名称查看详情。



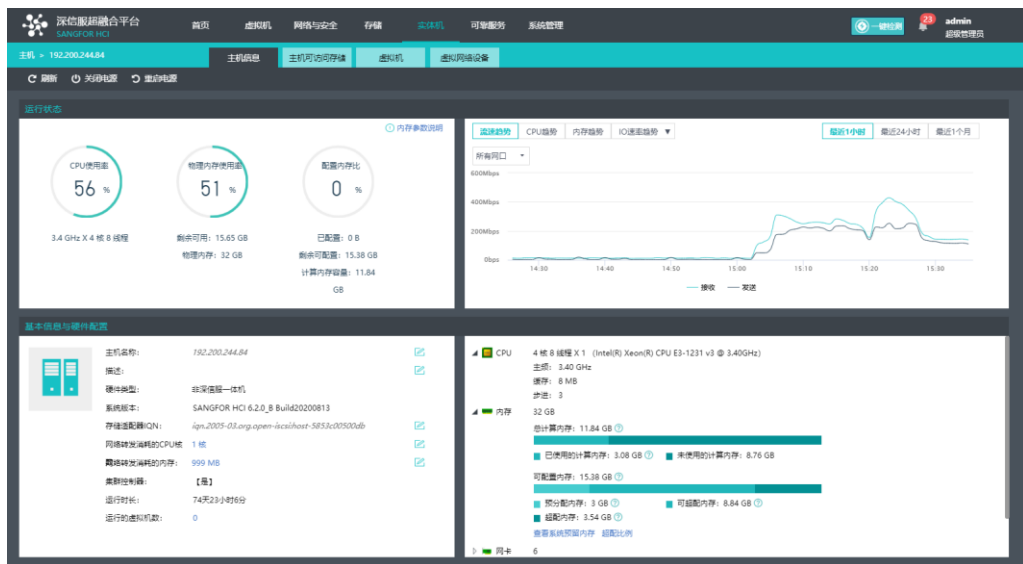
2. 在详情页面就可以看到存储卷的详细信息，包括容量、故障域和主机信息以及运行状态等，其中运行状态中包括IO读写次数和IO读写速率等信息；在出现虚拟机比较卡时，可以在虚拟机存储位置查看IO读写次数和IO读写速率等信息，辅助排查问题。



3. 在[实体机]选择相应主机，点击<详情>可以查看主机存储信息。



4. 在虚拟机详情可以看到运行参数信息、流量监控信息、硬件配置基本信息等。



### 7.2.2. 添加卷

### 7.2.2.1. 添加普通卷

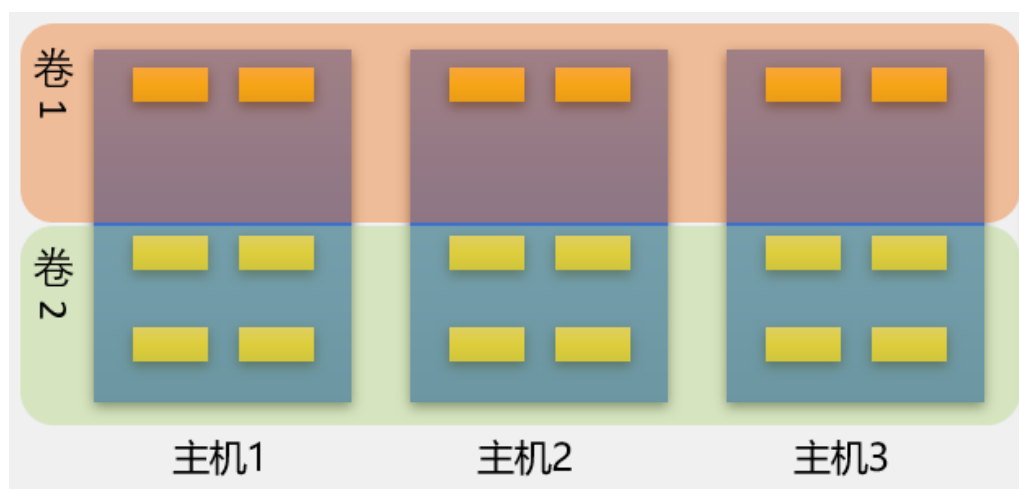
## 功能说明

HCI 支持多卷管理，一个集群上可以同时存在普通卷，也可以存在延伸卷，在一个超融合的集群中可以创建多个虚拟存储卷，组建多卷可以以主机为单位，也可以以磁盘为单位，卷与卷之间物理上和逻辑上都是隔离的，但是对于虚拟机而言可以在卷之间进行选择 and 迁移，也可以满足集群中不同业务对于硬件的异构要求。以下操作作为添加普通卷的操作。

以主机为单位的多卷至少需要6台主机，3台主机一个卷，另外3台组成一个卷。而以磁盘为单位的多卷，3台主机或以上即可划分多卷，因此单主机可以在创建1个混合

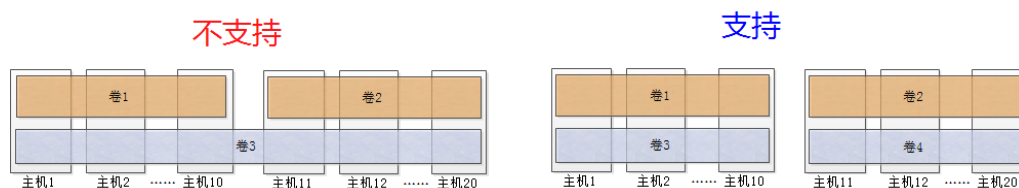
卷的基础之上再单独划分出1个全闪卷，将对磁盘性能要求高的业务放在全闪卷中运行，提高磁盘的利用率。主机多卷和磁盘多卷的方式可以在一个 HCI 集群上并存。

以三主机为例，现支持的组多卷方式如图所示。

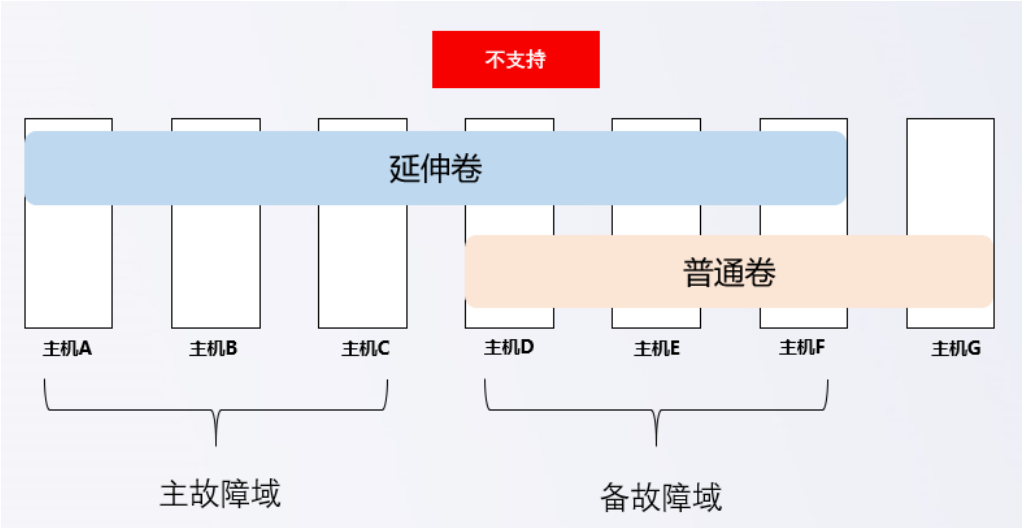


## 注意事项

1. 新添加的卷在创建时会将卷进行格式化，在添加前请确认用于添加新卷的磁盘上没有需要保留的数据。
2. 一个集群最多允许存在6个存储卷，其中最多允许存在一个延伸卷。
3. 1个卷至少由3台主机上的硬盘组成，1台主机上最多划分2个卷。
4. 虚拟存储不支持单副本，单副本时虚拟存储没有冗余，有丢数据风险。
5. 两主机不支持数据平衡。
6. 两主机的虚拟机不支持使用条带化功能。
7. 虚拟存储是全HDD部署，不支持升级，也不支持全新部署。
8. 三主机容量异构过大的场景，会限制部署虚拟存储。要求一台主机的容量不能超过其余主机容量之和，例如：主机A 1TB，主机B 1TB，主机C 5TB，不支持部署。
9. 一个卷横跨的主机不能分别属于另外两个卷。



10. 延伸集群不支持多卷。即如下图所示，一个主机不能既属于延伸卷，又属于普通卷。



- 11. 全闪卷（重删压缩），不支持硬盘分卷，只支持主机卷；硬盘分卷的全闪子卷，不支持重删压缩。
- 12. 普通卷的单台主机至少存在一块SSD，全闪卷内的单台主机至少存在两块SSD。

前提条件

- 1. 组建多卷每个卷至少需要3台主机，请准备足够服务器。
- 2. 组建磁盘多卷至少需要3台主机，请准备足够服务器。
- 3. 扩容主机的管理口、存储口、数据通信口和业务口已经接入到网络中去。

操作步骤

添加存储卷

- 1. 在[实体机/物理主机]中点击<添加主机>。





2. 选择需要添加的主机，如果需要添加的主机不再列表中，点击< + >进行添加。



3. 添加主机，将会删除被添加主机的防火墙配置，点击<确定>。



4. 检测到数据通信口MTU不一致，进行重新配置，勾选“开启网口高性能模式”即可。



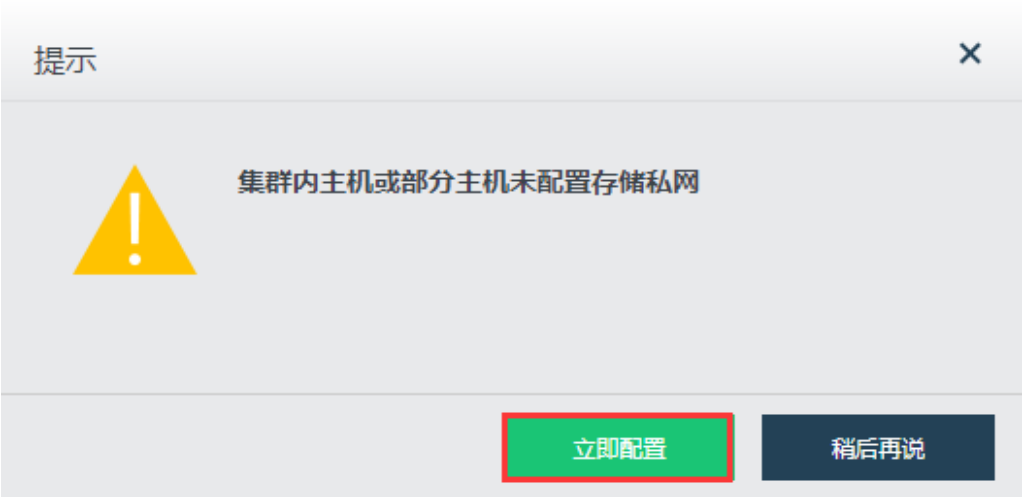
5. 添加成功后，配置数据通信口，完成后，可以在[首页]看到添加的实体机。



6. 在[存储/虚拟存储]中点击<创建卷>，进行新卷的添加。



7. 配置存储私网口和IP地址。



8. 根据实际情况选择虚拟存储通信网络部署模式。



9. 选择用作存储私网的网口并配置IP地址。



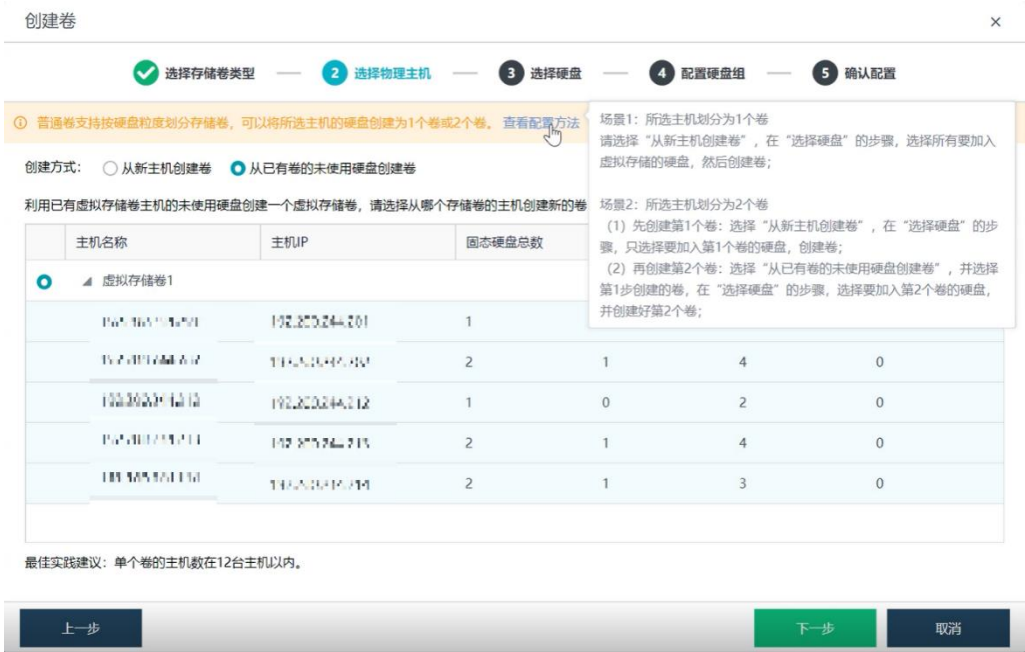


10. 再次点击<创建卷>，创建一个普通卷，进入<下一步>。

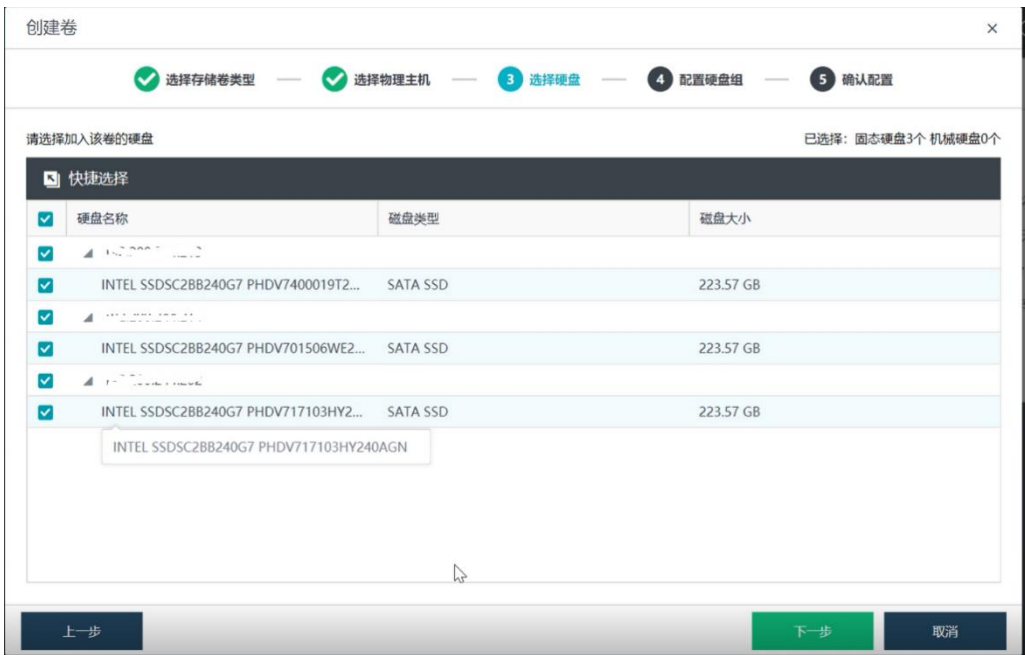


11. 选择[创建方式]。此处选择从新主机创建卷。

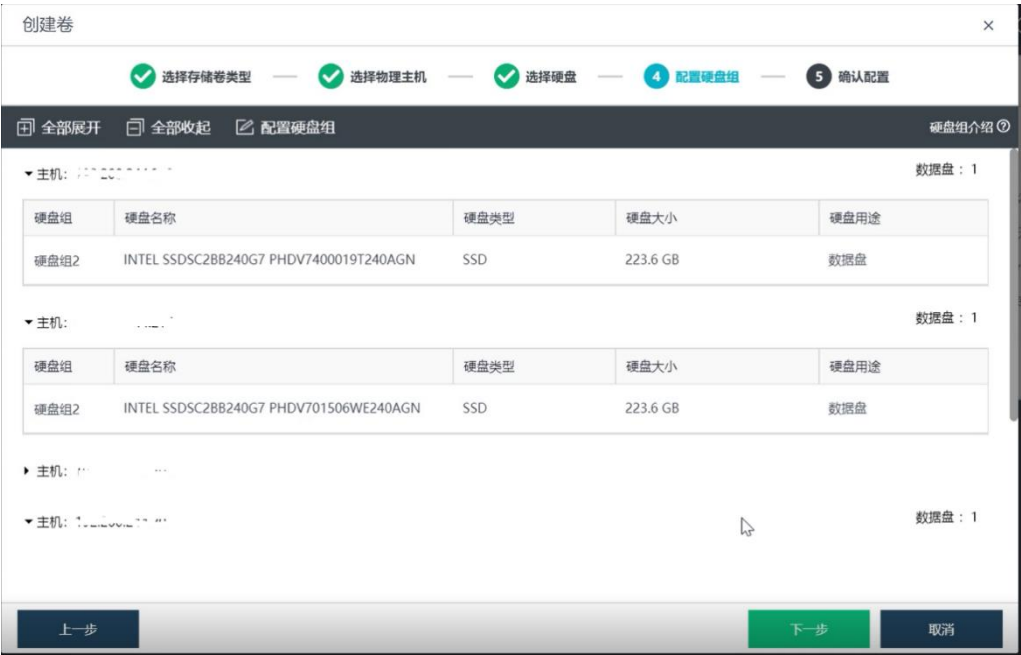
- 从新主机创建卷：重新选择集群中的 3 台或以上的主机创建一个新卷。
- 从已有卷的未使用硬盘创建卷：在已有卷的基础之上选择该卷包含的主机中的未使用的硬盘来选择创建新卷。



12. 选择要加入新卷的硬盘。



13. 为新卷配置硬盘组，同样如果不是全闪卷的话需要SSD作缓存盘。



14. 确认配置信息，新卷创建完成。

### 添加主机多卷

1. 在[实体机/物理主机]中点击<添加主机>。





2. 选择需要添加的主机，如果需要添加的主机不在列表中，点击< + >进行添加。



3. 添加主机，将会删除被添加主机的防火墙配置，点击<确定>。



4. 检测到数据通信口MTU不一致，进行重新配置，勾选“开启网口高性能模式”即可。



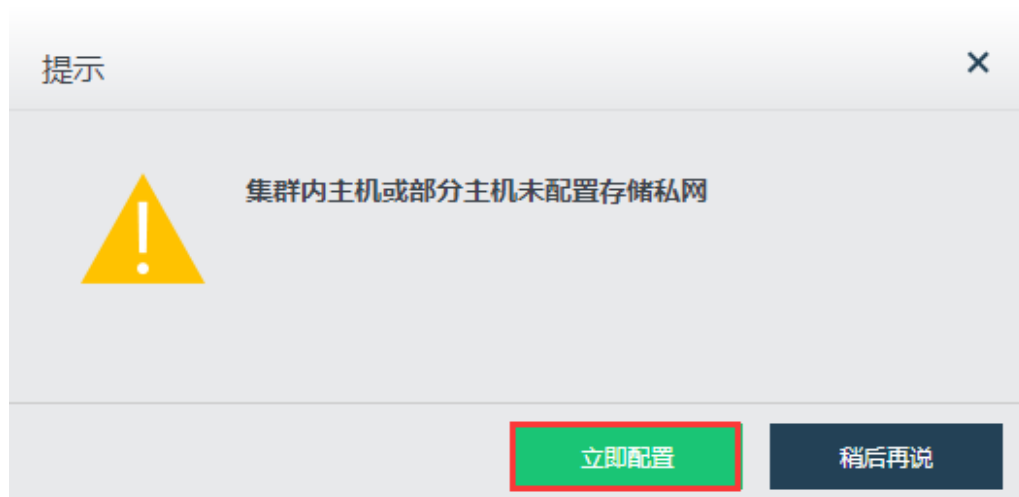
5. 添加成功后，配置数据通信口，完成后，可以在[首页]看到添加的实体机。



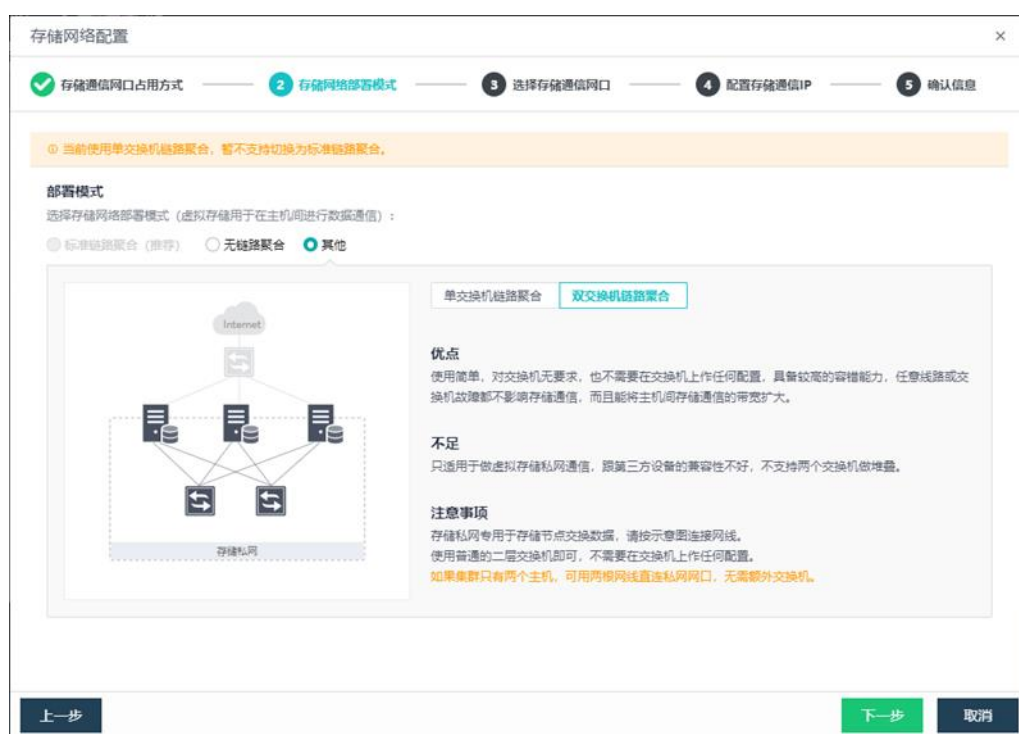
6. 在[存储/虚拟存储]中点击<创建卷>，进行新卷的添加。



7. 配置存储私网口和IP地址。



8. 根据实际情况选择虚拟存储通信网络部署模式。



9. 选择用作存储私网的网口并配置IP地址。



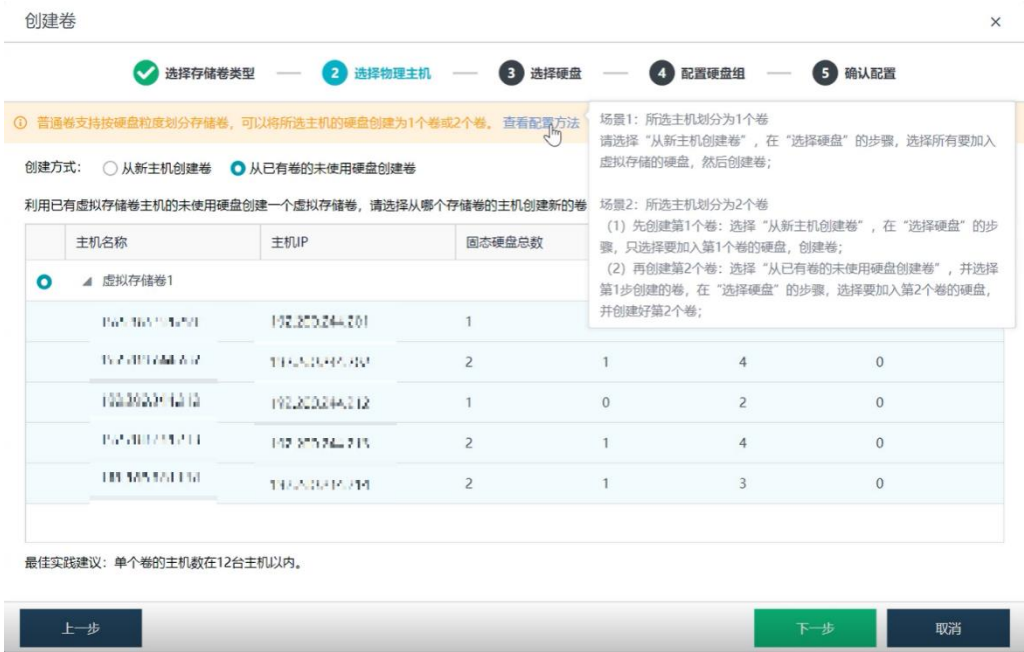
10. 再次点击<创建卷>，创建一个普通卷，进入<下一步>。



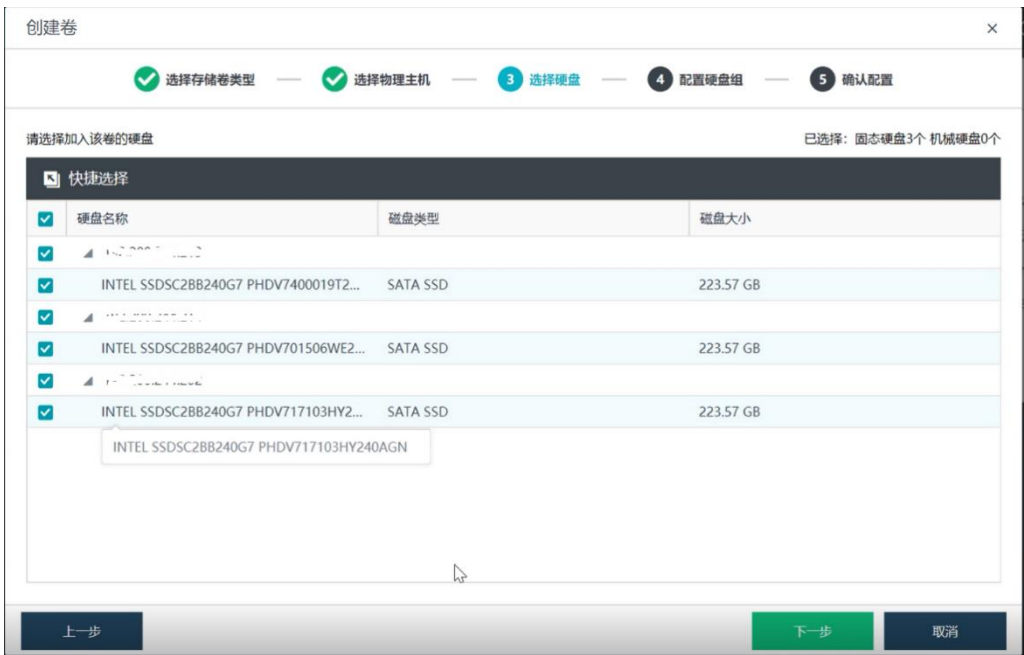
11. 选择[创建方式]。此处选择从新主机创建卷。

从新主机创建卷：重新选择集群中的 3 台或以上的主机创建一个新卷。

从已有卷的未使用硬盘创建卷：在已有卷的基础之上选择该卷包含的主机中的未使用的硬盘来选择创建新卷。

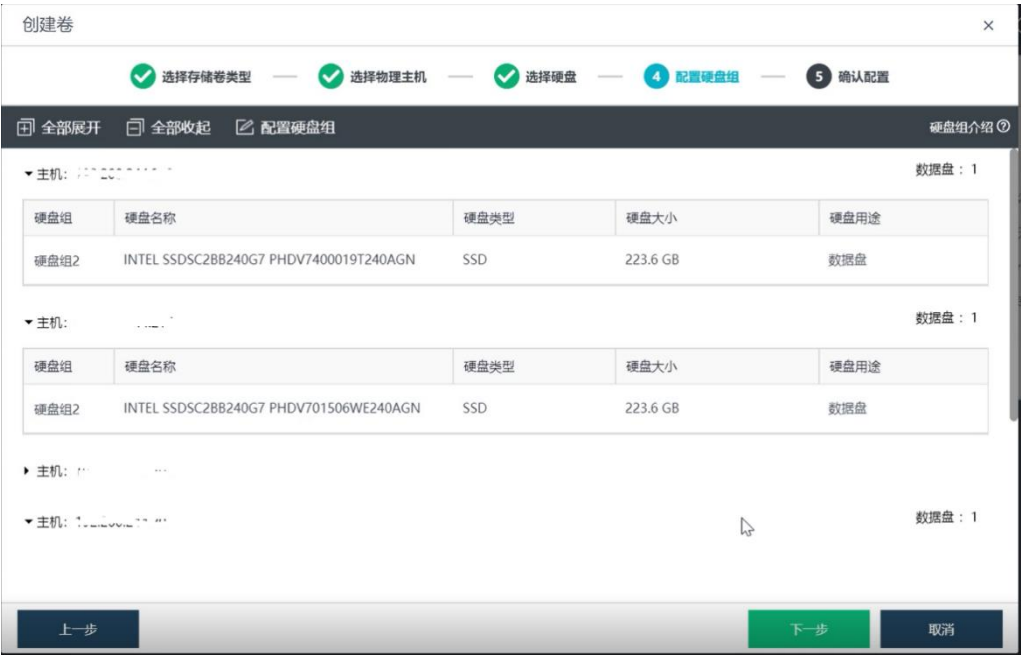


12. 选择要加入新卷的硬盘。



13. 为新卷配置硬盘组，同样如果不是全闪卷的话需要SSD作缓存盘。





14. 确认配置信息，新卷创建完成。
15. 配置存储卷类型：点击[存储/虚拟存储]打开虚拟存储页面，然后点击<创建卷>，选择卷类型为“普通卷”。



16. 选择物理主机：选择从新主机创建卷，选择需要加入存储卷的物理主机，此处选择的主机为集群中未创建过存储卷的主机。

创建卷

选择存储卷类型

2 选择物理主机

3 选择硬盘

4 配置硬盘组

5 确认配置

① 普通卷支持按硬盘粒度划分存储卷，可以将所选主机的硬盘创建为1个卷或2个卷。查看配置方法

创建方式：

从新主机创建卷

从已有卷的未使用硬盘创建卷

从新主机（未加入虚拟存储的主机）创建一个虚拟存储卷，请选择加入该卷的主机：已选中4台主机

| <input checked="" type="checkbox"/> | 主机名称          | 主机IP          | 固态硬盘总数 | 机械硬盘总数 |
|-------------------------------------|---------------|---------------|--------|--------|
| <input checked="" type="checkbox"/> | 192.168.1.101 | 192.168.1.101 | 2      | 0      |
| <input checked="" type="checkbox"/> | 192.168.1.102 | 192.168.1.102 | 2      | 0      |
| <input checked="" type="checkbox"/> | 192.168.1.103 | 192.168.1.103 | 2      | 0      |
| <input checked="" type="checkbox"/> | 192.168.1.104 | 192.168.1.104 | 2      | 0      |

最佳实践建议：单个卷的主机数在12台主机以内。

上一步

下一步

取消

17. 选择主机中要加入的硬盘。配置硬盘和硬盘组，然后为每个主机的每个磁盘进行详细用途规划。系统会对集群中所有主机的磁盘进行自动检测，默认选择机械磁盘作为数据盘，固态硬盘作为缓存盘。一般建议采用默认配置，也可以自行修改。如果需要部署磁盘多卷，需要规划预留第二卷组的磁盘。

创建卷

选择存储卷类型

选择物理主机

3 选择硬盘

4 配置硬盘组

5 确认配置

请选择加入该卷的硬盘 已选择：固态硬盘8个 机械硬盘0个

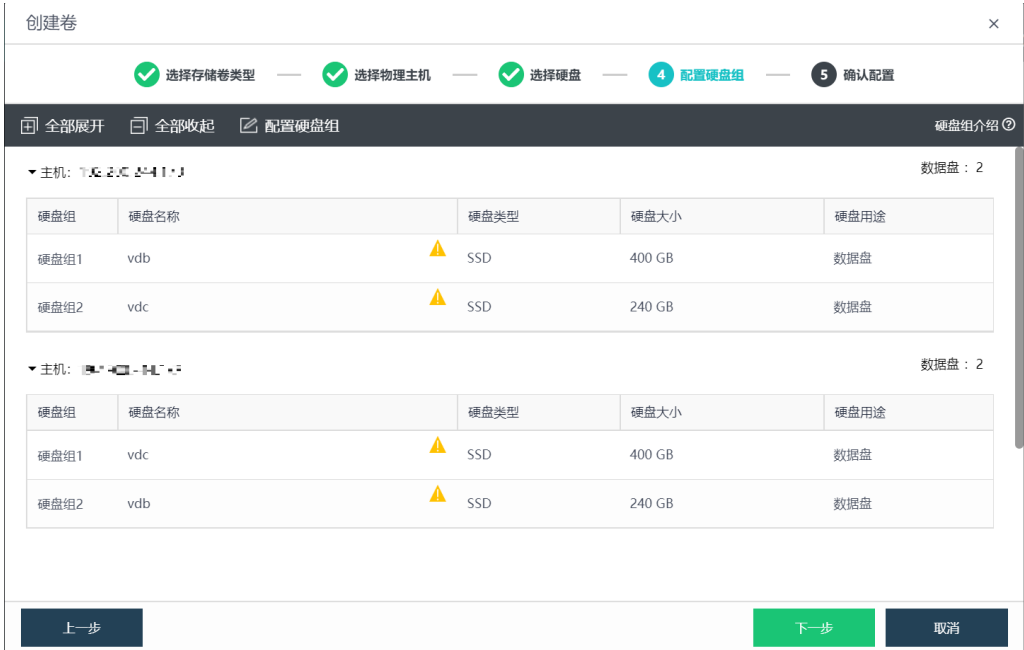
快捷选择

| <input checked="" type="checkbox"/> | 硬盘名称          | 磁盘类型 | 磁盘大小   |
|-------------------------------------|---------------|------|--------|
| <input checked="" type="checkbox"/> | 192.168.1.101 |      |        |
| <input checked="" type="checkbox"/> | vdc           | SSD  | 240 GB |
| <input checked="" type="checkbox"/> | vdb           | SSD  | 400 GB |
| <input checked="" type="checkbox"/> | 192.168.1.102 |      |        |
| <input checked="" type="checkbox"/> | vdb           | SSD  | 240 GB |
| <input checked="" type="checkbox"/> | vdc           | SSD  | 400 GB |
| <input checked="" type="checkbox"/> | 192.168.1.103 |      |        |
| <input checked="" type="checkbox"/> | vdb           | SSD  | 240 GB |
| <input checked="" type="checkbox"/> | vdc           | SSD  | 400 GB |
| <input checked="" type="checkbox"/> | 192.168.1.104 |      |        |
| <input checked="" type="checkbox"/> | vdb           | SSD  | 240 GB |

上一步

下一步

取消



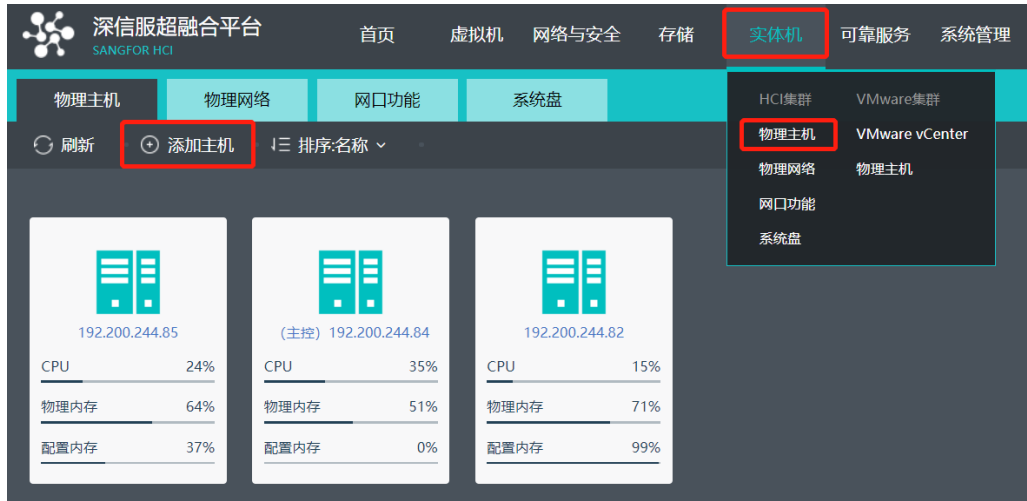
18. 确认最终信息，成功创建卷。



19. 确认配置：最后显示虚拟存储的配置结果信息，包括最终存储容量、副本数量和磁盘数量。确认配置无误后，需要输入管理员密码，点击<完成>以开始初始化虚拟存储。

## 添加磁盘多卷

1. 在[实体机/物理主机]中点击<添加主机>。



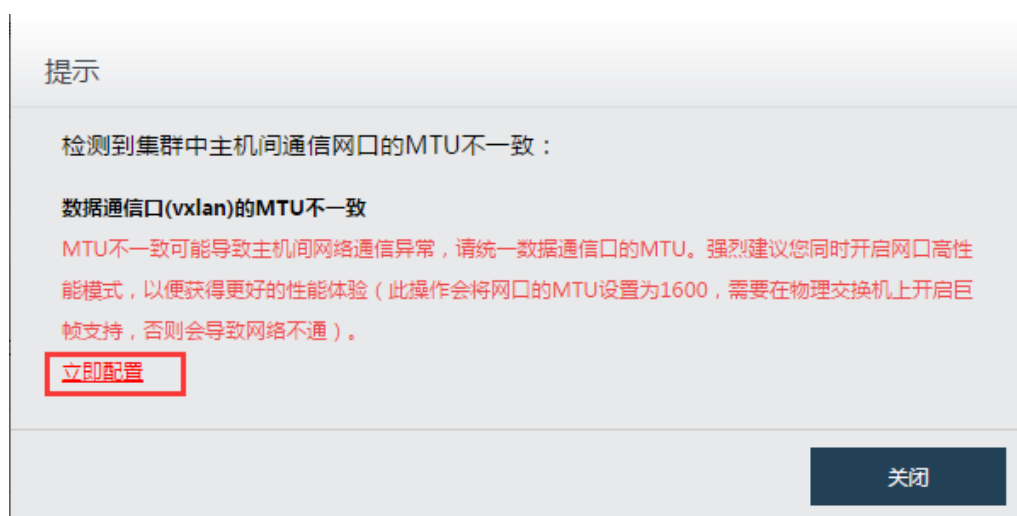
2. 选择需要添加的主机，如果需要添加的主机不再列表中，点击< + >进行添加。



3. 添加主机，将会删除被添加主机的防火墙配置，点击<确定>。



4. 检测到数据通信口MTU不一致，进行重新配置，勾选“开启网口高性能模式”即可。



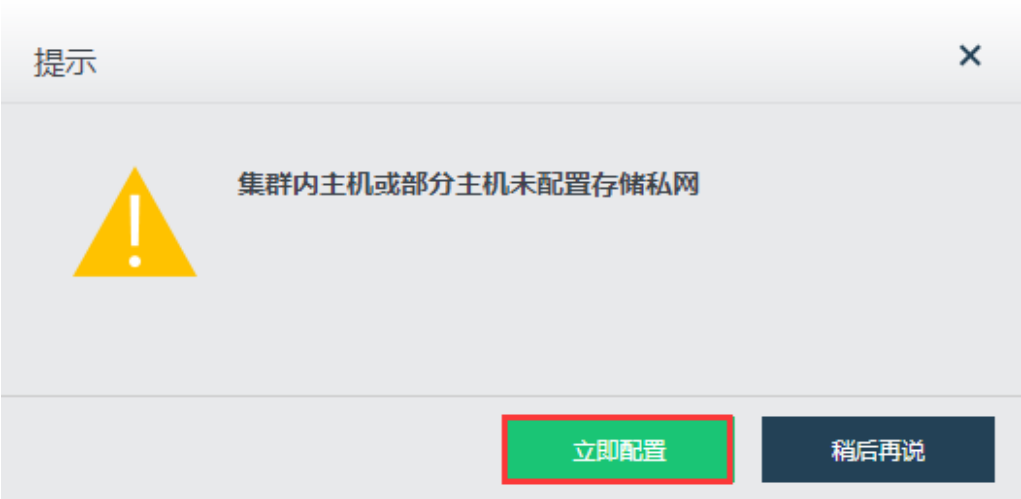
5. 添加成功后，配置数据通信口，完成后，可以在[首页]看到添加的实体机。



6. 在[存储/虚拟存储]中点击<创建卷>，进行新卷的添加。



7. 配置存储私网口和IP地址。



8. 根据实际情况选择虚拟存储通信网络部署模式。



9. 选择用作存储私网的网口并配置IP地址。



10. 再次点击<创建卷>，创建一个普通卷，进入<下一步>。



11. 选择[创建方式]。此处选择从新主机创建卷。

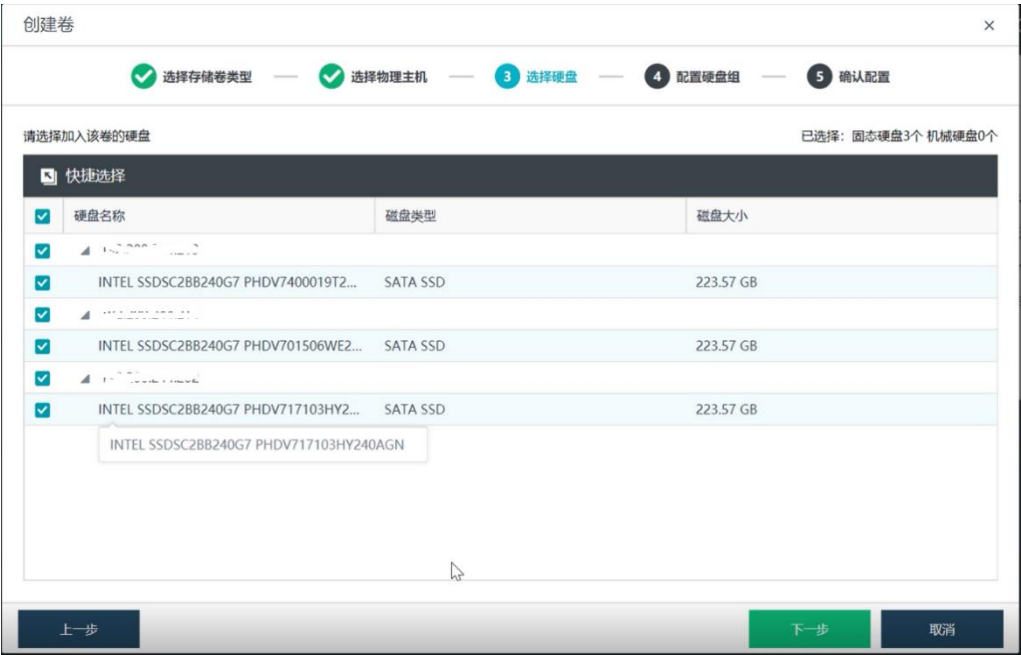
从新主机创建卷：重新选择集群中的 3 台或以上的主机创建一个新卷。

从已有卷的未使用硬盘创建卷：在已有卷的基础之上选择该卷包含的主机中的未使用的硬盘来选择创建新卷。

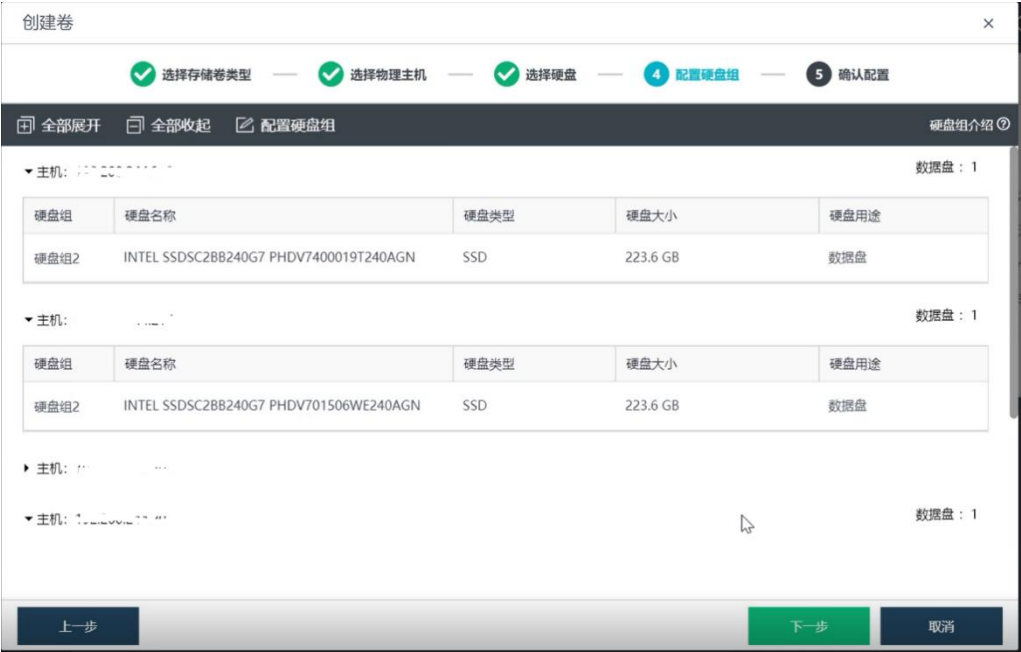


12. 选择要加入新卷的硬盘，此处勾选主机中的部分磁盘，需为主机后面创建第二个存储卷预留相应磁盘资源。





13. 为新卷配置硬盘组，同样如果不是全闪卷的话需要SSD作缓存盘。



14. 确认配置信息，新卷创建完成。

15. 配置存储卷类型：点击[存储/虚拟存储]打开虚拟存储页面，然后点击<创建卷>，选择卷类型为“普通卷”。



16. 选择物理主机：选择从已有卷的未使用磁盘创建卷，选择需要创建磁盘多卷的虚拟存储。



17. 选择主机中要加入的硬盘。配置硬盘和硬盘组，然后为每个主机的每个磁盘进行详细用途规划。系统会对集群中所有主机的磁盘进行自动检测，默认选择机械磁盘作为数据盘，固态硬盘作为缓存盘。一般建议采用默认配置，也可以自行修改。

创建卷

选择存储卷类型

选择物理主机

3 选择硬盘

4 配置硬盘组

5 确认配置

请选择加入该卷的硬盘

已选择：固态硬盘8个 机械硬盘0个

快捷选择

| <input checked="" type="checkbox"/> | 硬盘名称         |   | 硬盘类型 | 硬盘大小   |
|-------------------------------------|--------------|---|------|--------|
| <input checked="" type="checkbox"/> | 192.168.1.10 |   |      |        |
| <input checked="" type="checkbox"/> | vdc          | ▲ | SSD  | 240 GB |
| <input checked="" type="checkbox"/> | vdb          | ▲ | SSD  | 400 GB |
| <input checked="" type="checkbox"/> | 192.168.1.11 |   |      |        |
| <input checked="" type="checkbox"/> | vdb          | ▲ | SSD  | 240 GB |
| <input checked="" type="checkbox"/> | vdc          | ▲ | SSD  | 400 GB |
| <input checked="" type="checkbox"/> | 192.168.1.12 |   |      |        |
| <input checked="" type="checkbox"/> | vdb          | ▲ | SSD  | 240 GB |
| <input checked="" type="checkbox"/> | vdc          |   | SSD  | 400 GB |
| <input checked="" type="checkbox"/> | 192.168.1.13 |   |      |        |
| <input checked="" type="checkbox"/> | vdb          | ▲ | SSD  | 240 GB |

上一步

下一步

取消

创建卷

选择存储卷类型

选择物理主机

选择硬盘

4 配置硬盘组

5 确认配置

全部展开

全部收起

配置硬盘组

硬盘组介绍

▼ 主机：192.168.1.10

数据盘：2

| 硬盘组  | 硬盘名称 |   | 硬盘类型 | 硬盘大小   | 硬盘用途 |
|------|------|---|------|--------|------|
| 硬盘组1 | vdb  | ▲ | SSD  | 400 GB | 数据盘  |
| 硬盘组2 | vdc  | ▲ | SSD  | 240 GB | 数据盘  |

▼ 主机：192.168.1.11

数据盘：2

| 硬盘组  | 硬盘名称 |   | 硬盘类型 | 硬盘大小   | 硬盘用途 |
|------|------|---|------|--------|------|
| 硬盘组1 | vdc  | ▲ | SSD  | 400 GB | 数据盘  |
| 硬盘组2 | vdb  | ▲ | SSD  | 240 GB | 数据盘  |

上一步

下一步

取消

18. 确认最终信息，成功创建卷。

文档版本 06（2023-02-21）

270

创建卷 ×

✔ 选择存储卷类型

✔ 选择物理主机

✔ 选择硬盘

✔ 配置硬盘组

**5 确认配置**

请确认普通卷 虚拟存储卷1 的配置信息:

4

2.5 TB ⓘ

1.15 TB ⓘ

788 GB ⓘ

主机数

存储卷裸容量

2副本可用容量

3副本可用容量

存储卷信息:

| 主机名称             | 硬盘组数 | 数据盘数 | 数据盘裸容量 |
|------------------|------|------|--------|
| 12.18.18.144 128 | 2    | 2    | 640 GB |
| 12.18.18.144 128 | 2    | 2    | 640 GB |
| 22.200.211 74    | 2    | 2    | 640 GB |
| 12.200.244 71    | 2    | 2    | 640 GB |

上一步

确定

取消

19. 确认配置：最后显示虚拟存储的配置结果信息，包括最终存储容量、副本数量和磁盘数量。确认配置无误后，需要输入管理员密码，点击<完成>以开始初始化虚拟存储。

7.2.2.2. 添加延伸卷

功能说明

HCI 支持多卷管理，一个集群上可以同时存在普通卷，也可以存在延伸卷，在一个超融合的集群中可以创建多个虚拟存储卷，卷与卷之间物理上和逻辑上都是隔离的，但是对于虚拟机而言可以在卷之间进行选择和迁移，也可以满足集群中不同业务对于硬件的异构要求。以下操作为添加延伸卷的操作。

注意事项

- 1. 新添加的卷在创建时会将卷进行格式化，在添加前请确认用于添加新卷的磁盘上没有需要保留的数据。
- 2. HCI 组建卷是以主机为选择基本单位，请提前做好规划创建好集群。
- 3. 仲裁节点的部署方式支持物理机部署和VMware虚拟化部署，推荐用管理口与数据节点进行通信。

前提条件

- 1. 延伸集群至少4主机起步，加上1个仲裁节点。在实际部署中，要确保页面配置

的主机位置与实际物理位置一致，否则不能起到机房级别的保护作用。两个故障域机房必须二层打通，仲裁节点链路不需要二层打通，只需要网络可达即可。

2. 仲裁节点需要满足本手册“[仲裁节点配置要求](#)”章节的配置。

## 操作步骤

1. 配置卷类型及数据副本数量：点击[存储/虚拟存储]打开虚拟存储页面，然后点击<创建卷>，选择卷类型为“延伸卷”。

创建卷

1 选择存储卷类型

2 选择物理主机

3 配置故障域

4 选择硬盘

5 配置硬盘组

6 确认配置

存储卷名称：

延伸卷

存储卷类型：

普通卷

延伸卷



延伸卷介绍

延伸卷用于构建双活数据中心，卷内的物理机部署在两个机房并配置成主、备故障域，数据的多份副本则会写入到两个故障域内，实现RPO=0的容灾效果。

配置要求

延伸卷需要配置单独的仲裁物理节点。

下一步

取消

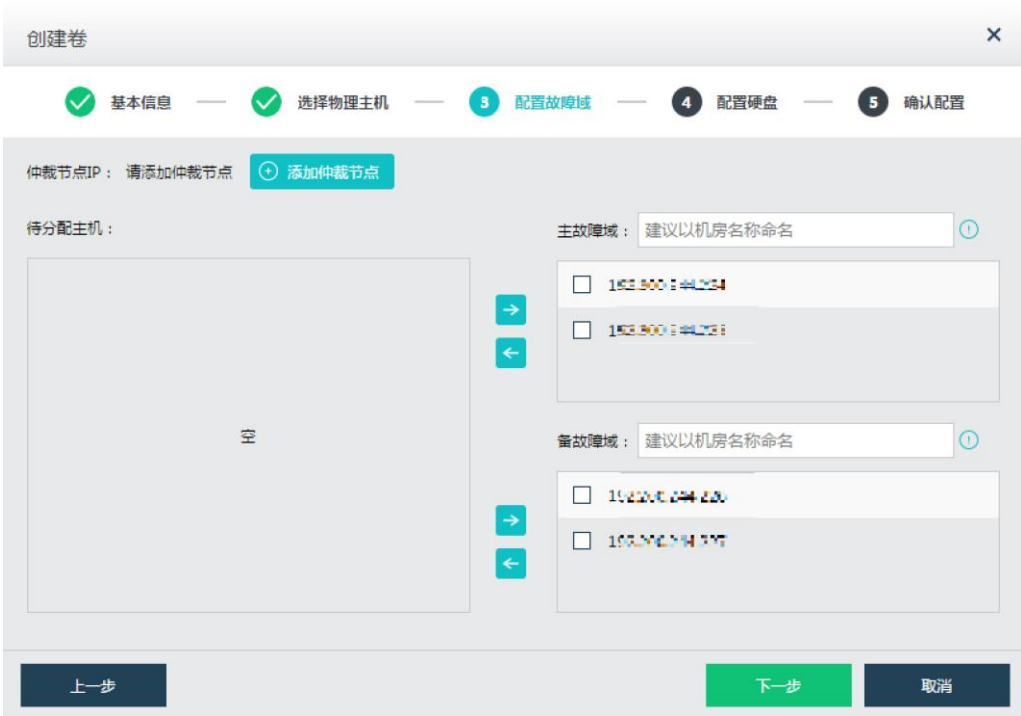
2. 选择物理主机：选择需要加入延伸卷的物理主机，延伸集群需要至少4台主机，分别将2台主机设置在不同的故障域中。

文档版本 06（2023-02-21）

272



3. 配置故障域：分别将需要的主机加入相应的故障域，本例中有四台主机，则两台主机加入主故障域，两台主机加入备故障域。



4. 添加仲裁节点：给主机房和备机房命名后，根据事先安装好的仲裁节点配置仲裁节点IP。按照向导输入密码确认配置仲裁节点，然后确认配置。

创建卷

×

✓ 基本信息

—

✓ 选择物理主机

—

3 配置故障域

—

4 配置硬盘

—

5 确认配置

仲裁节点IP： 请添加仲裁节点

添加仲裁节点

待分配主机：

主故障域： 建议以机房名称命名

①

☐ 192.168.1.1

☐ 192.168.1.2

→

←

备故障域： 建议以机房名称命名

①

☐ 192.168.1.3

☐ 192.168.1.4

→

←

上一步

下一步

取消

添加仲裁节点

×

仲裁节点IP：

192.168.1.1

用户名：

admin

密码：

.....

确定

取消

创建卷

✓ 基本信息

✓ 选择物理主机

3 配置故障域

4 配置硬盘

5 确认配置

仲裁节点IP：192.200.144.233

添加仲裁节点

待分配主机：

主故障域：机房1

192.200.144.234

192.200.144.235

备故障域：机房2

192.200.144.236

192.200.144.237

上一步

下一步

取消

5. 确认配置：确认故障域的配置，卷创建后不支持修改主机所在的故障域。
6. 配置硬盘：接下来需要规划磁盘用途。磁盘用途包括数据盘、缓存盘和热备盘。通常用SSD磁盘作为缓存盘，提升虚拟存储的IO性能。系统通常会根据配置自动推荐硬盘用途，默认按照系统推荐的配置即可。

确认配置

① 请确认故障域的配置是否跟主机在两个机房的实际部署一致，卷创建后，不支持修改主机所在的故障域，如果配置不正确，会导致双活功能不正常，例如：有一些数据块2个副本都写到同一个机房。

仲裁节点IP：

主故障域：机房1

192.200.144.234

192.200.144.235

备故障域：机房2

192.200.144.236

192.200.144.237

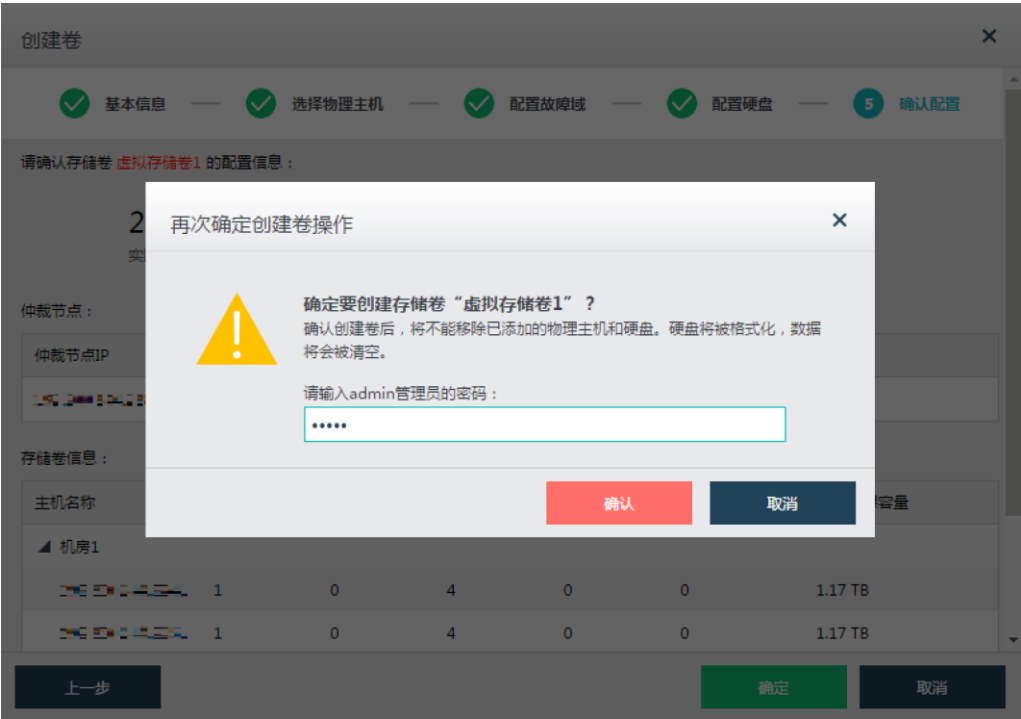
确定

取消





7. 确认配置：最后显示虚拟存储的配置结果信息，包括最终存储容量、副本数量和磁盘数量。确认配置无误后，需要输入管理员密码，点击<完成>以开始初始化虚拟存储。



### 7.2.3. 延伸卷修改故障域

#### 功能说明

搭建了延伸集群的HCI集群，由于主、备机房变更，HCI管理员可以通过配置故障域来切换主、备故障域。

## 注意事项

需要删除的卷明确确认数据为无效数据。

## 7.2.4. 删除卷（高危操作）

### 功能说明

HCI管理员可以以卷为单位对集群中的存储进行管理，可以将某一个卷进行删除，然后再将主机剔除，达到自由对集群进行扩容、缩容的目的。

### 注意事项

需要删除的卷明确确认数据为无效数据。

### 前提条件

1. 关闭运行在该存储卷主机上的所有虚拟机。
2. 关闭存储位置在该存储卷，运行在其他存储卷主机的虚拟机。
3. 该存储卷的虚拟iSCSI硬盘不再被使用，断开使用该存储卷虚拟iSCSI硬盘的所有连接。
4. 当HCI6.8.0及以上的版本，当集群配置保存在虚拟机存储中时，不允许删除该卷，需更改集群配置保存路径后再删。

### 操作步骤

1. 点击[存储/虚拟存储]，点击需要删除的卷的名称。



2. 点击后跳转到卷管理界面，点击<删除卷>。



3. 点击<确认>。



4. 输入管理员密码，点击<确认>。



## 7.2.5. 配置数据平衡计划

### 功能说明

HCI支持数据平衡，通过数据平衡可以保障数据在存储卷内的各个组件内尽可能地分布均衡，通过数据平衡，可以使新增磁盘或者主机的空间和性能得到及时的合理利用。

### 注意事项

1. 数据平衡计划所设置的时间范围，一般建议是用户业务的空闲时间，使执行数据平衡时所产生的I/O对业务的正常I/O影响尽可能小。若在当天所设定时间范围内仍未平衡完毕，平衡任务会停止，等到下一个计划时间继续完成平衡。
2. 若存储卷内所有磁盘都超过90%，并且任意两块磁盘的容量使用率都小于2%，此时说明整个存储卷的容量即将用尽，已无法通过数据平衡使得各个组件仍有充裕的空间继续用于数据的正常写入，此时必须扩充存储卷的空间。

前提条件

1. 在用户设置了数据平衡计划的情况下，当发现卷内最高和最低的磁盘容量使用率之差超过30%即触发平衡，直至卷内任意两块硬盘的使用率不超过20%。
2. 在用户未设置数据平衡计划的情况下，当存储卷内存在某块磁盘空间使用率已超过90%，即触发自动平衡，直至卷内最高和最低的磁盘容量使用率小于3%。

操作步骤

1. 在[存储/虚拟存储]中点击<高级配置>。



2. 选择[可靠性配置/数据平衡计划]，启用数据平衡，并设置数据平衡执行时间，建议设置为业务空闲时间。



7.2.6. 配置定时坏道扫描

功能说明

系统将定时周期性的扫描硬盘上的数据，当检测到存在坏道时，将自动修复坏道上的数据。

## 注意事项

1. 坏道扫描是针对机械盘，全闪存环境不支持坏道扫描和修复。
2. 坏道扫描会在设定的时间段内进行，如本次未完成一轮扫描，则会在下次扫描时从本次扫描结束位置开始。
3. 坏道扫描的速度会根据磁盘繁忙程度动态调整，对存储性能影响<5%。
4. 坏道扫描和修复仅对数据区进行，不扫描磁盘空白区。
5. 延伸集群仅支持坏道扫描，不支持坏道恢复。
6. 触发坏道修复任务时，会界面同时存在一个数据同步任务。

## 前提条件

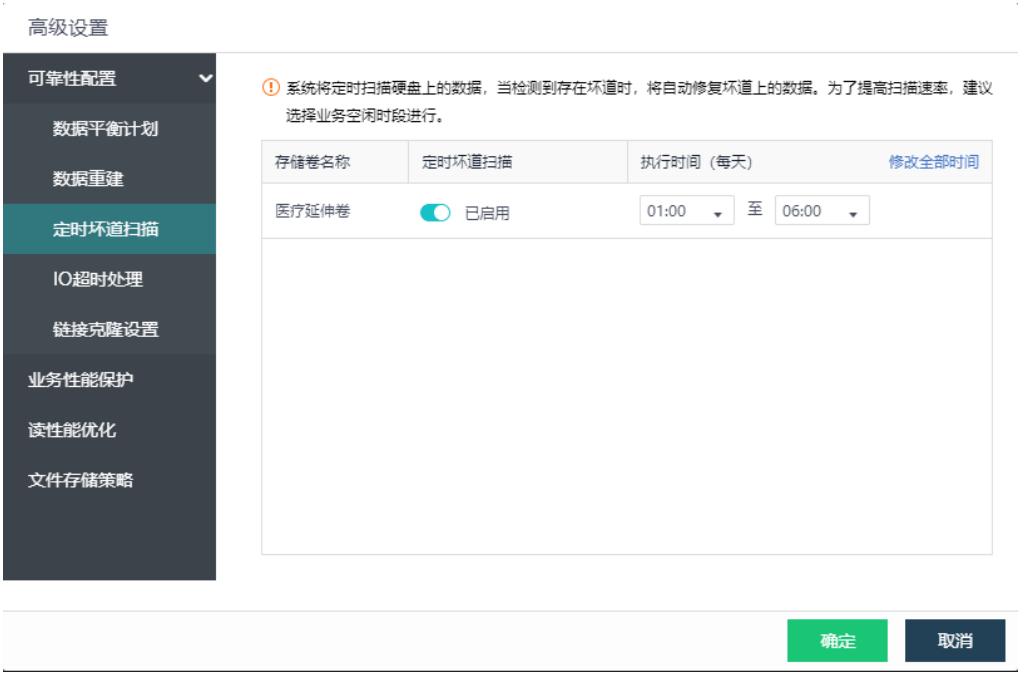
无

## 操作步骤

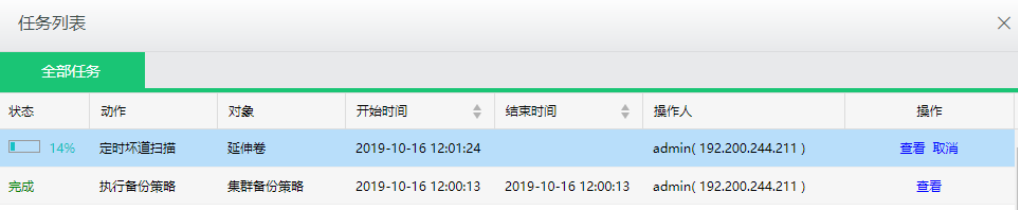
1. 在[存储/虚拟存储]中点击<高级配置>。



2. 在定时坏道扫描进行时间配置。



3. 开启之后，在任务列表可以看到一个坏道扫描的任务。



### 7.2.7. 配置数据重建等待时间

#### 功能说明

以数据采用两副本策略为例，当存储卷内的组件（磁盘或主机）发生物理故障时，故障组件上的数据还有另一的副本存储其他的组件上，仍然可以保障虚拟机的正常读写，但此时存储卷的冗余度实际上已变低，假如此时另一副本所在的组件也发生故障，就会导致数据丢失。通过数据重建功能，在组件发生故障后，将以故障组件上数据的另一副本作为修复源，以分片为单位在目的组件上重建出新的副本，恢复副本的完整性，实现系统自愈。

#### 注意事项

1. 要支持主机的自动重建功能，HCI集群主机台数必须为4台及4台以上。
2. 两主机无热备盘时，发生磁盘故障，不支持自动重建。

#### 前提条件

1. 必须满足分片的副本之间主机互斥。
2. 在满足条件1的情况下，集群中有磁盘容量不超过85%的磁盘。

操作步骤

1. 在[存储/虚拟存储]中点击<高级配置>。



2. 选择[可靠性配置/数据重建], 设置主机重建及磁盘重建的等待时间。



7.2.8. 配置快照熔断

功能说明

快照熔断功能通过调整分层淘汰与回写阈值，防止由于定时快照数据过多，而影响集群业务。

注意事项

此功能默认不开启，开启后由于调整了分层回写和淘汰的阈值，可能会影响部分业



务性能，建议只在使用定时快照进行安全防护的场景开启。

前提条件

无

操作步骤

1. 在[存储/虚拟存储]中点击<高级配置>。



2. 选择[业务性能保护]，“是否启用快照熔断”项设置为“已启用”。

高级设置

可靠性配置

数据平衡计划

数据重建

定时坏道扫描

IO超时处理

链接克隆设置

业务性能保护

⚠ 智能限速：当存在数据迁移、重建、创建定时快照等非业务流量时，系统将根据业务的IO情况智能限速，保证业务正常运行。

快照熔断：建议只在使用定时快照进行安全防护的场景开启，通过降低部分业务性能来支撑更多定时快照，同时增加了对定时快照删除、合并的限制。

| 存储卷名称                            | 是否启用智能限速 | 是否启用快照熔断 |
|----------------------------------|----------|----------|
| 逻辑侧井_vs_rm_全闪卷&逻辑侧井_vs_rm_全闪卷... | 已启用      | 未启用      |
| 逻辑侧井_vs_rm_延伸卷                   | 已启用      | 未启用      |

默认关闭状态

7.2.9. 更改虚拟存储网络配置（高危操作）

功能说明

存储私网是单独为虚拟存储搭建通信网络，可以提升数据传输的效率，也可以保障数据同步的一致性。

通常情况，虚拟存储中包含了非常重要的用户数据，为了避免因为网络问题带来的数据同步风险，可以搭建存储私网来保障。但存储私网要求物理主机提供单独的网口来供存储通信使用。

注意事项

1. 检查存储私网口采用链路聚合方式或者万兆口。

2. 禁止在HCI平台运行过程中调整网络布线，容易因插拔网线出现交替断网，导致数据脑裂，数据丢失。
3. HCI运行过程中禁止拔缓存盘。必要时通过磁盘管理替换磁盘，或停机处理。
4. 存储由无链路聚合更改为别的模式时，需保证主机有不少于一个空余网口，否则将无法更改存储网络部署模式。

前提条件

需要关闭所有运行的虚拟机以及虚拟网络设备。

操作步骤

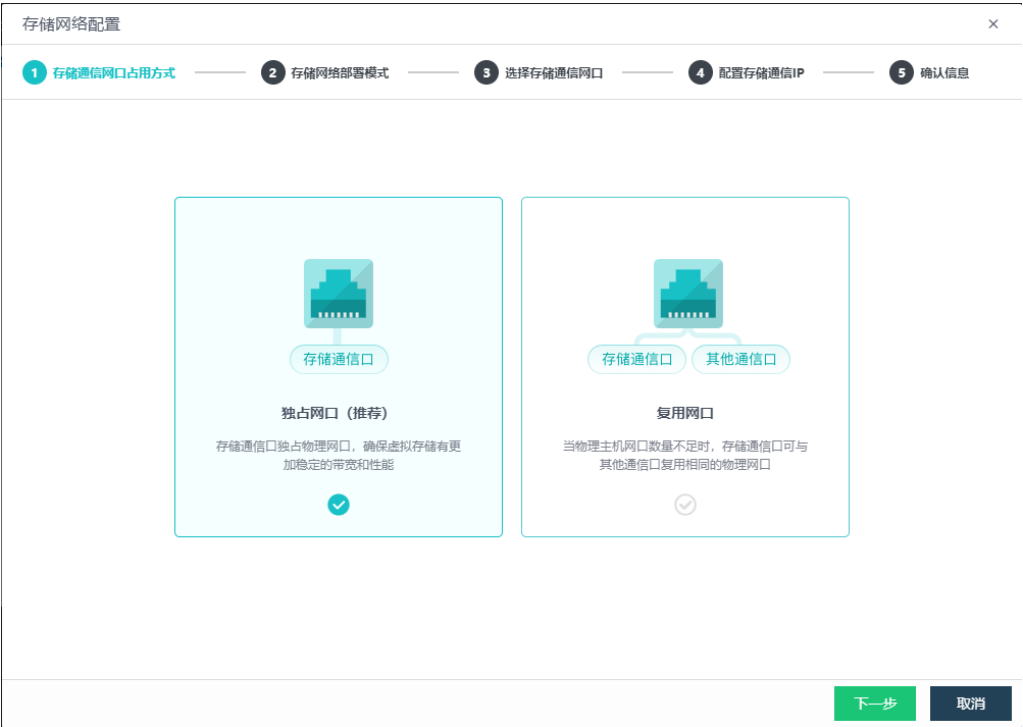
1. 在[存储/虚拟存储]中点击<存储网络配置>。



2. 选择[存储通信口]，并点击<重置存储网络>。



3. 根据规划，选择相应的存储网口占用方式。



4. 根据规划，选择相应的存储通信部署方式。



存储网络配置

✓ 存储通信网口占用方式

2 存储网络部署模式

3 选择存储通信网口

4 配置存储通信IP

5 确认信息

① 当前使用单交换机链路聚合，暂不支持切换为标准链路聚合。

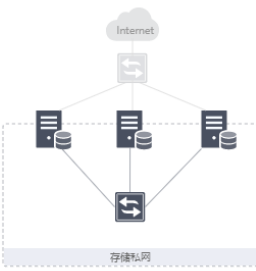
部署模式

选择存储网络部署模式（虚拟存储用于在主机间进行数据通信）：

☐ 标准链路聚合（推荐）

☒ 无链路聚合

☐ 其他



优点

将存储数据通信的网络独立出来，能提升虚拟存储的稳定性。

不足

当某条链路出现故障，会直接导致连接主机上的存储无法使用。

注意事项

存储私网专用于存储节点交换数据，请按示意图连接网线。  
使用普通的二层交换机即可，不需要在交换机上作任何配置。  
如果集群只有两个主机，可用网线直连私网网口，无需额外交换机。

上一步

下一步

取消

存储网络配置

✓ 存储通信网口占用方式

2 存储网络部署模式

3 选择存储通信网口

4 配置存储通信IP

5 确认信息

① 当前使用单交换机链路聚合，暂不支持切换为标准链路聚合。

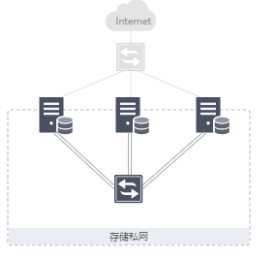
部署模式

选择存储网络部署模式（虚拟存储用于在主机间进行数据通信）：

☐ 标准链路聚合（推荐）

☐ 无链路聚合

☒ 其他



单交换机链路聚合

双交换机链路聚合

优点

使用简单，对交换机无要求，也不需要交换机上作任何配置提升网络可靠性，单条链路故障不会影响虚拟存储。

不足

只适用于做虚拟存储私网通信，跟第三方设备的兼容性不好，单交换机存在单点故障问题，交换机故障后，虚拟存储无法使用。

注意事项

存储私网专用于存储节点交换数据，请按示意图连接网线。  
使用普通的二层交换机即可，不需要在交换机上作任何配置。

上一步

下一步

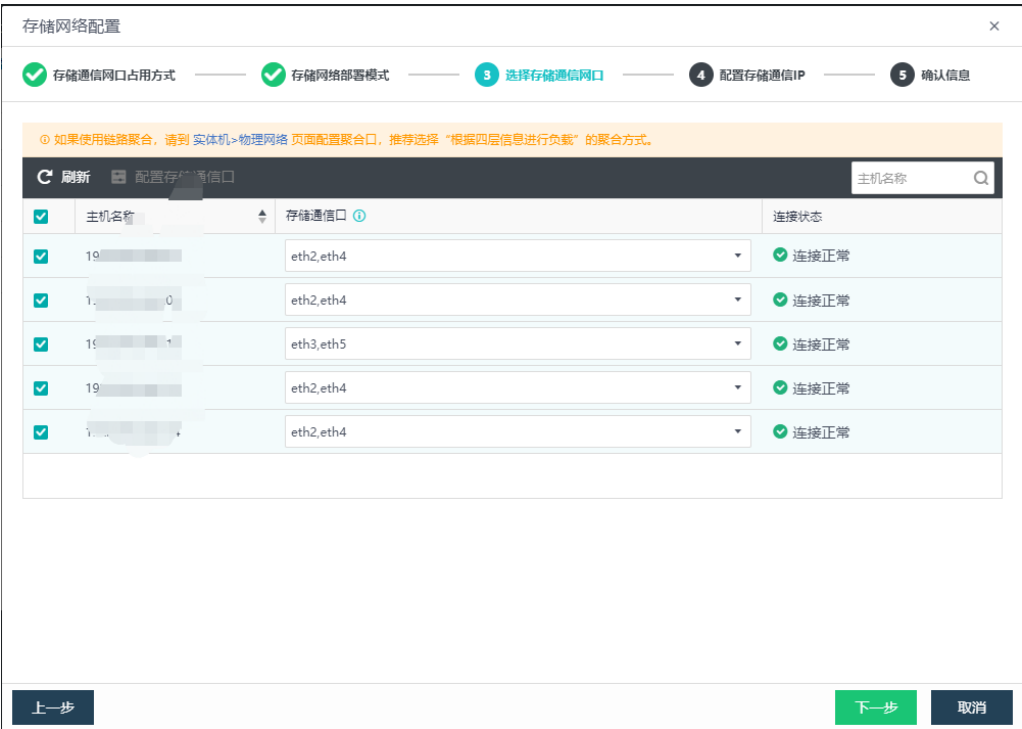
取消

文档版本 06（2023-02-21）

287



5. 配置存储通信网使用的网口。



6. 配置存储通信私网IP地址，要求存储私网IP地址必须为同一个IP段。

存储网络配置

✔ 存储通信网口占用方式

✔ 存储网络部署模式

✔ 选择存储通信网口

4 配置存储通信IP

5 确认信息

修改存储通信IP

配置子网掩码

主机名称

| <input type="checkbox"/> | 主机名称        | 存储通信IP            |
|--------------------------|-------------|-------------------|
| <input type="checkbox"/> | 10.20.20.2  | 10.20.20.4 / 24   |
| <input type="checkbox"/> | 192.168.1.1 | 10.20.20.1 / 24   |
| <input type="checkbox"/> | 10.20.20.1  | 10.25.25.1.4 / 24 |
| <input type="checkbox"/> | 10.20.20.5  | 10.20.20.5 / 24   |
| <input type="checkbox"/> | 10.20.20.2  | 10.20.20.1.2 / 24 |

上一步

下一步

取消

7. 确认存储通信配置信息。

存储网络配置

✔ 存储通信网口占用方式

✔ 存储网络部署模式

✔ 选择存储通信网口

✔ 配置存储通信IP

5 确认信息

存储通信网口占用方式

独占网口 (推荐)

存储网络部署模式

单交换机链路聚合

虚拟存储通信网口及通信IP

| 主机名称        | 存储通信口      | 存储通信IP          |
|-------------|------------|-----------------|
| 10.20.20.2  | eth2, eth4 | 10.20.20.4      |
| 10.20.20.1  | eth2, eth4 | 10.20.20.1      |
| 10.20.20.1  | eth2, eth4 | 10.20.20.1      |
| 10.20.20.1  | eth3, eth5 | 10.20.20.1      |
| 192.168.1.1 | eth2, eth4 | 10.20.20.5 / 24 |

上一步

确定

取消

7.2.10. 更改网络连通性探测 IP 地址（两主机场景）

功能说明

文档版本 06（2023-02-21）

289

探测IP地址是一个网络连通性探测的IP，通过ping这个IP地址，来判断是否因为网络中断而导致物理主机被孤立。

注意事项

- 1. 两台主机才需要探测IP，三台主机不需要。
- 2. 探测IP跟管理网络在同一网段，且能够ping通。

前提条件

无

操作步骤

- 1. 在[存储/虚拟存储]中点击<存储网络配置>。



- 2. 选择[存储通信口]，并点击<设置访问IP池>。



- 3. 填写规划好的探测IP地址，建议填写集群管理口的网关IP地址。



## 7.2.11. 配置跨卷访问 IP 池

### 功能说明

HCI支持多卷，配置虚拟IP池，支持虚拟机可以跨存储卷运行。

### 注意事项

若只有一个卷，不需要配置虚拟IP池，且确保没有其它集群或者主机使用该子网的IP。

### 前提条件

集群中配置2个或更多存储卷。

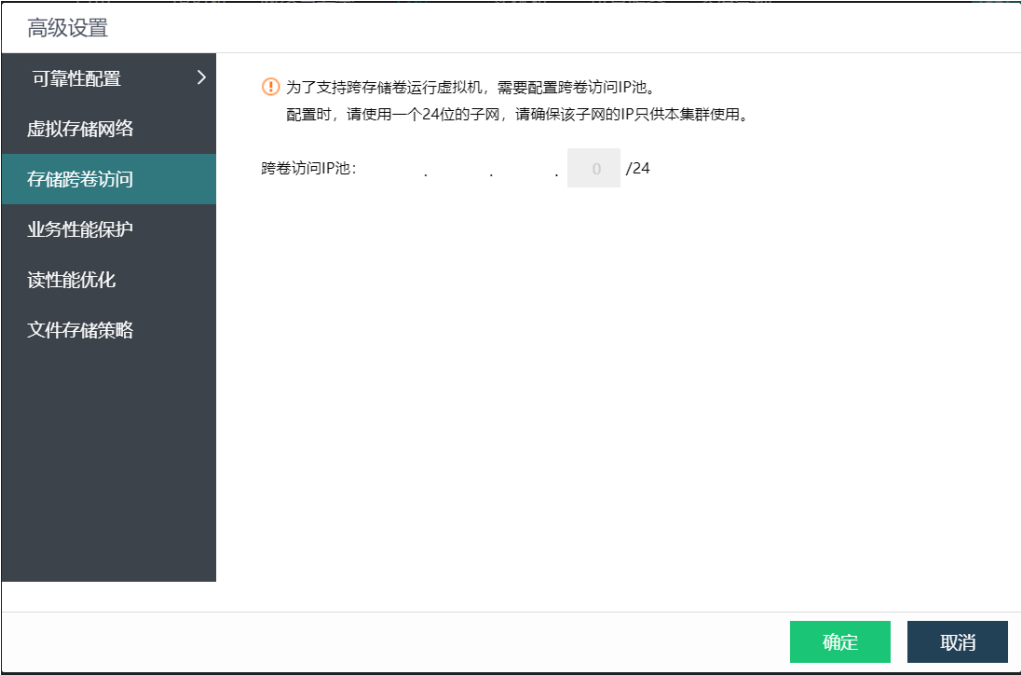
### 操作步骤

1. 在[存储/虚拟存储]中点击<高级配置>。



2. 选择[存储跨卷访问]，并填写规划好的探测IP地址，建议单独规划一个网段。





7.2.12. 配置读性能优化

功能说明

HCI支持内存读优化，即通过主机内存来提升读性能，在业务对性能要求比较高的场景建议启用，例如数据库高性能场景。

注意事项

无

前提条件

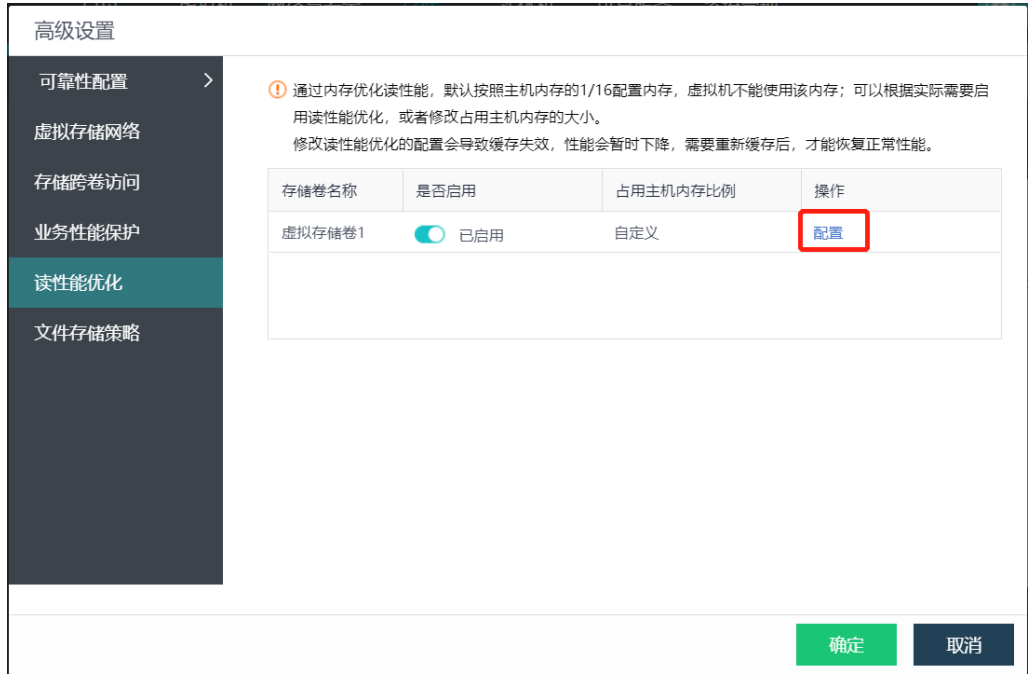
无

操作步骤

- 1. 在[存储/虚拟存储]中点击<高级配置>。



2. 选择[读性能优化]，选择是否启用读性能优化，点击[配置]，配置占用主机内存的比例。并可设置该功能是否对所有IO生效。配置建议如下：
- 数据库高性能场景建议多配置一些内存，按照主机 1/4 的比例配置内存。
  - 普通场景按照 1/16 或者 1/8 的比例配置内存。
  - 性能要求不高，但是要求多跑虚拟机的场景，建议关闭内存性能优化。



7.2.13. 新增及配置虚拟共享盘

功能说明

虚拟共享盘主要是用来提供给Oracle RAC使用的，利用共享盘方式的部署可以大幅简化Oracle RAC传统部署模式下的复杂度和成本，支持100个共享盘的不中断业务切换。

注意事项

在超融合集群中使用虚拟共享盘部署Oracle RAC，存储卷必须由3台以上的主机组成。

前提条件

无

操作步骤

1. 设置访问IP池：打开web控制台，选择[实体机/网口功能/存储通信口]，点击<设置访问IP池>。根据需要填写访问IP池信息。

深信服超融合平台  
SANGFOR HCI

首页 虚拟机 网络与安全 存储 实体机 可靠服务 系统管理

物理主机 物理网络 网口功能 系统盘

管理通信口  
数据通信口 (vxlan)  
业务通信口  
存储通信口  
网络流量控制

刷新 设置访问IP池 重置存储网络

存储通信口：用于集群内部不同主机之间存储的通信，当虚拟机需要跨主机访问存储资源的时候，需要通过存储口。

| 主机名称       | 存储通信口      | 存储通信IP      | 网口协商速率   |
|------------|------------|-------------|----------|
| 192.20.1.1 | eth2, eth4 | 10.255.3/24 | 1000Mb/s |
| 192.20.1.2 | eth2, eth4 | 10.255.4/24 | 1000Mb/s |
| 192.20.1.3 | eth3, eth5 | 10.255.5/24 | 1000Mb/s |
| 192.20.1.4 | eth2, eth4 | 10.255.6/24 | 1000Mb/s |
| 192.20.1.5 | eth2, eth4 | 10.255.7/24 | 1000Mb/s |

设置访问IP池

① 用于虚拟机跨存储卷运行，及虚拟共享盘接入。  
所配网段不能与存储通信IP网段相同，并确保只被本集群使用。

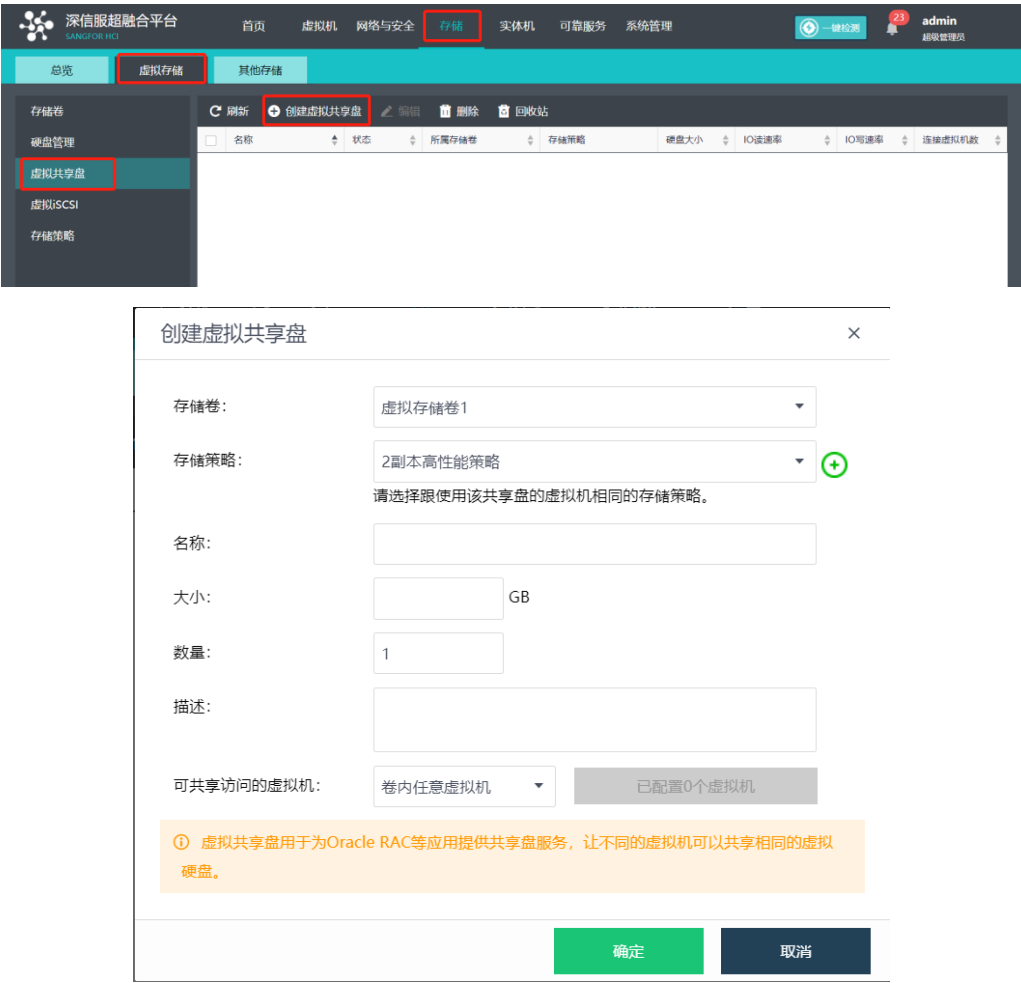
访问IP池：

10 . 251 . 42 . 0 / 24

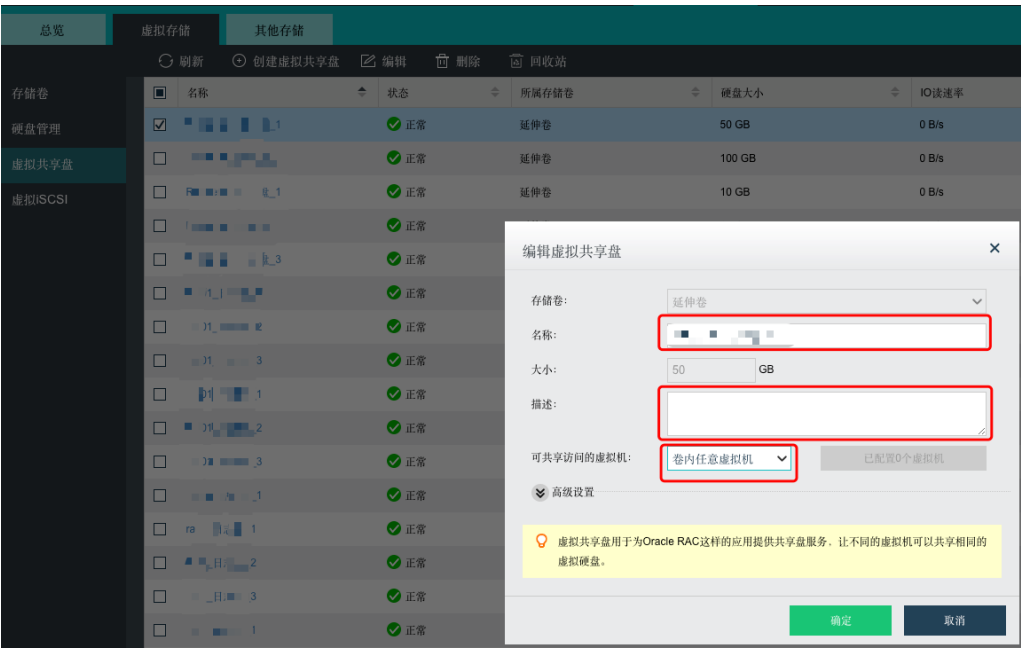
确定 取消

2. 新增共享盘：打开web控制台，选择[存储/虚拟存储/虚拟共享盘]，点击<创建虚

拟共享盘>。根据需要填写共享盘信息。



3. 配置共享盘：打开web控制台，选择[存储/虚拟存储/虚拟共享盘]，勾选需要修改的共享盘，点击<确定>。



## 7.2.14. 删除虚拟共享盘

### 功能说明

虚拟共享盘不再有用，删除虚拟共享盘。

### 注意事项

无

### 前提条件

虚拟共享盘的连接的主机数为0。

### 操作步骤

1. 打开web控制台，选择[存储/虚拟存储/虚拟共享盘]，勾选需要删除的共享盘，点击<删除>。



2. 确认删除：点击<确认>，即可删除共享盘。



7.2.15. 存储策略

功能说明

引入存储策略，以虚拟机为粒度，可以根据不同的业务类型，选择不同的存储策略。创建好虚拟存储卷后，虚拟存储会根据常用的存储配置，自动生成内置存储策略。如果内置策略满足不了需求，可以新增存储策略来自定义副本数、智能分层QoS、条带数等存储相关配置。

注意事项

无

前提条件

无

操作步骤

- 1. 打开web控制台，选择[存储/虚拟存储/存储策略]，可以查看默认的存储策略。
- 2. 主要场景及对应默认存储策略如下：
  - 普通虚拟机：2 副本默认策略。
  - 部署 Oracle、SQL Server：3 副本高性能策略。
  - 创建共享盘：3 副本高性能策略。
  - 创建虚拟 iSCSI 磁盘：2 副本默认策略。

| 策略名称     | 描述            | 副本数 | 智能分层QoS | 条带数  | 副本数  | 应用对象数量 | 操作           |
|----------|---------------|-----|---------|------|------|--------|--------------|
| 2副本默认策略  | 该策略支持普通通卷和延伸卷 | 2副本 | 默认性能    | 自动适配 | 自动适配 | 19     | 编辑 删除 设为默认使用 |
| 2副本高性能策略 | 该策略支持普通通卷和延伸卷 | 2副本 | 高性能     | 自动适配 | 自动适配 | 0      | 编辑 删除 设为默认使用 |
| 3副本默认策略  | 该策略只支持普通通卷    | 3副本 | 默认性能    | 自动适配 | 自动适配 | 0      | 编辑 删除 设为默认使用 |
| 3副本高性能策略 | 该策略只支持普通通卷    | 3副本 | 高性能     | 自动适配 | 自动适配 | 0      | 编辑 删除 设为默认使用 |
| FIO性能测试  | 该策略支持普通通卷和延伸卷 | 2副本 | 默认性能    | 自动适配 | 应用   | 55     | 编辑 删除 设为默认使用 |

- 3. 点击<新增存储策略>，可以自定义存储策略。输入存储策略的名称、描述，选择合适的副本数，自定义条带数、智能分层QoS，选择是否启用副本聚合，选择是否设置为默认存储。
  - 条带数：绝大部分场景下，采用默认的“自动适配”即可；全闪场景，可以将条带数设置为单台主机的 SSD 硬盘数量，让虚拟机可以使用上 1 台主机所有 SSD 的并发性能。

- 智能分层 QoS：建议只将性能要求高的少数虚拟机配置成高性能，其他的虚拟机都采用默认配置；文件服务器、用于备份的虚拟磁盘或虚拟 iSCSI 磁盘，分层的性能优化作用很小，可以配置成低性能。
- 聚合副本：大多数情况下，采用默认配置“自动适配”即可；全闪卷启用聚合副本，混合卷根据缓存盘的容量和虚拟机的负载自动选择是否聚合；对于大容量的数据库，如果超过了单台主机的缓存盘空间，不启用聚合副本，打散到多台主机，虚拟机可以使用多台主机的缓存盘空间，可提升命中率，从而提升性能。
- 设置默认使用：针对经常选择使用的存储策略，可以将其设置为默认使用的存储策略，减少在新增虚拟机，导入虚拟机、集群内迁移虚拟机、虚拟机的备份恢复、创建虚拟共享盘以及虚拟 iSCSI 盘等场景中的重复操作。

新增存储策略 ×

名称：

2副本全闪高性能

描述：

该策略支持普通卷和延伸卷

存储规则

副本数：

☒ 2副本（支持普通卷和延伸卷）

☐ 3副本（只支持普通卷）

☐ 3副本（只支持延伸卷）

数据保存2份，需要2倍的存储空间，可以容忍单台主机或单台主机的硬盘故障。

数据保存3份，需要3倍的存储空间，3至4主机场景，可以容忍单台主机或任意2块盘故障；大于等于5主机场景，可以容忍2台主机或者2台主机的硬盘故障。

副本分配方式：

条带数：

自动适配

智能分层QoS：

默认性能

聚合副本：

☒ 自动适配 ☐ 启用聚合副本 ☐ 不启用聚合副本

设为默认使用：☒

确定

取消

## 7.2.16. 配置虚拟 iSCSI 磁盘

### 功能说明

虚拟iSCSI磁盘主要是给有iSCSI存储需求用户使用，可以将虚拟存储分出来一部分以iSCSI存储的方式提供服务。

### 注意事项

1. 配置的虚拟iSCSI磁盘大小可以选择是否是预分配，如果是预分配，也就是配置了一个100G的磁盘在超融合上就会占用100G的空间。如果不勾选“预先分配存储空间”，则是按需分配存储空间。
2. 超融合平台必须要有虚拟存储才可以配置虚拟iSCSI磁盘，因为虚拟iSCSI磁盘是基于虚拟存储来做的。

## 前提条件

无

## 操作步骤

1. 打开web控制台，选择[虚拟存储/虚拟iSCSI磁盘]中并点击<配置iSCSI服务器>。



2. 选择需要提供iSCSI服务的虚拟存储卷。



3. 配置iSCSI认证用户名和密码。



4. 配置接入IP（具体作用可参照界面的“详细介绍”）。



配置iSCSI服务器（虚拟存储卷2）

配置iSCSI认证

配置接入IP

外接网口：

虚拟存储网口（推荐）

接入IP：

172.200.200.100

子网掩码：

255.255.255.0

虚拟IP池：

系统会从虚拟IP池为每台主机分配一个虚拟IP，外部主机统一通过接入IP接入后，会均衡重定向到不同主机的虚拟IP。

本存储卷当前有3台主机，请至少配置3个IP，并且要求跟接入IP在同一网段。

172.200.100.1-172.200.200.100

格式说明

外部主机可以通过“接入IP”来访问虚拟iSCSI磁盘，以获得高可用和负载特性。详细介绍

确定

取消

5. 在虚拟iSCSI磁盘页面，点击<创建虚拟iSCSI磁盘>。

深信服超融合  
SANGFOR HCI

首页 虚拟机 网络与安全 存储 实体机 可靠服务 系统管理

一键检测 15 admin 超级管理员

总览 虚拟存储 其他存储

存储卷  
硬盘管理  
虚拟共享盘  
虚拟iSCSI  
存储策略

刷新 创建虚拟iSCSI磁盘 配置iSCSI服务器 帮助 删除

| 名称       | 状态 | 所属存储卷 | 存储策略     | SCSI ID     | LUN ID | 磁盘大小  | IO读取率 | IO写入率 | 接入IP          | 连接数 |
|----------|----|-------|----------|-------------|--------|-------|-------|-------|---------------|-----|
| 10       | 正常 | 混合卷   | 2副本默认... | 6073bbc4... | 1      | 10 GB | 0 B/s | 0 B/s | 192.200.24... | 0   |
| 10g-test | 正常 | 混合卷   | 2副本默认... | 3c55da8a... | 3      | 10 GB | 0 B/s | 0 B/s | 192.200.24... | 0   |
| 12345    | 正常 | 混合卷   | 2副本默认... | 81940124... | 25     | 10 GB | 0 B/s | 0 B/s | 192.200.24... | 0   |
| 45678    | 正常 | 混合卷   | 2副本默认... | ef753bb9... | 26     | 10 GB | 0 B/s | 0 B/s | 192.200.24... | 0   |

6. 选择存储卷，配置名称、磁盘大小，以及可访问的客户端。勾选“优化硬盘性能”会优先占用SSD缓存盘空间，同时可以对连接的客户端进行限制，还可以限制是否允许多客户端同时接入。



## 7.2.17. 硬盘维护模式（硬盘隔离）

### 功能说明

当硬盘寿命到期、坏道数量过多、处于亚健康状态，需要进行硬盘替换操作时。如果有数据同步任务需要从即将替换的硬盘上读取数据，此时拔出此硬盘可能导致双点故障，进而影响业务，此时应当使用此功能。隔离硬盘之前，会对数据进行全面的巡检，确保硬盘隔离时业务不受影响。

### 注意事项

1. 支持数据盘，缓存盘的维护模式。
2. 进入维护模式支持两种方式。

#### 迁移数据：

- 提示进入维护模式需要搬迁\*\* GB 的数据的确认框，勾选后方可进行下一步。（若是缓存盘，迁移该缓存盘所在硬盘组所有数据）。
- 提示需等待数据搬迁成功后，才能进入维护模式。
- 提示搬迁该数据盘上收影响的虚拟机。

#### 不迁移数据：

- 仅确保该盘涉及的数据在该盘离线后仍可正常访问。

### 前提条件

硬盘处于亚健康状态。

### 操作步骤

## 7.2.17.1. 硬盘隔离

1. 进入[存储/虚拟存储/硬盘管理]界面，点击处于亚健康状态的硬盘（标识为黄色的硬盘）。



2. 点击<隔离硬盘>，前端会提示需选择对数据的处理方式。
3. 在进行硬盘隔离时，可以选择[快速隔离硬盘]，选择这种方式替换时间会比较短，与此同时会有一段单副本时间窗口。如果选择[优先保证数据安全]，系统会将硬盘上的数据先迁移到其它磁盘组上，以确保环境中始终存在两个健康的数据副本。

隔离硬盘

当缓存盘隔离后，该缓存盘所在硬盘组将停止服务，请先选择对整个硬盘组数据的处理方式。

处理方式：

快速隔离硬盘

不迁移数据，直接让硬盘进入隔离模式，数据会减少一个副本。  
如果2副本的虚拟机原先就已经有一个副本损坏，再减少一个副本，虚拟机就无法运行，虚拟存储会对数据进行检查，阻止对该硬盘进行隔离。

优先保证数据安全

先把这块缓存盘的磁盘组上的数据迁移到其他磁盘组，然后再让这块缓存盘进入维隔离模式，进入隔离模式耗时较长，但是数据更加安全。

处理对象：

| 对象名称        | 对象类型   | 数据量       |
|-------------|--------|-----------|
| 1vm1disk    | 虚拟机    | 26.74 GB  |
| 1vm6disk    | 虚拟机    | 160.29 GB |
| 非虚拟机文件      | 其他类型文件 | 2.18 TB   |
| cluster0010 | 虚拟机    | 84.18 GB  |

确定

取消

7.2.17.2. 硬盘替换

1. 进入[存储/虚拟存储/硬盘管理]界面，点击处于亚健康状态的硬盘（标识为黄色的硬盘）。



2. 点击<隔离硬盘>，前端会提示需选择对数据的处理方式。
3. 在进行硬盘隔离时，可以选择[快速隔离硬盘]，选择这种方式替换时间会比较短，与此同时会有一段单副本时间窗口。如果选择[优先保证数据安全]，系统会将硬盘上的数据先迁移到其它磁盘组上，以确保环境中始终存在两个健康的数据副本。

隔离硬盘

当缓存盘隔离后，该缓存盘所在硬盘组将停止服务，请先选择对整个硬盘组数据的处理方式。

处理方式：

快速隔离硬盘

不迁移数据，直接让硬盘进入隔离模式，数据会减少一个副本。  
如果2副本的虚拟机原先就已经有一个副本损坏，再减少一个副本，虚拟机就无法运行，虚拟存储会对数据进行检查，阻止对该硬盘进行隔离。

优先保证数据安全

先把这块缓存盘的磁盘组上的数据迁移到其他磁盘组，然后再让这块缓存盘进入维隔离模式，进入隔离模式耗时较长，但是数据更加安全。

处理对象：

| 对象名称        | 对象类型   | 数据量       |
|-------------|--------|-----------|
| 1vm1disk    | 虚拟机    | 26.74 GB  |
| 1vm6disk    | 虚拟机    | 160.29 GB |
| 非虚拟机文件      | 其他类型文件 | 2.18 TB   |
| cluster0010 | 虚拟机    | 84.18 GB  |

确定

取消

4.

等待磁盘隔离完成后，进入[存储/虚拟存储/硬盘管理]界面，点击处于亚健康状态的硬盘（标识为黄色的硬盘），点击<替换磁盘>。
5.

在主机上先将故障磁盘拔出，再插入新磁盘，勾选“我已准备完成”，并点击<下一步>。



6. 选择新磁盘，再点击<下一步>。



7. 确认新磁盘及故障磁盘的信息，勾选“我确定要更换磁盘”，点击<完成>后平台开始执行更换磁盘的操作。



### 7.2.18. 亚健康磁盘坏道预测

#### 功能说明

通过采集硬件信息，对硬盘七天内的状态进行坏道预测，配合坏道扫描，及时发现坏道并修复，保证更高的数据可靠性。

#### 注意事项

1. 坏道预测仅支持希捷和西部数据品牌的SATA HDD盘。
2. 非虚拟存储卷下的磁盘不支持坏道预测。
3. 坏道预测仅预测未来七天硬盘是否会出现坏道情况。
4. 低版本升级后或新建虚拟存储环境，环境持续运行七天，才会产生坏道预测结果。

#### 前提条件

无

#### 操作步骤

1. 进入[存储/总览]界面，在存储状态模块中有“坏道预测准确率”，展示出七天内的坏道预测数、坏道扫描数以及坏道修复数。





2. 点击[坏道预测准确率]，弹出坏道处理详情页签，此处可查看具体扫描的进度和状态。



## 7.2.19. 智能预测

aSAN分析大量真实业务场景数据，底层算法库集成了多种机器学习和深度学习算法，自主研发出智能预测模块，包含坏道预测、容量预测与SSD寿命预测功能。

### 7.2.19.1. 坏道预测

#### 功能说明

深信服通过收集分析大量客户真实使用场景中坏道硬盘的SMART数据、性能参数与硬盘日志信息，结合先进的算法训练模型，自主研发出高精度的坏道预测功能，通过大量差异业务场景测试，aSAN坏道预测准确率高达95%以上。

aSAN可以根据上层业务压力与集群硬盘使用情况动态感知集群中哪些硬盘最有可能出现坏道，并对其优先进行坏道扫描，可将硬盘坏道被发现的实际窗口从原来的一周甚至一个月缩短至一天，结合aSAN坏道扫描与修复，形成硬盘坏道的闭环处理，

极大缩短数据因硬盘坏道而处于“单副本”的风险期。

在坏道预测界面，用户可以看到硬盘的坏道预测结果、实际扫描结果与坏道修复情况，同时还会根据硬盘坏道数量对硬盘进行风险评估，针对历史出现坏道数量较多的硬盘进行告警，提示用户尽早更换硬盘，防止因坏道数量过多导致硬盘损坏出现数据丢失。

注意事项

无

前提条件

无

操作步骤

1. 进入[存储/总览]页面，在智能预测模块可查看硬盘的健康状态。
2. 点击<硬盘坏道处理>查看硬盘坏道预测结果和修复情况。
- 累积物理坏道数大于等于 40 个的硬盘，评定为“风险”。

• 累积物理坏道数大于等于 100 个的硬盘，评定为“高风险”硬盘。

• 根据历史累积物理坏道总数，对硬盘进行风险评估，请及时更换评定为“风险”或“高风险”的硬盘。



7.2.19.2. 容量预测

功能说明

aSAN可以根据客户集群的容量使用情况动态预测出未来90天内的容量增长趋势。在

容量预测界面，用户可以切换查看不同的存储卷裸容量、实际使用容量与动态预测曲线，并在页面提示用户预计xx天后，使用容量将达到容量告警阈值（90%）。

注意事项

新部署的集群使用180天后可获得预测结果。

前提条件

无

操作步骤

- 1. 进入[存储/总览]页面，在智能预测模块可查看虚拟存储容量的健康状态。
- 2. 点击<虚拟存储容量预测>查看虚拟存储容量的预测结果。
- 风险：预测 xx 天后使用率将超过告警阈值。
- 高风险：预测 xx 天后使用率将超过告警阈值。
- 虚拟存储容量使用率预测高风险或风险时请尽快启动虚拟存储扩容流程。



7.2.19.3. SSD 寿命预测

功能说明

aSAN收集分析集群中SSD硬盘IO数据，计算出SSD硬盘的剩余寿命，并结合上层业务压力显示预计SSD剩余可用时长，按照预测结果划分“健康”、“风险”、“高风险”三个寿命等级，提示用户及时更换集群中寿命告急的SSD硬盘。

注意事项

无

前提条件

无

操作步骤

- 1. 进入[存储/总览]页面，在智能预测模块可查看SSD寿命的健康状态。
- 2. 点击<SSD寿命>查看SSD寿命的预测结果和告警情况。
  - 根据剩余寿命和预计剩余可用时长评估 SSD 硬盘的风险。建议尽快更换风险和高风险的 SSD 硬盘。
  - 高风险：寿命<=10%。
  - 风险：寿命<=15%。
  - 健康：寿命>15%。



7.2.20. 卡慢盘处理

功能说明

当硬盘出现问题时，落在该硬盘的IO可能会卡住或者变慢。深信服超融合平台识别出卡慢盘后，虚拟存储会自动隔离掉卡慢盘，避免对客户业务造成持续影响。

慢盘：

- 若在 5 分钟内，统计到 60 秒 IO 延时大于 25 毫秒，则产生轻微慢盘的告警提示。
- 若在 5 分钟内，统计到 60 秒 IO 延时大于 125 毫秒，则该硬盘会被隔离，并产生严重慢盘告警提示。

卡盘：

- 当 IO 超过 3 秒不返回，则认为 IO 已经卡住。若在 13 秒内有 10 秒的 IO 都被卡住，则认为该盘为卡盘。识别出卡盘后，软件会将卡盘进行隔离处理，切换读写源到正常的磁盘。

## 7.2.20.1. HDD 卡慢盘处理

### 功能说明

本章节指导管理员进行HDD卡慢盘处理。

### 注意事项

1. 只支持虚拟存储场景，不使用虚拟存储的场景，无此功能。
2. 2主机场景不支持自动隔离硬盘，需要手动隔离，隔离后不支持磁盘数据重建，需要尽快进行硬盘替换，保证数据完整性。
3. 热备盘不会自动替换被隔离掉的卡慢盘。
4. 主机维护模式和硬盘维护模式下，不会自动隔离卡慢盘。
5. 自动隔离硬盘之前，虚拟存储会检查副本完整性，如果检测到其他主机存在副本处于异常状态，隔离当前硬盘可能造成该硬盘上的虚拟机无法运行。可根据实际情况手动隔离，但这种情况可能会造成业务中断。
6. 升级过程中出现的卡慢盘，不会进行自动隔离处理。
7. 若有重启主机的操作，卡慢盘处理服务将在半小时后生效。

### 前提条件

无

### 操作步骤

登录超融合HCI平台，在[存储/虚拟存储/磁盘管理]界面可以查看硬盘状态，当出现卡慢盘故障时，界面会产生告警提示。

- 当出现轻微慢盘告警提示时，如果影响到了业务，可点击<隔离硬盘>手动隔离该硬盘；



- 当出现严重慢盘告警提示时，软件会自动隔离该硬盘，建议尽快进行磁盘更换。



7.2.20.2. SSD 卡盘处理

功能说明

本章节指导管理员进行SSD卡盘处理。

注意事项

- 1. 以下情况暂不支持SSD卡盘自动隔离处理：
  - 当系统盘出现卡慢时，不会进行自动隔离，请联系深信服技术支持处理。
  - 2 主机场景不支持自动隔离硬盘，需要手动隔离，隔离后不支持磁盘数据重建，需要尽快进行硬盘替换，保证数据完整性。
  - 主机维护模式和硬盘维护模式下，不会自动隔离卡盘。
  - 自动隔离硬盘之前，虚拟存储会检查副本完整性，如果检测到其他主机存在副本处于异常状态，隔离当前硬盘可能造成该硬盘上的虚拟机无法运行。可根据实际情况手动隔离，但这种情况可能会造成业务中断。
  - 升级过程中出现的卡盘，不会进行自动隔离处理。
  - 正在执行坏道修复任务的卡盘，不会进行自动隔离处理。
  - 暂不支持对虚拟仲裁节点 SSD 卡盘进行自动处理。
- 2. 以下情况暂不支持对SSD卡盘进行永久隔离：

- 3 主机每主机 1 个磁盘组或 2 个磁盘组并且有 3 副本文件情况下，不支持 SSD 卡盘永久隔离。
  - 如果进行永久隔离处理时，发现隔离之后会出现数据无法全部重建情况，不进行 SSD 卡盘隔离处理。
  - 对于物理仲裁节点仲裁盘，当出现 SSD 卡盘时，不会做永久隔离处理，只会临时拔盘，且当出现 SSD 卡盘时，需联系客户尽快进行磁盘更换。
3. 当前版本支持SSD卡盘处理，暂不支持SSD的慢盘处理。
  4. 只支持虚拟存储场景，不使用虚拟存储的场景，无此功能。
  5. 若有重启主机的操作，卡盘处理服务将在半小时后生效。
  6. 当前不支持识别Raid卡原因导致的卡盘。
  7. 如果有多个磁盘被识别为SSD卡盘，则会逐个处理，暂不支持批量处理。
  8. PCIE盘卡盘被踢盘后再删卷，重新建卷无法被扫描到。
  9. PCIE多个盘会互相影响，当出现一个卡慢盘时，可能会导致其他盘都卡慢。
  10. 若手动隔离处理SSD盘，会影响整个磁盘组的业务，请谨慎操作。

## 前提条件

无

## 操作步骤

SSD卡盘处理分为临时隔离、永久隔离、手工隔离三个阶段：

- 判定为卡盘后首先进行临时隔离（前提是不会造成双点或者多点故障），约 5 分钟会重新上线，重新上线后需确认硬盘是否恢复。





- 临时隔离三次后，如果再次被判定为卡盘，就会进行永久隔离（前提是有足够的空闲容量用于数据重建）。



- 如果发现无法隔离（如环境检测不通过），页面会显示手动隔离按钮，可以选择强制隔离问题盘。



### 7.2.21. 只读盘处理

#### 功能说明

如果因硬盘出现异常，导致硬盘挂载为只读，则落在该硬盘的写操作将被卡住，深信服虚拟存储aSAN会识别只读硬盘并做隔离处理，若在24小时内，出现3次只读，则隔离该硬盘，避免对客户业务造成影响。

#### 注意事项

1. 2主机不支持隔离只读硬盘。

2. PCIE磁盘暂不支持只读处理。
3. 仲裁节点暂不支持只读处理。
4. 若尚未组虚拟存储卷，暂不支持只读盘处理。
5. 混合卷只支持数据盘的只读盘处理，暂不支持缓存盘。
6. 全闪卷中的数据盘支持只读盘处理。
7. 若存在磁盘新建/扩容/替换场景，磁盘上线30分钟后，只读盘处理服务将生效。

## 前提条件

无

## 操作步骤

登录超融合HCI平台，在[存储/虚拟存储/磁盘管理]界面可以查看硬盘状态，当出现只读盘故障时，平台会自动隔离该硬盘，并在界面产生告警提示。



## 7.3. 其他存储配置指导

### 7.3.1. 添加 FC 存储

#### 功能说明

HCI支持添加FC存储作为外置存储，让虚拟机的存储位置放到FC存储上。FC作为外置共享存储，存储位置为共享存储的虚拟机可以实现HA功能。

#### 注意事项

1. 添加FC存储的卷到HCI时会将卷进行格式化，在添加前请确认该卷没有被其他主机使用。（如果所连接的外置存储格式为SFFS，则不会格式化）
2. 如果待添加的FC存储卷之前被HCI添加过，那么再次添加时会提示是否恢复FC存储上的虚拟机。

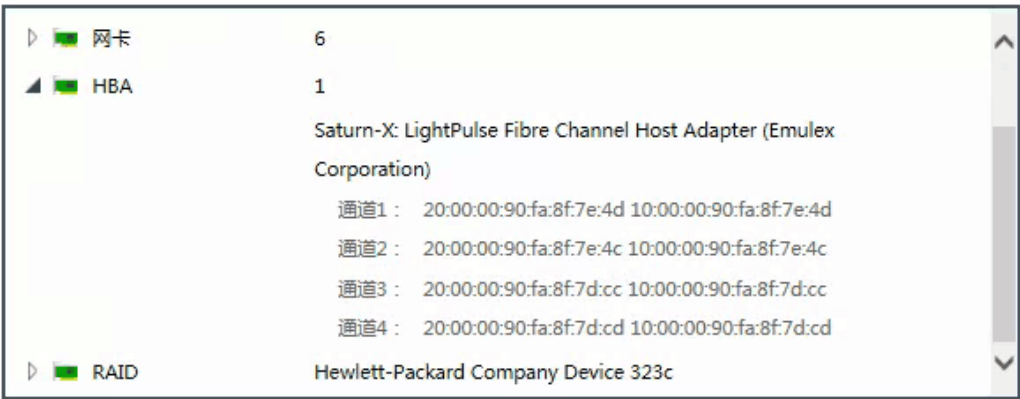
- 3. 建议云服务器配置两个HBA卡,每个HBA卡配置一个存储光模块，单链路带宽6GE以上。
- 4. 禁止在HCI使用的外置存储做缩容操作。
- 5. 禁止在HCI使用的外置存储上，使用精简分配/动态分配进行磁盘超配。
- 6. 添加FC外置存储之前，需先点击<重新发现硬盘>，再点击<添加存储>。

前提条件

- 1. HCI主机上有HBA卡，可以连接到FC存储的光纤交换机上。
- 2. FC存储和光纤交换机需要正确配置，将相应的卷映射给HCI主机使用。
- 3. 存储必须支持硬件加速或ATS特性，否则无法添加到HCI平台。

操作步骤

- 1. 在HCI主机上插入HBA卡，通过光纤直连或经过FC交换机连接到FC存储。
- 2. 首先检查HCI能否正常识别到HBA卡，可以在[实体机]中选择主机，进入相关主机的[主机信息]页面查看HBA卡状态。



- 3. 在FC存储和光纤交换机上做正确的配置，将相应的卷映射给HCI集群内所有主机。
- 4. 在[存储/其他存储]中点击<添加存储>并选择[FC存储]进行FC存储添加。



- 5. 选择FC存储，添加磁盘，添加后需要配置可访问的主机为所有当前集群内的主机。



### 7.3.2. 添加 iSCSI 存储

#### 功能说明

HCI支持添加iSCSI存储作为外置存储，让虚拟机的存储位置放到iSCSI存储上。  
iSCSI作为外置共享存储，存储位置为共享存储的虚拟机可以实现HA功能。

#### 注意事项

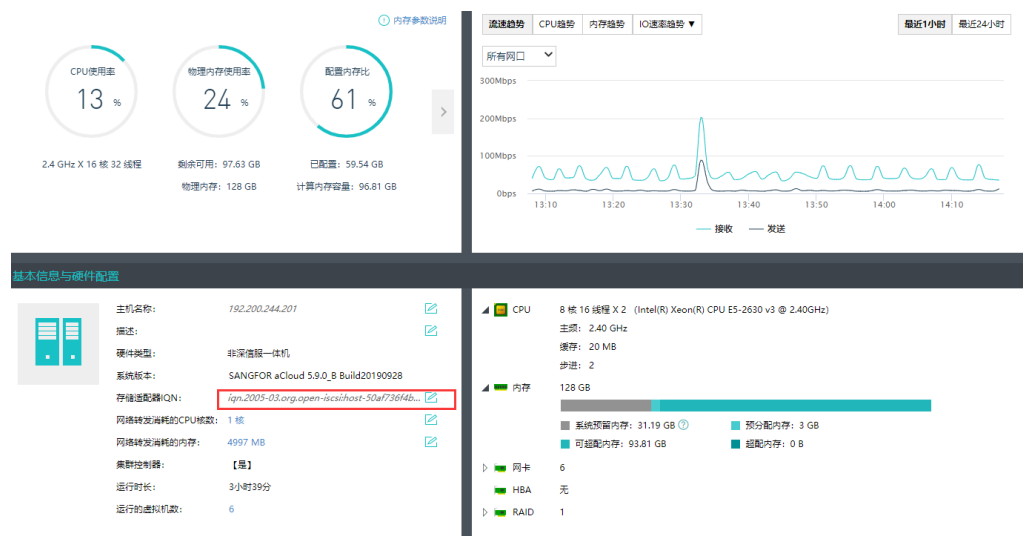
1. 添加iSCSI存储的卷到HCI时会卷进行格式化，在添加前请确认该卷没有被其他主机使用。（如果所连接的外置存储格式为SFFS，则不会格式化）
2. 配置iSCSI外置存储时，存储配置中的“iscsi 别名”建议不做配置。
3. 添加iSCSI外置存储之前，需先点击<重新发现硬盘>，再点击<添加存储>。
4. 禁止在HCI使用的外置存储上，使用精简分配/动态分配进行磁盘超配。

#### 前提条件

1. HCI主机上的用于和iSCSI通信的网口和存储服务器能够正常通信。
2. 存储必须支持硬件加速或ATS特性，否则无法添加到HCI平台。

#### 操作步骤

1. 配置HCI主机上用作存储网口的IP地址，使其能够和iSCSI存储服务器正常通信。
2. 配置iSCSI存储，将LUN映射给超融合主机使用，需要查看超融合的IQN。



3. 在控制台中打开[存储/其他存储]，点击<iSCSI服务器连接配置>。



4. 添加iSCSI服务器，配置服务器的IP地址，端口和相关的认证信息。配置完后点击<发现目标>。

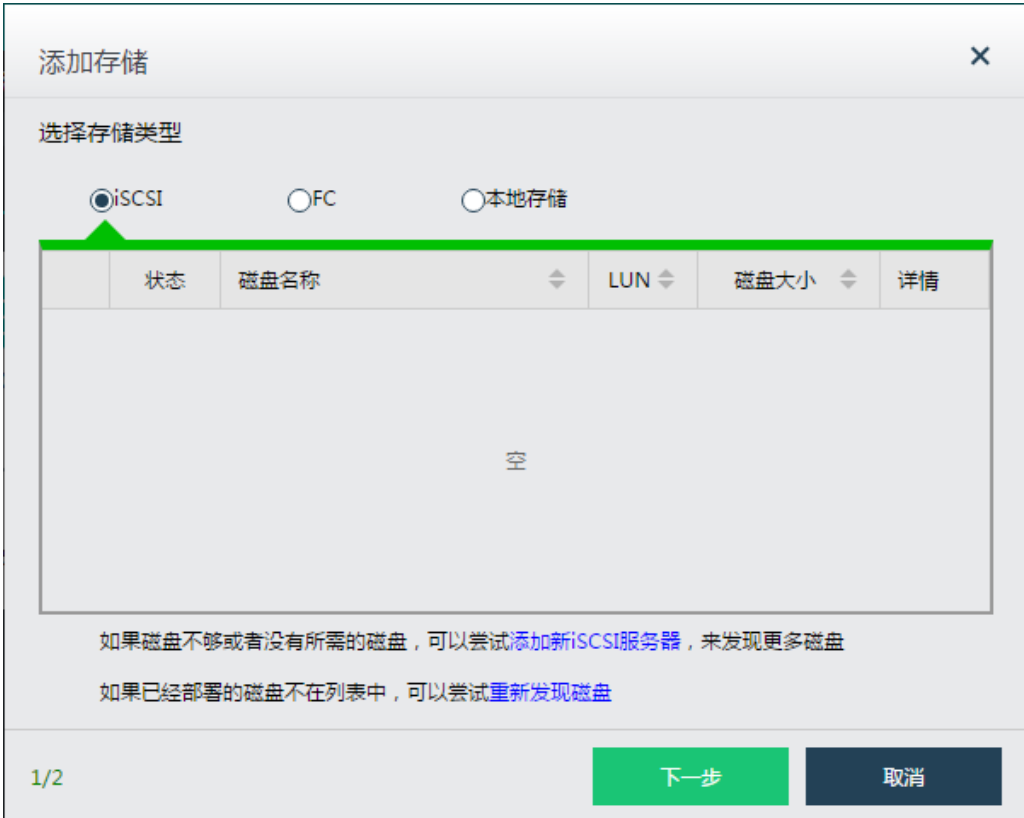
The screenshot shows the '添加新的iSCSI服务器' (Add New iSCSI Server) dialog box. It contains the following fields and options:

- iSCSI服务器** (iSCSI Server)
- 服务器IP:** 输入服务器IP (Server IP: Enter server IP)
- 端口:** 3260 (Port: 3260)
- 配置认证信息** (Configure authentication information):
  - ☐ 服务器验证本机(CHAP) (Server authenticates this host (CHAP))
  - 以下用户名和密码为该台设备连接iSCSI服务器时使用的认证帐号信息。由iSCSI服务器提供帐号，本地仅连接即可。(The following username and password are the authentication account information used by this device to connect to the iSCSI server. The account is provided by the iSCSI server, and local connection only is required.)
  - 用户名:** (Username)
  - 密码:** (Password)
  - ☐ 本机验证服务器(双向CHAP) (This host authenticates the server (bidirectional CHAP))
- 发现目标** (Discover target) button
- 关闭** (Close) button

5. 点击<添加存储>并选择[iSCSI存储]。



6. 选择iSCSI，选择相应的卷进行添加。添加后需要配置可访问的主机为所有当前集群内的主机。



### 7.3.3. 添加 NFS

#### 功能说明

HCI支持添加NFS作为虚拟机的备份位置，让虚拟机备份到NFS上，保证虚拟机的数据安全。

#### 注意事项

- 1. NFS不可作为虚拟机存储位置，只能用于备份使用。
- 2. 禁止HCI服务器使用外置windows共享目录。
- 3. 添加NFS存储之前，需先点击<重新发现硬盘>，再点击<添加存储>。

前提条件

HCI主机上的存储网络需要和NFS存储能够正常通信。

操作步骤

1. 在[存储/其他存储]中点击<添加存储>并选择[NFS存储]。



2. 配置NFS存储的名称、服务器IP以及选择相应的文件夹，勾选需要连接的主机，点<确定>即可。



7.3.4. 添加本地存储

功能说明



HCI支持添加服务器系统盘之外的本地磁盘或服务器上磁盘组建RAID之后的逻辑磁盘作为虚拟机的存储位置。

## 注意事项

1. 添加磁盘到本地存储会将磁盘格式化。
2. 添加本地存储之前，需先点击<重新发现硬盘>，再点击<添加存储>。

## 前提条件

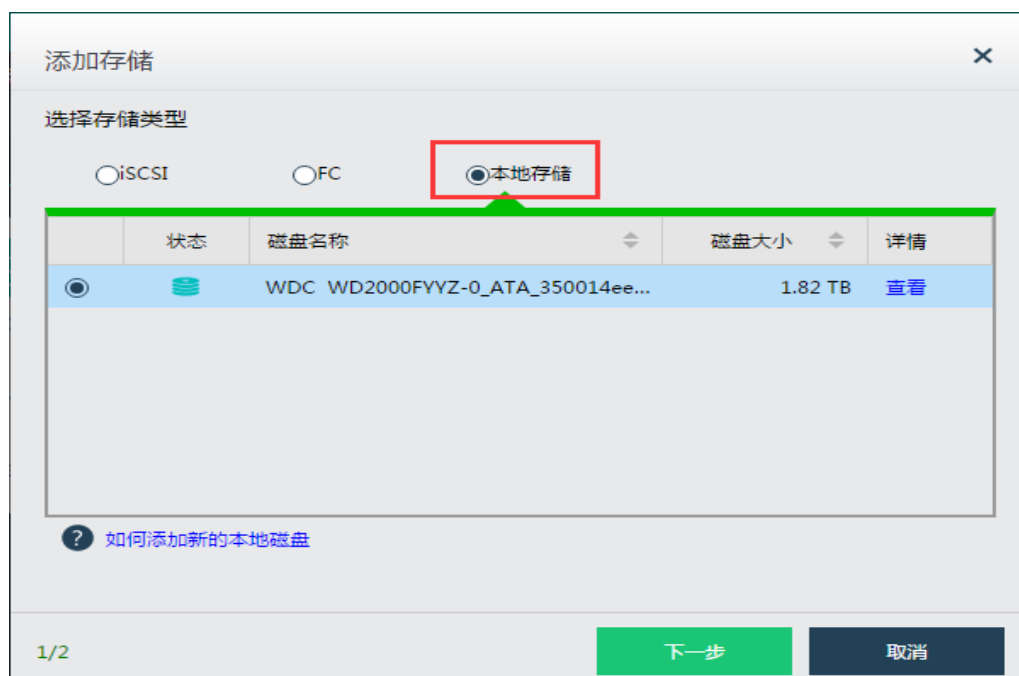
HCI主机上必须有空闲可用于本地存储的磁盘，需要RAID卡做好相关的配置。

## 操作步骤

1. 打开控制台，在[存储/其他存储]中点击<添加存储>并选择[本地存储]。



2. 选择本地存储后，选择需要添加的磁盘，点击<下一步>，配置本地存储名称后确认即可。



3. 填写相应信息。

添加存储

存储名称：

test

描述：

连接到主机

☐

主机名称

IP

☒

172.20C...101

172.20C...101

☒ 同时加入备份池中用于虚拟机备份

最大备份容量占比：

40

%

详情

2/2

上一步

确定

取消

7.3.5. 删除存储（高危操作）

功能说明

需要将存储从超融合中删掉，不再供超融合使用。

注意事项

- 1. 从HCI上删除存储会将存储位置为该存储的虚拟机从平台上删除，删除后虚拟机无法正常启动。
- 2. 外置存储和本地存储都可以被删除。

前提条件

无

操作步骤

[存储/其他存储]，选择要删除的存储，在名称右边的下拉箭头里边选择<删除>。



## 8. 可靠服务配置指导

### 8.1. HA 配置

#### 功能说明

共享存储上的虚拟机，可以使用“故障迁移”功能，通过配置一定的检测条件，当探测到主机发生以下故障且持续一定时间时，触发虚拟机HA功能使其从其他主机上恢复运行。

#### 注意事项

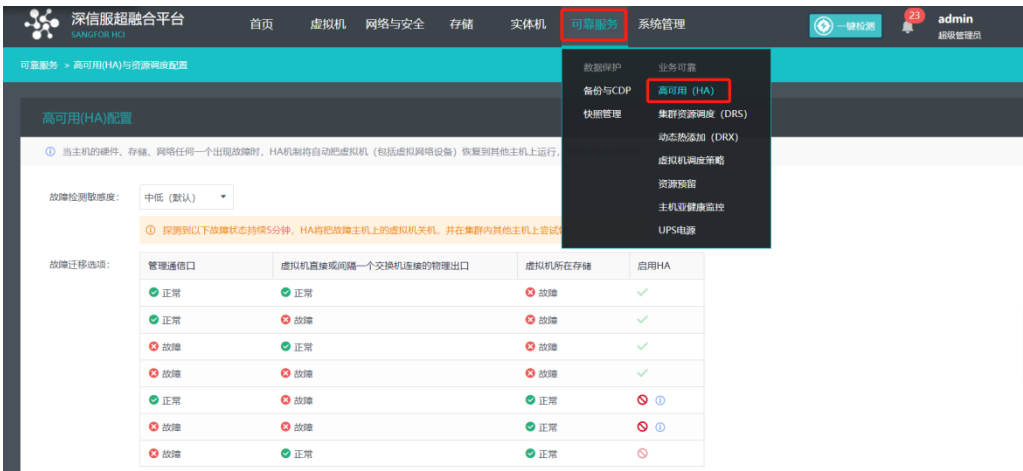
1. 故障迁移功能，只针对勾选了HA的虚拟机。
2. 存储位置为虚拟存储或外置存储的虚拟机才可以勾选HA选项。
3. 大量虚拟机HA场景，当客户集群资源不足时，会导致HA会失败。
4. 平台序列号过期后，不支持虚拟机HA。
5. 测试HA时不要编辑HA配置。
6. 建议核心应用，在[可靠服务/资源预留] 在部分主机上预留一定资源空间，以保证核心业务在发生HA的时候，有足够资源拉起虚拟机。
7. 在管理通信口和业务通信口故障场景下启用HA，仅支持在两主机集群生效，三主机及以上集群不生效。
8. 在业务通信口故障场景下启用HA，仅支持在两主机集群生效，三主机及以上集群不生效。

#### 前提条件

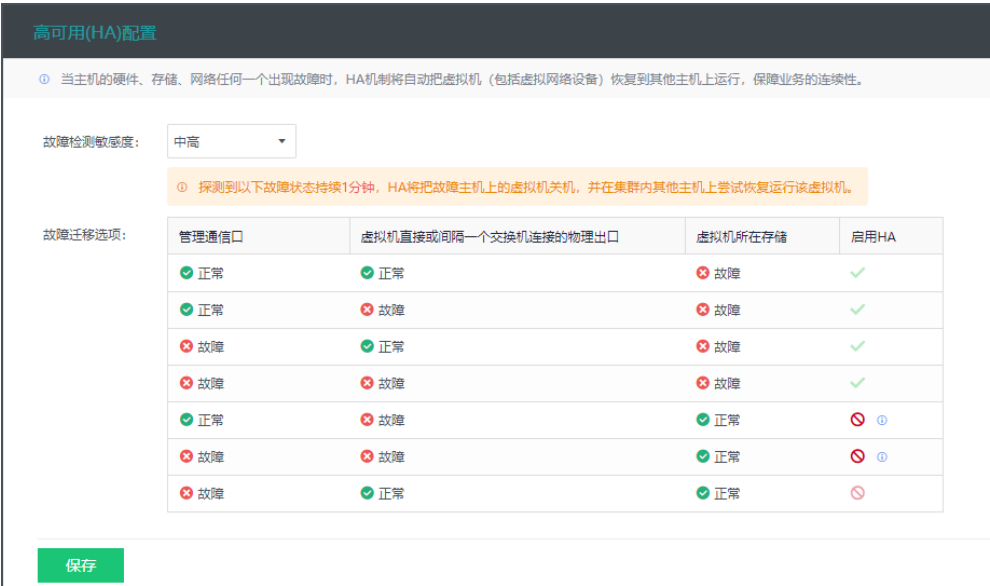
多台HCI主机组成集群。

#### 操作步骤

1. 在控制台上打开[可靠服务/高可用（HA）]。



2. 启用你想要实现HA的场景（要求平台上虚拟机非极端情况下不要重启的，可以不启用两个选项），点击<保存>。



## 8.2. 集群资源调度配置

### 功能说明

集群资源调度，在特定的场景下会调度集群资源，这里的资源是指虚拟机，“调度”这个操作实际是迁移虚拟机。我们可以设置CPU和内存阈值，如果有主机超过了阈值，就会触发集群资源调度，并且会根据自动化级别对虚拟机进行调度。调度的结果是，将虚拟机从CPU或者内存利用率比较高的主机迁移到利用率比较低的主机上，将负载过高的主机的利用率降到阈值以下。

### 注意事项

无

## 前提条件

1. 多台HCI主机组成集群。
2. 虚拟机存储在外置存储或虚拟存储。
3. 虚拟机运行位置配置为自动选择。
4. 虚拟机未开启CDP功能，未配置CPU独占功能，未配置USB映射。

## 操作步骤

1. 在控制台上打开[可靠服务/集群资源调度（DRS）]。



2. 用户可选择是否开启AI智能预测，集群可基于主机或者虚拟机过去7天的负载预估未来2天的负载进行智能DRS调度，假如开启该功能，集群资源调度会使用AI智能探测算法，让资源调度更加的智能化。
3. 用户可用设定集群资源调度的衡量因素，可选择CPU，内存或CPU和内存三种，假如选择的是CPU和内存，其中任何一个达到阈值触发条件时，则触发集群资源调度策略。
4. 用户可以设定分级策略，不同的敏感度对应不同的主机负载阈值，假设选择了中性，则主机负载大于60%，且主机负载差值超过20%时，则触发集群资源调度，最激进的主机负载>50%，且主机负载差值超过5%触发集群资源调度。
5. 用户可以选择调度方式（自动和手动），当你设置了自动，并且有主机触发了阈值，生成了建议后，这里会自动执行建议，无需人为操作。如果来实现主机触发阈值后只生成建议，不发生迁移，需要自己手动迁移，则调度方式选择手动。
6. 若有些虚拟机的调度方式因为某些场景需要特殊处理，则配置特定虚拟机调度。调度方式可选择：手动、自动、禁用。



### 8.3. 动态热添加配置

#### 功能说明

需要在业务高峰期间，虚拟机自动的添加CPU和内存的资源，以保障业务系统的正常使用。

#### 注意事项

1. 动态热添加只能增加资源，不能自动减少。
2. 动态热添加的资源，在虚拟机重启后会失效。
3. 动态热添加的最大值为配置大小（也就是原配置\*2），CPU每次增加原配置一个插槽的核数，内存为配置的1/8按上取整，单位为GB。
4. 模板虚拟机和虚拟网络设备暂不支持动态热添加。

#### 前提条件

操作系统需要支持动态热添加，具体操作系统的列表如下所示。

1. 支持热添加内存的操作系统。

表8 支持热添加内存的OS列表

| Windows     | Linux         |
|-------------|---------------|
| 2008 Ent 32 | RHEL6.5 64bit |
| 2008 Ent 64 | RHEL 7 64bit  |

|                                      |                      |
|--------------------------------------|----------------------|
| 2008 DC 32                           | ubuntu 14 64bit      |
| 2008 DC 64                           | CentOS Linux 6 64bit |
| 2008 R2 Ent 64                       | CentOS Linux 7 64bit |
| 2008 R2 DC 64                        | -                    |
| 2012 Std                             | -                    |
| 2012 DC                              | -                    |
| 2012 R2 Std/DC 64                    | -                    |
| 2016 Std/Ent/DC 64                   | -                    |
| 2019 Std/Ent/DC 64（需要官方补丁 KB4501371） | -                    |

## 2. 支持热添加CPU的操作系统。

表9 支持热添加CPU的OS列表

| Windows                              | Linux                |
|--------------------------------------|----------------------|
| 2008 DC 64                           | RHEL6 64bit          |
| 2008 R2 DC 64                        | RHEL 7 64bit         |
| 2012 Std                             | ubuntu 14 64bit      |
| 2012 DC                              | Ubuntu 16 64bit      |
| 2012 Ent                             | Ubuntu 18 64bit      |
| 2012 R2 Std/DC 64                    | CentOS Linux 6 64bit |
| 2016 Std/Ent/DC 64                   | CentOS Linux 7 64bit |
| 2019 Std/Ent/DC 64（需要官方补丁 KB4501371） | -                    |

## 操作步骤

1. 打开控制台进入虚拟机编辑页面，在硬件配置的CPU处勾选“启用CPU热添加”。





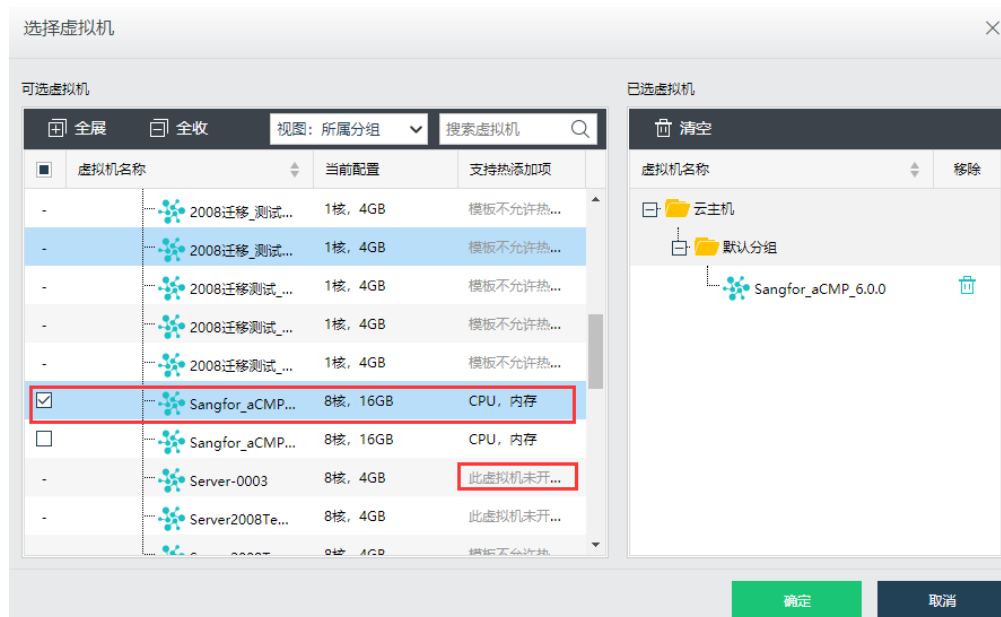
2. 在硬件配置的内存配置里面勾选“启用内存热添加”。



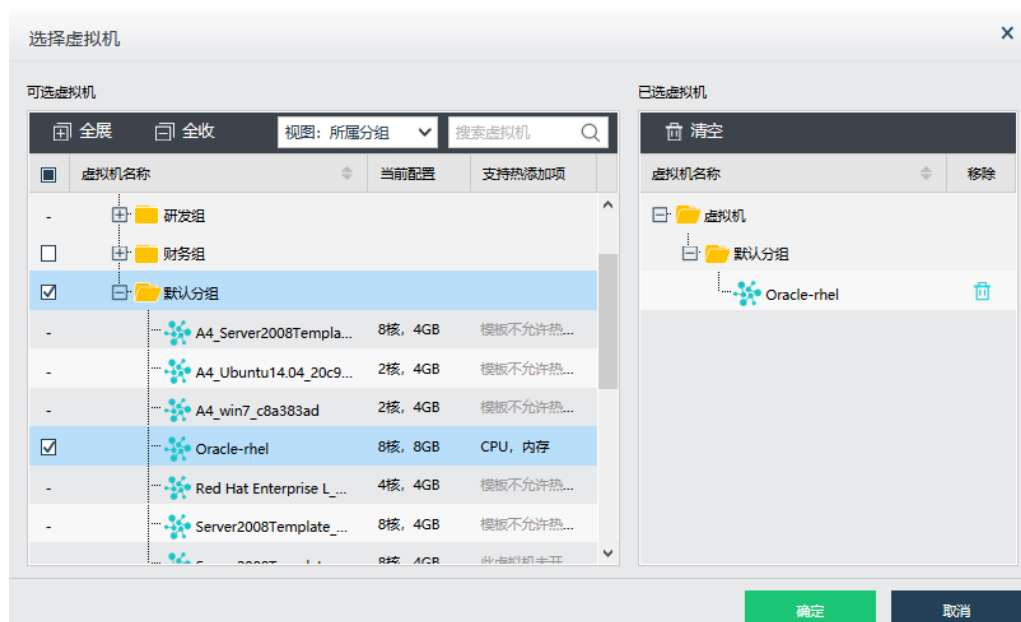
3. 打开[可靠服务/动态热添加（DRX）]。



4. 在[动态热添加]页面中勾选“启用虚拟机动态热添加”。



5. 配置需要动态热添加的虚拟机，并配置动态热添加的条件。



## 8.4. 虚拟机调度配置

虚拟机调度策略支持对多个虚拟机和集群配置互斥或聚集策略，通过调度策略，可以对虚拟机的运行位置实现精确控制，满足虚拟机业务调优需求。

### 8.4.1. 聚集虚拟机

#### 功能说明

聚集虚拟机允许将多个虚拟机绑定运行在某台物理主机上。例如将业务互访频繁的虚拟机或同一业务组的虚拟机绑定在同一台服务器上，提升业务访问性能。

#### 注意事项

1. 运行中的虚拟机不支持修改“运行位置”配置。
2. 运行中的虚拟机创建调度策略后，需要重启云主机电源才能生效。

#### 前提条件

无

#### 操作步骤

进入[可靠服务/虚拟机调度策略]界面，点击<创建>将规划为同一运行位置的虚拟机配置聚集策略。



8.4.2. 互斥虚拟机

功能说明

互斥虚拟机支持将所选虚拟机运行在不同物理主机上。例如将Oracle RAC等集群系统互斥在不同物理服务器上保证业务可靠性。

注意事项

- 1. 运行中的虚拟机不支持修改“运行位置”配置。
- 2. 运行中的虚拟机创建调度策略后，需要重启虚拟机电源才能生效。

前提条件

无

操作步骤

进入[可靠服务/虚拟机调度策略]界面，将规划运行位置互斥的虚拟机添加到互斥策略。



### 8.4.3. 虚拟机组互斥

## 功能说明

虚拟机组互斥支持将所选多个虚拟机组运行在不同的物理主机上。例如将A业务的三台虚拟机和B业务的三台虚拟机配置云主机组互斥，当运行A业务的物理主机失效时，不会对B业务造成影响，提高业务可用性。

## 注意事项

1. 同一个虚拟机组，运行位置必须配置成同一个故障域或者自动选择。
2. 运行中的虚拟机不支持修改“运行位置”配置。
3. 运行中的虚拟机创建调度策略后，需要重启虚拟机电源才能生效。
4. 同一虚拟机组内的虚拟机不会默认聚集，需手动配置聚集策略。

## 前提条件

无

## 操作步骤

1. 进入[可靠中心/虚拟机调度策略/虚拟机组]界面，将规划为同一运行位置的虚拟机添加到虚拟机组。

创建虚拟机组

同一个虚拟机组，运行位置必须配置成同一个故障域或者自动选择。运行中的虚拟机不支持设置运行位置。

名称：

业务组A

描述：

虚拟机：

展开收起批量设置运行位置刷新

视图：所属分组虚拟机或虚拟机组

|                                     | 虚拟机或虚拟网络设备   | 状态  | 存储位置   | 运行位置   |
|-------------------------------------|--------------|-----|--------|--------|
| <input type="checkbox"/>            | audit        | 已关机 | 虚拟存储卷1 | <自动选择> |
| <input checked="" type="checkbox"/> | audit_克隆0001 | 已关机 | 虚拟存储卷1 | <自动选择> |
| <input checked="" type="checkbox"/> | audit_克隆0002 | 已关机 | 虚拟存储卷1 | <自动选择> |

已选 (2)

清空

| 名称           | 操作 |
|--------------|----|
| audit_克隆0001 | 移除 |
| audit_克隆0002 | 移除 |

2. 进入[可靠中心/虚拟机调度策略]界面，点击<创建>，策略类型选择“虚拟机组互斥”选中互斥的虚拟机组，点击<确定>。



8.4.4. 虚拟机组到主机组

功能说明

虚拟机组到主机组支持将所选虚拟机组运行在不同的物理主机组上。例如将双活业务的A业务组运行在延伸集群主故障域，将双活业务的B业务组运行在延伸集群的备故障域，保证数据和业务同时双活。

注意事项

- 1. 同一个虚拟机组，运行位置必须配置成同一个故障域或者自动选择。
- 2. 运行中的虚拟机不支持修改“运行位置”配置。
- 3. 运行中的虚拟机创建调度策略后，需要重启虚拟机电源才能生效。
- 4. 延伸集群会默认将相同故障域的主机划分入同一主机组。

前提条件

无

操作步骤

- 1. 进入[可靠中心/虚拟机调度策略/虚拟机组]界面，将规划为同一运行位置的虚拟机添加到虚拟机组。



2. 进入[可靠中心/虚拟机调度策略/主机组]界面，将主、备故障域内的主机加入到同一主机组。



3. 策略类型选择“虚拟机组到主机组”，将业务A固定在主故障域，将业务B固定在备故障域。



## 8.5. 资源预留配置

### 功能说明

通过配置资源预留，可以预留主机的内存，当虚拟机发生故障HA的时候，可以优先使用这部分的预留资源进行恢复。

### 注意事项

无

### 前提条件

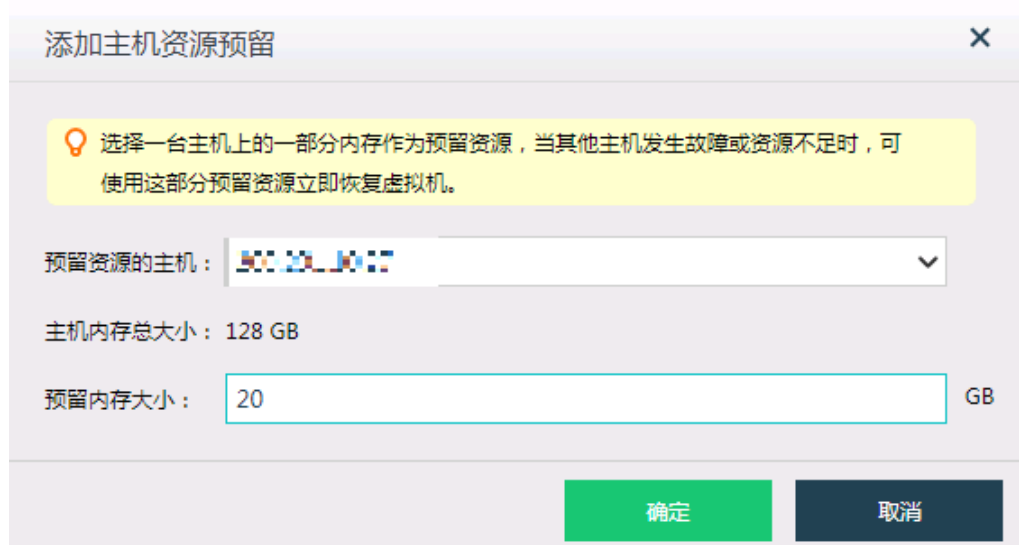
1. 多台HCI主机组成集群。
2. 虚拟机存储在外置存储或虚拟存储。
3. 虚拟机运行位置配置为自动选择。

## 操作步骤

1. 在控制台上打开[可靠服务/资源预留]。



2. 点击<添加主机资源预留>，根据业务的实际使用情况及主机的资源情况，设置预留资源。



## 8.6. 主机亚健康监控

### 功能说明

超融合平台可自动识别并展示亚健康主机（有假死风险或已处于假死状态下的主机），对于已经判断为亚健康的主机，在进行虚拟机开机或HA时对其进行降级处理。针对集群扩容、主机替换等场景，检测硬件状态，避免硬件故障导致节点频繁宕机或系统假死，降低因硬件问题带来的业务风险。

### 注意事项

1. 仅支持硬件类故障导致主机假死的识别与处置。
2. 如果是内存故障导致的假死问题，在主机开启&重启时，如果没有踩到故障内存位置，那么将不会自动释放主机，需用户手动释放。

## 前提条件

无

## 操作步骤

1. 进入[可靠服务/主机亚健康监控]界面，若已自动识别到物理主机处于亚健康状态，则会在“亚健康主机列表”中显示。



2. 点击进入[亚健康主机设置]界面，可进行亚健康检测相关设置。



可靠服务 > 主机亚健康监控

亚健康主机列表 亚健康主机设置

① 系统可自动识别物理主机是否处于亚健康状态。主机在执行虚拟机开机、HA等任务时，不会优先选择亚健康主机，并

识别条件：☒ 主机硬件（内存、系统盘、RAID卡）健康异常 ①

☒ 主机在 1 天宕机达到 2 次

检测方式：☒ 每次开机或重启自动检测

☒ 每 30 分钟自动检测

通知方式：发送到邮箱 ① [告警通知设置](#)

处理方式：☐ 自动将亚健康主机上的虚拟机迁移至其余健康的主机 ①

恢复方式：☒ 非亚健康的主机，自动从亚健康主机列表移除

保存

- 识别条件：若勾选“主机硬件健康异常”，可对主机进行内存 ECC、UECC，系统盘坏道、系统盘只读、系统盘寿命不足，RIAD 卡故障等硬件检测。同时可手动设置宕机频率，自定义主机宕机满足一定条件时，识别为亚健康主机。
- 检测方式：可选择亚健康主机检测方式。通常情况下，若开启主机亚健康检测，则在主机开机&重启时，会进行自动检测。也可勾选“每 XX 分钟自动检测”，自定义开机检测频率。
- 通知方式：如检测到亚健康主机后，需要邮件通知检测结果，则可点击[告警通知设置]，跳转到设置界面，可参考“[配置告警通知](#)”章节进行配置。
- 处理方式：此处置机制只会迁移虚拟机的运行位置。启用后，亚健康主机上的虚拟机会往健康主机迁移。

若该虚拟机已有调度策略，则优先按照调度策略进行调度；

若虚拟机无调度策略时，只会将运行位置迁移到其他相对健康的亚健康主机上。若集群内无健康主机时，此处置机制不会生效，此外此机制也不会对NFV设备生效。

- 恢复方式：勾选后，当亚健康主机恢复健康状态后，会自动从亚健康主机列表中移除。

## 8.7. 内存 ECC 隔离

### 8.7.1. 内存 CE 错误隔离

#### 功能说明

当业务或平台进程运行在内存 ECC 错误的内存空间上时，内核会收到内存上报的 ECC 报错信息；深信服超融合平台内存隔离机制将会尝试隔离该内存空间，避免后续业务或者平台进程再次使用该内存空间。

#### 注意事项

内存 ECC 功能需要服务器 CPU 支持 MCE 功能，如涉及到硬件确认，可联系深信服技术支持。

#### 前提条件

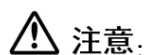
无

#### 操作步骤

1. 登录超融合 HCI 平台，当出现内存 ECC 隔离时，界面会产生告警提示，提示“主机（xxx.xxx.xxx.xxx）的内存条（Px-DIMMxx、Px-DIMMxx）出现内存 ECC CE 可纠正错误过多且无法进行隔”。
- 单个内存条 ECC 隔离地址块数量占比超过 10%，或 1 小时内单个内存条出现 ECC 错误次数超过 2000 次（无论是否隔离成功）时，会产生普通告警提示；
- 单个内存条 ECC 隔离地址块数量占比超过 25%，可用内存很少，或 1 小时内单个内存条出现 ECC 错误次数超过 6000 次（无论是否隔离成功）时，会产生紧急告警提示。



2. 当平台出现告警提示时，建议联系服务商更换内存条。更换内存条时，请将相应主机开启单主机维护模式后再进行更换。

**注意：**

告警提示中的内存条地址是内存条的逻辑地址，需要参照服务器的内存布局示意图才能更换内存条。

## 8.7.2. 内存 UE 错误隔离

### 功能说明

当内存 ECC UE错误的内存空间位于应用层进程时，该物理节点不会宕机，只会杀死该进程，内存隔离机制将会尝试隔离该内存空间；当内存 ECC UE错误的内存空间位于内核层进程时，该物理节点会宕机，重启后超融合平台会收到ECC UE报错信息，内存隔离机制将会尝试隔离该内存空间，避免后续业务或者平台进程再次使用该内存空间。

### 注意事项

内存UE隔离功能对硬件有相关的要求：

1. CPU架构型号：要求为Purley平台。
2. BIOS版本要求：BIOS RC code 610D02 (BKC: Purley BKC IPU 2020.2) 及以上版本。
3. 服务器厂商固件不能屏蔽扫描出来的UE/CE错误和用户态访问触发的UE/CE错误。
4. BIOS功能设置开关：system memory poison -> enabled（UE恢复功能，必须），并开启patrol scrub（内存硬件扫描功能，必须），Patrol Scrub Error Downgrade（错误降级功能，可选）

**注意：**

涉及硬件信息确认，可联系深信服技术支持获取。

### 前提条件

无

### 操作步骤

登录超融合HCI平台，当出现内存ECC隔离时，界面会产生告警提示，提示“主机（xxx.xxx.xxx.xxx）的内存条（Px-DIMMxx、Px-DIMMxx）出现内存ECC UE错误

过多且无法进行隔离”。

|      |                     |    |                                        |               |                                                                                                                               |
|------|---------------------|----|----------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| ● 紧急 | 2021-08-23 13:12:56 | 主机 | 主机 (10.103.128.5) 的内存条 (CPU1-MC0-CH... | 内存ECC不可纠正错误过高 | 主机 (10.103.128.5) 的内存条 (CPU1-MC0-CHAN2-DIMM0) 出现不可纠正ECC (UE) 内存错误, 为保障虚拟机业务的稳定性, 请立即联系服务商更换内存条。更换内存条时, 请相应...                 |
| ● 紧急 | 2021-08-23 10:31:35 | 主机 | 10.103.128.8                           | 内存亚健康 (CE错误)  | 主机 (10.103.128.5) 的内存条 (CPU1-MC0-CHAN2-DIMM0) 出现不可纠正ECC (UE) 内存错误, 为保障虚拟机业务的稳定性, 请立即联系服务商更换内存条。更换内存条时, 请将相应主机开自单主机维护模式后再进行更换。 |

## 8.8. UPS 电源

### 功能说明

HCI主机可关联UPS电源，当市电路故障时，支持给不同重要程度的虚拟机设置不同的关机阈值。默认UPS剩余电量降低到80%时关闭非核心虚拟机，达到30%时关闭核心虚拟机（用户可以根据自己的需求设置触发阈值），达到保护业务的效果。

### 前提条件

平台只能检测到UPS和主机的网络连通状态，请确保主机的电源已接上关联的UPS，并且主机与UPS连接的物理交换机也有电源供电。

### 注意事项

1. 当物理主机同时由市电和UPS电源供电时（如图所示），建议不要启用关机策略，防止当UPS连接的电源断电时，触发联动关机机制。

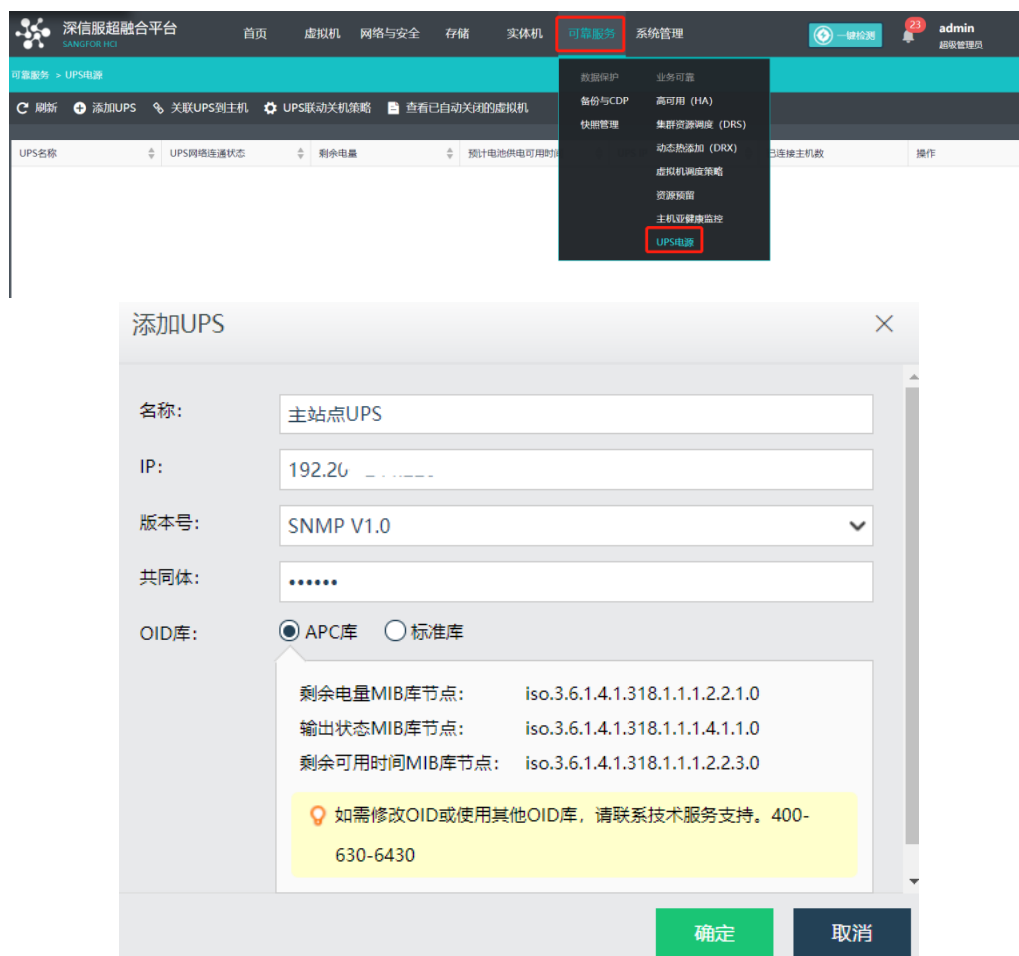


2. 启用关机策略后，当UPS为电池供电且电量小于设定的阈值时，将会关闭与之关联主机上开机运行的虚拟机，但不会关闭物理主机。
3. 当主机关联多台UPS时，关联的UPS需同时处于电池供电，并且电量小于设定阈值才会触发联动关机机制。
4. 如果已启用集群资源调度（DRS），则虚拟机不会调度到由UPS电池供电的物理主机上。

5. 如果UPS在页面已经显示为离线状态，则平台不会对该UPS关联的主机执行联动关机策略。

## 操作步骤

1. 打开控制台，点击[可靠服务/UPS电源]。点击<添加UPS>，可以添加已和HCI集群相连的UPS电源，输入UPS名称、IP、版本号、共同体、选择合适的OID库，点击<确定>，完成添加。



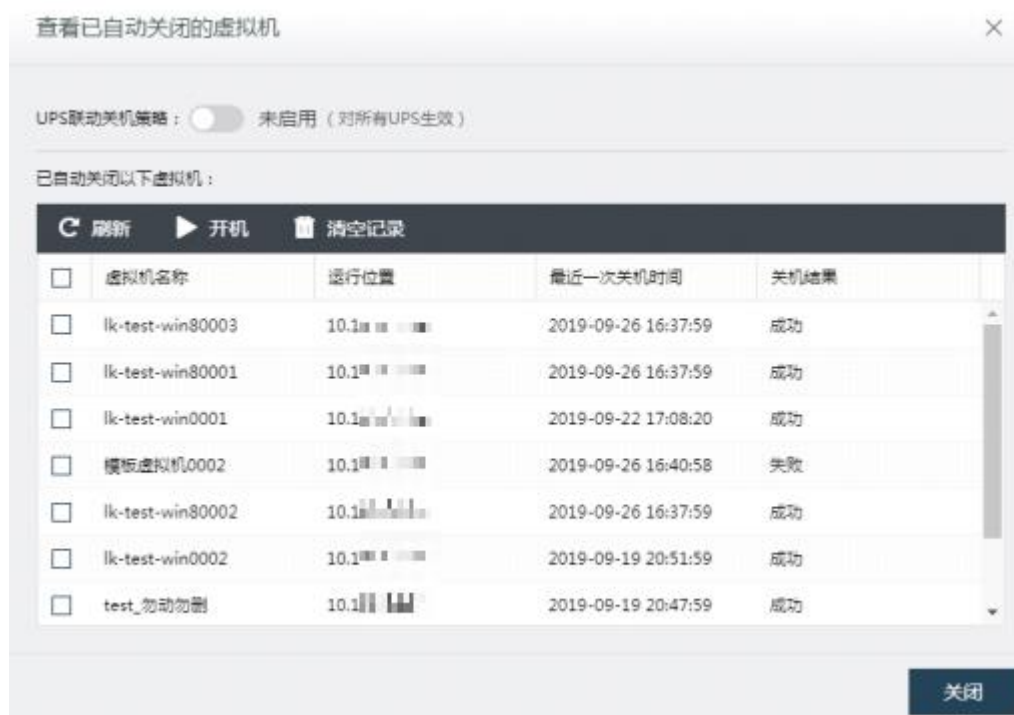
2. UPS电源添加至平台后，点击关联UPS到主机，将UPS与主机关联。



3. 点击<UPS联动关机策略>，可以启用或关闭UPS联动关机策略，并进行具体策略设置，设置第一阶段阈值与第二阶段阈值，可以选择虚拟机为核心虚拟机。



4. 点击<查看已自动关闭的虚拟机>，可以查看已经被关闭的虚拟机，并可在禁用UPS联动策略后，开启虚拟机。



## 8.9. RAID 卡故障处理

### 功能说明

当HCI集群中某一节点RAID卡异常时（如卡慢），会拉低集群存储性能，甚至导致业务/存储卡死。RAID卡故障检测功能可检测到RAID卡异常，及时告警管理员，并能在卡死时将该RAID卡对应的物理主机进行隔离，避免影响整个集群的稳定性，导致整个存储或者集群业务中断。

### 注意事项

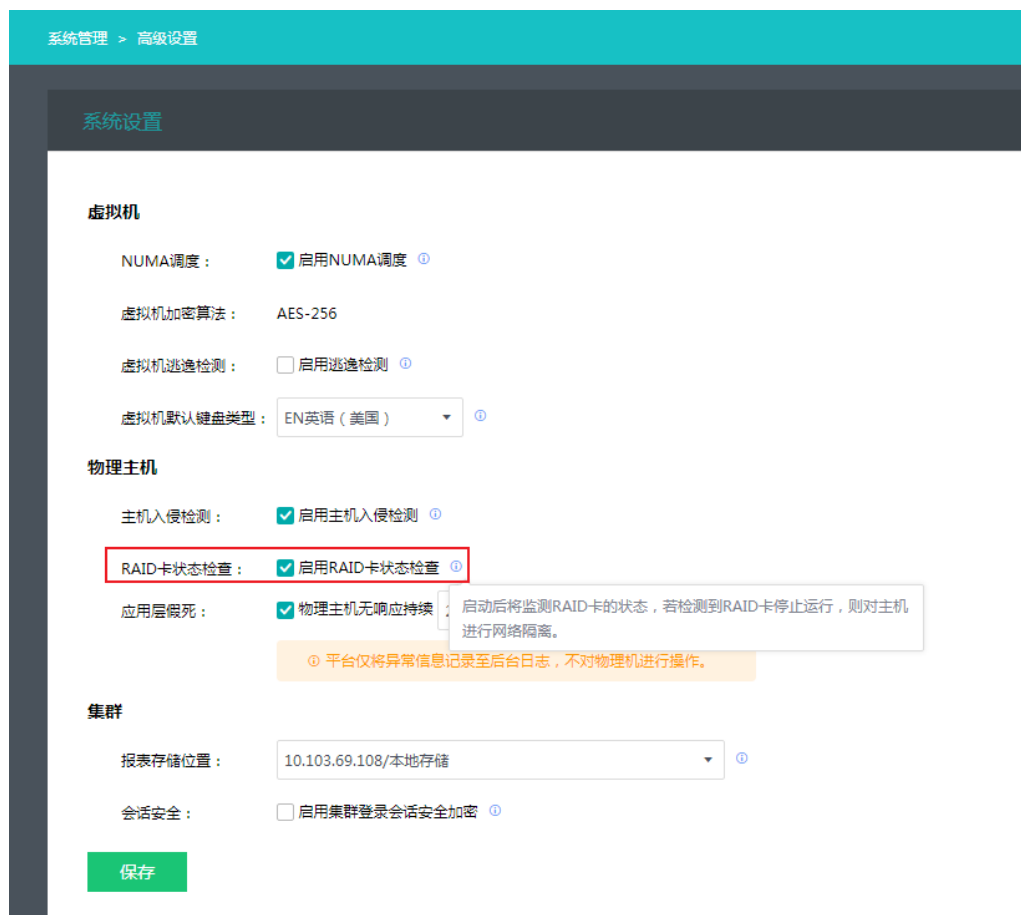
1. 主机需配置IPMI，否则主机被隔离后无法远程恢复。
2. RAID卡死时，告警信息上报可能会失败。
3. 两主机VS集群（未配置仲裁节点的场景下），主机被隔离后可能导致虚拟机脑裂。

### 前提条件

无

### 操作步骤

1. 登录超融合HCI平台，进入[系统管理/高级设置]页面。进入“系统设置/物理主机”目录下，找到“RAID卡状态检查”，勾选“启用RAID卡状态检查”。



2. 当出现内存 RAID 卡故障时，界面会产生告警提示，提示“主机（xxx.xxx.xxx.xxx）的raid卡异常，将对主机进行网络隔离”。该主机被隔离后，其上虚拟机会自动HA，避免整个集群业务中断。



## 8.10. 虚拟机容灾与备份

### 注意事项

1. 数据保护要求的虚拟机开启自动备份策略，并备份到外置存储。
2. 建议使用企业级块、NAS存储。



3. 禁止使用开源软件在服务器上装free NAS做备份。
4. 禁止在低于千兆环境的网络中做iSCSI/NAS备份。
5. 禁止跨广域网做iSCSI/NAS挂载做备份。
6. 禁止Windows文件共享来做备份。
7. 核心业务备份：核心业务必须要做备份，建议1天1备（使用HCI自带备份，或者客户自己的备份软件均可，但一定要有备份）。
8. 备份目标存储空间：建议备份空间利用率低于80%。
9. 虚拟机备份失败情况：若出现备份失败情况，直接联系深信服技术支持（转研发）处理。

## 8.10.1. 快速备份与恢复

### 8.10.1.1. 手动备份

#### 功能说明

该任务指导管理员进行虚拟机手动备份。

#### 注意事项

1. 虚拟机开机或者关机状态下均可备份。
2. 首次备份为完整备份，相同存储位置备份为增量备份。
3. 当备份位置为虚拟存储、FC存储或者iSCSI存储时，支持将备份恢复时将虚拟机快速拉起。
4. 从5.0升级到5.3之后，首次触发备份，旧备份就会移动到回收站，然后才做新的备份。30天之后，回收站的旧备份会被清理掉，但是有新的可用备份了。如果旧备份需要长期保留的需求，建立联系技术支持处理。

#### 前提条件

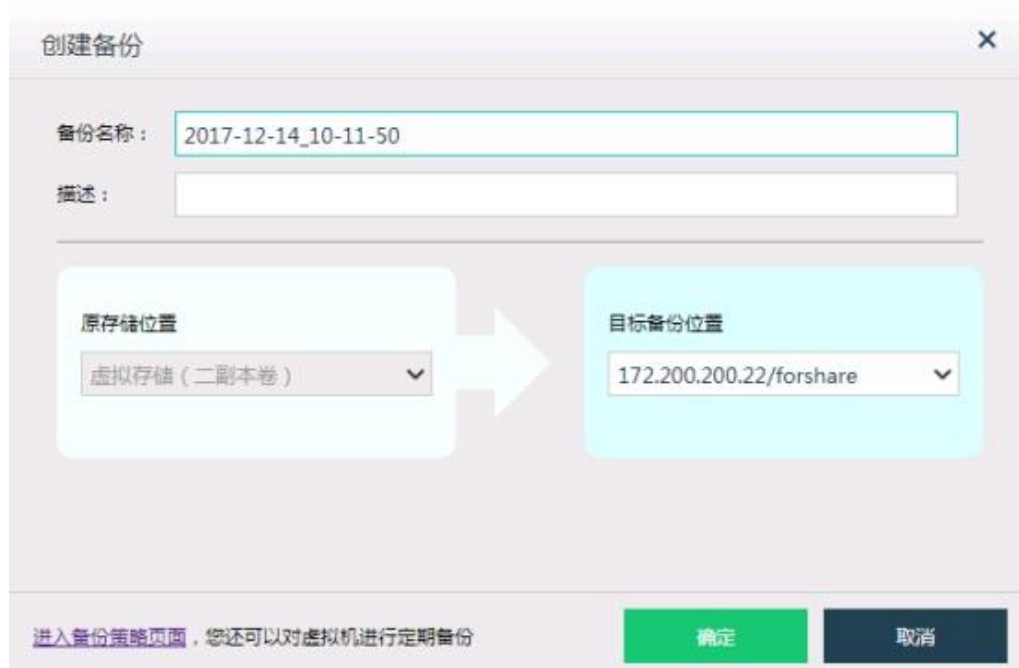
已经配置了备份位置（建议配置第三方备份位置）。

#### 操作步骤

1. 在[虚拟机]页面虚拟机列表中点击更多，弹出虚拟机操作列表。



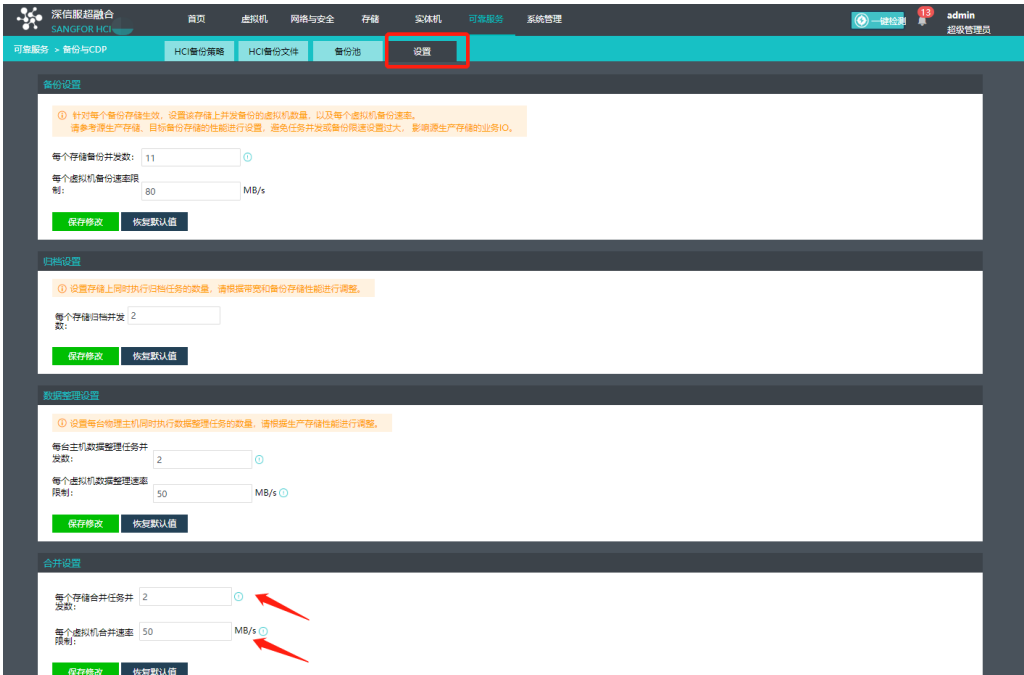
2. 点击<创建备份>，进入创建备份页面并输入自定义备份名称、描述信息并选择目标备份位置。



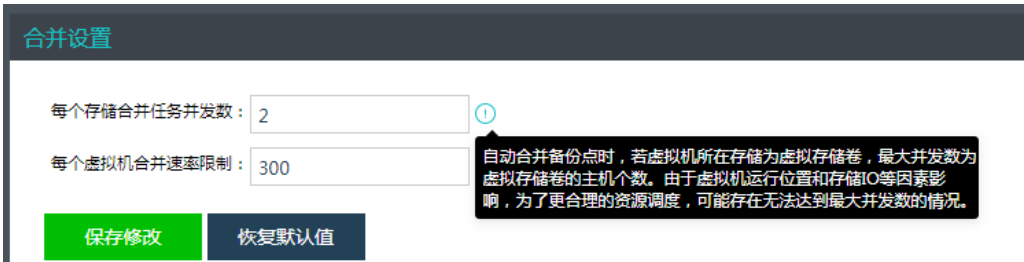
3. 点击<确定>，虚拟机进入备份状态，几分钟后虚拟机完成备份。
4. 在虚拟机[详情状态/备份&CDP]中可查看已创建备份信息。



5. 备份合并限速：从虚拟机备份与恢复中的设置选项进入备份合并限速配置页面。



6. 备份合并限速并发数可配置最大值为16个，速率限制最大可达300MB/S。



### 8.10.1.2. 备份策略备份

#### 功能说明

指导管理员进行虚拟机自动备份操作场景下的自动备份策略配置。备份清理策略设

定更加灵活，备份保留时间最多可以设置为100年。支持按月设置定期全量备份。支持将备份文件自动归档到第二存储中，并可以通过归档文件恢复虚拟机。

## 注意事项

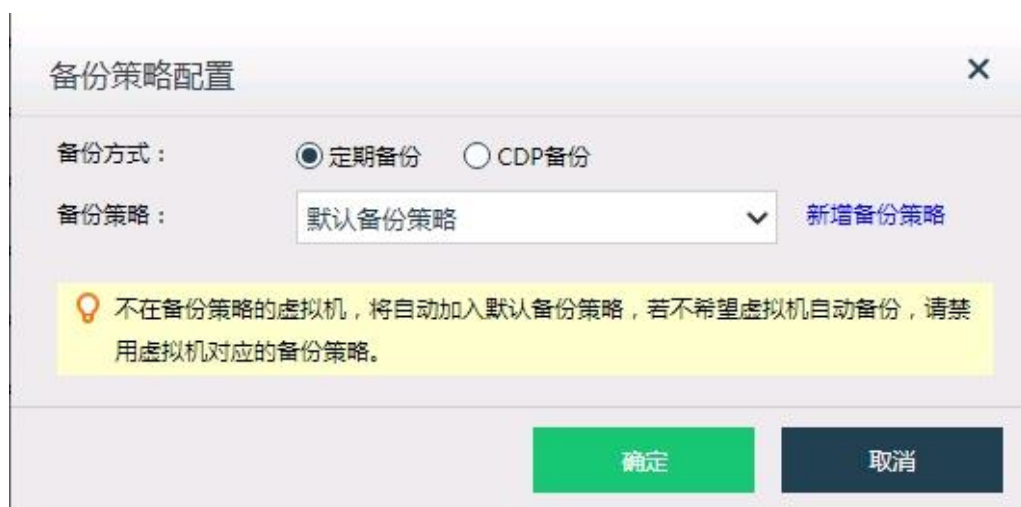
1. 虚拟机开机或者关机状态下均可备份。
2. 第一次备份为全量备份，在备份保留时间周期内其他备份为增量备份。
3. 每个备份保留时间周期内只保留一份全量备份，在下一个备份保留周期开始的时间节点系统会自动将第一次的全量备份和多个增量备份合并为一个新的全量备份。
4. 当备份位置为虚拟存储、FC存储或者iSCSI存储时，支持备份恢复时将虚拟机快速拉起。
5. 每个虚拟机只能加入一个备份策略。
6. 备份归档启用压缩时，压缩归档时间会较未压缩情况增加3倍或更长时间，恢复后的数据整理时间较未压缩增加约3倍或更长时间，建议按实际情况选择是否进行压缩归档。

## 前提条件

1. 已经配置了第三方备份位置（建议配置第三方备份位置）。
2. 使用归档功能时，要求有单独的归档存储，需要到备份池添加存储后再配置归档；归档存储不可选择Windows共享目录以及与备份位置相同的存储。

## 操作步骤

1. 在[虚拟机]页面虚拟机列表中点击虚拟机名称，进入虚拟机信息页面。点击配置[备份&CDP策略]，进入虚拟机备份页面。



**备份策略配置**

备份方式：☒ 定期备份 ☐ CDP备份

备份策略： [新增备份策略](#)

 不在备份策略的虚拟机，将自动加入默认备份策略，若不希望虚拟机自动备份，请禁用虚拟机对应的备份策略。

[确定](#) [取消](#)

2. 备份方式选择“定期备份”，备份策略选择[新增备份策略]，进入备份策略设置页面，设置备份频率、备份日期、持续时长。根据实际需求选择是否勾选“启用定期全量备份”。

### 注意

- 定期全量备份任务的优先级高于普通备份任务。
- 虚拟机即使没有增量数据产生也会按照定期全量备份策略进行备份，且不会被超时取消。
- 启用定期全量备份会消耗更多的存储资源，可能需要较长时间才能完成，并且在此期间无法做增量备份，但是可以减少虚拟机的备份链长度，提升虚拟机恢复后处于数据整理阶段的 IO 性能。

新增备份策略

1 配置备份频率 2 选择虚拟机 3 选择备份位置 4 填写基本信息 5 完成

备份频率: ☒ 按周备份 ☐ 按天备份 ☐ 按小时备份

备份日期: 周五 23:00

持续时长: 48 小时

☐ 超出持续时长后，取消正在执行的备份任务

☒ 启用定期全量备份

1. 定期全量备份任务的优先级高于普通备份任务  
2. 虚拟机即使没有增量数据产生也会按照定期全量备份策略进行备份，且不会被超时取消  
3. 启用定期全量备份会消耗更多的存储资源，可能需要较长时间才能完成，并且在此期间无法做增量备份，但是可以减少虚拟机的备份链长度，提升虚拟机恢复后处于数据整理阶段的IO性能

全量备份月份: 一月,二月,三月,四月,五月,六月,七月,八月,九月,十月,十一月,十二月

全量备份时间: 所选月份的 最后一个 周五 22:00

自动合并备份点，节省存储空间

下一步 取消

3. 在树形结构中选择要备份的虚拟机，点击<下一步>。



4. 选择相应的备份位置，如果集群配置有归档存储，可勾选归档到其他存储，点击<下一步>。



5. 填写备份策略名称和描述信息，点击<下一步>。



6. 确认备份策略的配置情况，如果有误可以返回点击<上一步>进行逐步修改，确认没问题后点<确定>，使自动备份策略生效。



### 8.10.1.3. 备份恢复

#### 功能说明

该任务指导管理员对备份虚拟机行恢复。

#### 注意事项

无

#### 前提条件

1. 需要恢复备份的虚拟机在操作前已有备份文件。
2. 移到回收站的备份文件不支持手动恢复。

#### 注意事项

恢复虚拟机（不论是新建还是覆盖原虚拟机）后磁盘分配模式变成精简分配了，会导致性能下降，可以手动到[虚拟机/编辑/磁盘]进行设置调整为预分配。

#### 操作步骤

1. 在[虚拟机]页面虚拟机列表中点更多，弹出虚拟机操作列表。



2. 点击[备份&CDP]找到该虚拟机的备份文件。



3. 点击<恢复>即可恢复相应的备份文件，可以选择[生成全新虚拟机]或者[覆盖原虚拟机]两种方式进行恢复。



恢复虚拟机

×

1 选择恢复方式

2 配置运行位置

恢复方式:

☒ 生成全新虚拟机 (推荐)

1. 将从该备份点新建一台全新的虚拟机，原有的虚拟机将不受影响。

2. 验证确认内部数据正确之后，可以手动将这台虚拟机替换为生产虚拟机。

3. 为了避免IP地址和现有的虚拟机冲突，需要手动将虚拟机连接到网络中。新生成的虚拟机将会有新的硬件特征，如果虚拟机操作系统或者软件绑定了硬件信息进行授权，需要重新授权，或者使用覆盖原虚拟机方式。

☐ 覆盖原虚拟机

1. 原虚拟机将被关机并删除，30天内可以联系技术支持还原，超期将被自动清理。

2. 此方式不会改变虚拟机的硬件信息，虚拟机操作系统或者软件不需要重新进行授权。

3. 虚拟机恢复完之后，网络会与当前保持一致。

4. 配置了调度策略的虚拟机，从备份恢复虚拟机后，请到虚拟机调度策略页面检查调度策略是否跟运行位置产生冲突。如果产生冲突，请修改虚拟机的运行位置。

下一步

取消

## 8.10.2. CDP 备份与恢复

### 8.10.2.1. 备份策略备份

#### 功能说明

该任务指导管理员进行虚拟机自动备份操作场景下的CDP策略配置。超融合平台提供了虚拟机级别的持续数据保护（CDP）方案，记录重要业务的每一个IO，可以恢复到秒级的完整业务服务器，也可以快速地找回该过去任意一个IO时刻中的业务系统文件。

#### 注意事项

- IO日志最大使用空间计算公式：平均写IO速度 \* 3600（1小时秒数） \* 保留时间（小时数） / 1024 = GB。例如，业务系统平均写IO速度为10MB/s，保留时间为1天，间隔1小时，则IO日志最大使用空间为：10 \* 3600 \* 24 / 1024 = 844 GB。
- HCI集群节点建议3台起步。
- 不支持对虚拟机中映射的裸磁盘进行CDP保护。

文档版本 06（2023-02-21）

356

4. 仅支持将CDP的目的存储配置到iSCSI、FC、aSAN上。
5. 使用CDP功能，如果备份和I/O日志都放在外置存储上面，因为I/O日志和备份抢占空间，导致I/O日志来不及存储，把I/O log buffer耗尽，导致CDP中断，建议备份和日志不放到同一个存储。

## 前提条件

已经配置了第三方备份存储。

## 操作步骤

1. 在[虚拟机]页面虚拟机列表中点击更多，弹出虚拟机操作列表。



2. 点击<配置备份&CDP策略>，进入虚拟机备份页面。

**备份策略配置**

备份方式：☐ 定期备份 ☒ CDP备份

备份策略： [新增CDP策略](#)

IO日志存放位置：

IO日志最大空间： GB

**警告：**不在备份策略的虚拟机，将自动加入默认备份策略，若不希望虚拟机自动备份，请禁用虚拟机对应的备份策略。

[确定](#) [取消](#)

3. 选择[CDP 备份/新增CDP策略]，进入新增CDP策略设置页面，设置备份频率及IO日志保留时间，备份保留时间。

**新增CDP策略**

1 CDP保护配置 — 2 选择云主机 — 3 选择备份位置 — 4 填写基本信息 — 5 完成

IO日志保留时间： (超过保留时间的IO日志将会被自动合并)

IO日志间隔时间：

定期备份频率： [生成一个备份](#)

备份保留时间：

☒ **自动合并备份点，节省存储空间**  
合并超过备份保留时间的备份点，至少保留5个未开启保护的备份文件。  
近3天，保留全部备份点；3天到一周，将每天保留一个备份点；超过一周，只保留周日的备份点。

4. 在树形结构中选择要配置CDP策略的虚拟机，点击<下一步>。



5. 选择相应的备份位置及IO日志存放位置，点击<下一步>。



6. 填写备份策略名称和描述信息，点击<下一步>。



7. 确认备份策略的配置情况，如果有误可以返回点击<上一步>进行逐步修改，确认没问题后点<确定>，使自动备份策略生效。

新增CDP策略

1 CDP保护配置

2 选择云主机

3 选择备份位置

4 填写基本信息

5 完成

备份策略总结

|          |                |
|----------|----------------|
| 名称       | CDP_test       |
| 定期备份频率   | 每隔 1 小时 生成一个备份 |
| 备份保留时间   | 最近两周           |
| 备份存储位置   | 虚拟存储卷1         |
| 首次备份占用空间 | 8 MB           |

|          |              |
|----------|--------------|
| IO日志保留时间 | 最近24小时       |
| IO日志存放位置 | 虚拟存储卷1       |
| IO日志占用空间 | 每个云主机 200 GB |

上一步

确定

取消

8.10.2.2. CDP 恢复系统

功能说明

该任务指导管理员进行对备份文件进行恢复，CDP支持记录业务系统的每一个IO，支持恢复到5秒前的业务系统状态。

注意事项

- 1. 支持将备份恢复时将虚拟机快速拉起。
- 2. 恢复虚拟机（不论是新建还是覆盖原虚拟机）后磁盘分配模式变成精简分配了，会导致性能下降，可以手动到[虚拟机/编辑/磁盘]进行设置调整为预分配。

前提条件

需要恢复备份的虚拟机的在操作前已有CDP备份文件。

操作步骤

- 1. 在[虚拟机]页面虚拟机列表中点击虚拟机名称，进入虚拟机详情状态页面。



2. 点击[备份&CDP]可以找到该虚拟机的备份文件点，点开备份文件点的箭头，可以看到恢复点。



3. 点击<恢复>即可恢复相应的备份文件，可以选择[生成全新虚拟机]或者[覆盖原虚拟机]两种方式进行恢复。

恢复虚拟机

×

1 选择恢复方式

2 配置运行位置

恢复方式:

☒ 生成全新虚拟机 (推荐)

1. 将从该备份点新建一台全新的虚拟机，原有的虚拟机将不受影响。

2. 验证确认内部数据正确之后，可以手动将这台虚拟机替换为生产虚拟机。

3. 为了避免IP地址和现有的虚拟机冲突，需要手动将虚拟机连接到网络中。新生成的虚拟机将会有新的硬件特征，如果虚拟机操作系统或者软件绑定了硬件信息进行授权，需要重新授权，或者使用覆盖原虚拟机方式。

☐ 覆盖原虚拟机

1. 原虚拟机将被关机并删除，30天内可以联系技术支持还原，超期将被自动清理。

2. 此方式不会改变虚拟机的硬件信息，虚拟机操作系统或者软件不需要重新进行授权。

3. 虚拟机恢复完之后，网络会与当前保持一致。

4. 配置了调度策略的虚拟机，从备份恢复虚拟机后，请到虚拟机调度策略页面检查调度策略是否跟运行位置产生冲突。如果产生冲突，请修改虚拟机的运行位置。

下一步

取消

### 8.10.3. 文件恢复

#### 功能说明

该任务指导管理员进行对备份文件进行浏览和下载。

#### 注意事项

1. 当前仅支持Windows的NTFS、FAT32文件系统格式和Linux系统的ext2、ext3、ext4、xfs文件格式找回文件。
2. 无法支持package\_name的中存在特殊字符，如%，&为文件名
3. 虚拟机的备份在sffs存储时，虚拟机的软连接文件链接到/proc，/run目录下不支持文件下载
4. 当虚拟机中选择的待下载文件大于5G时不支持下载。
5. 当虚拟机使用物理盘时，物理盘不支持文件浏览。

#### 前提条件

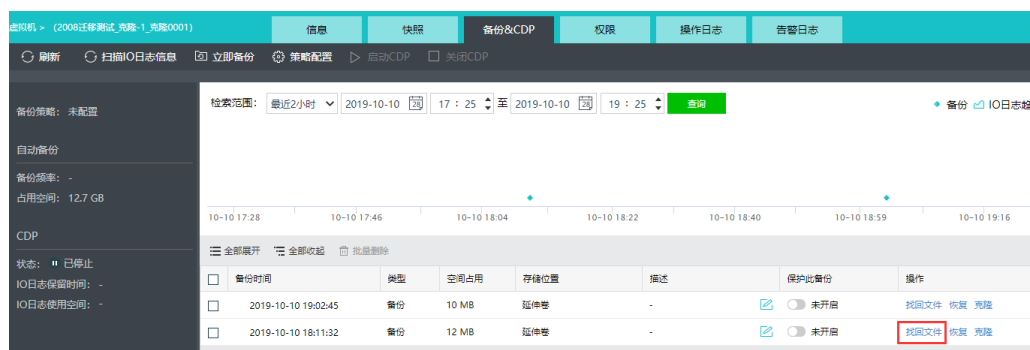
需要浏览或下载文件的虚拟机在操作前已有备份文件。

## 操作步骤

4. 在[虚拟机]页面虚拟机列表中点击虚拟机名称，进入虚拟机详情状态页面。



5. 点击[备份&CDP]可以找到该虚拟机的备份文件点，点开备份文件点的箭头，可以看到恢复点。

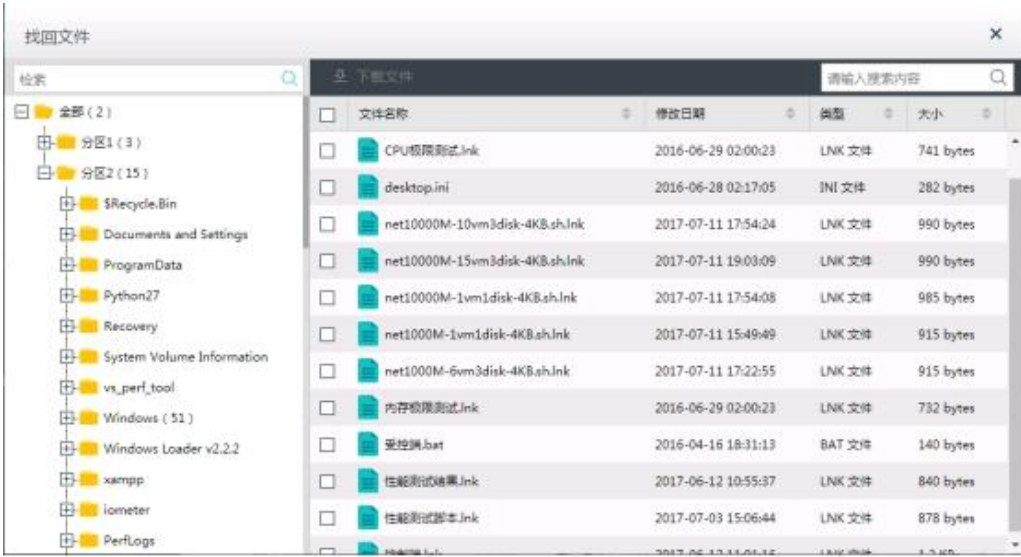


6. 点击[找回文件]会弹出如下提示框，选择<确定>。



7. 可以看到[找回文件]的下载页面，可以通过查找文件的下载路径或者搜索文件名，找到需要下载的文件，点<下载文件>即可。





8.10.4. 备份管理

功能说明

该任务指导管理员进行对备份文件、备份池、备份策略进行管理。

注意事项

无

前提条件

无

操作步骤

8.10.4.1. HCI 备份策略

功能说明

该任务指导管理员在HCI平台上创建和管理备份策略。

注意事项

无

前提条件

无

操作步骤

- 1. 在[可靠服务/备份与CDP]，进入备份管理页面。
- 2. 在[HCI备份策略]开启或者关闭当前备份策略，并对现有备份策略进行增删改查。



8.10.4.2. HCI 备份复制策略

功能说明

指导管理员创建和管理备份复制策略。

注意事项

- 1. 备份复制的目的存储不支持为本地存储。
- 2. 备份复制的源存储和目的存储不支持为同一个存储。
- 3. 备份复制个数不做限制，可以在多个外置存储上创建多个备份复制策略。

前提条件

无

操作步骤

- 1. 在[可靠服务/备份与CDP]，进入备份管理页面。
- 2. 在[HCI备份复制策略]中开启或者关闭当前备份复制策略，并对现有备份复制策略增删改查。



8.10.4.3. VMware 备份策略

功能说明

指导管理员创建和管理VMware备份策略。

注意事项

无

前提条件

无

操作步骤

在[可靠服务/备份与CDP]，进入备份管理页面。



8.10.4.4. HCI 备份文件

功能说明

用于对集群中的虚拟机备份文件进行管理，可通过备份文件恢复虚拟机或对备份文件进行复制。

注意事项

无

前提条件

无

操作步骤

- 1. 在[可靠服务/备份与CDP]，进入备份管理页面。

2. 在[HCI备份文件]中查看当前HCI平台中的虚拟机的备份文件。



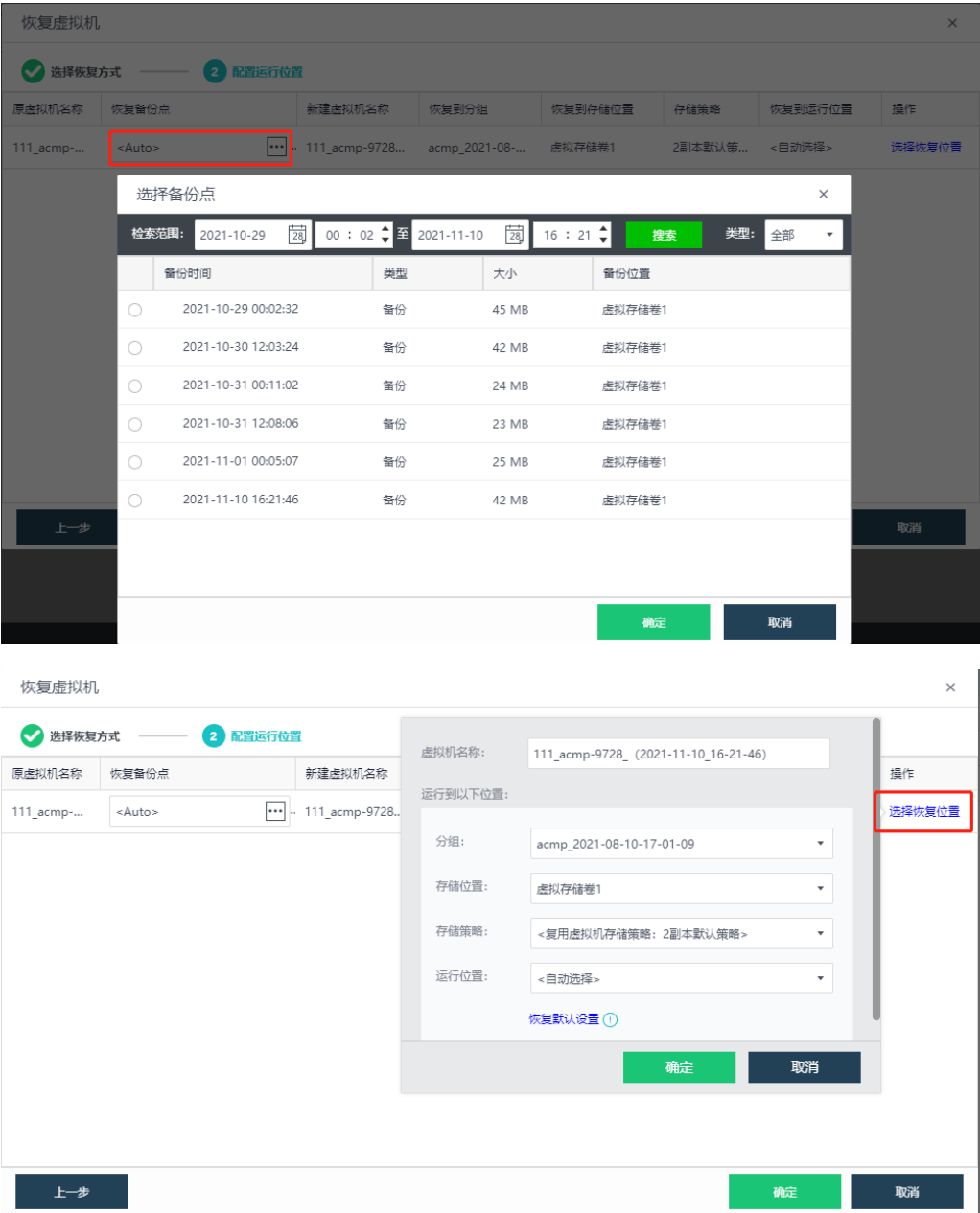
3. 勾选需要操作的虚拟机，并点击<恢复>。



4. 选择虚拟机恢复方式，并点击<下一步>。



5. 选择虚拟机的恢复备份点和恢复位置，并点击<确定>完成恢复。



### 8.10.4.5. VMware 备份文件

#### 功能说明

用于对集群中纳管的VMware上的虚拟机备份文件进行管理，可通过备份文件恢复虚拟机或对备份文件进行复制。

#### 注意事项

无

#### 前提条件

无

操作步骤

在[可靠服务/备份与CDP]，进入备份管理页面。



8.10.4.6. 备份池

功能说明

备份池是指备份的存储系统，存储当前的虚拟机文件。备份池推荐使用aSAN分布式存储，但是需要指定使用容量空间，以便分布式存储对其进行隔离管理。鼠标点到备份空间上，可以对备份空间进行设置。可添加存储介质进入备份资源池。

注意事项

无

前提条件

无

操作步骤

- 1. 在[可靠服务/备份与CDP]，进入备份管理页面。
- 2. 在[备份池]中查看当前备份容量使用情况。



- 3. 点击<新增/添加现有存储到备份池>。



4. 勾选需要添加进备份池的存储，并设置用于备份的空间大小，点击<确定>完成资源池添加。



8.10.4.7. 设置

功能说明

可对备份任务进行设置。

- **存储备份：**设置存储备份时的最大任务并发数。
- **存储备份复制：**设置存储备份复制时的最大任务并发数。
- **存储归档：**设置存储归档时的最大任务并发数。
- **每台主机数据整理任务数：**设置每台主机数据整理任务的最大并发数，。
- **存储合并：**设置存储合并时的最大任务并发数，在自动合并备份点时，若虚拟机所在存储为虚拟存储卷，最大并发数为虚拟存储卷的主机个数。
- **备份限制：**限制虚拟机备份时的最大备份速率。
- **每个主机数据整理速率限制：**限制每台数据数据整理最大速率，快速恢复的虚拟机，在闪电图标消失前，会限制虚拟机的数据整理速率，以免影响虚拟机性能。
- **合并限制：**限制虚拟机数据合并时的最大速率，设置为 0 时为不限制。

注意事项

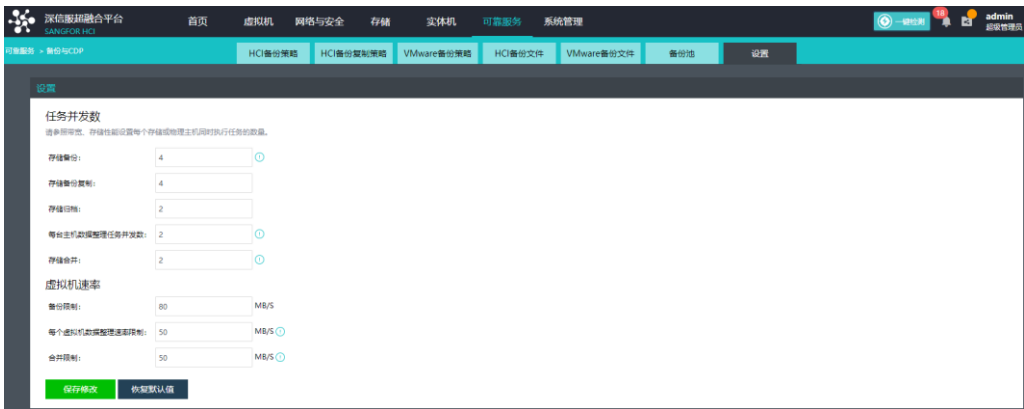
无

前提条件

无

操作步骤

- 1. 在[可靠服务/备份与CDP]，进入备份管理页面。
- 2. 在[设置]中可以调整每个存储的备份、恢复、合并任务并发数与速率。



8.11. GPU 虚拟机调度

功能说明

HCI6.8.0及其之后的版本支持设置GPU虚拟机开机调度模式：

- 密度模式：优先运行在已有正在运行的 GPU 虚拟机的物理主机上，确保资源能够被充分利用。
- 性能模式：将 GPU 虚拟机均衡分布在对应的不同显卡上，尽可能保障每一台 GPU 虚拟机性能最佳。

注意事项

无

前提条件

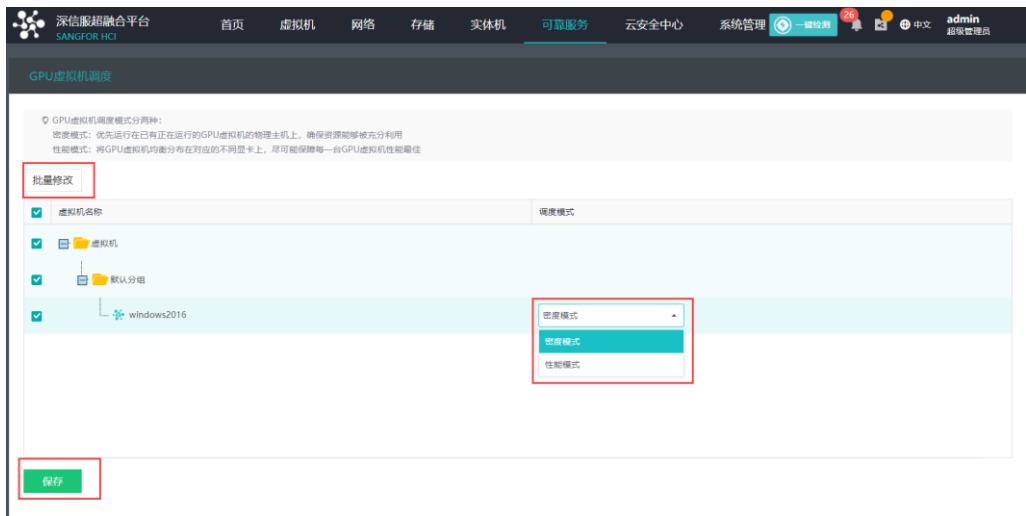
无

操作步骤

进入[可靠服务/GPU虚拟机调度]页面，选择需要修改调度方式的虚拟机进行修改后，点击<保存>；如需将多台虚拟机的调度方式设置为同一种，则可点击上方<批量修改>



按钮，进行批量修改。



## 9. 云安全中心配置指导

深信服云安全中心基于统一的安全策略和安全管理构建云上统一安全平台；基于资产的精准识别，对不同业务进行针对性保护；安全能力自适应开启，无需部署，与平台能力深度融合。

### 9.1. 查看平台安全状态

#### 功能说明

云安全中心的总览页面能够展示平台安全概览信息，包括虚拟机是否开启安全防护、待处置安全事件数量、云安全中心自上线以来已自动处置的安全事件数量、30天内安全事件概览。

#### 前提条件

无

#### 注意事项

已自动处置的安全事件每天0点进行更新，暂不支持实时更新。

#### 操作步骤

1. 进入[云安全中心/总览]页面，可以查看到平台安全概览信息，页面上方分别展示了平台虚拟机总数、已开启安全防护的虚拟机数量、存在安全事件的虚拟机数量、安全防护被恶意破坏的虚拟机数量、未开启安全防护的虚拟机数量，点击对应的数字可直接跳转到虚拟机安全列表，查看详细内容。



2. [待处置安全事件]展示了平台未进行处置的安全事件数量，包括暴力破解攻击数量、WebShell后门攻击数量、挖矿病毒数量、疑似勒索病毒数量。



3. [安全防御]通过深信服人工智能检测引擎、基因特征检测引擎、行为分析检测引擎、云查杀检测引擎四大检测机制，自动检测并处置虚拟机的安全事件。



4. [安全事件概览]展示近30天内安全事件数量概览、漏洞类型数量概览，同时也支持按安全事件类型、漏洞类型进行筛选。



## 9.2. 虚拟机安全

- 云安全中心支持统一资产管理，显示 HCI 平台全部虚拟机，及虚拟机基础信息与安全信息，无需复杂盘点，不会遗漏资产。
- 云安全中心支持对特定虚拟机下发安全扫描任务，提供病毒处置策略：处置、信任、恢复、取消信任、忽略。
- 云安全中心支持安全事件一键处置，提供安全事件从网络隔离、快照兜底，病毒处置的全栈的向导化处置。
- 云安全中心提供勒索应急恢复能力，支持勒索病毒从紧急隔离到恢复网络全流程向导式勒索应急恢复，无需专家介入即可快速安全的恢复业务。

## 9.2.1. 资产管理

### 功能说明

资产管理支持自动获取虚拟机的基础信息和安全信息，包括：安全状态、运行状态、虚拟机名称、IP地址、操作系统、应用以及安全事件。

### 前提条件

无

### 注意事项

1. 资产信息上报有时间间隔，基础信息上报时间间隔是1分钟，安全信息上报时间间隔是5分钟，应用信息上报时间间隔是4小时。
2. 虚拟机列表默认按照安全状态排序，排序规则为：恶意破坏-高危-中危-防护离线-低危-未防护-防护中，其中：当安全状态相同时，按应用信息排序：数据库-web-未识别出的应用。

### 操作步骤

1. 进入[云安全中心/虚拟机安全]页面，支持按照不同的分类进行平台资产管理：
  - 存在疑似勒索病毒：存在未处置疑似勒索病毒的虚拟机列表。
  - 安全防护被恶意破坏：安全状态为恶意破坏的虚拟机列表，即当虚拟机安全组件受到恶意破坏时，虚拟机安全状态会显示为“恶意破坏”。
  - 存在安全事件：存在未处置安全事件的虚拟机列表。
  - 未防护：安全状态为未防护的虚拟机列表。
  - 已隔离：被隔离的虚拟机列表。



2. 在 [云安全中心/虚拟机安全/全部虚拟机] 页面，可以查看到当前超融合平台全部虚拟机运行状态和信息状态。

- 安全状态包括：恶意破坏、高危、中危、低危、防护离线、未防护、防护中。

恶意破坏：安全防护被恶意破坏，一般是由勒索事件引发。

高危：存在高威胁病毒等高危安全风险。

中危：存在中威胁病毒、暴力破解等中危安全风险。

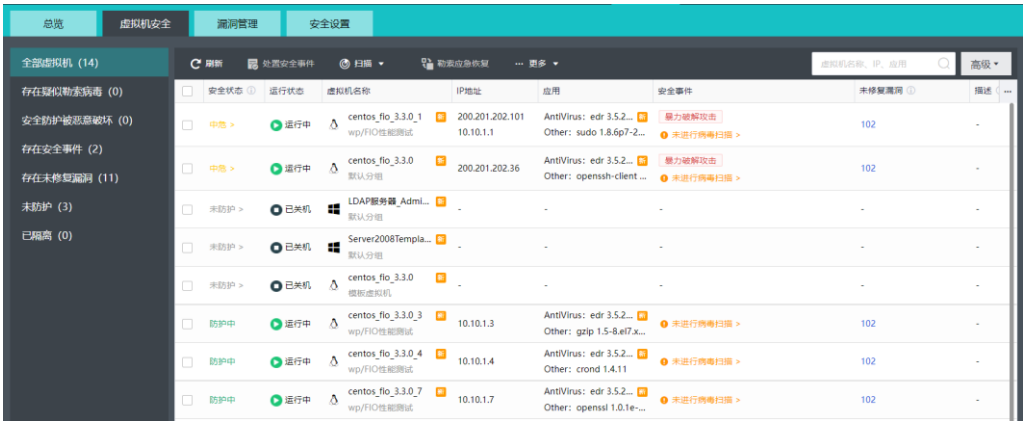
低危：存在低威胁病毒等低危安全风险。

防护离线：安全组件离线，一般是由网络故障、虚拟机或安全组件处于启动状态等原因导致。

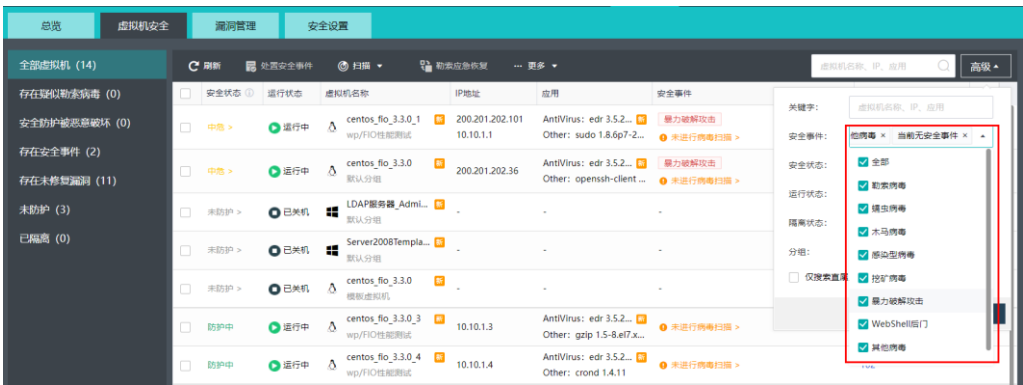
未防护：安全防护未开启。

防护中：虚拟机受安全功能保护。

- 运行状态包括：运行中、已挂起、已关机。
- 安全事件包括：勒索病毒、蠕虫病毒、木马病毒、感染型病毒、挖矿病毒、暴力破解攻击、WebShell 后门、其他病毒、当前无安全事件。



3. 点击<高级>按钮，支持按照不同分类筛选虚拟机列表。



## 9.2.2. 病毒/漏洞扫描

### 功能说明

云安全中心通过深信服人工智能检测引擎、基因特征检测引擎、行为分析检测引擎、云查杀检测引擎四大检测机制，支持对虚拟机下发病毒扫描、漏洞扫描任务，发现病毒或漏洞，进行安全处置。

### 前提条件

无

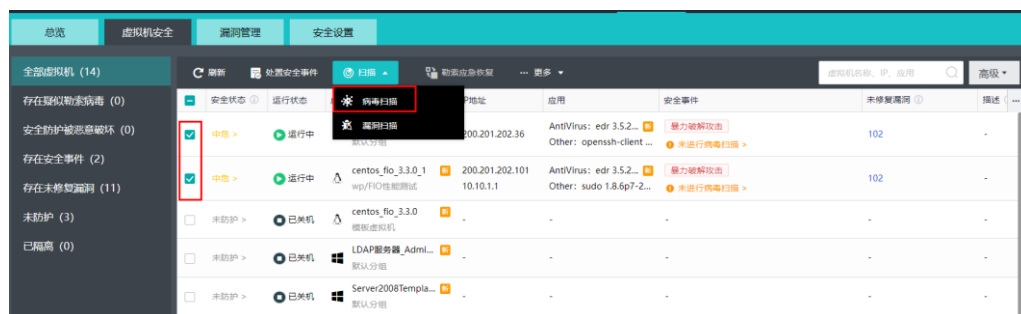
### 注意事项

1. 最多可支持选择100台虚拟机同时进行病毒扫描。
2. 病毒扫描记录中仅保存近30天内的扫描记录。
3. 病毒扫描将占用一定的CPU、内存，建议选择业务空闲时段进行扫描。
4. 平台当前仅支持针对Windows漏洞进行修复处理，暂不支持对Linux系统漏洞、应用漏洞自动修复。

## 操作步骤

### 一、病毒扫描

1. 在[虚拟机安全]列表中，选择需要进行病毒扫描的虚拟机，点击<扫描/病毒扫描>按钮。



2. 选择扫描方式。

- 快速扫描：扫描系统关键目录、关键注册表项、内存和系统运行进程等，扫描时间较快；
- 全盘扫描：扫描系统内存、系统运行进程、关键注册表项和所有磁盘分区文件，扫描时间相对较长。



3. 待扫描完成后，点击 [更多/病毒扫描记录] 进入扫描结果页面。

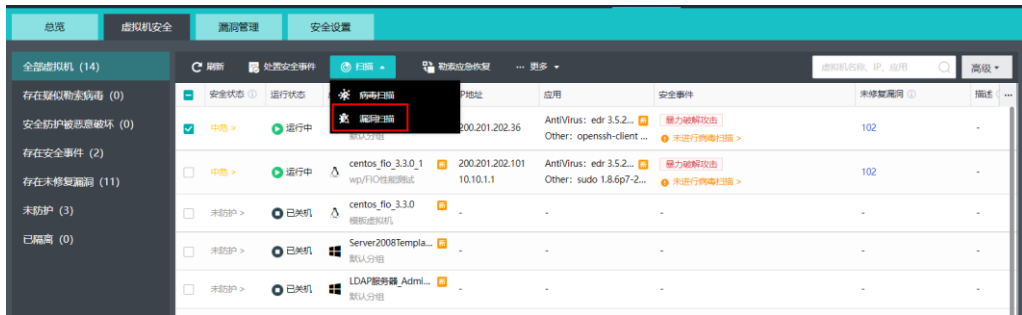


4. 在扫描记录中选择虚拟机点击<查看详情>，可对该次扫描任务发现的病毒进行处理：处置，信任，恢复，取消信任，忽略。

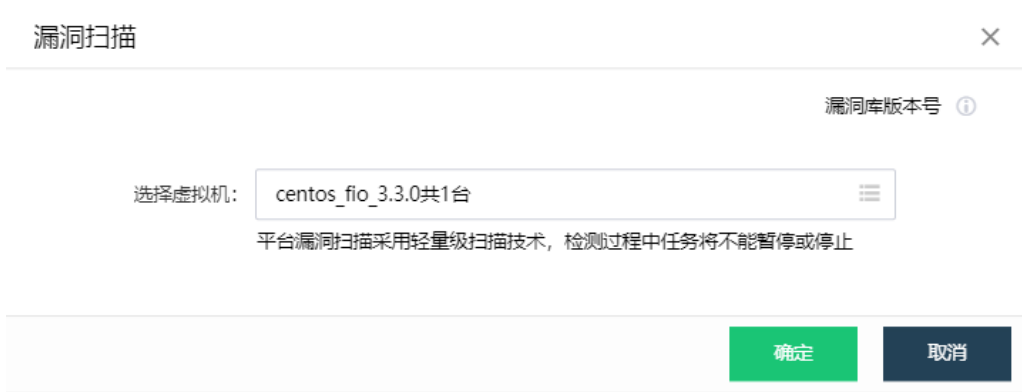


## 二、漏洞扫描

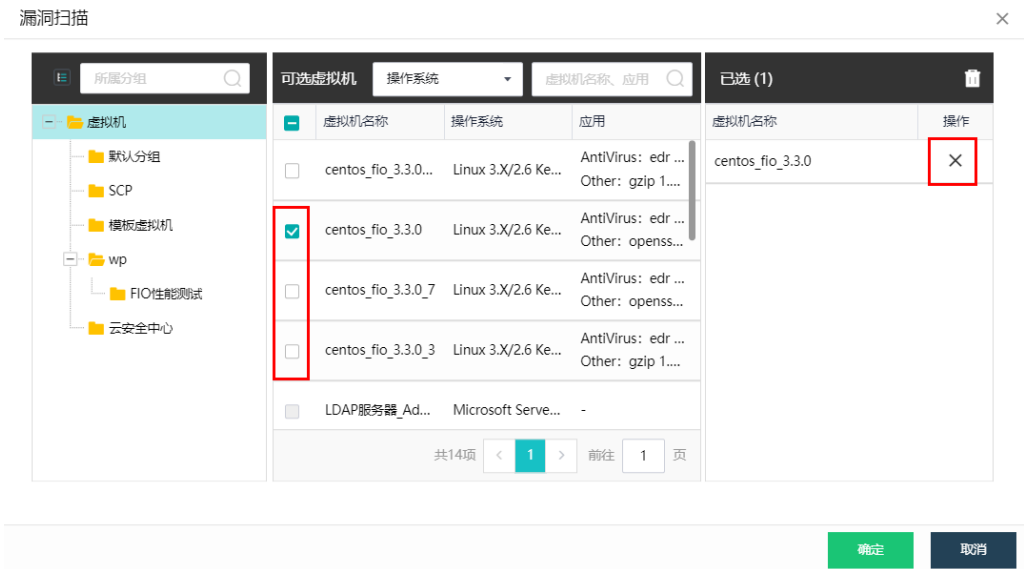
1. 在[虚拟机安全]列表中，选择需要进行漏洞扫描的虚拟机，点击<扫描/漏洞扫描>按钮。



2. 进入[漏洞扫描]页面，可以继续添加或删除需要进行漏洞扫描的虚拟机。



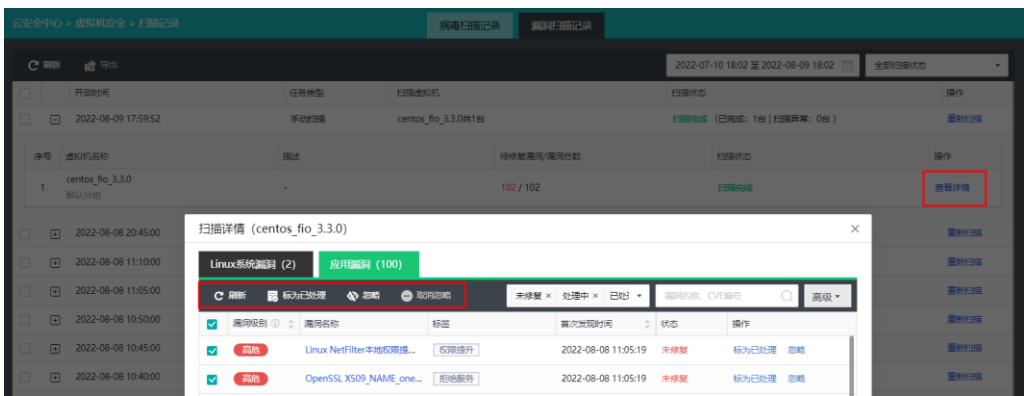




5. 待扫描完成后，点击 [更多/漏洞扫描记录] 进入扫描结果页面。



6. 在扫描记录中选择虚拟机点击<查看详情>，可对该次扫描任务发现的漏洞进行处理，其中Windows漏洞可进行标记为已处理、忽略、修复等操作，Linux系统漏洞、应用漏洞可进行标记为已处理、忽略等操作。



### 9.2.3. 紧急隔离

#### 功能说明

当发生病毒危害后，为了防止病毒扩散，云安全中心提供了紧急隔离的能力，对于已经被加密的资产可以秒级完成隔离，确保病毒不会再进行扩散。

## 前提条件

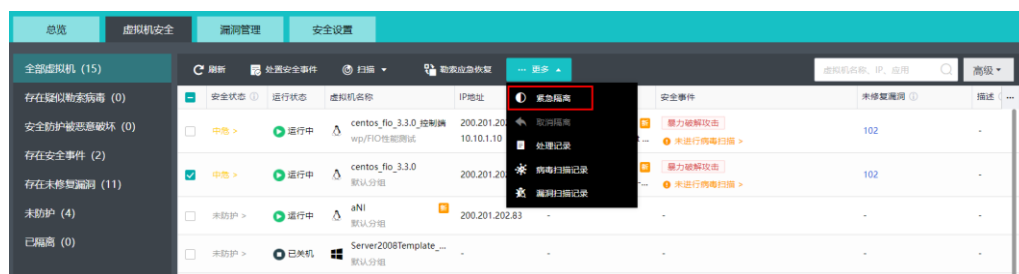
无

## 注意事项

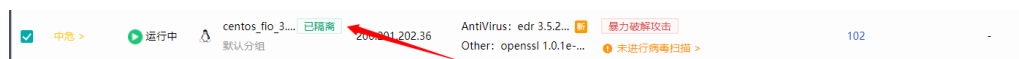
1. 紧急隔离会将虚拟机网络彻底断开，造成中断业务；对于重要业务，可前往“分布式防火墙”配置策略，以达到不中断业务且隔离风险的效果。
2. 紧急隔离的虚拟机会加入云安全中心网络隔离策略，若虚拟机直连物理出口，则策略不生效。

## 操作步骤

1. 在[虚拟机安全]列表中，勾选有病毒扩散风险的虚拟机，点击<更多/紧急隔离>。



2. 隔离完成后虚拟机将变为“已隔离”状态。



3. 当已隔离虚拟机消除风险，可以解除隔离时，点击<更多/取消隔离>即可。



## 9.2.4. 勒索应急恢复

### 功能说明

1. 云安全中心提供向导化的勒索应急恢复流程，无需专家介入即可快速安全的恢复业务。
2. 云安全中心采用链接克隆的方式进行业务验证，能够秒级完成创建，过程中不额外占用存储空间，环境完全独立，过程中恢复到带毒时间点也不会导致病毒

扩散。

3. 在确定恢复点并执行恢复后，整个过程被加密资产与其他资产严格隔离，恢复完成病毒查杀确认安全后才解除隔离上线。

前提条件

无

注意事项

勒索应急恢复的快照数据与当前数据存在时间差，回滚快照会造成数据丢失。在正式业务场景下，请评估勒索影响决定是否回滚快照。

操作步骤

1. 在[虚拟机安全]列表中，勾选存在勒索病毒的虚拟机，点击<勒索应急恢复>。



2. 首先需对虚拟机进行紧急隔离操作，以防止勒索行为进一步横向扩散。点击<紧急隔离>按钮，完成隔离后，点击<下一步>。

勒索应急恢复 (sec\_test)

1 紧急隔离

2 保留当前状态

3 恢复虚拟机

4 扫描病毒

5 恢复网络

被勒索

隔离前

隔离开启

被勒索

隔离后

若虚拟机被勒索，出现加密情况，请立即点击紧急隔离按钮对网络进行隔离，以防止勒索行为进一步横向扩散 ①

紧急隔离

下一步

取消

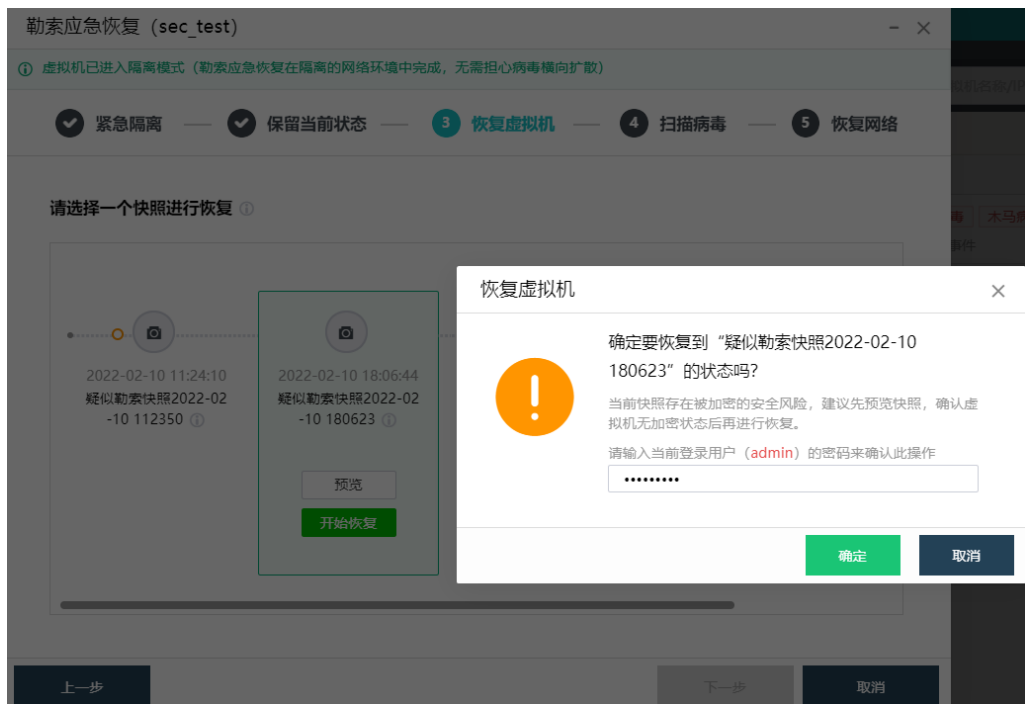
文档版本 06（2023-02-21）

382

3. 在进行勒索应急恢复前，点击<创建快照>按钮，为虚拟机打快照，恢复完成之后能够尝试通过此快照找回加密数据。



4. 快照创建完成后，点击<下一步>，对虚拟机进行恢复。这里会展示该虚拟机的全部快照，当平台检测到资产安全防护组件异常、疑似中勒索病毒时会自动触发快照，创建名为“疑似勒索快照XXX”的快照，点击<预览>按钮，平台将新建链接克隆虚拟机，克隆完成后，点击<控制台>按钮，进入虚拟机内部，可以查看该虚拟机是否被加密，若未被加密，则点击<开始恢复>，输入admin密码进行恢复。



5. 点击<确定>按钮后, 平台会自动删除上一步预览时创建的所有链接克隆虚拟机后, 恢复所选择的虚拟机快照。

任务列表

| 全部任务                       |         |                  |                     |      |                          |                                       |  |
|----------------------------|---------|------------------|---------------------|------|--------------------------|---------------------------------------|--|
| 状态                         | 动作      | 对象               | 开始时间                | 结束时间 | 操作人                      | 操作                                    |  |
| <div><div></div></div> 20% | 关闭虚拟机电源 | sec_test_克隆      | 2022-02-14 20:17:12 |      | admin( 10.103.212.203 )  | <a href="#">查看</a> <a href="#">取消</a> |  |
| <div><div></div></div> 20% | 关闭虚拟机电源 | sec_test_克隆_1... | 2022-02-14 20:17:05 |      | admin( 10.103.212.203 )  | <a href="#">查看</a> <a href="#">取消</a> |  |
| <div><div></div></div> 90% | 新建虚拟机快照 | sec_test         | 2022-02-14 20:16:54 |      | admin( 10.103.212.203 )  | <a href="#">查看</a> <a href="#">取消</a> |  |
| <div><div></div></div> 10% | 恢复虚拟机快照 | sec_test         | 2022-02-14 20:16:51 |      | admin( 10.103.212.203 )  | <a href="#">查看</a> <a href="#">取消</a> |  |
| <div><div></div></div> 0%  | 删除快照预览  | sec_test         | 2022-02-14 20:16:34 |      | admin( 192.200.114.114 ) | <a href="#">查看</a> <a href="#">取消</a> |  |
| <div><div></div></div> 0%  | 删除快照预览  | sec_test         | 2022-02-14 20:16:34 |      | admin( 192.200.114.114 ) | <a href="#">查看</a> <a href="#">取消</a> |  |
| <div><div></div></div> 0%  | 删除快照预览  | sec_test         | 2022-02-14 20:16:33 |      | admin( 192.200.114.114 ) | <a href="#">查看</a> <a href="#">取消</a> |  |

6. 快照恢复后点击<下一步>, 进入病毒扫描页面。这里建议对恢复后的虚拟机再次进行全盘扫描, 若发现安全事件, 可以立即处置。



7. 对于扫描出来的安全事件, 可以点击上方<处置>/<信任>/<忽略>按钮, 进行安全事件处置, 建议安全事件处置完成后点击<重新扫描>按钮, 再次进行病毒扫描, 确认所有安全事件均已处置完毕后, 点击<下一步>进入网络恢复。



8. 在恢复网络前, 由于当前虚拟机数据已恢复, 为避免二次感染, 建议排查并确

认相连的其他虚拟机安全状态无误后，再点击<恢复网络>按钮。网络恢复后，虚拟机将退出隔离模式。



9.2.5. 安全事件处置

功能说明

- 1. 云安全中心提供安全事件从网络隔离、快照兜底，病毒处置的全栈的向导化处置。
- 2. 网络隔离采用SDN能力的微隔离方案，无需修改任何guest内网络配置，对其他业务无影响，秒级完成。
- 3. 处置过程保证异常发生最小的RPO和RTO。云安全中心提供文件的处置前的灭活隔离，将该文件封存在一个独立的沙箱内。同时在处置之前，会自动进行一个快照，即使发生了误删除，可以快速通过恢复文件让业务正常，若系统崩溃无法进行开机时，也可以通过快照快速的恢复。

前提条件

无

注意事项

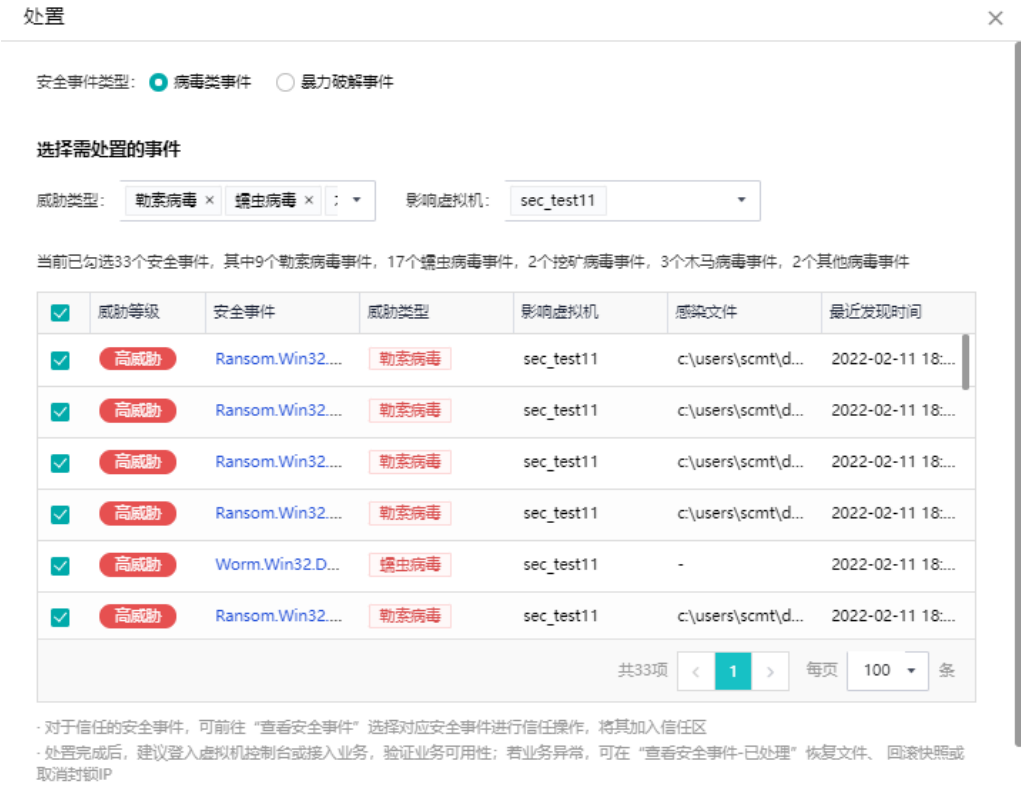
无

操作步骤

1. 在[虚拟机安全]列表中，勾选需要进行安全处置的虚拟机，点击<处置安全事件>按钮。



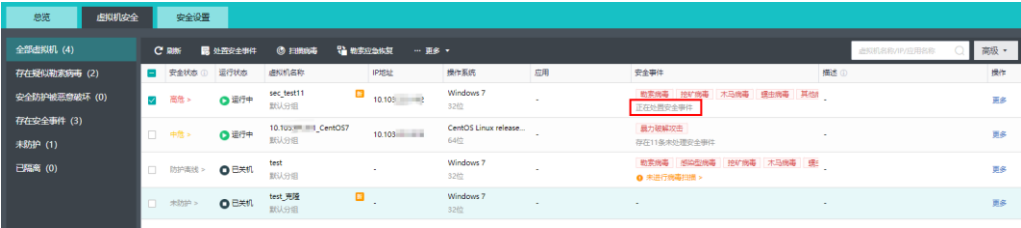
2. 进入[处置]页面：
- 安全事件类型分为：病毒类事件，暴力破解类事件。
  - 威胁类型：默认全选，也可单独针对某个或几个类型的事件进行筛选。
  - 需要处置的安全事件：默认全选，也可单独针对某个或某几个安全事件进行筛选。
  - 执行处置前先快照：默认关闭，执行安全事件处置前可手动开启，开启后将会对虚拟机自动打快照。注意：若同时对多台虚拟机创建快照可能会影响业务性能，建议在业务低峰期执行。
  - 快照虚拟机：开启快照保护开关后，可选择需打快照的虚拟机，最多支持选择10台虚拟机。







3. 选择并确认上述信息后，点击<确认>按钮，执行处置。

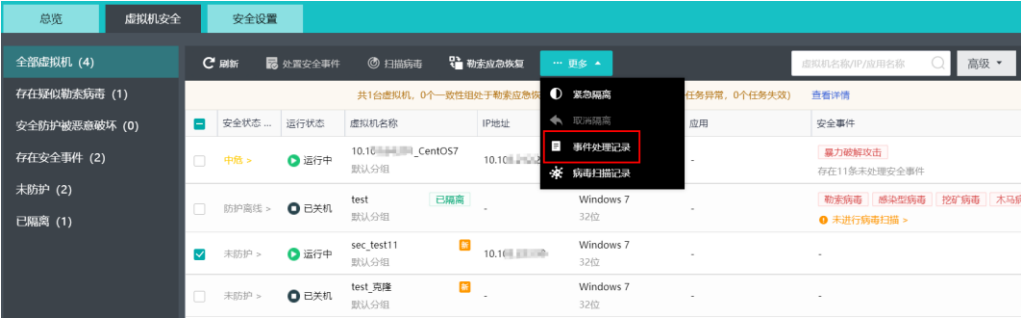


4. 处置完成后，虚拟机安全状态恢复。



5. 点击<更多/事件处置记录>，进入[已处理]列表，可以查看到上述处置的安全事件。若安全事件处置完成后业务异常，可点击<恢复>按钮：

- 恢复文件：所选择文件将会恢复到原位，该操作会覆盖已存在的同名文件，并且无法保证恢复此文件的安全性，默认恢复后所选择文件将会被标记为信任文件，请谨慎操作。
- 恢复快照：选择虚拟机快照进行恢复。注意：若进行快照恢复，虚拟机将恢复到所选时间点的状态，需确保已对虚拟机的数据进行了快照或备份，否则未被保护的数据将会丢失；恢复过程会对虚拟机进行关机，将造成业务中断，请选择业务低峰期恢复。





## 9.2.6. 查看安全事件/漏洞信息

### 功能说明

1. 云安全中心支持对虚拟机的安全事件进行处置、恢复、信任、取消信任、忽略处理。
2. 云安全中心支持对虚拟机的漏洞进行标记为已处理、忽略、修复等操作。

### 前提条件

无

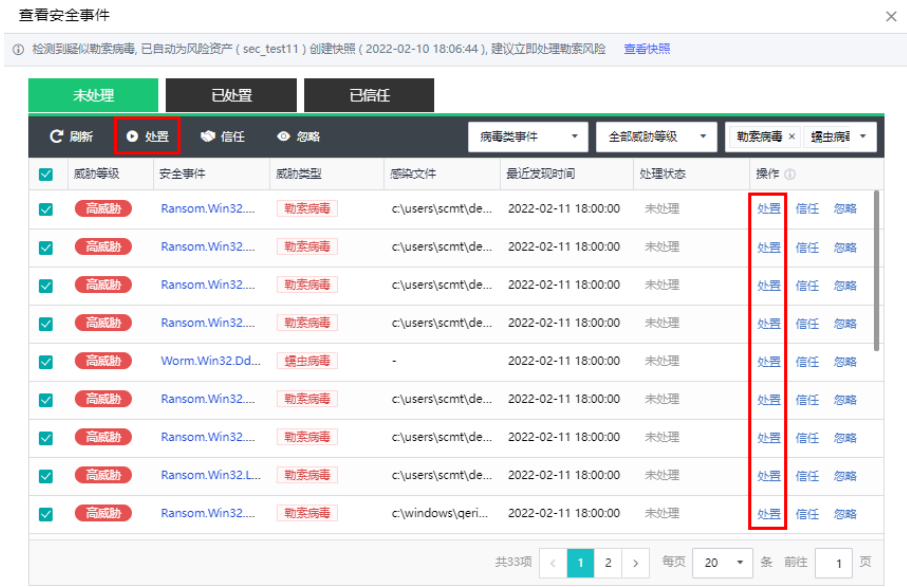
### 注意事项

平台当前仅支持针对Windows漏洞进行修复处理，暂不支持对Linux系统漏洞、应用漏洞自动修复。

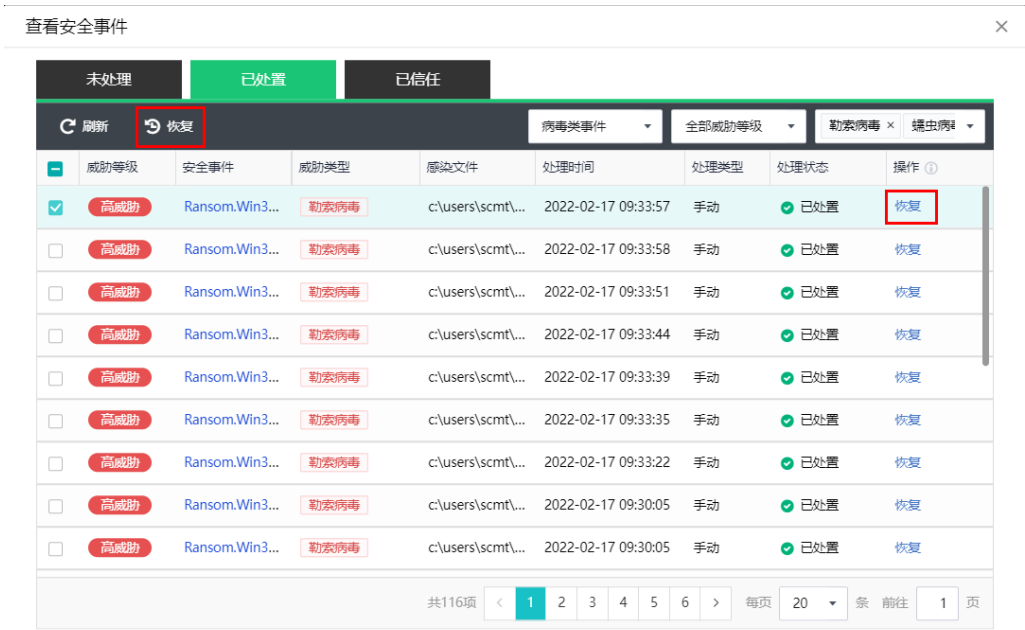
### 操作步骤

#### 一、安全事件

1. 点击所选虚拟机安全事件列，进入[安全事件]页面，选择需要处置的安全事件，点击<处置>按钮，可对安全事件进行处置。



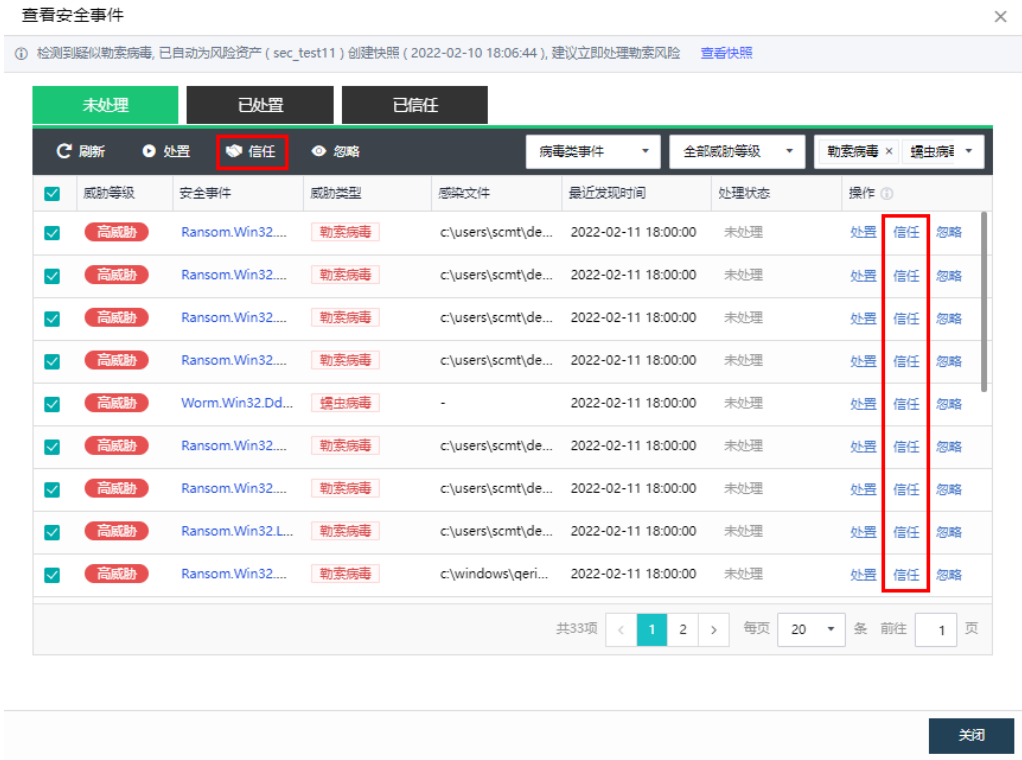
2. 若安全事件处置后业务异常, 可进入[已处置]列表, 点击<恢复>按钮, 对已隔离的文件进行恢复。



3. 当需要对安全事件文件添加信任时, 点击<信任>按钮, 执行信任处理。

注意:

- 执行信任后, 将同时信任其他虚拟机上具有相同 MD5 值的文件。
- 平台对信任的安全事件将不再进行风险和处置提醒。

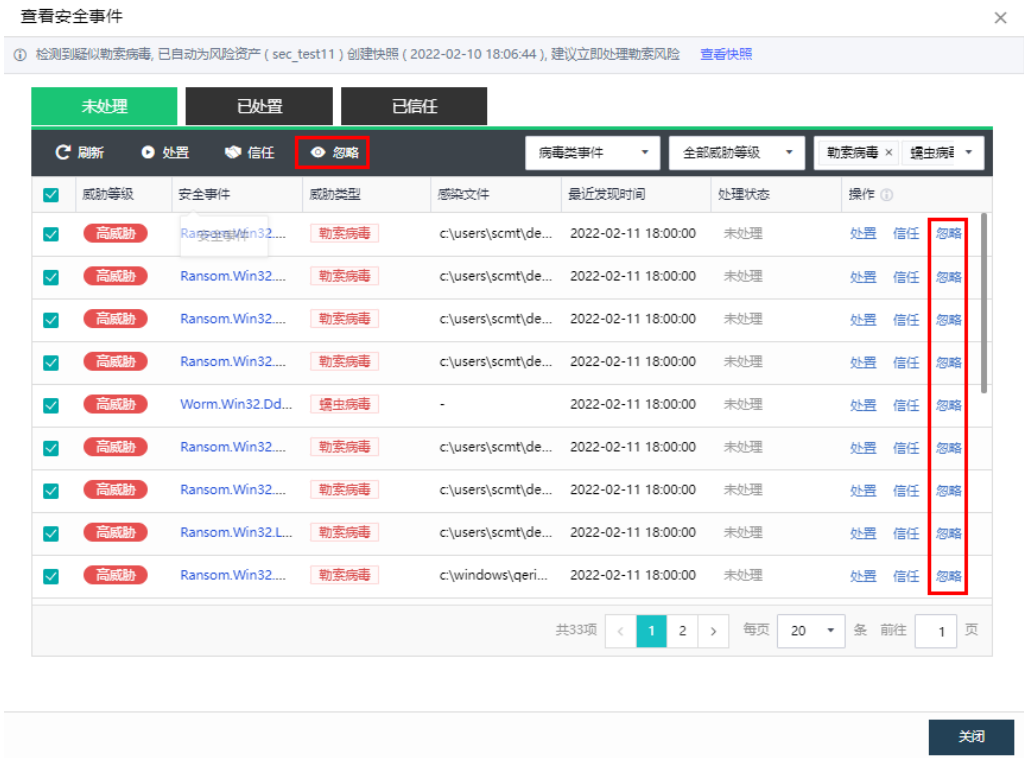


4. 若需要取消信任, 则进入[已信任]列表, 点击<取消信任>按钮, 将已信任的事件移出信任区。



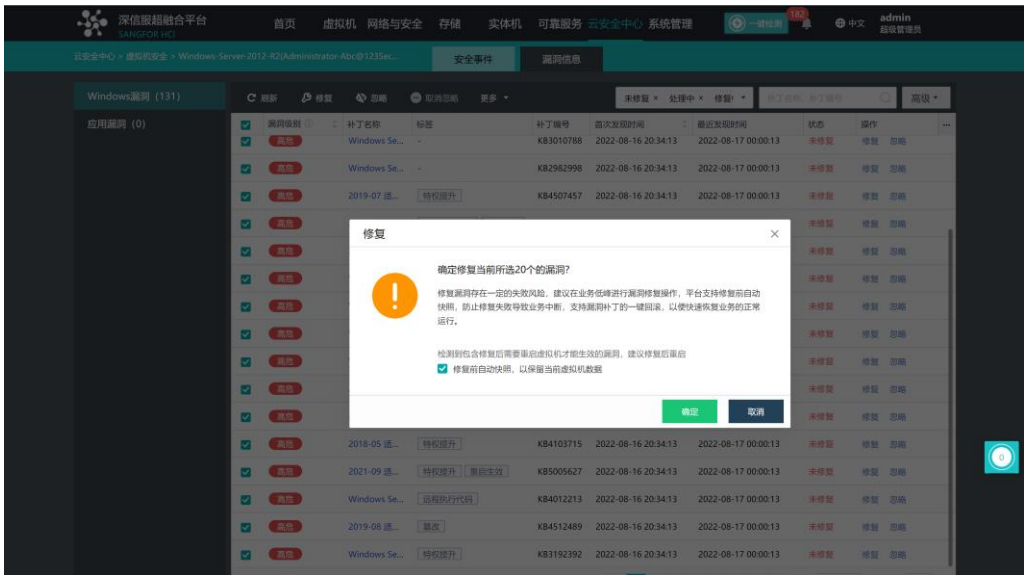
5. 若某安全事件暂不需要处理, 可勾选后点击<忽略>按钮, 进行忽略处理。

说明: 忽略后, 平台再次检测到所选的事件时仍会报警。



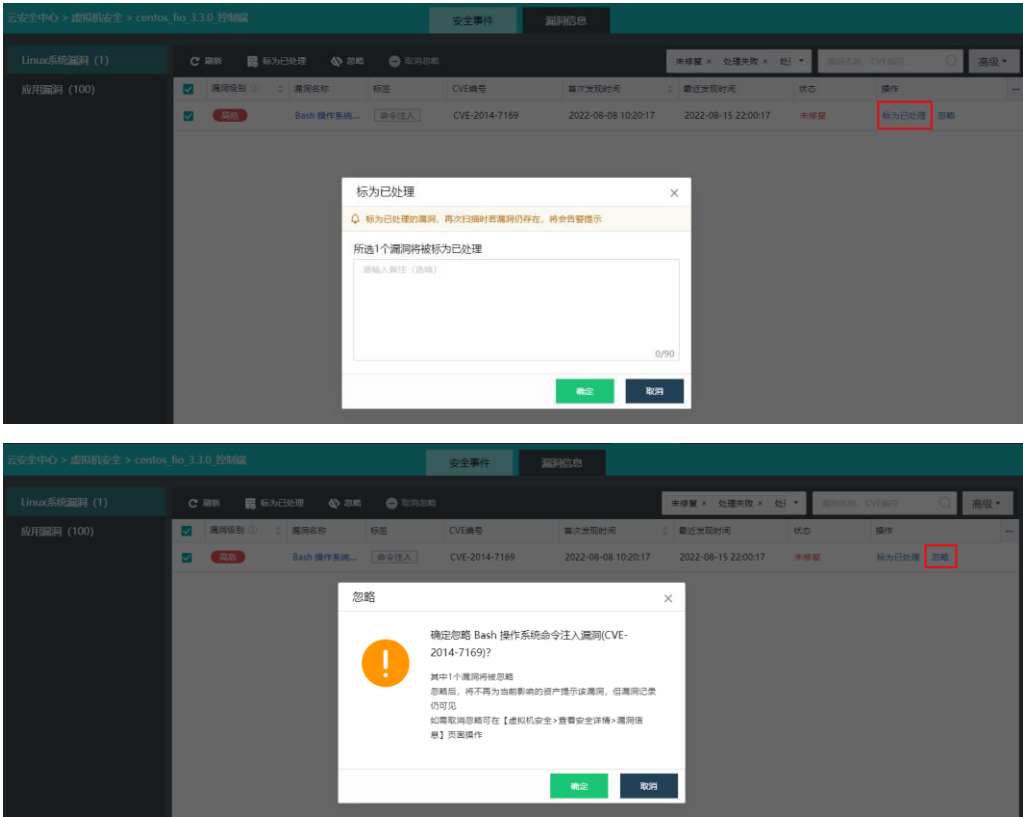
## 二、漏洞信息

1. 点击所选虚拟机的未修复漏洞列, 进入[漏洞信息/Windows漏洞]页面, 选择需要处置的漏洞, 点击操作栏相应按钮, 可对漏洞进行批量修复、忽略等处理。



2. 进入[Linux系统漏洞]或[应用漏洞]页面, 可对相应漏洞进行标记为已处理、忽略处理。
- 标记为已处理: 当用户已手动修复该漏洞, 可在此处将其“标为已处理”。标为已处理的漏洞, 再次扫描时若漏洞仍存在, 将会告警提示

- 忽略：若某漏洞暂不需要修复，可勾选后点击<忽略>按钮，进行忽略处理。忽略后，将不再为当前影响的资产提示该漏洞，但漏洞记录仍可见。



## 9.3. 漏洞管理

### 功能描述

深信服超融合云安全中心为所有业务虚拟机提供漏洞监控视图，全面了解业务系统漏洞风险，并提供一键批量Windows漏洞修复能力，提高业务安全防护。

### 前提条件

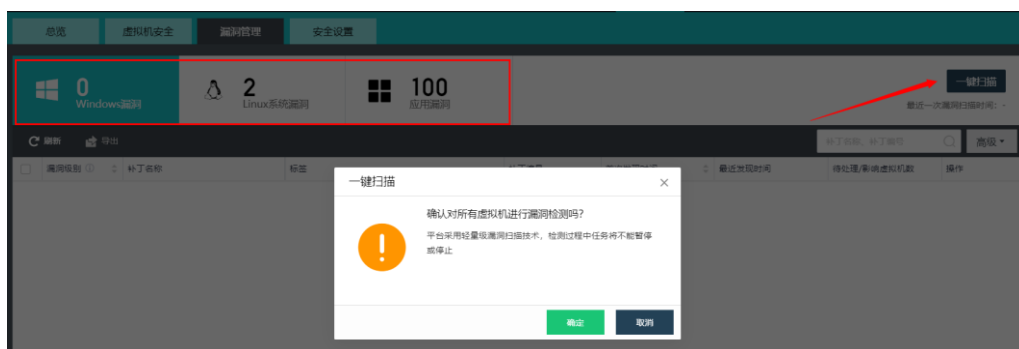
无

### 注意事项

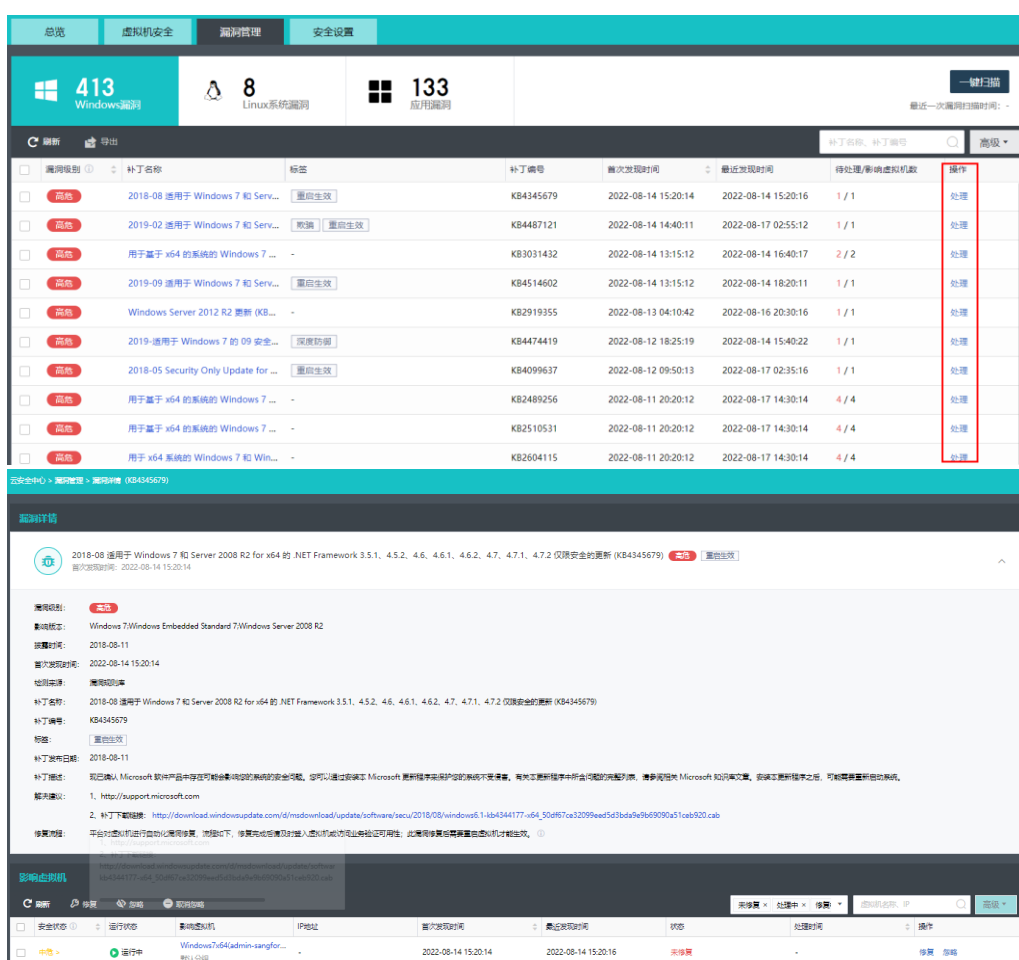
当前仅提供对Windows漏洞的修复能力，对于Linux系统漏洞、应用漏洞，仅支持一键扫描，暂不支持自动修复处理。

### 操作步骤

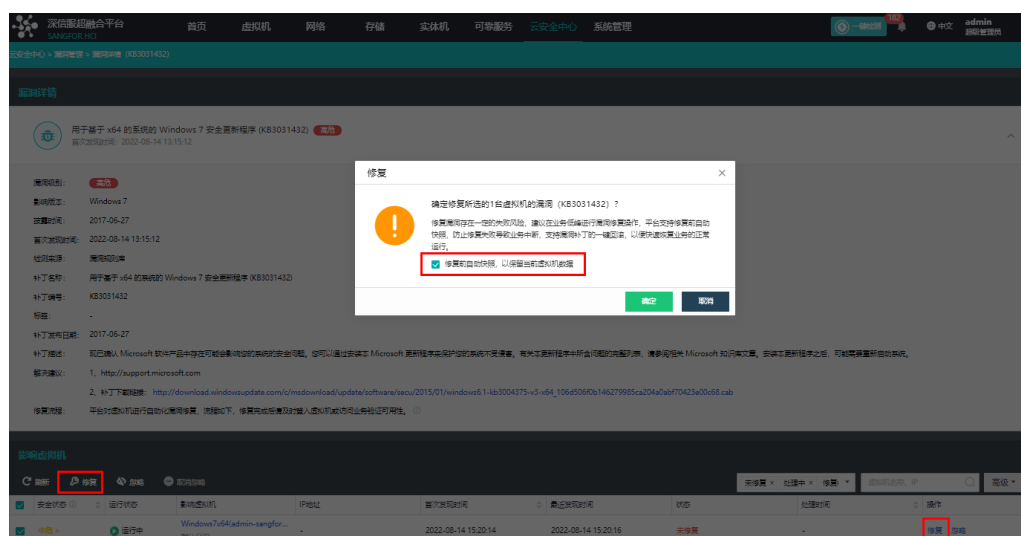
1. 进入[漏洞管理]页面，平台支持自动发现并上报Windows漏洞、Linux系统漏洞、应用漏洞，也支持手动扫描漏洞。



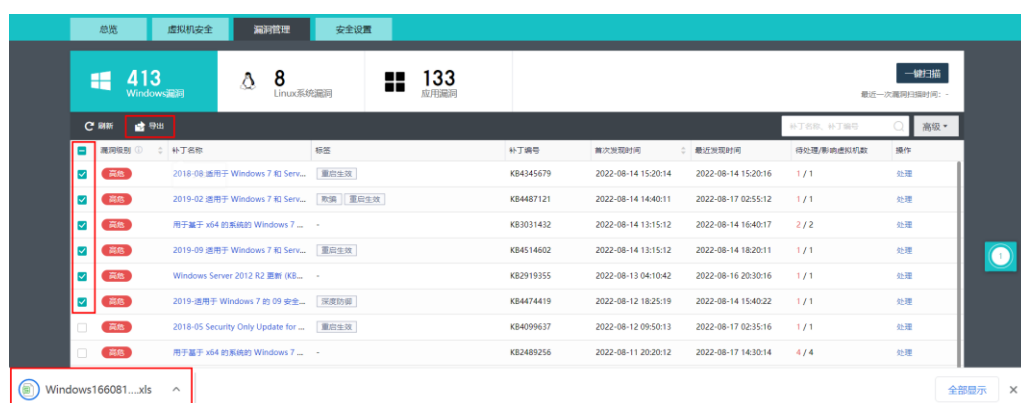
2. 在漏洞管理列表，可以看到漏洞信息，包括：漏洞级别、补丁名称、标签、补丁编号、发现时间、影响虚拟机，点击操作栏<处理>按钮，能够查看该漏洞的详细信息以及受影响虚拟机列表。



3. 勾选需要进行漏洞修复的虚拟机，点击上方<修复>按钮，进行单个或批量漏洞修复。建议勾选“修复前自动快照，以保留当前虚拟机数据”，勾选后平台会在漏洞修复前自动为该虚拟机打快照，以便修复失败场景下可以快速恢复业务。



4. 平台还支持选择单个或批量资产，导出漏洞检测结果，导出内容包括：漏洞级别、漏洞/补丁名称、标签、补丁/CVE编号、虚拟机名称、IP、修复状态、修复建议等。



## 9.4. 安全设置

### 9.4.1. 数据保护策略设置

#### 功能说明

云安全中心平台支持开启数据保护策略，全部资产通过定时快照进行天级别的保护；当检测到安全软件被卸载、疑似存在勒索风险时，立即触发快照进行数据保护；当检测到异常的同时，持久化原有的定时保护文件，避免被有毒数据覆盖。

#### 前提条件

超融合平台快照策略已设置为智能模式，手动模式下将无法开启数据保护策略。模式设置可参考“[快照策略](#)”章节。



## 注意事项

1. 数据保护策略每天为虚拟机自动创建快照，建议优先将重要业务虚拟机加入策略，以便在遇到勒索病毒等较严重安全问题时可快速恢复数据。
2. 策略通常只保留最新1个快照文件，当检测到恶意破坏、疑似勒索等严重安全事件时，事件发生前的最新快照文件将保留7天。
3. 数据保护策略中，每天打快照的数量存在一定的限制：
  - 混合卷： $vm\_num=(0.6(host\_num-3)4+12)*(单块\ ssd\ 容量*0.5*ssd\ 磁盘个数/480G)$ ，注意：如果存储容量异构（不相等）时，以最小的存储容量为准。
  - 全闪卷：2048
4. 若选择的虚拟机或一致性组已经存在快照策略，则将会从原策略移除，加入到当前数据保护策略中。
5. 加入到数据保护策略中的虚拟机/一致性组会在每天打一次快照。

## 操作步骤

1. 进入[安全设置/数据保护策略设置]页面，点击<启用>按钮（默认启用），开启数据保护策略。



2. 开启后进入[可靠服务/快照管理/快照策略]，可以看到系统自动生成的两条云安全中心的快照策略。



3. 选择“虚拟机”或“一致性组”，点击<添加虚拟机>或<添加一致性组>，将虚拟机/一致性组添加到数据保护策略中。



## 9.4.2. 告警设置

### 功能说明

云安全中心支持实时检测对虚拟机造成威胁的安全事件，如暴力破解，webshell后门，勒索病毒，木马病毒等，识别到病毒之后，会将告警以邮件的形式发送至预留邮箱中，告知用户当前平台检测到安全事件。

### 前提条件

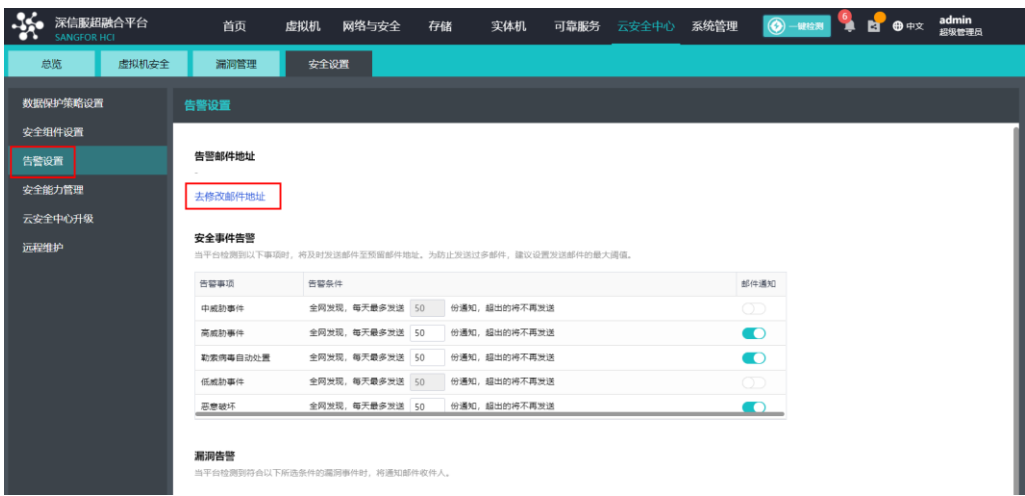
已配置邮件服务器。

### 注意事项

云安全中心暂不支持短信告警通知。

### 操作步骤

1. 进入[安全设置/告警设置]页面，点击<去修改邮件地址>，跳转到平台告警通知设置页面，点击<新增>按钮，勾选“云安全中心告警”。平台告警设置详情可参考“[平台配置指导/告警设置](#)”章节。



新增

×

邮箱地址：

请输入接收邮件通知的邮箱地址

告警类型：

☒ 平台告警

☒ 云安全中心告警

确定

取消

2. 当平台检测到安全事件，或漏洞事件时，将按照设置的告警条件发送告警邮件至预留邮箱。
- 安全事件告警：平台支持设置[安全事件告警]发送邮件的最大阈值，范围 1-1000。

**安全事件告警**  
当平台检测到以下事项时，将及时发送邮件至预留邮件地址。为防止发送过多邮件，建议设置发送邮件的最大阈值。

| 告警事项     | 告警条件                                                     | 邮件通知                                |
|----------|----------------------------------------------------------|-------------------------------------|
| 中威胁事件    | 全网发现，每天最多发送 <input type="text" value="50"/> 份通知，超出的将不再发送 | <input type="checkbox"/>            |
| 高威胁事件    | 全网发现，每天最多发送 <input type="text" value="50"/> 份通知，超出的将不再发送 | <input checked="" type="checkbox"/> |
| 勒索病毒自动处置 | 全网发现，每天最多发送 <input type="text" value="50"/> 份通知，超出的将不再发送 | <input checked="" type="checkbox"/> |
| 低威胁事件    | 全网发现，每天最多发送 <input type="text" value="50"/> 份通知，超出的将不再发送 | <input type="checkbox"/>            |
| 恶意破坏     | 全网发现，每天最多发送 <input type="text" value="50"/> 份通知，超出的将不再发送 | <input checked="" type="checkbox"/> |

- 漏洞告警：平台支持设置发送邮件的漏洞告警类型、漏洞告警频率，其中发送频率选择实时发送时，可以设置发送邮件的最大阈值，范围 1-1000。

**漏洞告警**  
当平台检测到符合以下所选条件的漏洞事件时，将通知邮件收件人。

漏洞告警类型：

☒ 高危漏洞

☒ 中危漏洞

☒ 低危漏洞

漏洞告警频率：

☒ 实时发送

☐ 每周发一次

☐ 每月发一次

全网发现，每天每种漏洞类型最多发送

份通知，超出的将不再发送

3. 点击<保存修改>，完成云安全中心告警设置。

### 9.4.3. 安全能力管理

#### 功能说明

云安全中心服务为平台提供自动化检测、监控与响应体系，实现一站式安全管控。

## 前提条件

已完成虚拟机安全防护管理平台安装部署，详情可参考“[虚拟机安全防护管理平台安装](#)”章节。

## 注意事项

无

## 操作步骤

1. 进入[安全设置/安全能力管理]页面，点击<查看默认安全配置>，可以分别选择Windows/Linux系统虚拟机安全防护默认设置。





2. 点击<前往安全防护管理平台>，登录虚拟机安全防护管理平台，进行其他个性化的配置。

### 9.4.4. 云安全中心升级

#### 功能说明

指导管理员进行云安全中心版本升级。

#### 前提条件

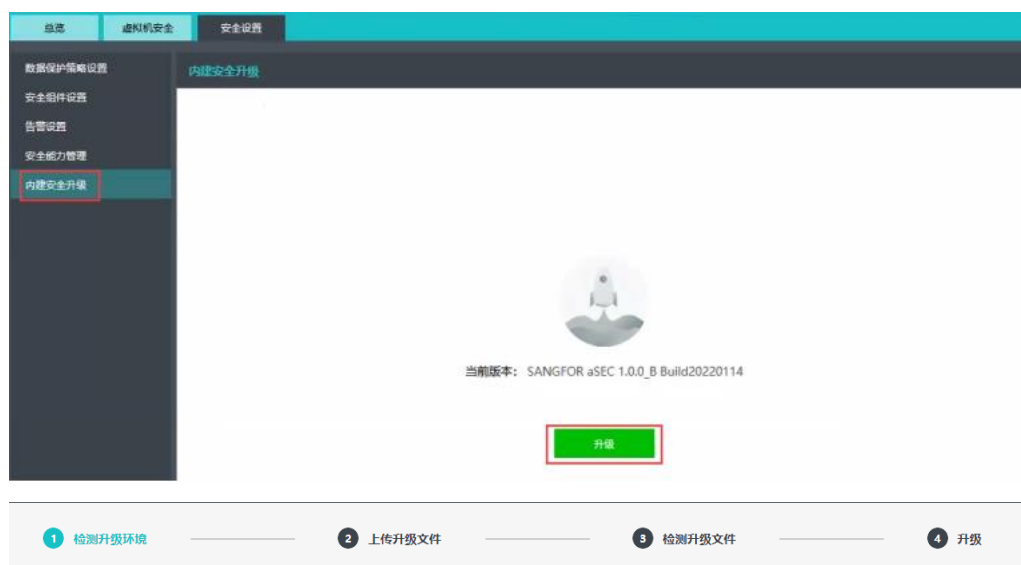
已获取最新版本升级包。

#### 注意事项

无

#### 操作步骤

进入[安全设置/云安全中心升级]页面，点击<升级>按钮，按照向导指引进行升级。



## 9.4.5. 远程维护

### 功能介绍

可联系技术服务远程协助排查、诊断、处理技术问题，以恢复业务或改善系统运行状态。

### 前提条件

无

### 注意事项

开启SSH端口，4小时后将会自动关闭。

### 操作步骤

进入[安全设置/远程维护]页面，点击<开启SSH端口>按钮，即可通过SSH远程运维云安全中心。



## 10. 超融合平台配置指导

### 10.1. 查看主机/集群运行状态

#### 功能说明

需要查看集群中主机的状态，了解平台的使用情况。

#### 注意事项

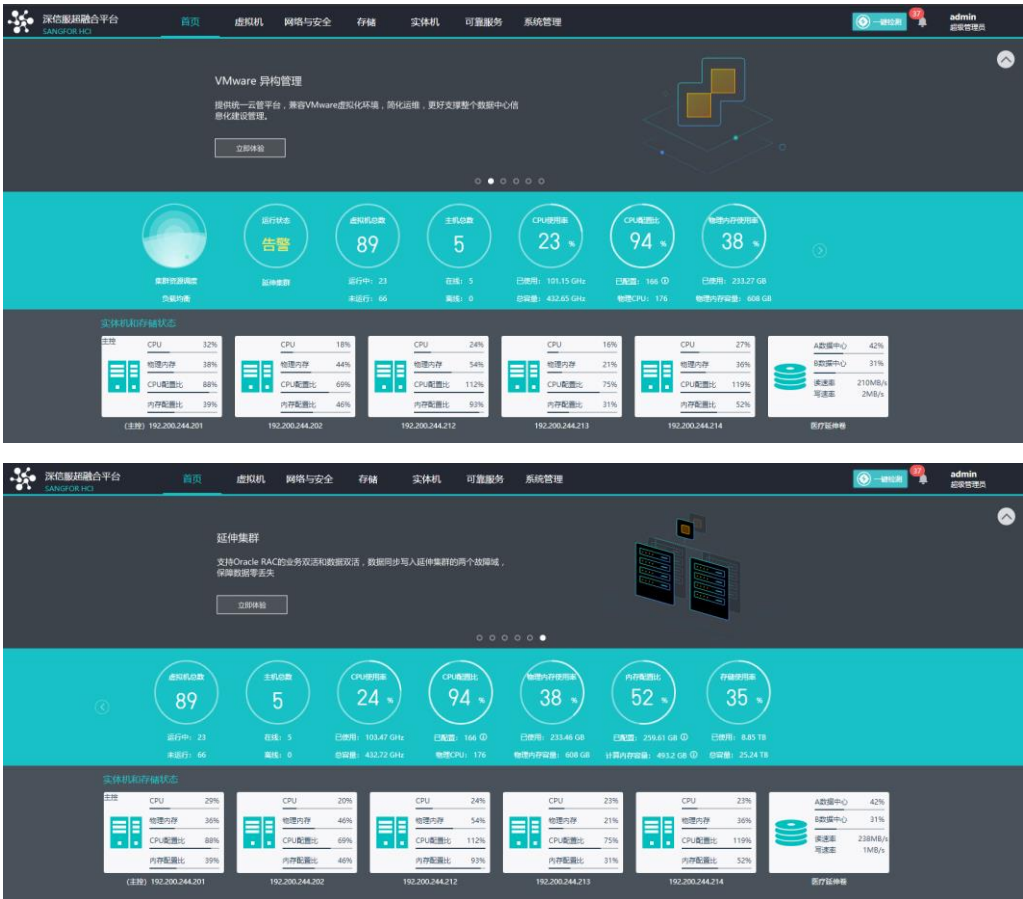
无

#### 前提条件

无

#### 操作步骤

在[首页]可以看到集群中主机的运行状态，包括集群中主机的数量、虚拟机的数量和存储的数量，并且显示了集群的CPU、内存和存储的使用情况以及各个主机的使用情况。



## 10.2. 端口管理

### 功能说明

支持手动关闭或打开平台端口。支持开启和关闭SSH端口，同时可设置访问SSH端口的IP白名单。

### 注意事项

1. 在端口管理界面对端口进行关闭，仅是关闭集群对外的端口，不影响集群内的功能。例如：关闭虚拟机迁移服务仅会影响跨集群迁移，不影响集群内迁移。
2. 在远程SSH登录超融合平台后，若超过10min无操作，会话将自动超时断开。
3. 单个IP在10分钟内只能访问单个HCI集群100次。
4. 如果需要部署VDI业务，请启用“桌面云接入服务”端口。

### 前提条件

1. 登录控制台，进入[系统管理/端口管理]界面，选中需要打开/关闭的端口，点击<启用>或<禁用>进行配置。



2. 设置开启/关闭SSH端口，开启端口后，可进行IP登录限制。勾选“启用SSH IP限制”，并在输入框中输入允许访问的IP，数量上限为100个，点击<保存>。





## 10.3. 证书配置

### 功能说明

SSL证书用于在客户端和超融合设备之间建立一条SSL安全通道，当客户端浏览器对https网站标记危险警告时，安装SSL证书可以使客户端受到浏览器信任，解除不安全警告。深信服超融合平台支持手动导入SSL证书。

### 注意事项

1. 证书文件当前仅支持.crt 格式，如有其他格式证书，需要转化。
2. Key文件大小上限限制在1MB以内。

### 前提条件

已经获取有效的.crt 格式证书文件。

### 操作步骤

1. 登录控制台，进入[系统管理/证书配置]界面，导入正确的.crt和.key证书，点击&ltlt保存>>。



2. 可以看到，导入被信任证书后，客户端受到浏览器信任，解除不安全警告。



## 此站点不安全

这可能意味着，有人正在尝试欺骗你或窃取你发送到服务器的任何信息。你应该立即关闭此站点。

✔ 关闭此标签页

🔍 详细信息



10.4. 查看告警日志

功能说明

需查看告警日志来定位问题。

注意事项

无

前提条件

无

操作步骤

- 1. 通过[系统管理/告警日志]可以查看HCI平台告警信息。



- 2. 通过过滤功能可以筛选需要的告警信息。



## 10.5. 告警设置

### 功能说明

1. 设置平台告警项目阈值，包括主机，存储，虚拟机，虚拟网络，序列号各类监控项目。
2. 将设定告警内容通过邮件/短信的方式发送到指定邮箱/手机号码。

### 注意事项

1. 短信通知：主控离线一段时间后恢复，有可能会出现用户同时收到多条短信（最多50条）的情况。主机离线情况下，会出现网络异常，可能导致相同的告警短信会发送两次（告警重试机制）。
2. 有些短信内容较多，可能会被运营商拆分成多条发送。

### 前提条件

邮件通知：已配置邮件服务器。

### 操作步骤

1. 配置告警设置。
2. 打开控制台，进入[系统管理/告警日志/告警设置]。选择需要调整的告警阈值并保存修改。主机告警条件设置。



3. 物理网络告警条件设置。可针对主机硬件告警条件进行设置，包括主机离线、网卡兼容性、网卡损坏、网卡光模块异常、网口错包等告警项的设置。



4. 存储告警条件设置。



5. 虚拟机告警条件设置。支持设置开启或屏蔽平台上符合条件的某一类告警，同时也支持以虚拟机维度屏蔽该类告警。



6. 虚拟网络告警条件设置。



7. 序列号告警条件设置。



## 10.6. Syslog 配置

### 功能说明

将操作日志和内核日志自动上传到日志服务器。

### 注意事项

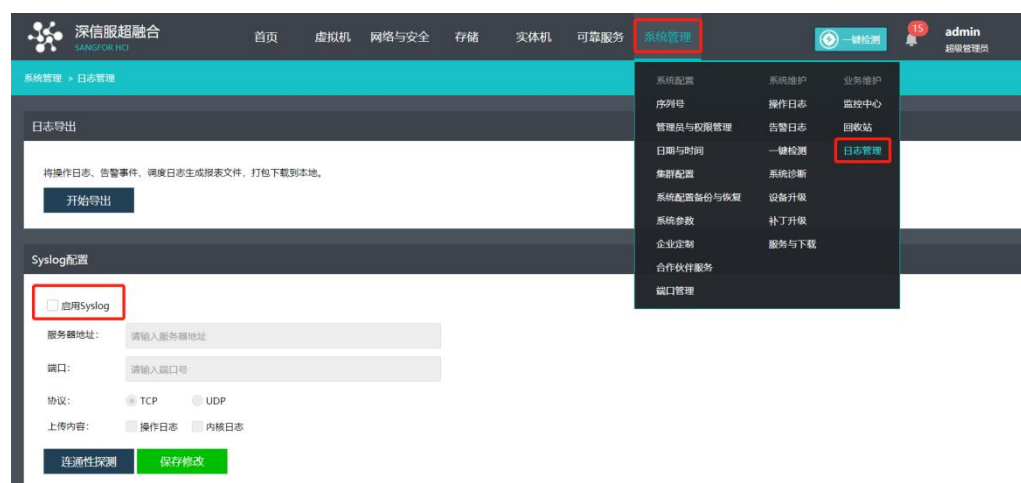
无

### 前提条件

已有日志服务器，且能与管理口通信。

### 操作步骤

打开控制台，进入[系统管理/日志管理/Syslog配置]。勾选“启用Syslog”，配置Syslog服务器的IP、端口、协议，配置后点击<连通性测试>确认Syslog服务器可以连通，点击<保存修改>，所选日志会自动上传到Syslog日志服务器。



## 10.7. 管理员与权限管理配置

### 10.7.1. 权限

#### 功能说明

这里的权限相当于一个角色功能，是对某个资源拥有什么样的权限。权限，是零个或者多个具体权限的集合。

#### 注意事项

无

前提条件

无

操作步骤

新增权限

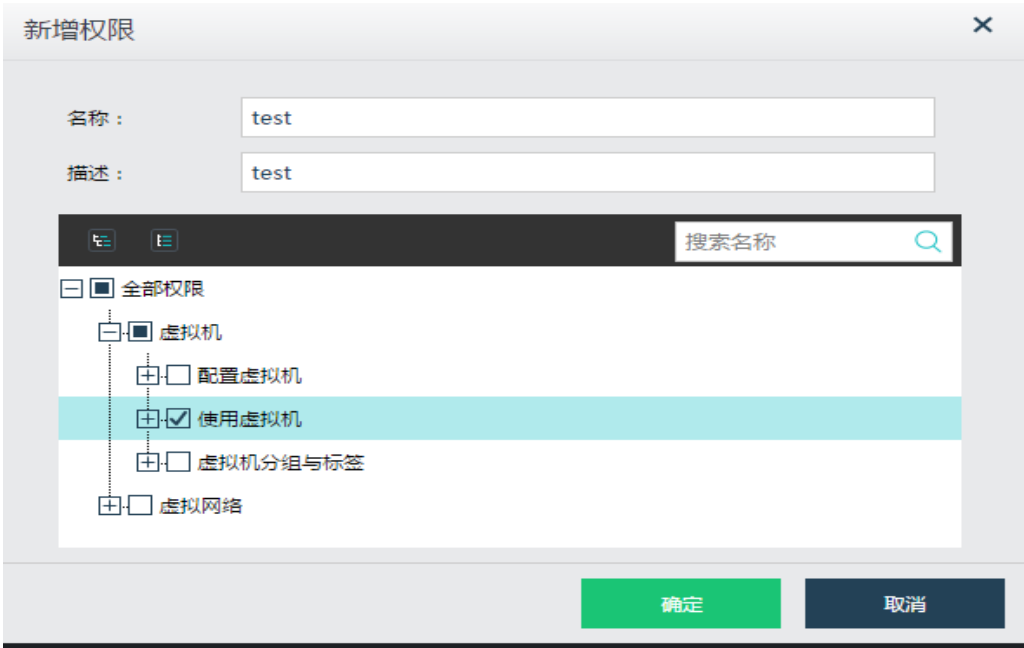
1. 打开控制台，进入[管理/管理员与权限管理]。



2. 在[权限]中点击<新增>，弹出[新增权限]窗口。



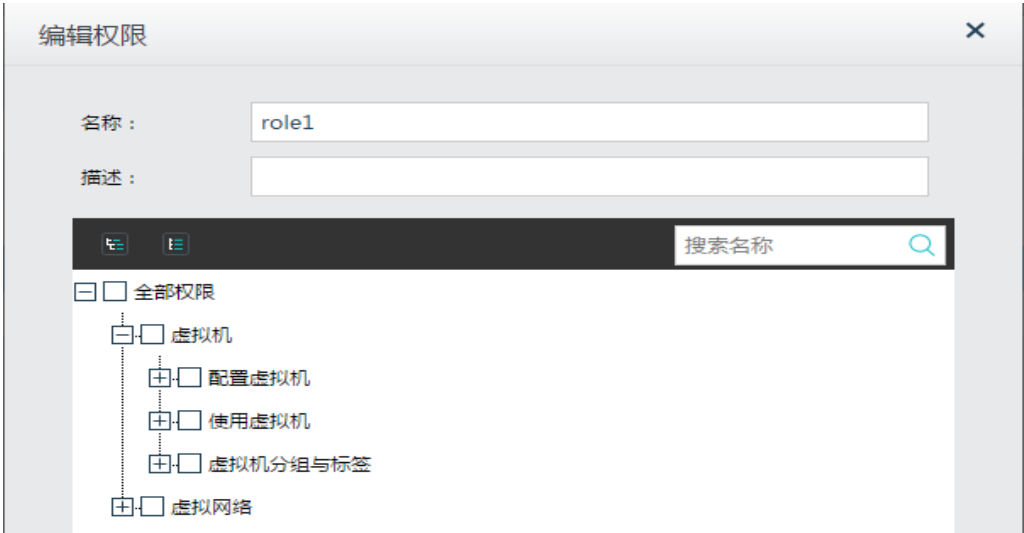
3. 输入权限名称以及描述（名称必填，描述选填，而且名称需要唯一），然后勾选所需要的具体权限，点击<确定>。



编辑权限

新增权限之后，可以根据需要，修改权限的名称、描述以及该权限包含的具体的权限内容。点击要编辑的权限右边的编辑图标，即可进行编辑。

| <input type="checkbox"/> | 名称    | 描述    | 编辑 |
|--------------------------|-------|-------|----|
| <input type="checkbox"/> | 管理员   | 全部权限  | -  |
| <input type="checkbox"/> | 只读    | 只读    | -  |
| <input type="checkbox"/> | 无权限   | -     | -  |
| <input type="checkbox"/> | 虚拟机用户 | 使用虚拟机 |    |
| <input type="checkbox"/> | 网络管理员 | 管理网络  |    |
| <input type="checkbox"/> | role1 | -     |    |



删除权限

勾选要删除的权限，点击<删除>。可同时删除多个权限。



**注意:**

当权限被赋予给某个用户的时候，删除会失败。



## 10.7.2. 新增用户

### 功能说明

需要在超融合上新建用户并赋予不同的权限。

### 注意事项

1. 用户名确定之后是不能修改的。描述选填，并且可以通过编辑用户修改。
2. 资源配额仅限制用户创建的虚拟机，对于授权其他用户创建的虚拟机给该用户使用，不占用该用户的资源配额。
3. 用户及权限只有admin用户能够配置。
4. 系统管理员对以下功能无配置权限：VMware相关功能、一致性组快照与快照策略、合作伙伴服务、P2V迁移。

### 前提条件

已经配置好了权限。

### 操作步骤

1. 打开控制台，进入[系统管理/管理员与权限管理]，点击<新增用户>，配置名称、描述、角色、分组、密码等信息，然后点击<配置>。

新增用户 ×

名称:

test

描述:

角色:

系统管理员 ▼ ⓘ

分组:

默认分组 ▼

密码:

ⓘ

确认密码:

系统权限:

对【可靠服务】、【系统管理】具有管理权限，但【系统管理】不包括“管理员与权限管理”、“日志管理”

资源权限与配额:

配置

确定

取消

2. 在[资源权限与配额]页面中勾选需要配置权限的资源，并赋予预先配置好的权限；资源包括存储、物理磁盘。

资源权限与配额 ×

物理资源

虚拟资源

虚拟资源配额

① 默认所有资源都没有权限，可以为该用户创建新的资源组或选择已有的资源来配置权限。

此处可以新增虚拟机分组或者网络设备分组  
这里新增的分组默认对该用户分配管理员权限

待选资源

已选资源权限

资源名称

搜索名称

资源名称

权限

移除

全部资源

存储

物理磁盘

全部资源

无权限

存储

管理员

123

192.200.244.201/本地存储

192.200.244.202/本地存储

192.200.244.212/本地存储

192.200.244.213/本地存储

192.200.244.214/本地存储

1tb

管理员 此处可以选择不同的权限

保持与上级权限一致 (管理...

保持与上级权限一致 (管理...

保持与上级权限一致 (管理...

保持与上级权限一致 (管理...

保持与上级权限一致 (管理...

保持与上级权限一致 (管理...

页面权限:

管理

(包括首页、存储、实体机、虚拟机列表)

确定

取消



3. 在[虚拟资源]页面为所选资源配置虚拟机、虚拟网络相关权限。



4. 在[资源配额]页面中可以针对当前用户配置CPU、内存和存储资源的使用限额。

资源权限与配额 ×

物理资源

虚拟资源

虚拟资源配额

CPU:

☒ 不限制

☐ 限制启动虚拟机的总CPU核数

核

内存:

☒ 不限制

☐ 限制启动虚拟机的总内存大小

GB

存储:

☒ 不限制

☐ 限制创建虚拟机的总磁盘大小

GB

注：资源配额仅限制用户创建的虚拟机，对于授权其他用户创建的虚拟机给该用户使用，不占用该用户的资源配额

确定

取消

10.7.3. 三员分立

功能说明

创建系统管理员、安全管理员、审计管理员三种管理员角色，分配不同的权限分管集群。

注意事项

1.

安全管理员拥有平台用户的查看权限，包括查看用户列表，查看用户配额，修改用户密码权限等，无法新增用户和修改用户配额。
2.

审计管理员拥有操作日志、告警日志、日志管理的配置权限，操作日志包括平台所有的操作日志，调度日志和HA日志。

前提条件

无

操作步骤

1.

打新建系统管理员步骤可参考“[新增用户](#)”章节。
2.

admin登录控制台，进入[系统管理/管理员与权限管理/用户]，点击<新增用户>，配置用户名、描述、分组、密码等信息，角色选择[安全管理员]，然后点击<确定>。

新增用户

名称: sectest

描述:

角色: 安全管理员

分组: 默认分组

密码:

确认密码:

系统权限: 对【系统管理】中的“管理员与权限管理”具有管理权限

资源权限与配额: 无权限

确定 取消

3. 点击<新增用户>，配置用户名、描述、分组、密码等信息，角色选择[审计管理员]，然后点击<确定>。

超级管理员 默认分组

普通管理

系统管理

普通管理

普通管理

普通管理

系统管理

安全管理

审计管理

系统管理

### 新增用户

名称: audtest

描述:

角色: 审计管理员

分组: 默认分组

密码:

确认密码:

系统权限: 对【系统管理】中的“操作日志”、“告警日志”、“日志管理”具有管理权限

资源权限与配额: 无权限

确定 取消

## 10.7.4. 密码策略

### 功能说明

可对平台上的所有用户强制下发密码策略，包括密码长度、密码复杂度、密码有效期与错误输入次数。

### 注意事项

1. 新建用户时必须遵循密码策略。
2. 若已有用户不符合密码策略，则会在登录时强制其进行修改。

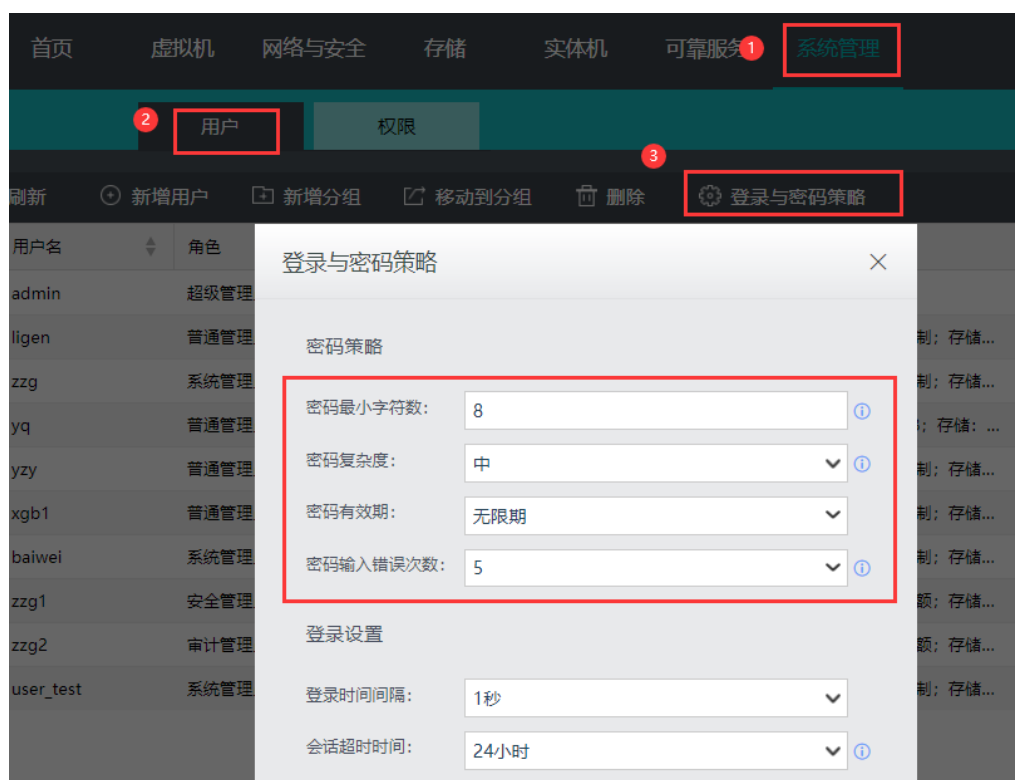
### 前提条件

无

### 操作步骤

使用admin登录控制台，进入[系统管理/管理员与权限管理/用户]，点击<登录与密码策略>，配置密码最小字符数、密码复杂度、密码有效期、密码输入错误次数，点击

<确定>。



## 10.7.5. 限制登录

### 功能说明

限制登录选项可以基于以下场景控制用户登录。

1. 基于IP地址、MAC地址的登录控制策略。
2. 基于终端设备的登录控制策略。
3. 基于时间段的登录控制策略。

### 注意事项

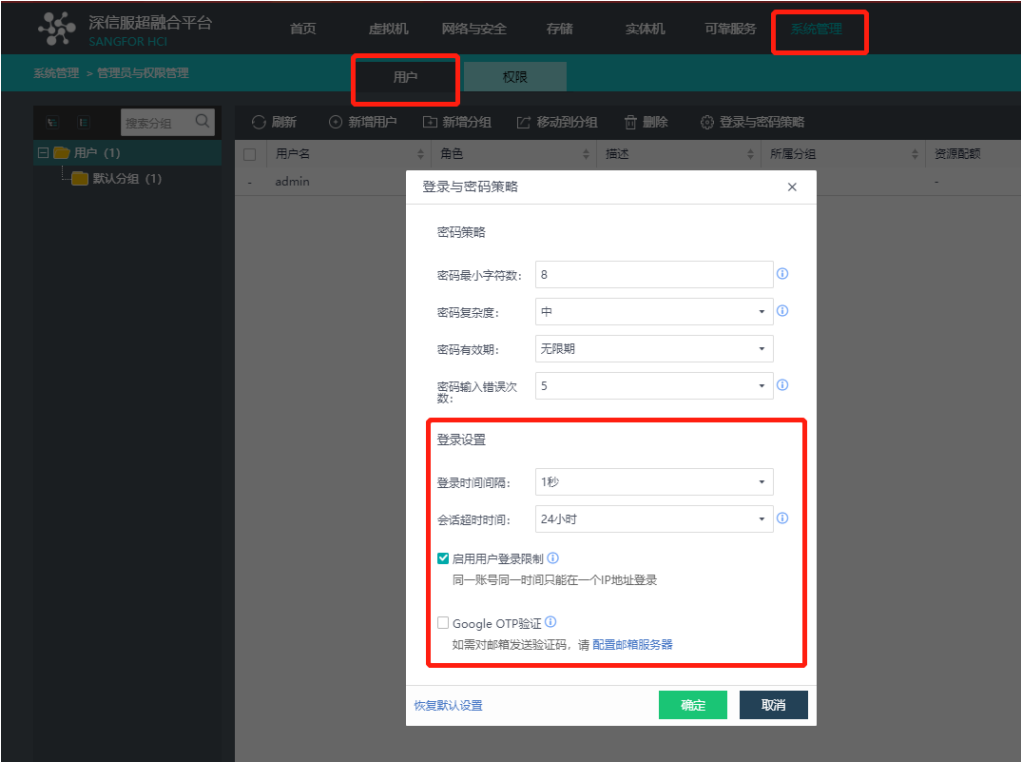
1. 如果设置了限制登录终端，必须在满足条件的终端上登录。
2. 终端设备UUID限制只支持Windows。

### 前提条件

用户已存在。

### 操作步骤

1. 打开控制台，进入[管理/用户权限/用户/用户登录设置]，勾选“启用用户登陆限制”。



2. 选择修改需要限制的用户，编辑此用户。



3. 根据限制的需要，添加限制条件。



编辑用户

基本信息

登录限制

☐ 启用登录允许范围 ?

| 序号                      | MAC地址 | IP地址 | 操作 |
|-------------------------|-------|------|----|
| <div><div></div>空</div> |       |      |    |

+

 添加规则

(还可以添加20条)

☐ 启用终端设备限制

UUID: 

?

☐ 启用登录时间限制

可访问时间: 

09:00

 至 

18:00

确定

取消

### 10.7.6. UKey 双因子登录配置

#### 功能说明

平台采取了基于USB-KEY和用户账号密码的双因子登录鉴别方式，管理员为平台全部用户设置UKey策略，包括是否绑定UKey，是否开启UKey登录认证。

UKey 认证登录的目的是限制非法用户登录平台，确保只有当用通过注册过的 UKey 才能正常登录。

UKey 认证功能模块以服务的形式存在于后台，浏览器通过服务提供的接口，可以获取终端的UKey 相关信息，也可以发送命令，使得服务向 UKey 烧制证书。

#### 注意事项

1. 每台终端同时只能连接一个UKey。
2. 重复写UKey会覆盖原有信息。
3. 绑定并启用UKey后，该用户登录的终端需插对应的UKey，再输入正确的账号

密码才能登录平台。

4. 只有系统管理员才可以进行绑定UKey的操作，其他管理员没有这项操作，绑定操作时需下载安装深信服UKey服务客户端。
5. 启用USB-KEY认证登录后，认证key丢失或者损坏，无法登录集群，只能联系技术支持处理。

## 前提条件

1. 对应用户已建立。
2. 已准备好UKey。
3. Windows终端。

## 操作步骤

1. 在操作的终端PC设备插上UKey，把该管理员与该UKey进行绑定：此时平台请求获取服务当前的版本号。若服务没有响应，就会提示安装服务并提供下载链接，用户下载后需要手动安装；如果服务响应的版本号不是最新的，就会提示用户下载最新的安装包，否则不能进行下一步操作。根据提示安装最新的安装包后重启浏览器，再次登录平台，操作进行步骤1，步骤2操作。正常应弹出如下窗口。如果不能使用可以点击弹出的[安装指引]选项，根据指引正确配置环境。



2. 点击<绑定UKey>：此时系统会确认当前插入到终端的 UKey个数。一次只能允许一个UKey的烧录，若没有UKey，或者超过一个，则提示用户操作不当。请求UKey的所属者。若当前插入的 UKey已存在其他用户信息，会弹出确认覆盖的提示。在UKey烧制完成后，平台会生成公私钥对，私钥存储在 UKey 中，公钥保存在后台。用户和KEY绑定完成后弹出完成的提示。
3. 绑定完成之后，即可对该用户开启证书管理，根据需要在用户列表管理启用或停用证书登录。



## 10.7.7. Google OTP 双因子登录配置

### 功能说明

HCI5.8.8R1版本开始支持了基于Google OTP和用户账号密码的双因子登录鉴别方式，平台用户登录设置里可配置Google OTP服务器验证。

### 注意事项

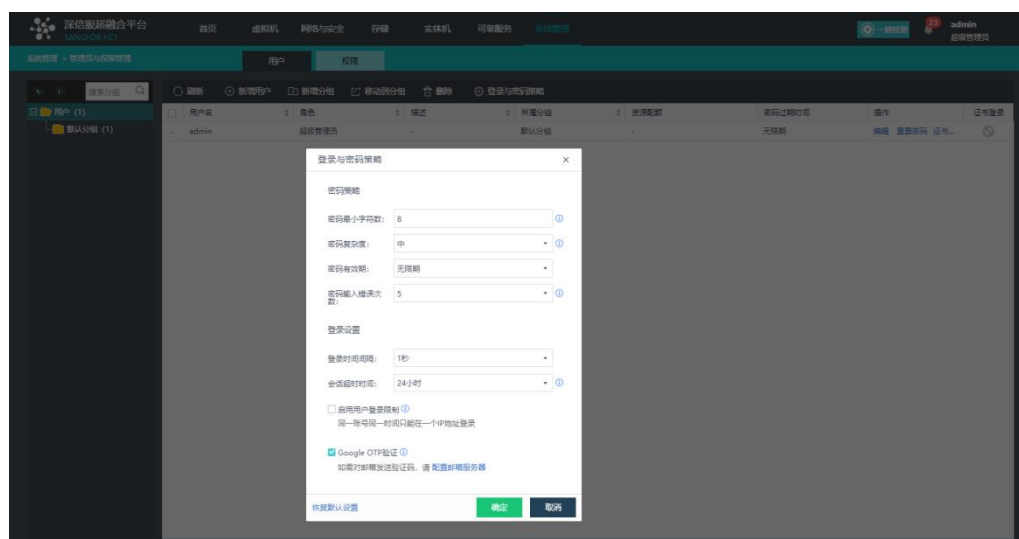
1. 此版本仅支持HCI启用OTP，SCP暂不支持。
2. 仅有admin管理员有开启启用Google OTP认证的权限。

### 前提条件

准备好Google OTP服务器与客户端。

### 操作步骤

1. 首先从[管理员与权限管理]下的<登录与密码策略>进入OTP开启页面。



2. 开启前，如需对邮箱发送验证码（使用邮箱接收登录验证码），需要配置邮箱服务器。

配置邮箱服务器

发件人邮箱:

SMTP服务器地址:

端口:

25

☐ 启用服务器安全连接

选型:

☐ 发送服务器要验证用户名和密码

用户名:

密码:

填写邮箱的授权码，非邮箱登录密码

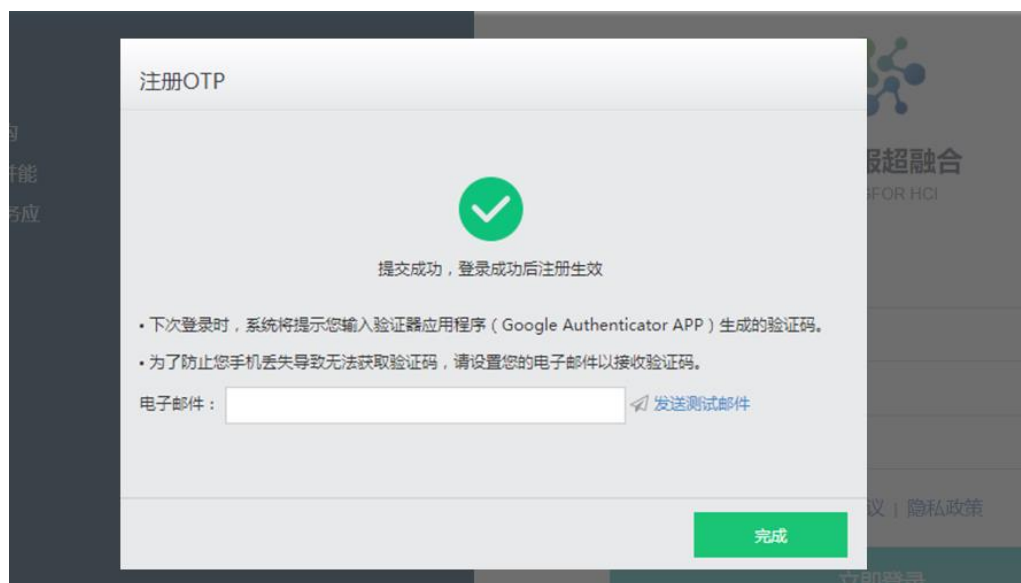
确定

取消

3. 开启Google OTP验证功能后，会自动退出当前的登录状态，重新登录。并且通过在移动设备上安装验证器应用程序（Google Authenticator APP）注册OTP，安装成功后，扫描二维码。



4. 输入验证码后，进入配置接收邮箱页面，配置指定的邮箱，当设备不在身边的时候，可以通过此邮箱获取验证码登录平台。



## 10.8. 修改集群 IP 地址

### 功能说明

修改集群IP地址分两种情况：

1. 只修改集群IP地址。
2. 集群中主机管理通信口IP和集群IP地址都要修改。

### 注意事项

1. 修改集群中主机的IP地址后，需要用新的IP进行登录，可能需要更改交换机的配置，修改相应的VLAN。
2. 只修改集群IP地址时，需确保修改后的IP跟原集群IP在同一个网段。
3. 主机管理口IP和集群IP都需要修改时，需确保管理口IP和集群IP在同一个网段。

### 前提条件

交换机需要做相应的配置，预约网络工程师做交换机配置。

### 操作步骤

1. 打开HCI控制台，并依次找到[实体机/网口功能/管理通信口]。



2. 如果要修改的集群IP地址和现有的IP地址是同一个网段，直接修改即可，后面的3、4步无须操作。如果要修改集群中主机的IP地址是不同网段，就需要先将集群IP地址的配置信息删掉，保存更改后，再执行3、4步操作。

### 设置集群IP

可以通过浏览器直接访问集群IP来管理此平台。

通常情况可以直接通过平台中的任一主机IP来管理此平台，但如果连接该主机失败后，将无法继续管理深信服企业级云。

使用集群IP后，可以避免直接连接某台主机时，因为故障而导致无法正常管理虚拟机的情况。

通过集群IP连接到此深信服企业级云，可以更加稳定的管理虚拟机。

集群IP:

子网掩码:

集群名称:

确定

取消

3. 然后点击<修改配置>。

### 修改配置

刷新

批量修改

| 主机名称            | 管理通信口 | 管理通信IP          | 掩码            | 网关              |
|-----------------|-------|-----------------|---------------|-----------------|
| 192.200.244.200 | eth0  | 192.200.244.200 | 255.255.255.0 | 192.200.244.254 |
| 192.200.244.201 | eth0  | 192.200.244.201 | 255.255.255.0 | 192.200.244.254 |
| 192.200.244.202 | eth0  | 192.200.244.202 | 255.255.255.0 | 192.200.244.254 |

4. 修改管理通信口的IP地址，然后再去配置集群IP地址的相关信息。

设置集群IP

可以通过浏览器直接访问集群IP来管理此平台。

通常情况可以直接通过平台中的任一主机IP来管理此平台，但如果连接该主机失败后，将无法继续管理深信服企业级云。

使用集群IP后，可以避免直接连接某台主机时，因为故障而导致无法正常管理虚拟机的情况。

通过集群IP连接到此深信服企业级云，可以更加稳定的管理虚拟机。

集群IP:

子网掩码:

255.255.255.0

集群名称:

HCI

确定

取消

## 10.9. 管理口不带 IP 切换

### 功能说明

通过管理口可实现集群对主机的管理，当重新规划了管理网络时，可支持批量不带IP地址切换管理网口，实现管理网络的平滑切换。

### 注意事项

1. 集群配置了集群IP，且集群IP与管理口在同一网段时，不支持不带IP切换管理口，只允许带IP切换管理口。
2. 对非主控不带IP修改管理口使非主控离线后，单独登录非主控将管理口切回来，需要登录非主控后台调用切换管理口的接口，将管理口切回来恢复在线。
3. 新管理口 IP 信息如为空，切换管理口时会将旧网口信息带往新网卡。

### 前提条件

无

### 操作步骤

1. 在[实体机/网口功能/管理通信口]界面，点击<修改配置>选项。

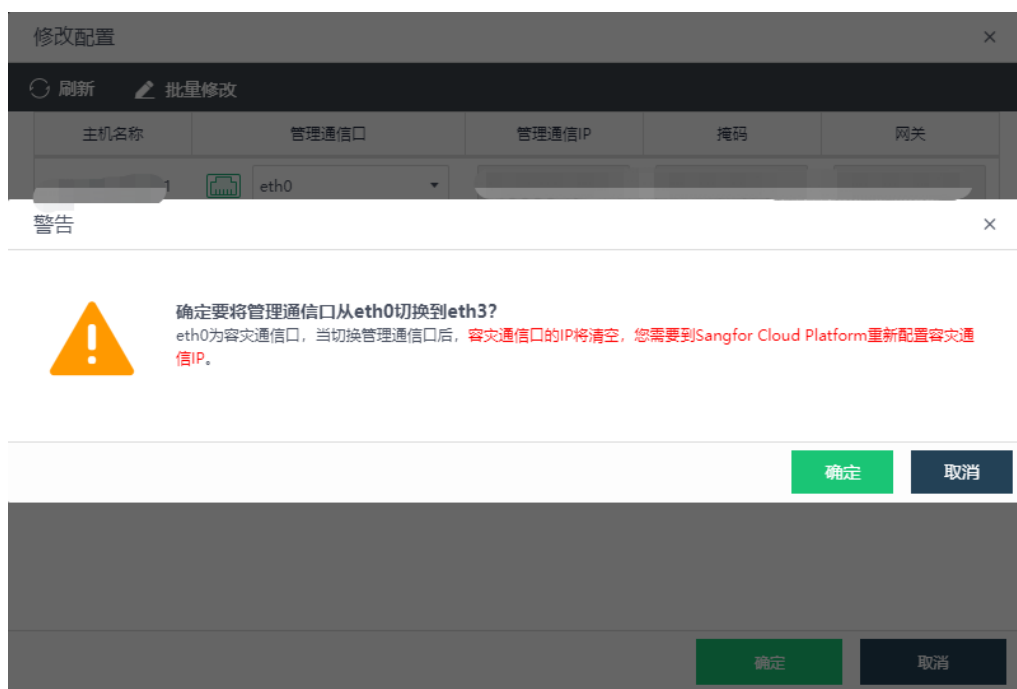


2. 选择新的管理通信口，并点击<确定>。

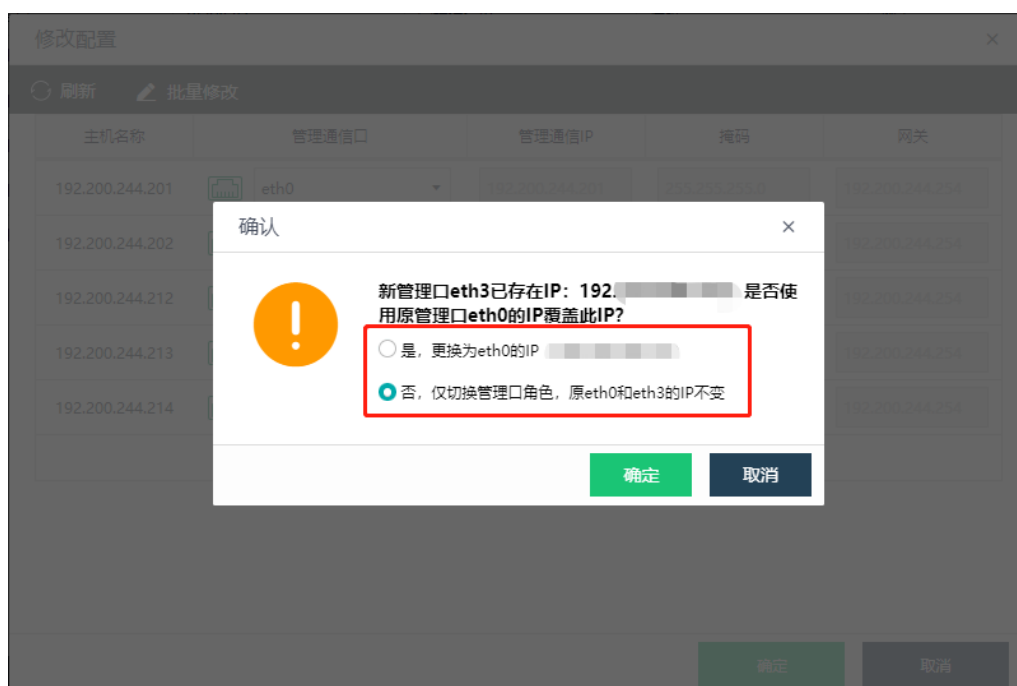


3. 在弹出的提示框点击<确定>。





4. 再次点击<确认>后, 在弹出的确认选项框中选择是否带IP地址切换管理口, 并点击<确定>。



## 10.10. 修改仲裁节点 IP 地址

### 功能说明

当需要调整延伸集群的网络配置时, 需要同步修改仲裁节点的IP使其能跟HCI集群IP正常通信。

注意事项

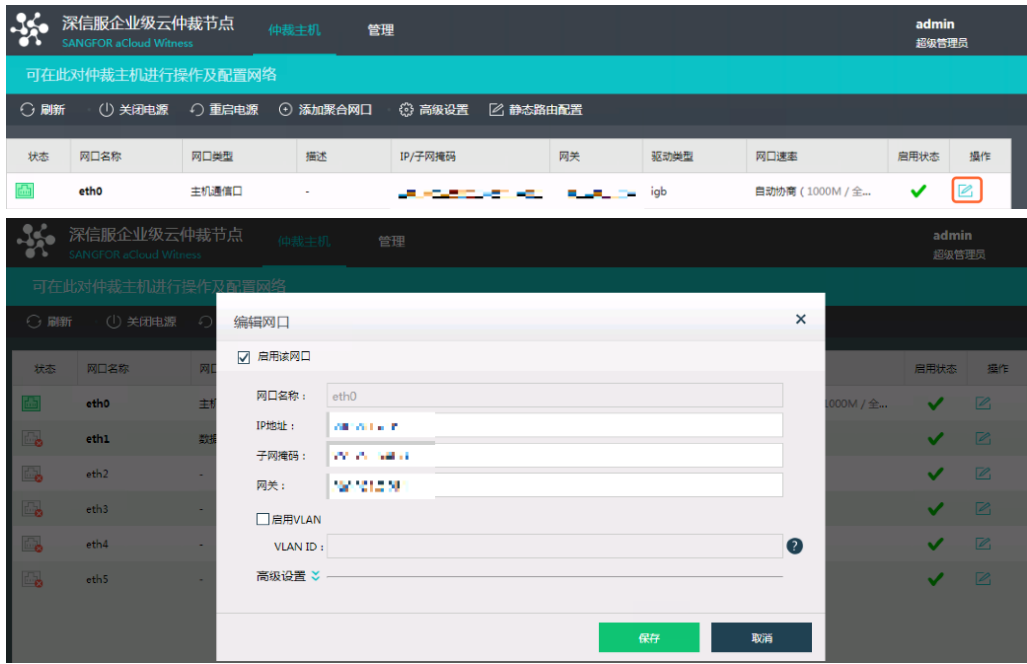
修改前需要确认HCI平台上是否有数据平衡、数据重建任务，如果有这些任务在运行，需要等待任务结束后才能进行修改。

前提条件

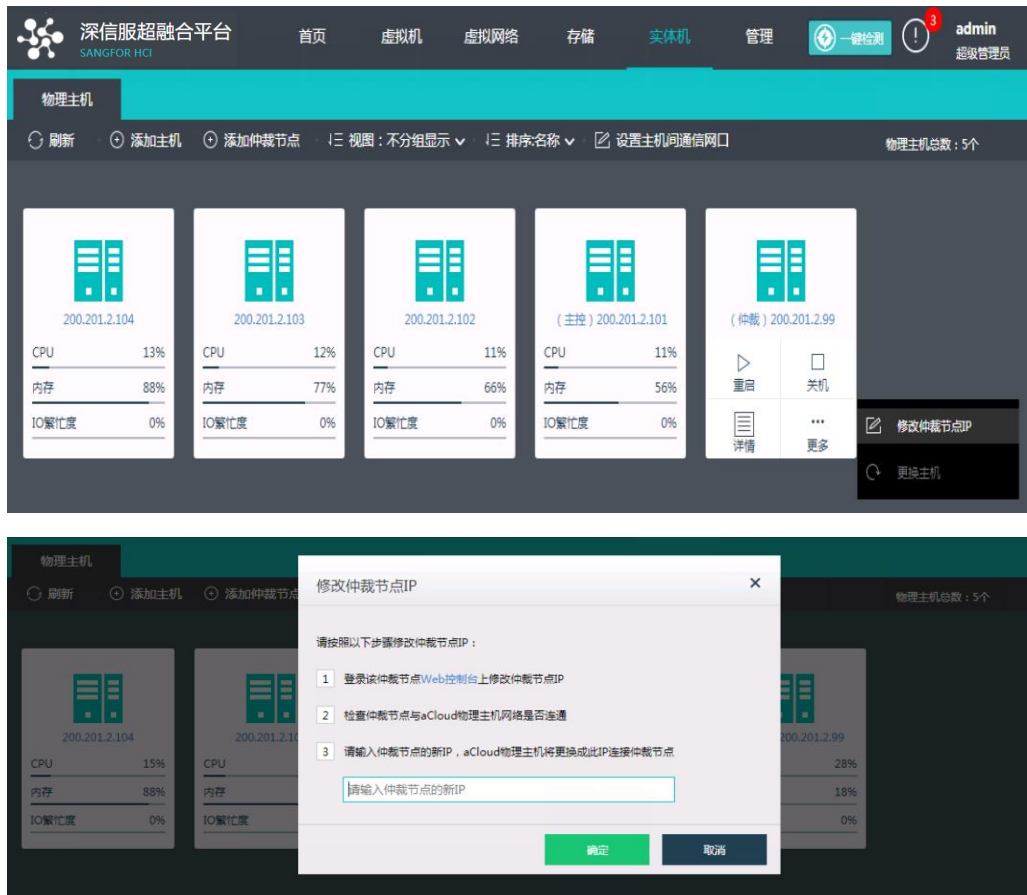
无

操作步骤

- 1. 进入仲裁节点的WEB控制台，将仲裁节点的仲裁网口IP修改为新的IP。



- 2. 检查新修改的仲裁节点的IP与HCI集群网络是否连通，确保仲裁节点能跟HCI集群网络正常通信。
- 3. 登录HCI集群，在[实体机/物理主机]仲裁节点中点击<修改仲裁节点IP>，填写新的仲裁IP，以便让HCI集群连接新的IP。



## 10.11. 数据通信口(VXLAN)配置修改

### 功能说明

1. 用户由于网络规划变更需要修改VXLAN网络对应的物理网口或VXLAN网络对应物理网口的IP地址。
2. 由于部署了容器类等应用导致与VXLAN口默认的端口冲突的情况下，需要修改VXLAN网络使用的端口。

### 注意事项

1. 修改VXLAN网络对应的物理网口、IP地址或端口，都会导致VXLAN网络短暂中断，请在停机窗口期内进行配置的修改。
2. 数据通信口要求使用千兆（或万兆）网口，并使用千兆（或万兆）交换机互联。（只有两台主机时，可以将数据通信口直连）。为了提升数据通信口的接口带宽和冗余，推荐配置聚合口作为数据通信口，此时对端交换机需配置相应的聚合模式。
3. 为了获得较高的网络转发性能，建议将管理通信口和数据通信口(VXLAN)设置

到不同的网口。

4. 不支持将两个不同角色的网口进行直接聚合，可将一个网口角色取消后再进行聚合。例：无法将eth0（管理口）和eth1（vxlan口）直接聚合，可将vxlan口调整为eth2，此时eth0（管理口）和eth1（无角色）可以聚合。

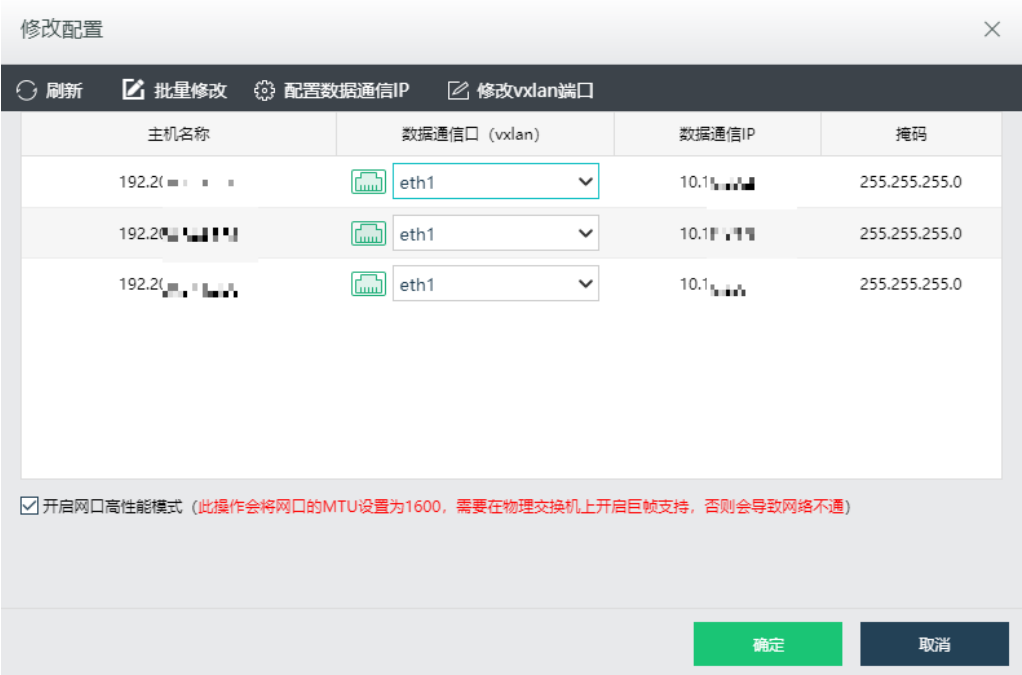
操作步骤

1. 推荐使用聚合网口：在HCI控制台中点击[实体机/物理网络]，点击<批量添加聚合口>，选择两个网口，例：eth2和eth3，聚合模式推荐根据MAC或IP地址进行负载。

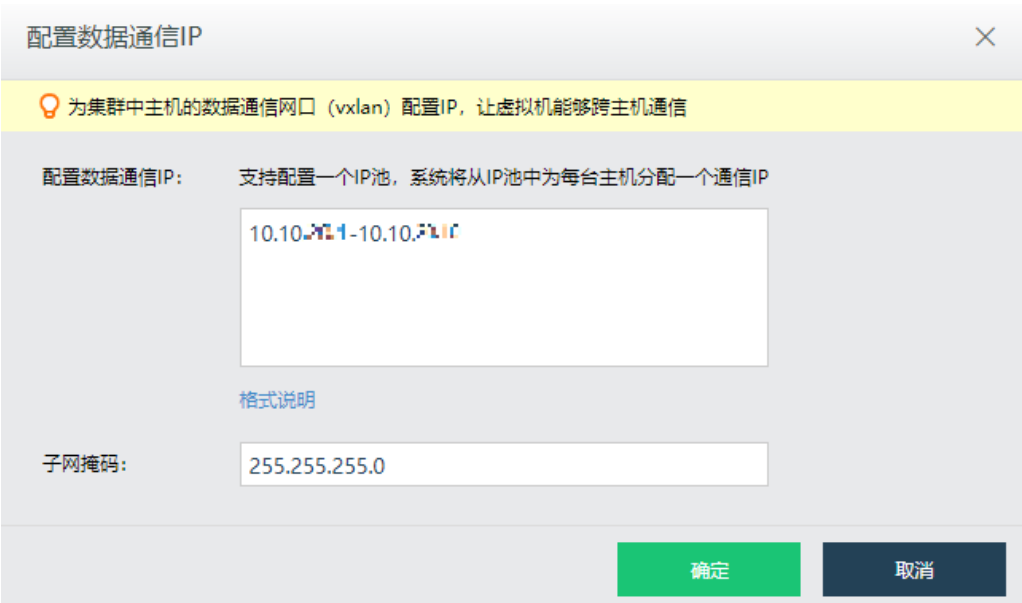


2. 在HCI控制台中点击[实体机/网口功能]。在四个网口角色中找到数据通信口（VXLAN）点击<修改配置>进入到配置页面，可修改数据通信网口。





3. 点击<配置数据通信IP>进行地址配置。在页面中输入数据通信IP所在的IP池以及子网掩码。IP池的范围必须大于等于主机数量。



4. 点击<修改VXLAN端口>进行VXLAN端口的配置，VXLAN端口支持在UDP的8472/4789/4790中进行选择。



5. 通过勾选[开启网口高性能模式], 会将HCI主机网口的MTU设置为1600字节, 这样VXLAN封装的数据发到物理网络时, 不会进行分片, 能显著提升虚拟网络转发性能; 此时对端的物理交换机需启用巨帧（Jumbo Frame）。

10.12. 一键检测的使用

功能说明

- 1. 用在平台部署完毕后, 检查集群各项配置是否正确。
- 2. 排除故障时, 首先用一键检测功能检查平台环境是否正常。

注意事项

- 1. 使用集群环境一键检测功能, 将对您正在运行的现有业务系统性能有一定的影响, 建议您在业务比较空闲的情况下运行。
- 2. 对集群做危险操作前, 例如对主机进行断电, 须先用一键检测检测下集群状态是否正常, 全部都正常的情况下才可进行操作。

前提条件

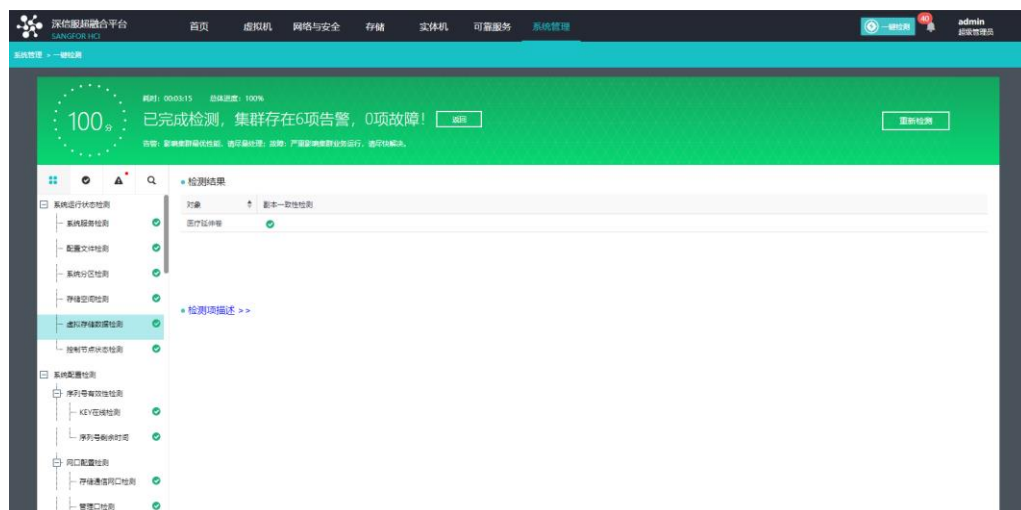
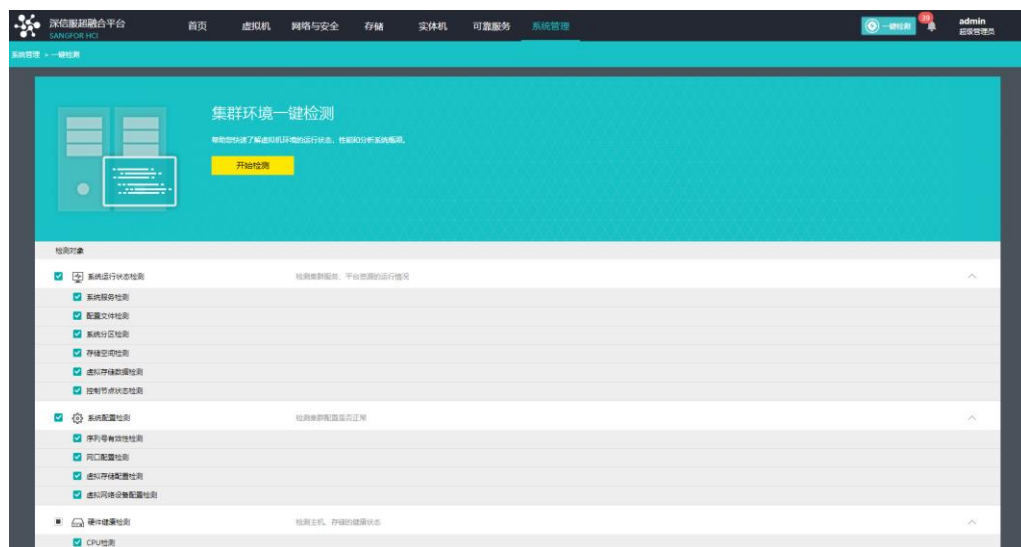
无

操作步骤

- 1. 在首页点击<一键检测>。



2. 勾选需要检测的对象，点击<开始检测>。检测完成之后，界面会得出一个当前集群健康指标分数，并将告警项和故障项标注在列表中。



## 10.13. 系统诊断

### 功能说明

在平常的日常运维过程中，可以通过系统诊断功能在HCI平台上执行一些常见的

Linux命令以快速排查问题。

注意事项

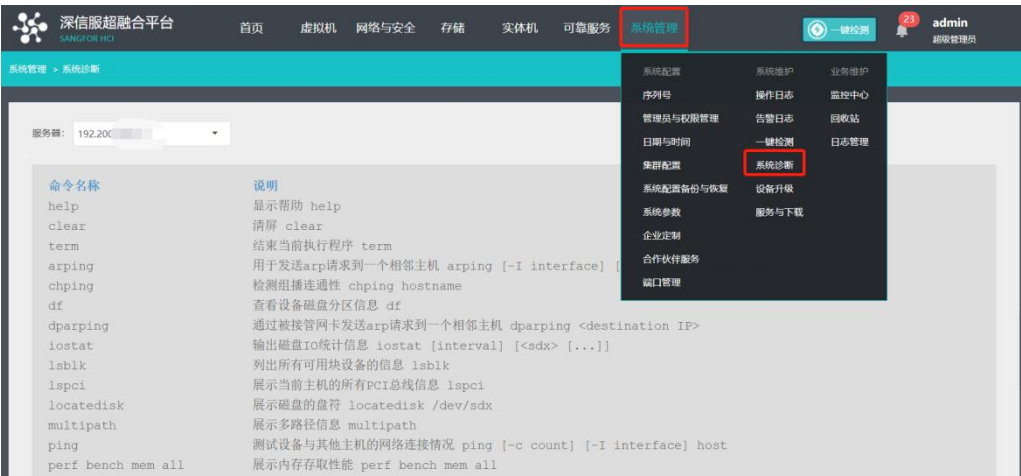
无

前提条件

无

操作步骤

- 1. 打开HCI控制台，并依次找到[系统管理/系统诊断]。



- 2. 切换需要执行命令的主机，执行命令。



## 10.14. 修改平台日期时间

功能说明

当平台时间和真实的时间不一致时需修改平台日期时间。

注意事项



无

## 前提条件

需要平台与外部的NTP服务器网络互通。

## 操作步骤

1. 在控制台中点击[系统管理/日期与时间]。



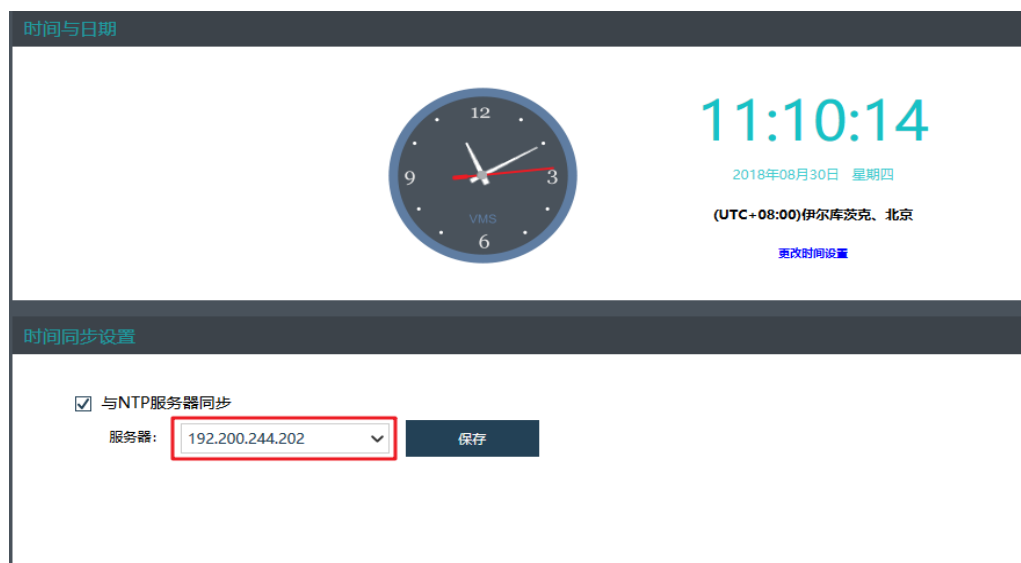
2. 点击[更改时间设置]，进入平台时间设置页面。



3. 这里可以通过点击三角形对时间进行微调，也可以通过获取本地电脑的时间来配置平台的时间。同时也可以修改平台的时区。



4. 如果让平台时间与内部NTP服务器进行同步，只需要勾选“与NTP服务器同步”，同时修改服务器的IP地址保存即可。



## 10.15. 备份和恢复系统配置

### 功能说明

1. 备份系统的相关配置，在遇到问题时进行恢复。系统配置包括：
  - aSV 集群配置。
  - 用户（包含了用户密码，勾选需谨慎）。

- 虚拟机备份策略。
  - 高可用(HA)配置。
  - 动态热添加配置。
  - 用户体验计划。
  - 时间同步设置。
  - 告警条件。
  - 集群资源调度配置。
  - 恢复 NUMA 配置。
2. 平台默认保存30天的系统日志，可以将系统日志手动保存到本地。

## 注意事项

1. 如需对集群的相关配置进行恢复，需联系深信服技术支持处理。
2. 系统备份删除，仅支持删除所有备份文件，不支持单个备份文件的删除。

## 前提条件

无

## 操作步骤

1. 在控制台上打开[系统管理/系统配置备份与恢复/集群配置备份]。



2. 点击[集群配置备份]，就可以设置备份策略，创建或删除备份。



3. 点击[系统日志备份]，就可以将系统日志备份到本地。



## 10.16. 恢复出厂设置（高危操作）

### 功能说明

可以通过恢复出厂设置的方式将整个平台格式化。



**警告：**

请谨慎操作。

### 注意事项

1. 恢复出厂设置后，所有主机将恢复到出厂状态，且会自动移出该aSV，需要重新加入才可以使用。
2. 同时所有该aSV配置的参数信息也会被还原到初始状态，包括：aSV集群配置，用户，虚拟机备份策略，用户体验计划，日期与时间，告警条件。
3. 在系统盘剩余本地存储中的虚拟机不会被删除。

### 前提条件

恢复出厂设置会将平台进行格式化，操作前确保平台上已没有需要的虚拟机。

### 操作步骤

1. 在控制台上打开[系统管理/系统配置备份与恢复/恢复出厂设置]。



2. 在归还测试设备和重置集群配置这两种情况下才可以恢复出厂设置。

恢复出厂设置后，所有主机将恢复到出厂状态，并且会被自动移出该深信服超融合平台。  
同时，该深信服超融合平台的所有参数信息都会被还原到初始状态，包括：集群配置，用户，虚拟机备份策略，日期与时间，告警条件等。  
请谨慎操作！

| 以下情况不可执行恢复出厂设置：           | 如需恢复出厂设置，请您选择原因：             |
|---------------------------|------------------------------|
| 0. 集群扩容（例如：想减少一台主机用作其他用途） | 0. 归还测试设备（例如：归还测试主机）         |
| 1. 解决系统异常问题（例如：系统出现某些错误）  | 1. 重置集群配置（例如：清空集群中所有主机的配置）   |
| 2. 替换主机（例如：更换损坏的主机）       | 若上述原因均不满足，请联系400-630-6430确认。 |

3. 点击[归还测试设备]，弹出[提示]窗口对用户进行警示恢复出厂设置的风险。若用户依然坚持恢复出厂设置，可以点击[继续]，系统会再次弹出[警告]窗口再次警示恢复出厂设置的风险。若用户依然坚持恢复出厂设置，可以点击[继续]，系统会弹出[警告]窗口最后警示恢复出厂设置的风险。若用户依然坚持恢复出厂设置，这窗口中的输入框中键入密码，并点击<确定>，系统将会立即执行恢复出厂设置。

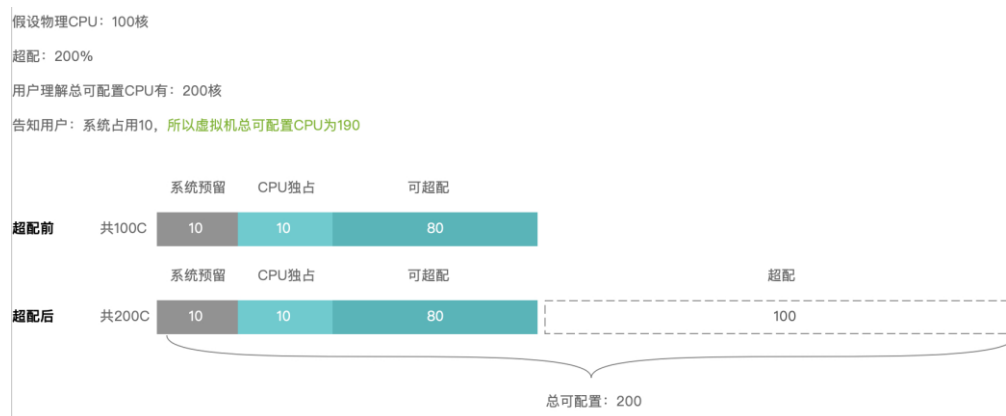




## 10.17. CPU 超配限制配置

### 功能说明

超融合使用虚拟化技术可实现CPU资源的超配复用，但超配过高情况下，可配置资源增加了实际可使用资源并未增加，可能导致虚拟机资源抢占，从而造成虚拟机无法正常运行，CPU超配限制可实现对CPU超配比的人为设定，避免因超配比过高对平台虚拟机产生影响，新建场景下默认超配比为“200%”，在升级场景下默认超配比为“不限制”。



### 注意事项

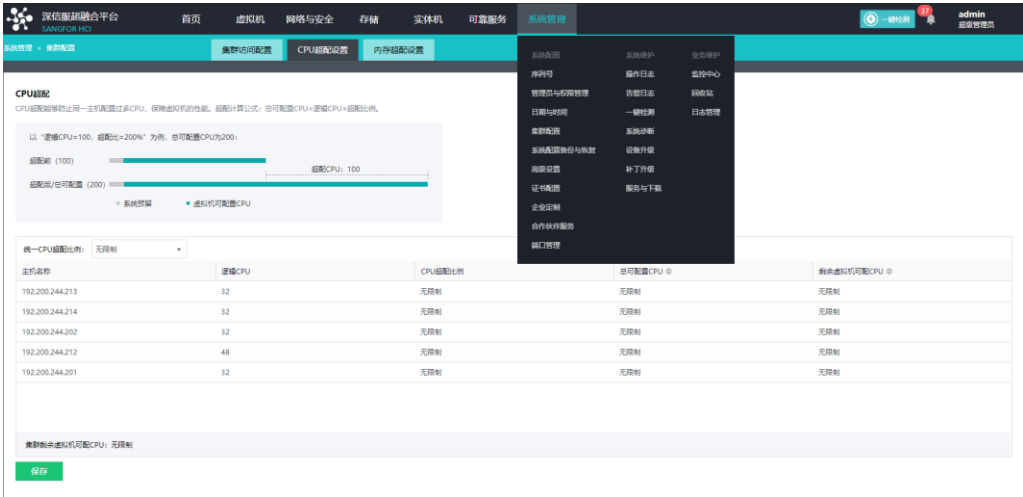
1. CPU超配比限制为100%-500%和不限两种类型。
2. 实际使用CPU超出计算CPU容量时，会导致虚拟机无法开机。
3. 运行中的虚拟机实际配置CPU超出可配置CPU时，会导致虚拟机无法开机。
4. CPU超配比例越大，可启动的虚拟机越多，过高的比例可能会使得虚拟机卡顿，请谨慎设置。核心业务场景不推荐开启CPU超配。

### 前提条件

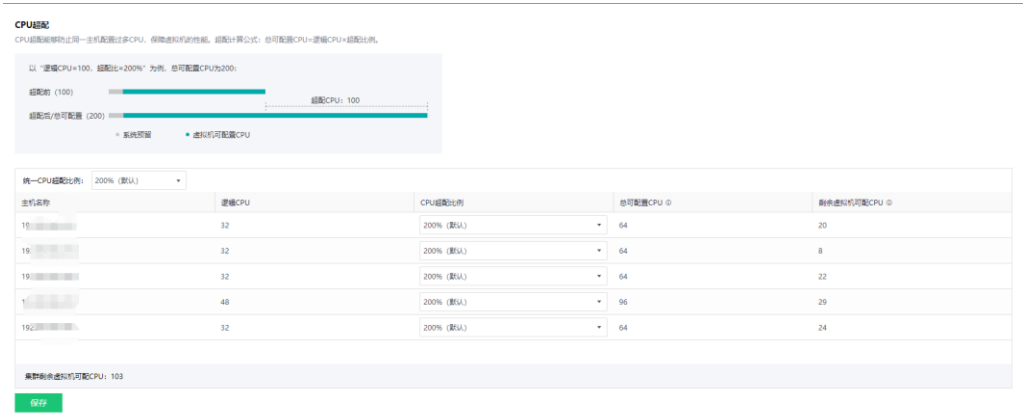
无

操作步骤

1. 在控制台上打开[系统管理/集群配置/CPU超配设置]。



2. 配置CPU超配。



10.18. 内存超配配置

功能说明

配置主机允许的内存超配参数，满足可配置内存超过物理内存的场景。



注意事项

1. 实际使用内存超出计算内存容量时，会导致虚拟机无法开机。

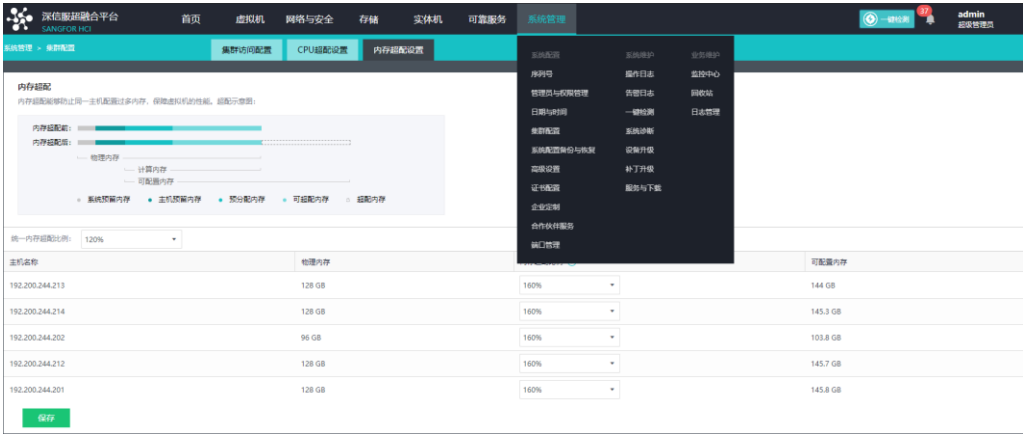
2. 运行中的虚拟机实际配置内存超出可配置内存时，会导致虚拟机无法开机。
3. 热升级后，内存保障机制和超配告警需要重启主机才生效。
4. 内存超配比比例越大，可启动的虚拟机越多，过高的比例可能会使得虚拟机卡顿，请谨慎设置。核心业务场景不推荐开启内存超配。
5. 如果升级前主机的内存超配比大于300%，则升级后，会强制设置为300%。

前提条件

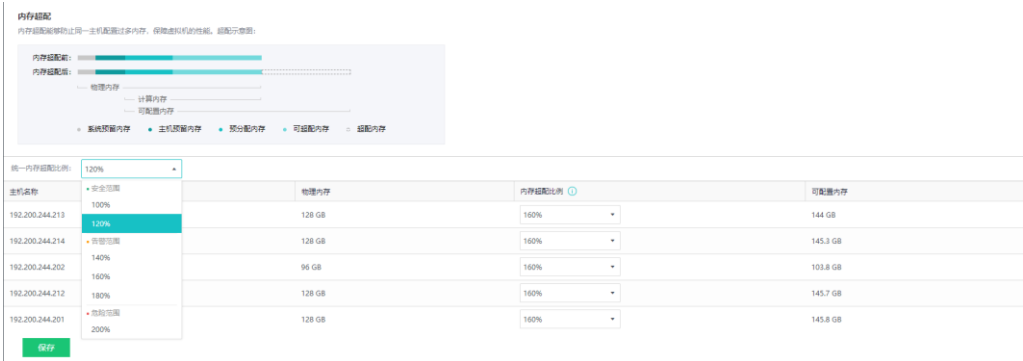
无

操作步骤

1. 在控制台上打开[系统管理/集群配置/内存超配设置]。



2. 配置内存超配。



10.19. 虚拟机逃逸检测

功能说明

虚拟机运行的恶意程序可以利用虚拟化的漏洞，打破虚拟化权限与数据隔离的边界，掌控Hypervisor和宿主机（Host）的攻击行为称之为虚拟机逃逸。



深信服超融合通过虚拟机行为分析，发现可疑事件输出告警日志以供审计。利用沙箱机制，实施多级防护，将被保护对象的权限降到最低，让攻击者即便成功利用了漏洞，能力也是受限的，不足以施展恶意行为。

## 注意事项

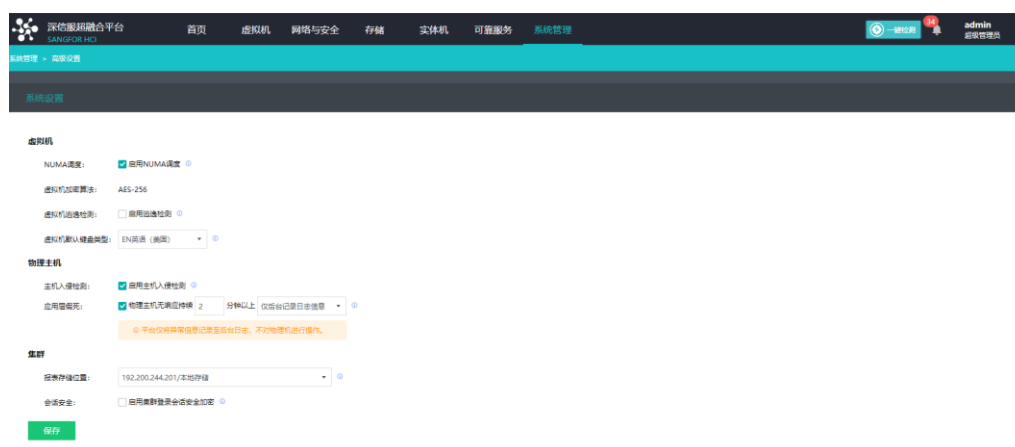
开启虚拟机逃逸检测有一定的性能消耗，需谨慎开启该功能。建议在业务系统过等保要求开启该功能时使用，不做要求则不建议开启。

## 前提条件

无

## 操作步骤

1. 进入[系统管理/系统参数]界面，勾选或取消[启用逃逸检测]复选框来打开或关闭虚拟机逃逸检测功能。



2. 点击<保存>按钮，保存配置。

## 10.20. 合作伙伴服务

### 10.20.1. SIP 安全联动

#### 功能说明

深信服安全态势感知平台SIP支持调用超融合平台接口，通过镜像的方式实时获取超融合集群中的流量，进行流量监控与分析，实现故障前的风险预测与防范、故障及时探测与处理。支持自动隔离中毒虚拟机、自动为风险虚拟机进行存储快照、自动关机/挂起风险虚拟机等功能。

## 注意事项

1. HCI接入SIP之后，可自动同步虚拟机列表到SIP上，无需手动输入IP。
2. 存储快照的场景需要HCI集群支持aSAN存储快照功能，否则SIP不支持使用联动快照功能。
3. SIP对一致性快照组中的虚拟机打快照，会对整个一致性快照组进行快照。
4. 支持将HCI上的NFV设备接入到SIP中。
5. HCI6.3.0及其之后的版本支持SIP联动，SIP版本：SIS3.0.67.0。

## 前提条件

此功能要求SIP和HCI同时开通对应授权。

## 操作步骤

1. HCI默认未启用合作伙伴服务，需要保证HCI拥有授权，进入[系统管理/合作伙伴服务]界面，点击<启用合作伙伴服务>开启功能。



2. 点击<新增服务账户>添加一个可调用对应API接口的账户。



3. 输入新增账户名称、密码、联动产品和开通服务等信息：联动产品可选第三方产品、PAAS、SIP，此处选择SIP，下面会自动识别出SIP的可联动服务模块，

如需更多模块可自行选择。

### 新增服务账户



账户名称：

sip\_test

描述：

密码：

.....



确认密码：

.....

联动产品：

SIP

开通服务：

☒ 全部

☒ 虚拟机

☒ 集群

☒ 网络

☐ 磁盘

☐ 回收站

☐ 存储

确定

取消

4. 进入SIP产品的[系统设置/设备管理]中，添加HCI，在“认证账号”的位置，写入上述在HCI上创建的服务账户，等待资产同步。

新增

\* 接入设备IP:

200.11.11.11

\* 设备名称:

SANGFOR HCI

设备类型:

☐ 上网行为管理(AC)

☐ 终端检测响应平台(EDR)

☐ SSL VPN

☐ 无线控制器(WAC)

☐ 数据库安全审计系统(DAS)

☐ 集中管理平台(BBC)

☐ 应用交付管理系统(AD)

☐ 统一身份安全管理平台(IDTrust)

☒ 超融合(HCI)

正在请求...

STA、AF、FW、云服、云镜无需在感知平台上配置即可支持接入,接入EDR、DAS时先确认平台是否开启7443端口

\* 认证账号

sip\_test

\* 认证密码

●●●●●●●●

测试

备注:

确定

取消

5. 在SIP平台的[响应工具箱/联动响应]中创建联动策略，此处以联动快照为例，配置如下，点击<开始快照>（虚拟机挂起和防火墙一致）。

联动响应

风险对象类型: IP地址

\* 风险IP:

20.1.1.4.2

IP所属:

资产

互联网

HCI虚拟机组-20.1.1.105

快照

联动设备: HCI (对HCI上中毒的虚拟主机进行快照, 备份现场)

设备IP: SANGFOR HCI(20.1.1.15)

快照

开始快照

## 10.20.2. PAAS 联动

### 功能说明

深信服容器云KubeManager 平台支持对接深信服虚拟存储 aSAN 或文件存储 NFS 进行数据持久化存储，用户可以将业务的数据存储在应用程序 Pod 的外部，当应用程序的 Pod 发生故障时，可以保护应用数据不受影响。将 KubeManager 平台与深信服 NFS 或 aSAN 存储进行对接，需要使用合作伙伴服务中PAAS联动功能。

### 注意事项

无

### 前提条件

1. 超融合平台需开通 aSI 授权。
2. KubeManager 平台与超融合平台的管理平面能正常通信。

### 操作步骤

1. 登录超融合平台，选择[系统管理/合作伙伴服务]，点击<新增服务账号>。
2. 自定义服务账户信息：
  - 账户名称：服务账户名称，例如：simon。
  - 描述：账户描述，例如：simon-paas。
  - 密码：服务账户密码。
  - 联动产品：PaaS。
  - 开通服务：勾选存储（默认已勾选）。
3. 点击<确定>后，服务账户添加完毕。

4. 登录 KubeManager 平台，切换至需要添加存储服务器的集群下，选择[存储/存储服务器]，点击<添加存储服务器>。



5. 输入存储服务器的名称，选择对应的存储类型，配置服务器基本信息。
  - a. 名称：自定义服务器名称。
  - b. 类型：支持 Sangfor NFS 和 Sangfor aSAN 两种存储服务器；推荐使用 Sangfor aSAN，可靠性高、性能稳定。
  - c. NFS 服务器信息：
    - 服务器地址：NFS 服务器的地址。
    - 存储路径：NFS 服务器存储的路径。
    - 版本：NFS 服务器的版本。
  - d. aSAN 服务器信息：
    - 网关地址：https:// HCI 集群 IP:4433。
    - 认证用户：步骤 2 中添加的服务账号名称。
    - 用户认证密码：步骤 2 中添加的服务账号的密码。
6. 点击<保存>，完成存储服务器的添加。

## 10.21. VMware 异构管理

### 10.21.1. 添加 vCenter

#### 功能说明

HCI平台通过添加vCenter平台实现对VMware进行管理。实现在HCI平台纳管所有VMware虚拟机，并可以配置VMware虚拟机在HCI平台进行备份。

#### 注意事项

无

#### 前提条件

1. HCI平台需要开启异构管理的授权。
2. 支持 vCenter5.0 、 vCenter5.1 、 vCenter5.5 、 vCenter6.0 、 vCenter6.5 和 vCenter6.7、vCenter7.0、vCenter7.0.1、vCenter7.0.2版本。

3. 保证HCI平台的管理IP和vCenter能够正常通信。
4. 添加vCenter的时候，vCenter账号需要具备管理员的权限。

## 操作步骤

1. 在[实体机/VMware vCenter]中点击<添加vCenter>。



2. 配置名称、vCenter地址、用户名、密码和端口等信息，配置完成后点<确定>。

The screenshot shows the 'Add vCenter' configuration form in the Sangfor HCI management console. The form is titled '请填写vCenter帐号信息并连接到该系统' (Please fill in vCenter account information and connect to the system). Below the title, there is a yellow warning box with the text: '① 添加的vCenter中如果存在以域名或主机名形式纳管的ESXi主机，请及时配置DNS服务，以免影响后续对vmware云主机的迁移与备份。 DNS配置：实体机->物理网络->主机高级设置->其他配置' (① If there are ESXi hosts managed by domain or host name in the added vCenter, please configure DNS service in time to avoid affecting the subsequent migration and backup of VMware cloud hosts. DNS configuration: Physical Machine -> Physical Network -> Host Advanced Settings -> Other Settings). The form fields are: '名称' (Name) with a placeholder '请设置仅在HCI显示的自定义名称' (Please set a custom name only displayed in HCI), 'vCenter地址' (vCenter Address) with a placeholder '请输入IP' (Please enter IP), '用户名' (Username), '密码' (Password), '端口' (Port) with a value of '443', and '描述' (Description) with a placeholder '选填' (Optional). A '连接' (Connect) button is at the bottom.

3. 配置完成后，在[实体机/VMware vCenter]中就可以看到vCenter的状态。

## 10.21.2. 管理 VMware 虚拟机

### 10.21.2.1. 新建 VMware 虚拟机

#### 功能说明

HCI支持对VMware进行新建、删除、开机、关机、挂起、重启、关闭电源、打开控制台等操作。

#### 注意事项

无

## 前提条件

1. 要想实现对VMware上的虚拟机进行关机操作，需要VMware虚拟机安装VMtools。
2. 要打开VMware虚拟机的控制台，需要安装VMware Remote Console工具。
3. 在HCI平台上新建VMware虚拟机，需要VMware平台上有相应的虚拟机模版。
4. VMware虚拟机，先安装好深信服性能优化工具，再备份恢复到HCI时IP才能自动恢复。

## 操作步骤

1. 在[虚拟机/VMware虚拟机]中点击<新增>。

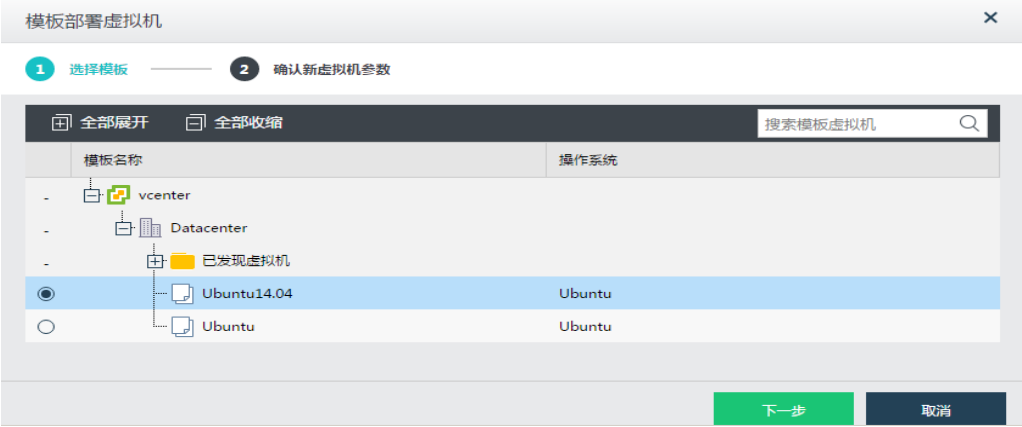


2. 创建方式选择<从模版部署虚拟机>。

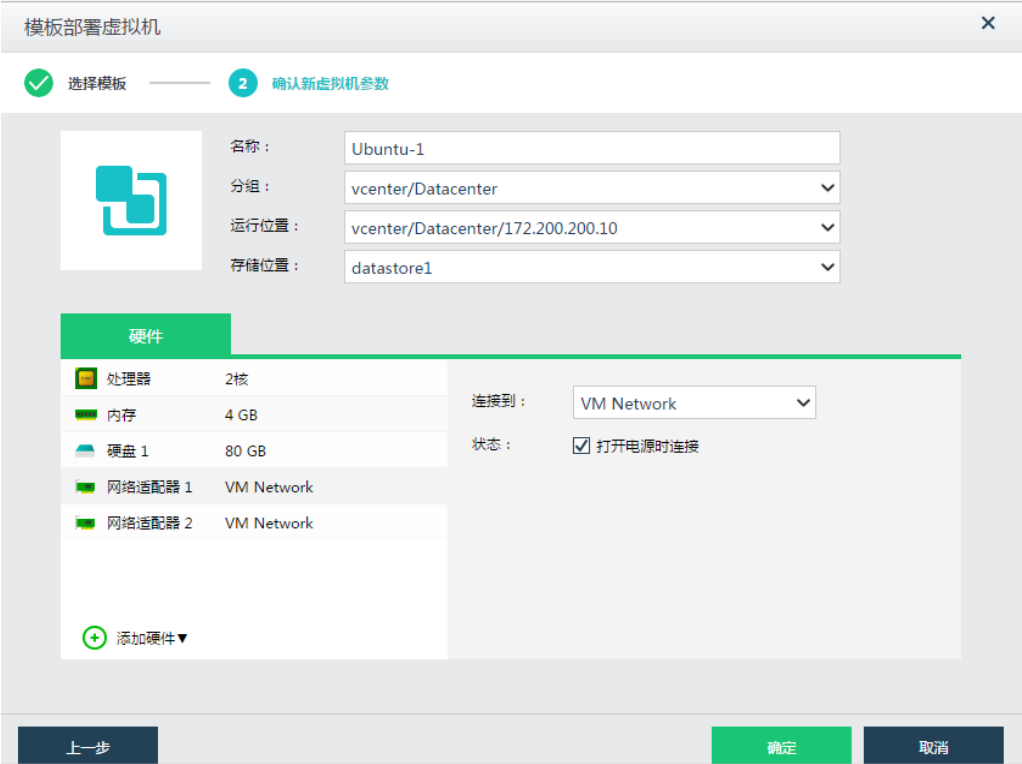


3. 选择虚拟机模版，点击<下一步>。





4. 配置虚拟机的名称、分组、运行位置、存储位置以及硬件相关的信息，配置完成后点<确定>。



### 10.21.2.2. 删除 VMware 虚拟机

#### 功能说明

HCI支持对VMware进行新建、删除、开机、关机、挂起、重启、关闭电源、打开控制台等操作。

#### 注意事项

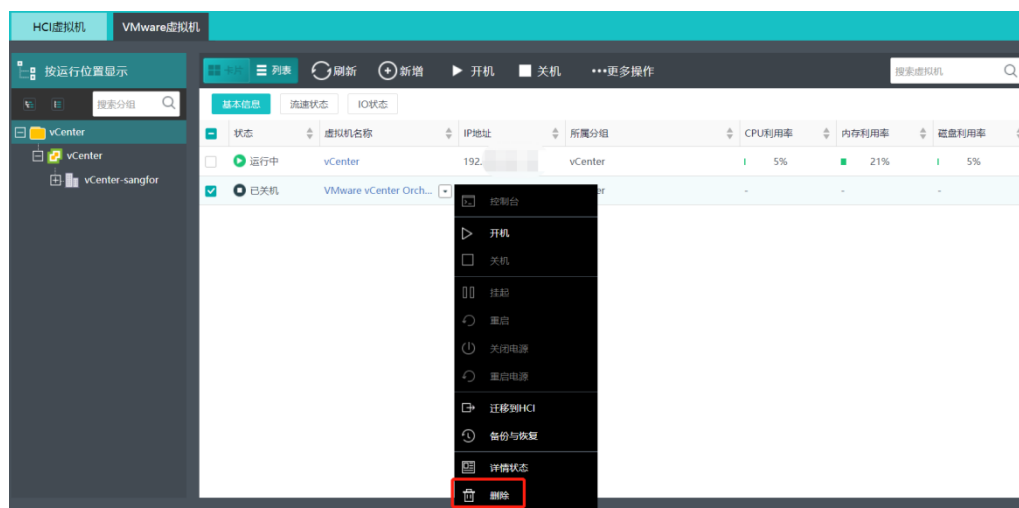
确认该虚拟机已经没有在用了，可以从VMware平台上删除，删除后虚拟机无法恢复。

## 前提条件

无

## 操作步骤

1. 在[虚拟机/VMware虚拟机]中找到需要删除的虚拟机，点击按钮，找到[删除]菜单项，点击<删除>。



2. 等任务完成后，该虚拟机已经成功删除。

### 10.21.2.3. 虚拟机开关机操作（开机、关机、重启、挂起）

#### 功能说明

HCI支持对VMware进行新建、删除、开机、关机、挂起、重启、关闭电源、打开控制台等操作。

#### 注意事项

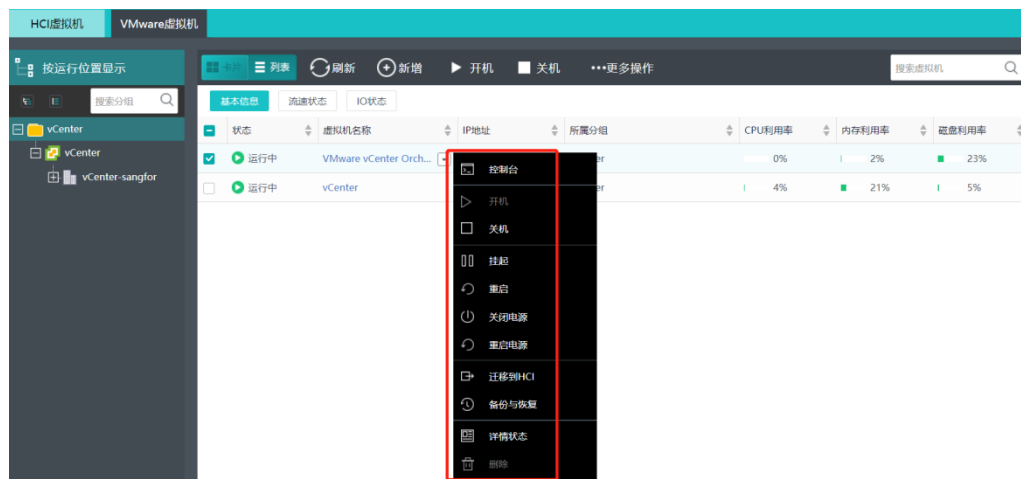
装完VMtools要重启虚拟机完成，不能直接关掉电源，否则可能导致蓝屏、驱动异常等问题。

#### 前提条件

1. 要想实现对VMware上的虚拟机进行关机操作，需要VMware虚拟机安装VMtools。
2. 要打开VMware虚拟机的控制台，需要安装VMware Remote Console工具。
3. 在HCI平台上新建VMware虚拟机，需要VMware平台上有相应的虚拟机模版。

## 操作步骤

1. 在[虚拟机/VMware虚拟机]中找到需要操作的虚拟机，点击按钮，找到操作菜单。



2. 按照菜单进行操作即可。

## 10.21.3. VMware 虚拟机的备份

### 功能说明

HCI支持将VMware虚拟机备份到自己的平台上，并且支持将备份的虚拟机恢复到HCI平台或者VMware平台。

### 注意事项

无

### 前提条件

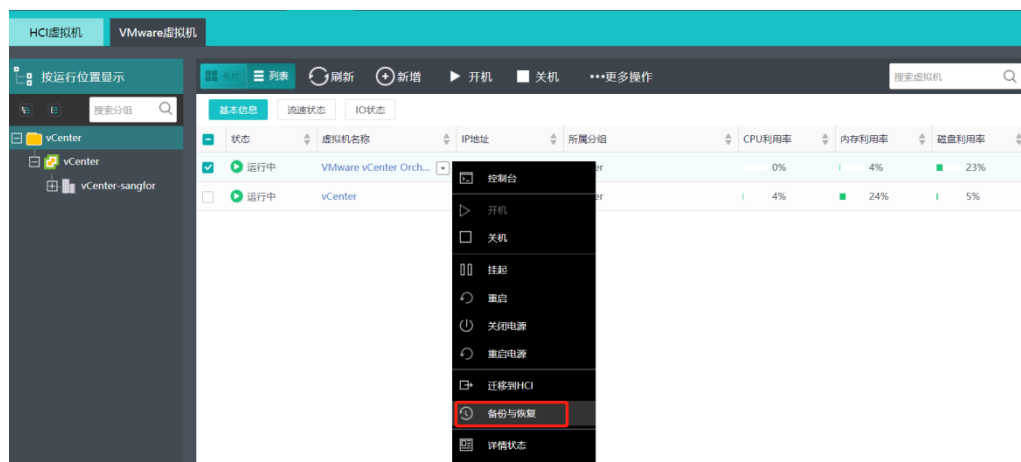
HCI需要开启备份虚拟机个数授权。

## 操作步骤

1. 在[虚拟机/VMware虚拟机]中找到需要备份的虚拟机。



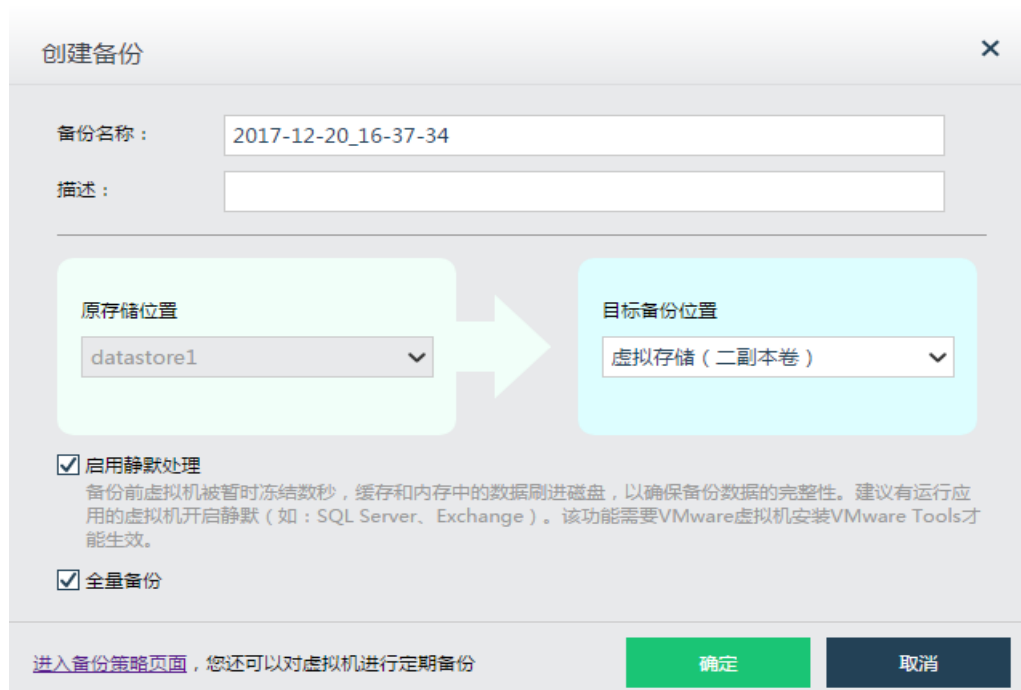
2. 点击  按钮，选择[备份与恢复]菜单项。



3. 进入备份界面后，点击<立即备份>。



4. 配置备份名称、目标备份位置，勾选“启用静默处理”和“全量备份”，然后点击<确定>后就开始备份了。



## 10.21.4. VMware 虚拟机的恢复

### 功能说明

HCI支持将VMware虚拟机备份到HCI平台上，并且支持将备份的虚拟机恢复到HCI平台或者VMware平台。

### 注意事项

VMware虚拟机在HCI平台从备份恢复时会自动安装性能优化工具。

### 前提条件

VMware虚拟机已经做好了备份。

### 操作步骤

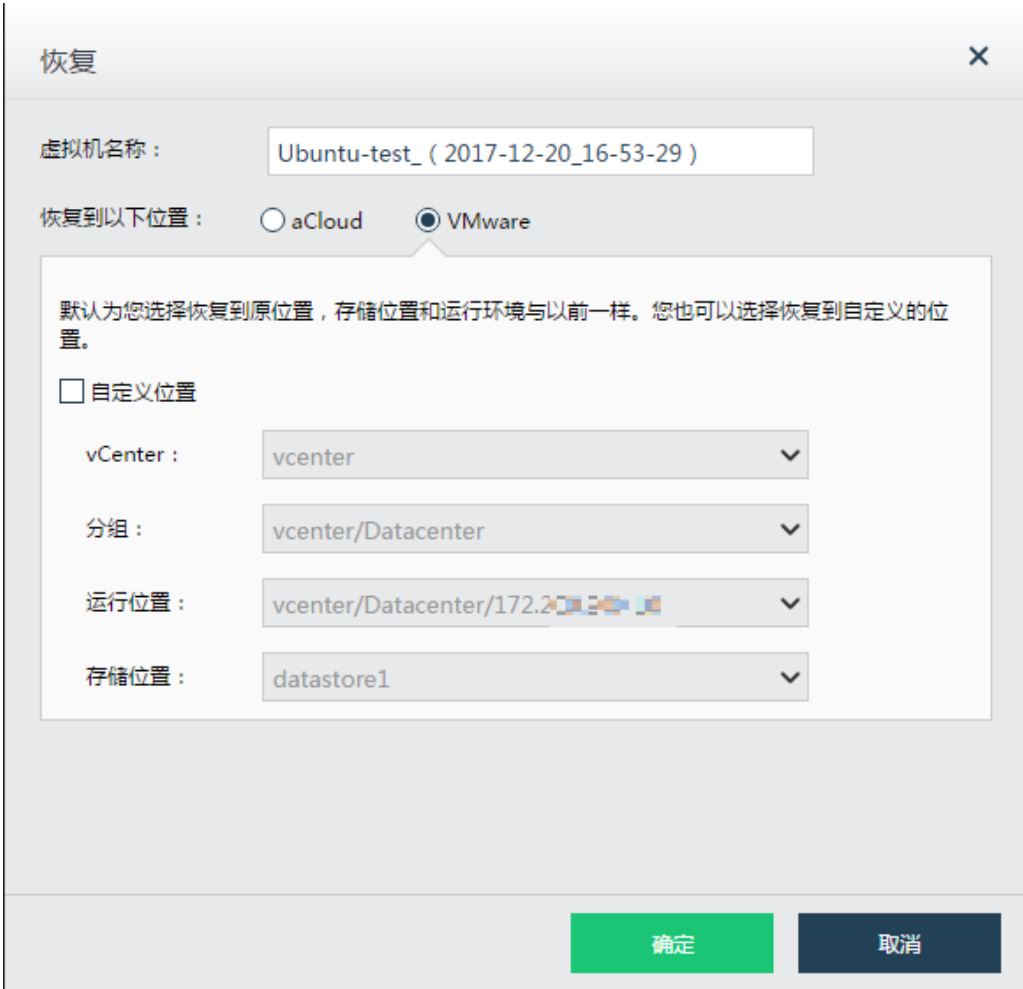
1. 在[可靠服务/备份与CDP/VMware备份文件]中找到需要恢复备份的虚拟机。



2. 点击<恢复>进入恢复确认界面。



3. 选择恢复的位置，支持恢复到HCI和VMware平台，然后点击<确定>。



4. 会弹出如下提示，再次点击<确定>后就开始恢复。



## 10.21.5. 迁移 VMware 虚拟机到 HCI 平台

### 功能说明

HCI平台支持将VMware平台的虚拟机迁移到自己的平台上进行运行，可以在开机状态下进行迁移，在迁移的最后阶段关闭VMware平台的虚拟机完成迁移。

### 注意事项

1. 已经迁移到HCI的VMware虚拟机回迁到VMware，需要卸载性能优化工具，性能优化工具会禁用VMware的VMtools。
2. Centos 7.0、7.1以及之前版本的Centos系统，在VMware平台以EFI固件形式启动的虚拟机，进行P2V迁移到HCI平台后，目标虚拟机第一次启动正常，第二次启动可能会进入EFI shell，重启后可以正常。
3. VMware虚拟机迁移到HCI平台时，会自动安装性能优化工具。
4. 支持的VMware版本：

VMware 5.0 、VMware 5.1、VMware 5.5、VMware 6.0、VMware 6.5。

aCloud 5.8.7 R1之后版本支持VMware 6.7 。

5. 迁移过程中如果取消迁移，HCI不会删除已经迁移过来的虚拟机，在HCI网络拓扑上可查看到虚拟机，需手动删除。

### 前提条件

无

### 操作步骤

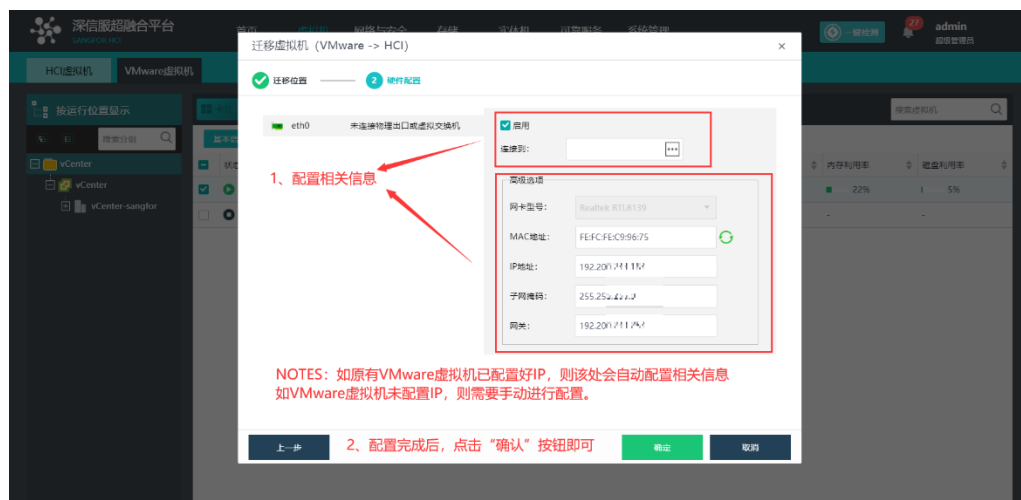
1. 在[虚拟机/VMware虚拟机]中找到需要迁移到HCI平台上的虚拟机，选择迁移到HCI。



2. 进入性能优化工具自动安装配置，支持配置名称、分组、位置等迁移信息。



3. 点击<下一步>，进入迁移后虚拟机硬件配置，支持配置网卡连接、网卡型号、MAC地址、IP地址等信息。如果原有VMware虚拟机已配置好IP，则会自动配置相关信息，如VMware虚拟机未配置IP，则需要手动进行配置。



4. 配置完成，点击<确定>之后就开始迁移。



## 10.22. 仲裁节点故障处理（高危操作）

### 功能说明

当集群中的仲裁节点由于物理故障离线时，需要用一台新主机进行替换。

### 注意事项

1. 要求新仲裁节点的配置不能低于原故障仲裁节点的配置。
2. 建议新仲裁节点的仲裁盘的容量和老仲裁节点的一致。
3. 更换仲裁节点的管理IP地址不能和原仲裁节点相同。

### 前提条件

1. 用于替换的仲裁节点系统已经安装好并且已配置好IP地址。
2. 用于替换的仲裁节点系统的IP地址能够正常与HCI集群进行通信。

### 操作步骤

1. 在[实体机/物理主机]中找到故障仲裁节点，点击<更换主机>。



2. 输入新的仲裁节点的IP和密码。

更换仲裁节点

1 更换前准备

2 替换主机硬盘

3 确认配置

请按以下步骤操作：

1

用OVA模板部署仲裁节点虚拟机，或者准备一台物理主机，下载并安装仲裁软件（[下载Sangfor Witness软件](#)）

2

输入主机IP和账号密码

仲裁节点IP

用户名：

admin

密码：

请输入admin的密码

下一步

取消

3. 更换仲裁盘后，确认配置即可。

更换仲裁节点

1 更换前准备

2 替换主机硬盘

3 确认配置

主机硬盘替换成功。

| 原主机硬盘 |       |      |      | 替换为  | 新主机硬盘 |       |      |
|-------|-------|------|------|------|-------|-------|------|
| 硬盘名称  | 硬盘大小  | 硬盘类型 | 硬盘属性 | 替换情况 | 硬盘名称  | 硬盘大小  | 硬盘类型 |
| DiskA | 500GB | 机械硬盘 | 仲裁盘  | ✓    | DiskA | 500GB | 机械硬盘 |

上一步

下一步

取消

## 10.23. 版本升级

### 功能说明

对HCI集群进行版本升级。

### 注意事项

- 热升级出现任何形式的失败，请一定不要擅自关闭维护模式，也不要擅自回滚和失败重试，请保留完整现场，联系技术支持处理。
- 若当前版本和目标版本支持热升级，请确保在客户业务量比较空闲的时间升级，升级过程中，数据库的TPM值会略有下降，持续1min左右恢复。

文档版本 06（2023-02-21）

461

3. 热升级成功后，请确保一定要手动关闭维护模式。
4. 热升级会对使用USB映射的虚拟机短暂中断USB映射10s，如果有用户的业务依赖USB，请先确认。
5. 升级过程中可能会出现页面提示通信超时，不能去动升级页面，只有页面提示需要重试的时候再手动点重试。
6. HCI6.8.0及其之后的版本升级支持滚动热升级，能够保障集群中的主机分批升级，最终达到整体完成升级。其中：
  - 本地存储的虚拟机、有直通设备（比如 GPU 直通、USB 直通、网卡直通等）的虚拟机、调度策略限制的虚拟机、其他节点资源不足的情况。需手动处理（关机、修改配置）后，重试升级。

## 前提条件

无

## 操作步骤

具体注意事项及操作步骤请参考当前版本的升级方案。升级方案请登录“[深信服社区-自助服务-软件下载](#)”页面，可以找到对应版本的升级包以及相应的升级方案。

## 10.24. 单主机维护模式

### 功能说明

硬件维护场景，当管理员需要对主机进行下电操作时，可以使用主机维护模式，启动维护模式后系统会先将平台上的业务迁移到其它主机上，确保替换过程中不对业务造成影响。通过维护模式可以达到自运维的效果。

### 注意事项

1. 主控不支持进入单主机维护模式，如果需要维护主控请先切换其他主机为主控。
2. 环境上有主机离线不能进入单主机维护模式。
3. 待维护主机上有任务在进行暂时不能进入单主机维护模式，需要等待任务完成后方可进入。
4. 目前仅允许同时有一台主机进入单主机维护模式。

## 前提条件

无

## 操作步骤

1. 在[实体机/更多]，选择进入单主机维护模式。



2. 输入密码后选择<确定>进入主机维护模式，此时系统会将主机进行隔离处理。



### 确定进入维护模式?

当前主机上没有正在运行的虚拟机或网络设备。进入维护模式后，可以对主机进行关机、重启、更换主机（主机为关机状态）操作。

**注意：**

- 1、如果虚拟机正在进行其它操作（例如正在进行CDP备份），则会导致进入单主机维护模式失败，您可以等任务完成后重试！
- 2、如果您选择的设备操作方式不合理（例如找不到合适的主机迁移虚拟机设备），您可以手动处理或者重新选择后再进入单主机维护模式！
- 3、进入主机维护模式后，该主机上的数据副本将停止服务，请完成处理后及时退出维护模式！

☐ 进入维护模式后，主机自动关机

请输入当前登录用户（admin）的密码来确认此操作。

请输入密码

确定

取消

3. 主机进入维护模式成功，可以开始对主机执行下电等运维操作。



## 10.25. 虚拟机磁盘加密

### 功能说明

启用虚拟机磁盘加密可以提高虚拟机磁盘的安全性。等保检测时镜像与快照的加密保护可通过对虚拟机磁盘加密实现。

## 注意事项

1. 虚拟机磁盘加密，支持AES 256对称加密算法。
2. 一个虚拟机一个加密选项，开启之后整个虚拟机都为加密虚拟机。
3. 一个虚拟机一个密钥，加密之后全部磁盘的密钥都为同一个。
4. 启用虚拟机磁盘加密后不可进行取消。
5. 虚拟机磁盘加密后不可逆，即无法解除加密。
6. 磁盘加密的虚拟机无法进行导出、克隆、模板部署等操作。
7. 平台加密功能采用纯软加密的方式，无需客户额外购买加密卡、加密机等硬件。
8. 密钥管理的功能全部在平台内模拟KMS实现。
9. 虚拟机加密在创建时或关机状态下进行，对已有业务的虚拟机进行加密需申请在无业务访问的时间窗口进行。
10. 虚拟机加密后，对磁盘数据读写需要进行加密和解密操作，有一定的性能消耗，需谨慎开启虚拟机加密功能。

## 前提条件

无

## 操作步骤

1. 进入[系统管理/系统参数]界面，查看虚拟机加密算法。



2. 打开[虚拟机] 页面，确保需要加密的虚拟机为关机状态。

- 3. 点击要加密的虚拟机<更多/其他操作/转换为加密虚拟机>选项，对虚拟机进行加密。
- 4. 加密完成后，[虚拟机] 页面会显示该虚拟机已被加密的标记。

|                                     |                                  |     |                               |   |             |                          |
|-------------------------------------|----------------------------------|-----|-------------------------------|---|-------------|--------------------------|
| <input checked="" type="checkbox"/> | <input checked="" type="radio"/> | 已关机 | test                          |   | -           | 默认分组                     |
| <input type="checkbox"/>            | <input checked="" type="radio"/> | 已关机 | test-centos_acmp-3ce0         |   | 192.168.0.2 | acmp_2020-07-30-14-55-47 |
| <input type="checkbox"/>            | <input checked="" type="radio"/> | 已关机 | test1_1_5ee03601_210_a9f6a5fa | - | -           | 默认分组                     |

10.26. 回收站

功能说明

用户在web控制台上删除虚拟网络设备、虚拟机、虚拟共享盘等会暂时保存在回收站中，防止由于误操作导致的数据丢失。在回收站中的文件支持恢复和彻底删除，如未手动执行彻底删除或清空回收站的动作，回收站文件将默认保留30天，之后会彻底删除。

注意事项

- 1. 回收站中彻底删除和清空回收站是高危操作，请确认回收站中的文件已经不再使用时在执行彻底删除或清空回收站的操作。
- 2. 回收站中的网络设备、虚拟机和虚拟共享盘支持在web控制台还原和彻底删除。残留目录（虚拟机备份）只支持在web控制台彻底删除，不支持还原。
- 3. 还原回收站中的文件，只会将文件还原，设备间的连接关系不会还原。

操作步骤

- 1. 进入[系统管理/回收站]界面，选择要还原的文件类型标签（“虚拟机”、“基础网络设备”、“网络安全设备”“虚拟共享盘”），勾选需要还原的文件，点击<还原>。

| 名称                                       | 描述 | 加密状态 | 存储                           | 类型 | 实际占用空间 | 删除时间                | 保留时间    |
|------------------------------------------|----|------|------------------------------|----|--------|---------------------|---------|
| <input checked="" type="checkbox"/> test | -  | 未加密  | 医疗延伸卷                        | 普通 | 200 GB | 2021-10-27 11:21:27 | 24天后可删除 |
| <input type="checkbox"/> test            | -  | 未加密  | TSANGFOR_ASAN-028-Safe-4a... | 普通 | 1.4 GB | 2021-10-19 17:19:55 | 16天后可删除 |
| <input type="checkbox"/> Server2008R09   | -  | 未加密  | 医疗延伸卷                        | 普通 | 93 GB  | 2021-10-29 18:31:19 | 26天后可删除 |

- 2. 点击<彻底删除>会将网络设备、虚拟机或虚拟机共享盘彻底删除，无法恢复。（高危操作）
- 3. 点击<清空回收站>会将该标签下的所有文件彻底删除，无法恢复。（高危操作）

## 10.27. 剩余信息保护

### 功能说明

HCI 剩余信息保护功能，可以使用户在资源回收时选择彻底擦除已有数据。等保或涉密场景要求存储空间在回收时，支持数据擦除，保证重要数据的安全性，用户可根据监管需求或业务需要，自定义覆写次数在资源回收时选择彻底擦除已有数据。

### 注意事项

1. 在使用数据擦除功能时会占用CPU和IO资源，同时擦除过程需要一定时间，故建议在业务空闲时进行。
2. 擦除后数据将无法恢复。
3. 擦除速率修改后，将对所有的数据擦除任务生效，实际速率会根据存储IO性能和繁忙程度动态调整。

### 操作步骤

1. 进入[系统管理/回收站]界面，点击[设置]页签配置数据擦除速率和擦除速度。
2. 默认勾选“启用残余数据保护”开启后，在删除回收站中的虚拟网络设备、虚拟机、虚拟共享盘、残余目录，以及删除虚拟机的虚拟磁盘的时，同时擦除数据，以保证数据安全。



3. 点击[虚拟机]页签。选中虚拟机，点击<彻底删除>，或点击<清空回收站>操作会提示“同时擦除虚拟机的业务数据”选项。勾选该选项，输入HCI 管理员密码即可彻底擦除虚拟机的业务数据。





## 10.28. 报表位置管理

### 功能说明

集群报表数据记录着集群各资源的趋势数据，用于用户查询1小时、24小时、1月的趋势数据，在集群模式中，为实现报表数据的高可用性，支持更改数据存储位置。

### 注意事项

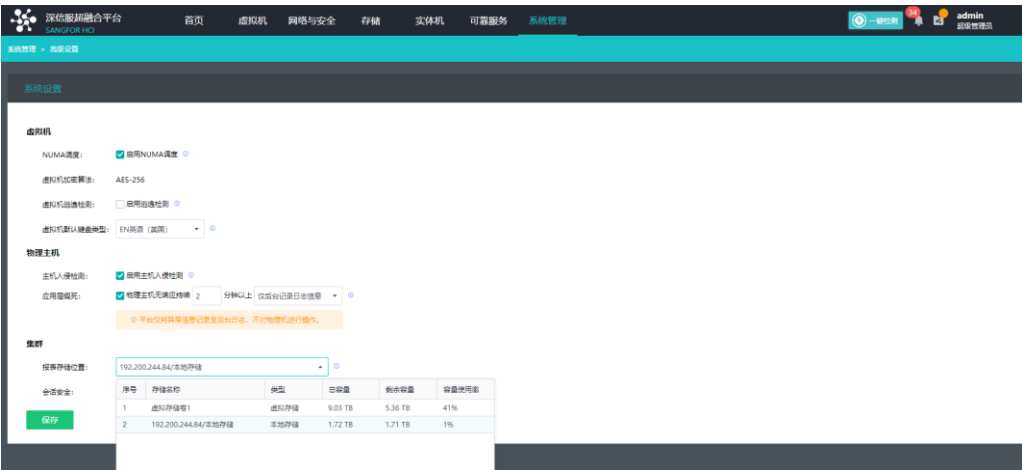
仅支持系统盘本地存储、虚拟存储（2主机VS卷不支持）、iSCSI存储和FC存储。

### 前提条件

无

### 操作步骤

进入[系统管理/高级设置]界面，选择保存存储位置，并点击<保存>。



## 10.29. 企业定制

### 功能说明

深信服超融合平台支持用户自定义设置企业定制信息，包括基础信息、图标自定义、链接自定义、功能禁用。

### 注意事项

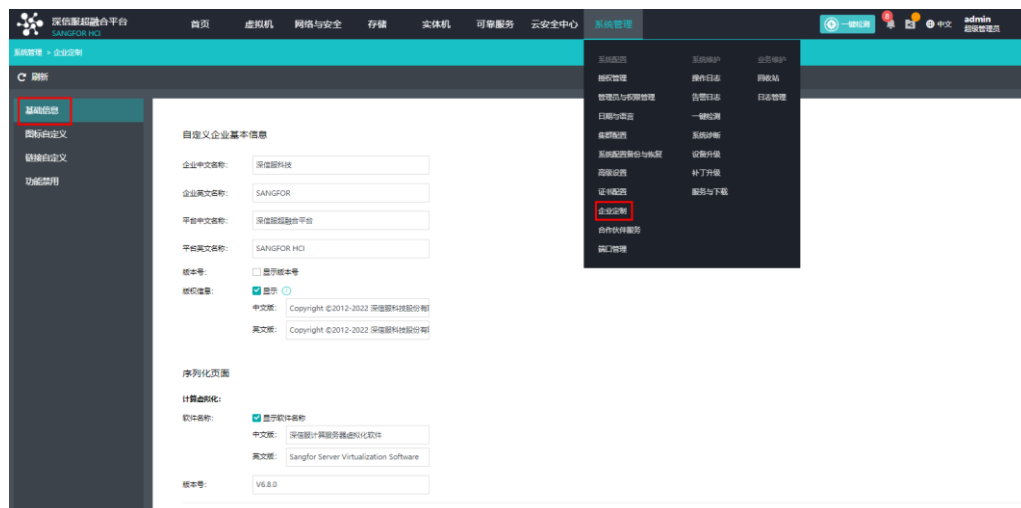
无

### 前提条件

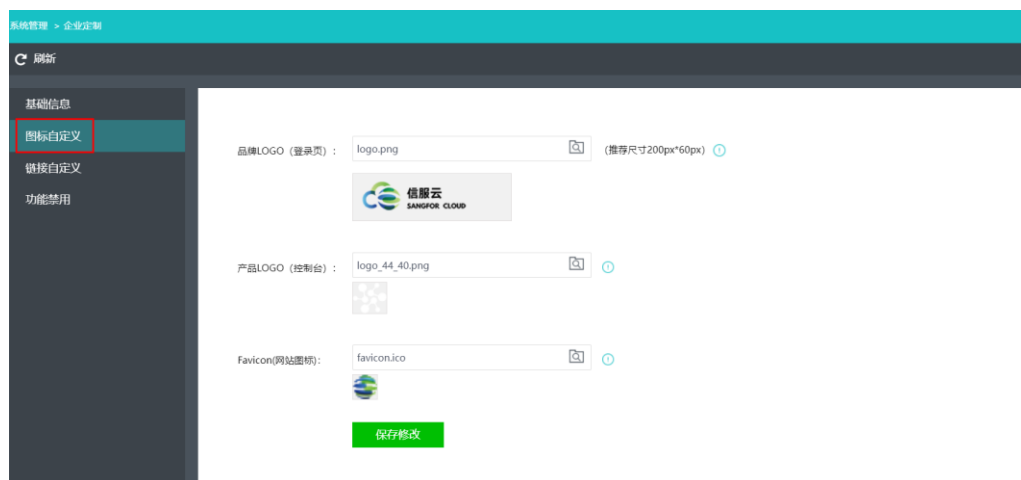
无

## 操作说明

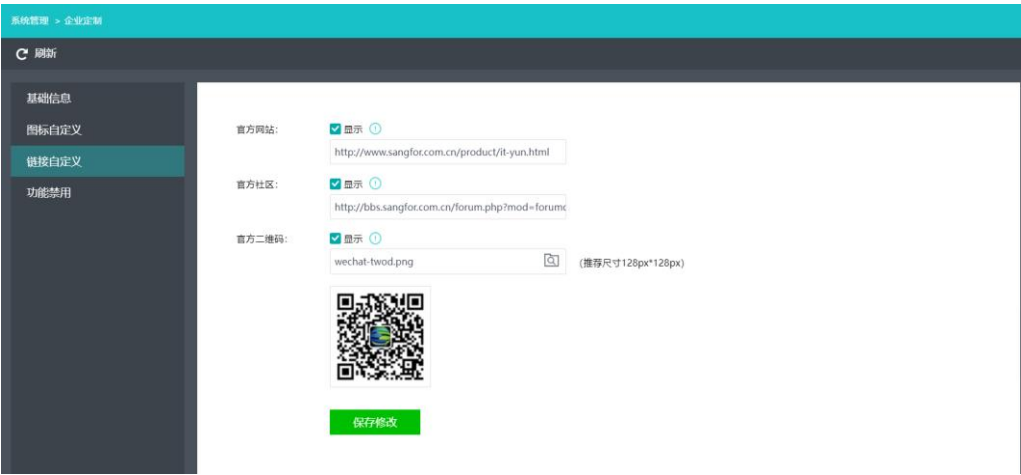
1. 进入[系统管理/企业定制]页面，选择[基础信息]，这里可以对平台基本信息、授权管理页面展示内容进行自定义设置，设置完成后点击<保存修改>按钮。



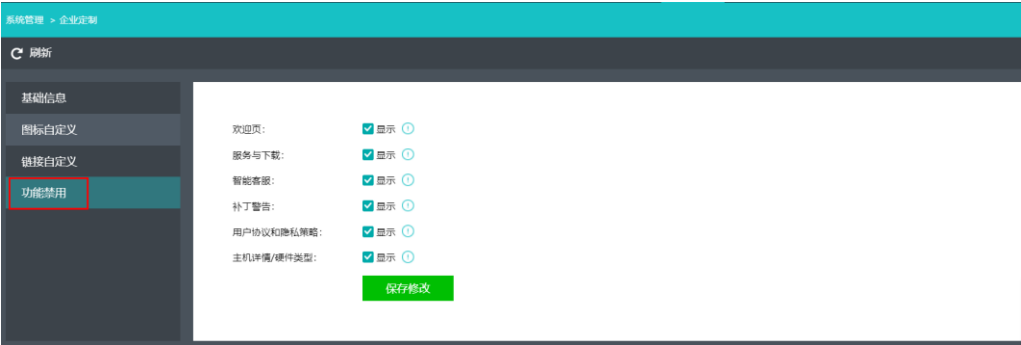
2. 选择[图标自定义]，支持对登录页、控制台、网站logo进行自定义设置，设置完成后点击<保存修改>按钮。



3. 选择[链接自定义]，支持自定义首页是否显示“官方网站”、“官方社区”、“官方二维码”，设置完成后点击<保存修改>按钮。



4. 选择[功能禁用]页面，支持自定义平台是否显示“欢迎页”、“服务与下载”、“智能客服”、“补丁告警”、“用户协议和隐私策略”、“主机详情/硬件类型”，设置完成后点击<保存修改>按钮。



## 10.30. 中/英文语言切换

### 功能介绍

深信服超融合平台支持中/英文语言切换功能，满足使用不同语言的运维人员管理平台场景。

### 注意事项

1. HCI6.8.0及其之后的版本支持中/英文切换，暂不支持地区切换。
2. NFV、aSEC、VDC不支持语言切换，请使用海外版的对应组件包。
3. 用户自定义内容，如：虚拟机名称/描述、网络设备名称/描述等不支持切换。
4. 支持会话级语言切换，多人在线可自行选择中/英文界面。

### 前提条件

无

## 操作步骤

在界面右上角，点击语言按钮，即可进行中/英文语言切换。



# 11. 平台运维

## 11.1. 运维工具/模块

### 11.1.1. 日常运维模块

#### 11.1.1.1. 告警监控

##### 操作场景

适用于超融合HCI平台的运维和监控场景，管理员可在超融合控制台首页查看平台的告警信息，并根据告警信息及时进行问题的闭环。

##### 操作步骤

1. 设置合理的告警选项和阈值是告警监控的前提条件，HCI平台的告警选项和阈值建议按照下表进行设置，具体设置方法可参考“[告警设置](#)”章节。

| 告警模块 | 监控项             | 普通告警                  | 紧急告警                      |
|------|-----------------|-----------------------|---------------------------|
| 主机   | 主机交换分区占用        | 持续 10 分钟，交换分区占用超过 10% |                           |
|      | 主机 CPU 占用       | 持续 10 分钟 CPU 占用超过 90% |                           |
|      | 主机 CPU 温度       | 温度异常持续 10 分钟          |                           |
|      | 主机 CPU 频率       | 主机 CPU 降频             |                           |
|      | 主机内存占用          | 持续 10 分钟内存占用超过 90%    |                           |
|      | 内存频率            | 内存降频                  |                           |
| 物理网络 | 主机网口错包          | 持续 10 分钟错包率超过 10%     |                           |
|      | 主机网口状态          |                       | 主机网口掉线                    |
|      | 集群主机状态          |                       | 主机离线                      |
|      | 数据通信网口（VXLAN）状态 |                       | 数据通信网口（VXLAN）不通           |
|      | 主机网卡工作状态        |                       | 主机网卡工作异常持续 10 分钟          |
|      | 主机网卡流量状态        |                       | 主机网卡流量持续 10 分钟达到流量上限的 90% |
|      | 网卡驱动固件兼容        |                       | 网卡驱动固件不兼容                 |

|      |                    |                       |                           |
|------|--------------------|-----------------------|---------------------------|
|      | 性                  |                       |                           |
|      | 网卡状态               |                       | 网卡损坏                      |
|      | 网卡光模块状态            |                       | 网卡光模块异常                   |
| 存储   | 存储 IO 状态           | 存储 IO 繁忙持续 10 分钟      |                           |
|      | 备份存储状态             | 备份存储 IO 繁忙            |                           |
|      | 存储 IO 时延状态         | 存储 IO 时延高持续 10 分钟     |                           |
|      | 存储与主机连接状态          |                       | 存储与主机连接断开                 |
|      | 存储状态               |                       | 存储状态异常                    |
|      | RAID 卡状态           |                       | RAID 卡状态异常                |
|      | 存储占用阈值             |                       | 超过 90%                    |
|      | 存储备份池占用阈值          |                       | 超过 90%                    |
| 虚拟机  | 虚拟机内存占用            | 持续 10 分钟内存占用超过 90%    |                           |
|      | 虚拟机 CPU 占用         | 持续 10 分钟 CPU 占用超过 90% |                           |
|      | 虚拟机镜像文件            |                       | 虚拟机镜像文件损坏                 |
|      | 虚拟机备份状态            |                       | 虚拟机备份失败                   |
|      | 虚拟机与外部网络连通性        |                       | 虚拟机与外部网络不通                |
|      | 虚拟机单网口 session 连接数 |                       | 持续 3 分钟，session 超过 100000 |
|      | 虚拟机状态              |                       | 虚拟机非法关机或重启                |
| 虚拟网络 | 虚拟网络设备 CPU 占用      | 持续 10 分钟 CPU 占用超过 90% |                           |
|      | 虚拟网络设备镜像文件         |                       | 虚拟网络设备镜像文件损坏              |
|      | 路由器运行状态            |                       | 路由器运行失败                   |
|      | 虚拟网络设备 ALG 使用率     |                       | 持续 30 秒 ALG 使用超过 90%      |
|      | 虚拟网络设备与外部网络连通性     |                       | 虚拟网络设备与外部网络不通             |
| 集群   | 提醒定期巡检频率           | 一月一次                  |                           |
|      | 序列号状态              |                       | 序列号过期                     |
|      | 序列号 key 状态         |                       | 序列号 key 状态异常              |

2. 建议设置邮件告警或短信告警，提高获取告警的效率。告警通知的具体配置可

参考“[配置告警通知](#)”章节。

### 3. 登录HCI控制台，在控制台首页点告警按钮，进入告警日志界面。



### 4. 在告警日志界面，可以查看告警日志的级别、时间、对象类型、告警对象、事件、描述、未确认告警数/总数。发现告警信息后，应及时进行处理并消除告警信息。



### 5. 在告警日志界面，还可以查看全部告警、过滤告警、搜索告警。



## 11.1.1.2. 一键检测

### 操作场景

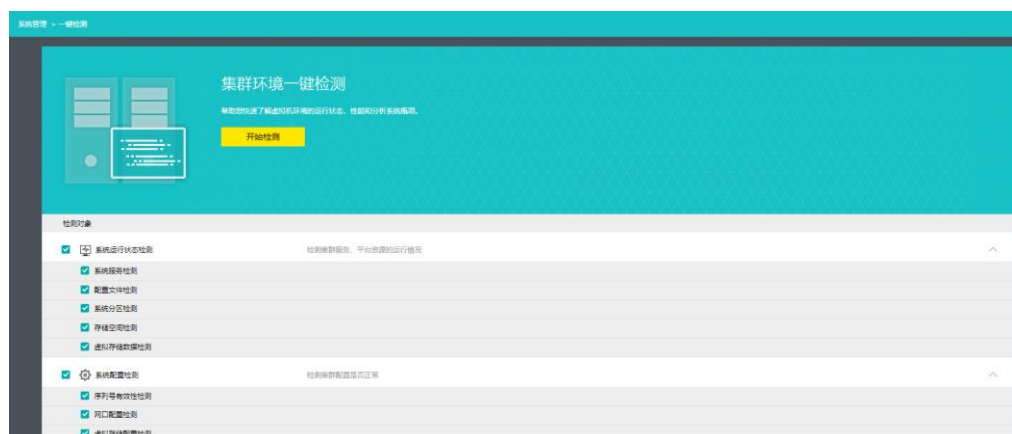
适用于超融合HCI平台的运维和监控场景，管理员可手动进行“一键式健康检查”，输出整个HCI平台的健康状况，并且可针对检测出的异常情况给出故障点和解决建议，便于故障定位和解决。

## 注意事项

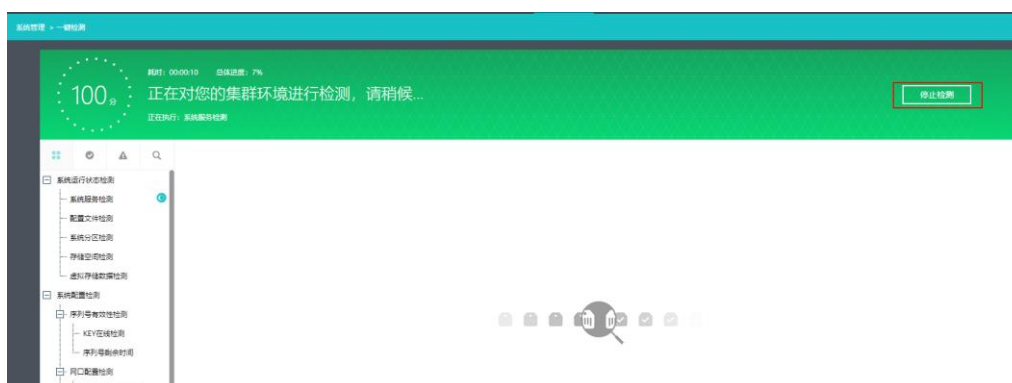
1. 一键检测的检查项默认不会勾选[磁盘性能检测]这一项，因为这一项检测会对测评的性能进行检测，可能会对客户的业务存储性能造成影响，若有需要可手动勾选并在业务空闲时进行检测。
2. 检测项包含三大类：
  - 系统运行状态检测
  - 系统配置检测
  - 硬件健康检测

## 操作步骤

1. 登录HCI控制台，在[系统管理/一键检测]页面下，勾选需要检测的检查项，点击<开始检测>即可。



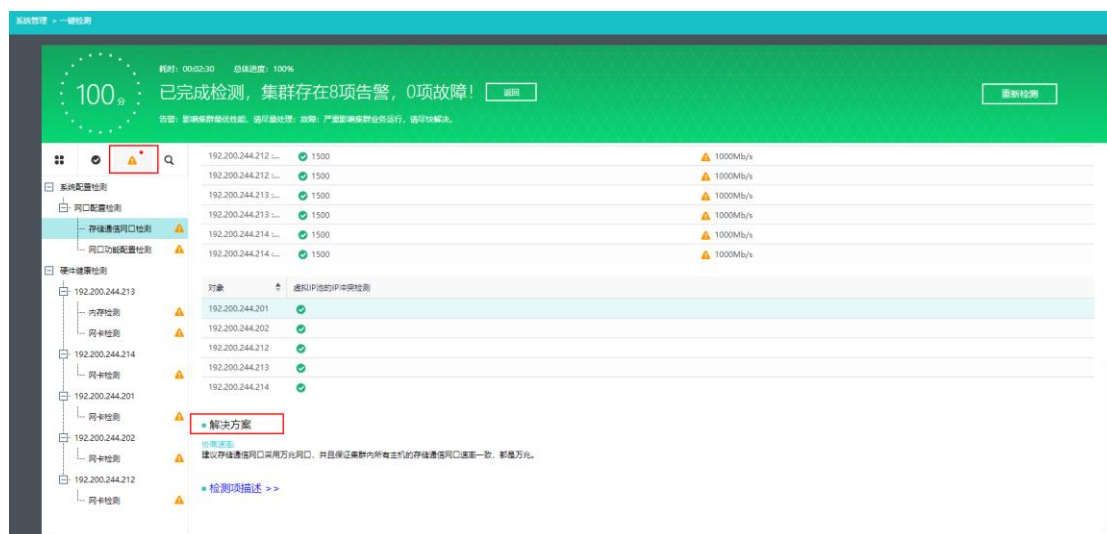
3. 检测的过程中会有耗时提示和进度提示，也可手动中断本次检测。



4. 检测结束后，可以在左上角筛选出全部检测项、正常检测项和异常检测项，也



可以对检测项进行搜索；点击异常的检测项，会提示当前集群检测出的异常情况，并在下面给出相应的解决方案。



### 11.1.1.3. 智能交付工具

#### 操作场景

适用于HCI交付、售后运维的场景，通过工具的巡检，对平台硬件健康状况、运行状况、预警补丁包检测等项目进行检查以及给出建议行动；智能交付工具的工具箱中提供平台日志收集、服务器IPMI信息收集等工具，满足运维人员日常排障需求。

#### 注意事项

当巡检结果异常出现“”严重级别的告警，则需要优先处理，可参考建议行动进行优化处理。

#### 操作步骤

1. 登录深信服社区（<https://bbs.sangfor.com.cn/>）。
2. 在[自助服务/工具下载]中，找到“HCI智能交付工具-aDeploy”，点击<进行下载>。



3. 下载解压后，打开工具进行巡检

| 名称          | 修改日期            | 类型          | 大小     |
|-------------|-----------------|-------------|--------|
| python      | 2021/1/28 21:10 | 文件夹         |        |
| webapp      | 2021/9/16 19:55 | 文件夹         |        |
| aDeploy.exe | 2021/8/26 15:08 | 应用程序        | 107 KB |
| aDeploy.py  | 2021/6/11 9:07  | Python file | 16 KB  |
| restart.exe | 2021/8/26 15:08 | 应用程序        | 103 KB |

4. 具体使用参考《深信服超融合智能交付工具aDeploy用户指南》。

11.1.1.4. 云端智能大脑

功能说明

深信服云端智能大脑是一款基于探针采集告警信息和云端智能大脑人工分析的风险预防和及时响应平台，通过对平台告警信息及时分析预测，及时发现可能存在的风险点并进行预防性处置，避免风险进一步升级扩大，降低对业务的影响程度，保障业务稳定可靠持续地运行。

注意事项

客户访问互联网地址应为固定公网IP地址，如通过拨号或其他非固定公网IP访问互联网，无法使用云端智能大脑探针告警上报功能。

前提条件

已获取云端智能大脑探针虚拟机vma包、和补丁包，获取地址：[深信服社区 – 自助服务 – 软件下载 – 超融合HCI](#)。

## 操作步骤

具体使用请参考《深信服云端智能大脑使用手册》。

### 11.1.1.5. Sangfor CLI

#### 功能说明

深信服超融合平台支持使用CLI 命令行工具运维HCI，无需登录 web 页面，操作命令行即可进行虚拟机管理、存储管理、磁盘管理、快照管理、备份管理、网络管理、主机管理、集群管理等。

#### 注意事项

无

#### 前提条件

1. 已获取SANGFOR CLI工具包，和powershell工具。
2. 已启用合作伙伴服务。

## 操作步骤

具体使用请参考Sangfor CLI手册。

### 11.1.2. 问题排障模块

#### 11.1.2.1. 系统诊断

#### 操作场景

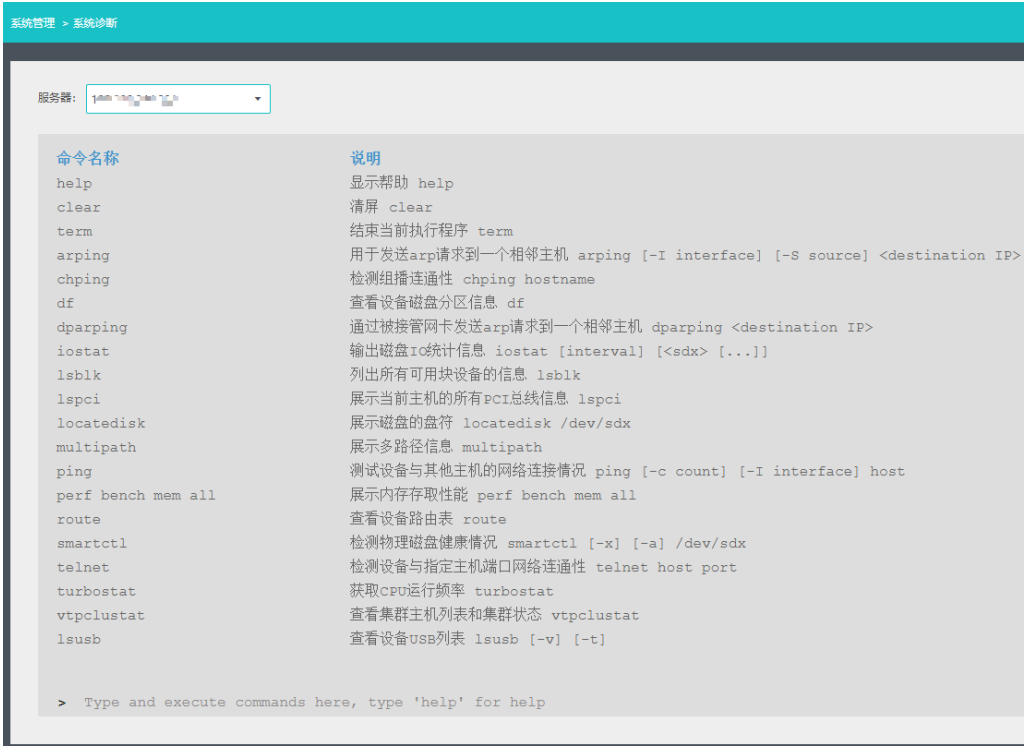
通过 Web 页面进行简单命令行操作，查看网络和后台的一些基本信息，简化问题排查过程。界面中列出HCI控制台所支持的命令以及命令的作用。

#### 操作步骤

1. 登录HCI控制台，在[系统管理]页面下，找到系统维护，点击<系统诊断>，跳转至系统诊断页面。
2. 在[服务器]中选择需要进行命令操作的实体机IP。



3. 界面中已列出目前所支持的命令名称以及命令的作用，根据需要输入并执行命令。



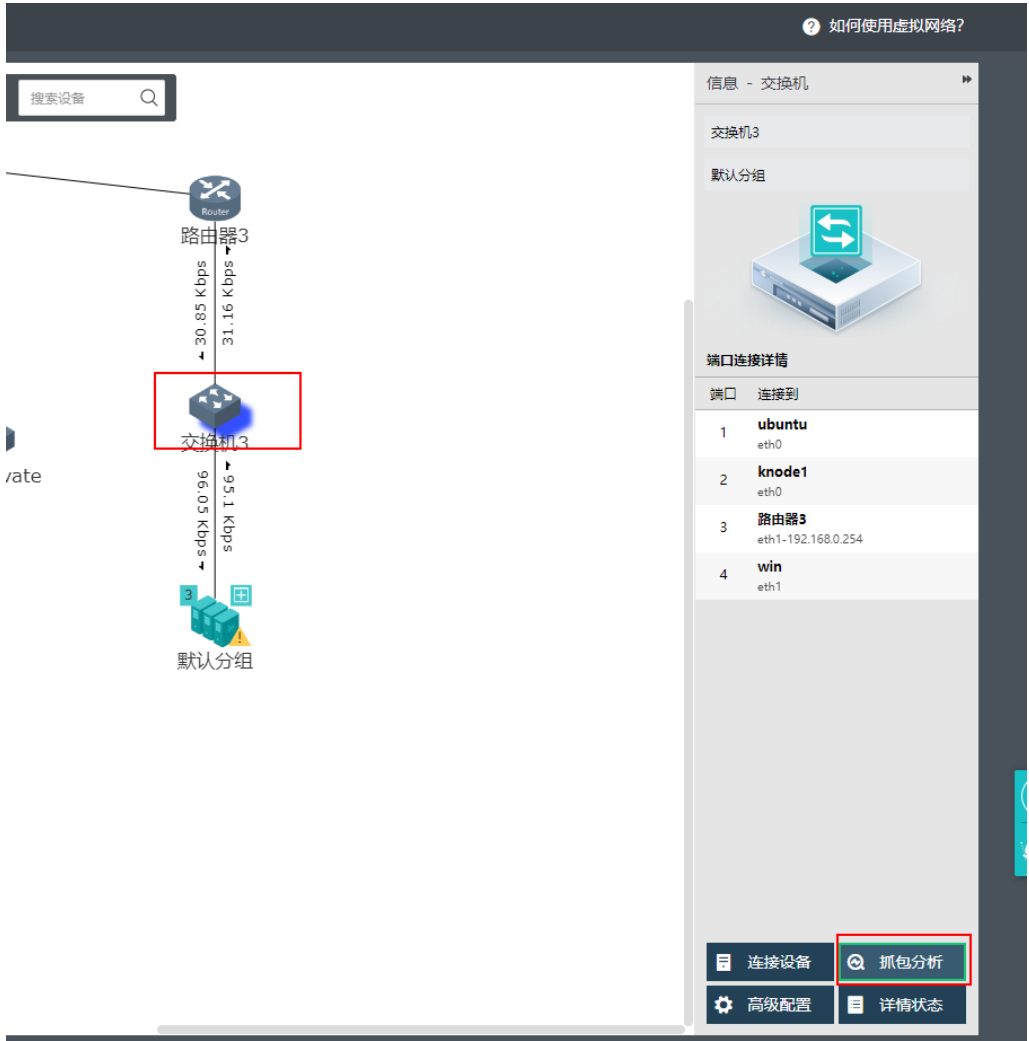
## 11.1.2.2. 控制台抓包

### 操作场景

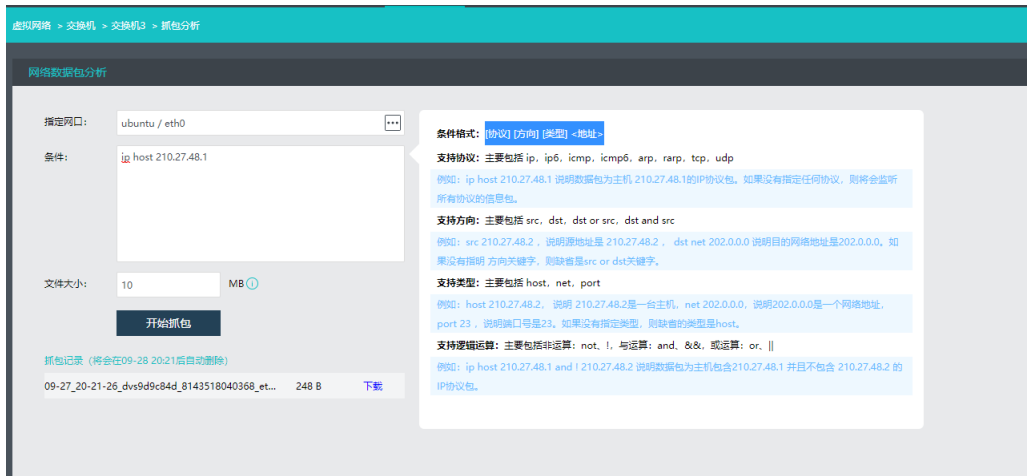
方便通过Web页面进行主机网口抓包操作，抓取的数据包可下载到本地进行分析。

### 操作步骤

1. 登录HCI控制台，在[网络与安全/网络拓扑]页面下，选择需要抓包的设备，点击<抓包分析>。



2. 通过指定虚拟设备网口及条件，抓取经过网口的数据包。



- 指定网口：选择需抓包的设备对应的网口。

- 条件：配置抓包条件，条件格式支持[协议] [方向] [类型] <地址>，同时支持逻辑运算。

抓包完成后可下载数据包到本地进行分析。

### 11.1.2.3. 连通性探测（网络故障排查）

#### 功能说明

该任务指导管理员进行虚拟机连通性检测，排查网络通信故障原因，支持IPv4/IPv6协议下构造ICMP、TCP、UDP包探测。

#### 注意事项

- 连通性探测不支持 IPv6 与 IPv4 互相访问。
- 关机状态虚拟机或网口禁用状态虚拟机置灰不可选。

#### 前提条件

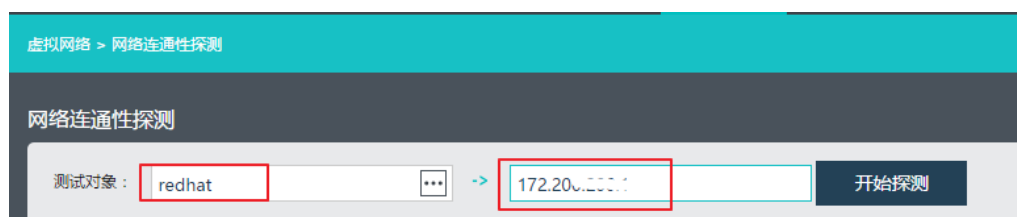
- 虚拟机已安装性能优化工具。
- Linux要求必须安装perl。

#### 操作步骤

- 在[网络拓扑]页面中点击<连通性探测>，进入[连通性探测]页面。



- 选择源虚拟机，输入目的IP。



- 点击<开始探测>，进行网络测试。
- 网络测试成功示例。



5. 故障测试示例，平台给出故障问题建议。



11.1.2.4. 端口管理

操作场景

当运维人员需要进行部分操作时，需要开启部分端口，比如运维人员需要进行主机扩容、主机替换、巡检等操作时，需要开启SSH端口。具体的端口和使用场景如下表：

| 服务名      | 端口                       | 协议      | 描述                                                |
|----------|--------------------------|---------|---------------------------------------------------|
| 新主机发现服务  | 4099                     | udp     | 用于发现安装了 HCI 的物理主机                                 |
| 虚拟机迁移服务  | 7001-7019                | tcp     | 用于集群内、跨集群虚拟机迁移；当集群被云管平台纳管后此端口将自动开启                |
| p2v 迁移服务 | 4000-4010<br>10809-10900 | tcp/udp | 用于执行 p2v 任务时，处理迁移请求任务和迁移数据传输                      |
| Samba 服务 | 139,445                  | tcp     | Samba 共享目录管理服务，提供文件共享功能                           |
| 合作伙伴服务   | 4433                     | tcp     | 用于提供 API 接口给第三方调用                                 |
| SNMP 服务  | 161                      | udp     | 通过 SNMP 服务可帮助管理员了解运行时的物理资源使用情况，需要通过独立的账号和密码来使用服务。 |
| SSH 端口   | 22                       | tcp     | 用于主机扩容、主机替换、巡检是连接主机                               |

操作步骤

1. 登录HCI控制台，在[系统管理/端口管理]页面下，对集群的端口进行启用和禁用。



2. 在该页面同时可对SSH端口进行开启和关闭。也可通过启用SSH IP限制来限制能够访问SSH端口的IP地址。





11.2. 平台日/周/月运维

为了规范的对HCI平台进行日常运维，可结合客户环境中的实际情况参考如下步骤，建立完整的日/周/月运维管理流程，以系统化的方式来保证整个平台的工作状态的稳定性。

11.2.1. 日维护

每日维护建议在HCI控制台查看对应的告警信息，对于紧急级别的告警应立即着手进行处理，对于普通级别的告警应制定处理计划。具体维护建议参考下表即可：

| 维护项目     | 维护场景                          | 维护建议                                    | 操作入口           |
|----------|-------------------------------|-----------------------------------------|----------------|
| HCI 状态查看 | 对 HCI 主机的硬件资源、组件进行监控，快速发现系统异常 | 检查实体机状态是否有物理主机离线；<br>存储状态是否有正常，磁盘状态是正常； | 登录 HCI 控制台首页查看 |
| 主机告警监控   | 主机交换分区占用过高                    | 建议对主机内存进行扩容或者关闭暂时不使用的虚拟机                | 登录 HCI 控制台首页查看 |
|          | 主机离线                          | 建议检查主机或网络是否异常，立即进行业务恢复。                 |                |
|          | 主机系统分区异常                      | 可能是系统盘有坏道或者故障，请联系深信服技术支持。               |                |
|          | 主机 GPU 占用过高                   | 请关闭部分虚拟机或迁移部分虚拟机到其他主机                   |                |
|          | 主机不能检测到显卡                     | 请登录 IPMI 查看显卡是否存在异常                     |                |
|          | 主机的显卡温度过高                     | 请检查主机散热或机房温度是否异常                        |                |
|          | 检测到具有多张不同类型显卡硬件               | 请移除异构显卡，否则 GPU 虚拟机无法运行在该主机上             |                |
|          | 主机显存不足                        | 请关闭部分虚拟机或迁移部分虚拟机到其他主机                   |                |
|          | 主机 CPU 占用过高                   | 建议对主机进行扩容或者关闭暂时不使用的虚拟机                  |                |

|        |                          |                                        |
|--------|--------------------------|----------------------------------------|
|        | 主机 CPU 温度异常              | 建议查看机房温度、主机风扇以及制冷设备是否正常                |
|        | 主机 CPU 降频                | 如果服务器频繁降频告警，需要通过 BMC 查看 CPU 硬件状态是否正常   |
|        | 主机内存占用过高                 | 建议对主机内存进行扩容或者关闭暂时不使用的虚拟机               |
|        | 主机内存降频                   | 建议登录主机的 BMC 控制台，对主机的内存进行检查             |
|        | RADI 卡状态异常               | RADI 卡状态异常 检查磁盘以及存储状态是否正常，不正常请及时联系 400 |
|        | 主机%s 的内存条%s 故障           | 请进行排障或者更换内存条                           |
|        | 短信功能异常，短信代理模块与发送模块连接异常   | 请检查短信配置是否正确以及网络连接是否正常。                 |
|        | 内存超配告警                   | 建议进行内存扩容                               |
|        | VCPU 超配告警                | 建议进行主机扩容                               |
|        | 网口速率过低                   | 建议更换网卡或者网线                             |
| 网络告警监控 | 主机网卡工作异常                 | 如果出现频繁告警，建议更换主机网卡                      |
|        | 网络丢包率过高                  | 检查物理网络是否异常                             |
|        | 主机出现持续丢包错误               | 检查物理网络是否异常                             |
|        | 主机 xx 和主机 xx 的 vxlan 口不通 | 检查 vxlan 口的配置和 vxlan 交换机的配置            |
|        | 主机 xx 的网口掉线              | 请检查主机的网口连接状态                           |
|        | 虚拟网络设备（%s）无响应            | 检查虚拟网络设备的状态                            |
|        | xx 主机到网关不通，请检查网络连接是否异常   | 建议检查网络是否正常                             |
| 存储告警监控 | 存储 IO 时延过高               | 建议检查存储网络是否正常                           |
|        | 存储占用过高                   | 1、删除不再需要的虚拟机；2、清除回收站的垃圾文件；3、对存储进行扩容    |
|        | 存储与主机断开/存储掉线             | 及时检查存储与主机网络状况                          |
|        | 存储状态异常                   | 及时检查存储是否故障                             |
|        | 主机 xx 访问存储 xx 持续出现繁忙     | 建议升级存储或迁移部分虚拟机至其他存储运行。                 |
|        | 磁盘状态错误，已重新挂载。            | 登录服务器 BMC 控制台，查看硬件相关日志，确认故障原因。         |
|        | 检测到存储存在数据块重              | 联系深信服技术支持协助解                           |

|     |                                                     |                                                                   |
|-----|-----------------------------------------------------|-------------------------------------------------------------------|
|     | 用, 请尽快联系技术支持协助解决                                    | 决                                                                 |
|     | 检测到热备盘替换                                            | 登录超融合 web 控制台, 查看被替换磁盘的状态<br>登录服务器 BMC 控制台, 查看硬件相关的日志             |
|     | 检测到硬盘 (主机<%s>, 硬盘名称: %s) 被拔出, 如果是误拔, 请尽快把硬盘重新插回原盘位! | 登录超融合 web 控制台, 查看磁盘的状态<br>登录服务器 BMC 控制台, 查看硬件相关的日志                |
|     | 磁盘状态异常                                              | 登录超融合 web 控制台, 查看磁盘的状态<br>登录服务器 BMC 控制台, 查看硬件相关的日志<br>尝试对磁盘执行插拔操作 |
|     | 磁盘坏道超过阈值                                            | 尽快更换磁盘                                                            |
|     | 磁盘 IO 错误                                            | 登录超融合 web 控制台, 查看磁盘的状态<br>登录服务器 BMC 控制台, 查看硬件相关的日志                |
|     | 存储私网异常                                              | 检查存储私网连通性                                                         |
| 序列号 | 序列号过期提醒                                             | 建议及时购买新序列号进行恢复                                                    |
|     | 序列号 KEY 状态异常                                        | 建议进行插拔 KEY, 如果还是不行联系 400                                          |
|     | 授权 USB-KEY 被拔出, 请插入, 否则系统可能会有异常                     | 检查授权 key 是否正常, 尝试插拔授权 key                                         |
| 虚拟机 | 自动备份虚拟机失败                                           | 检查备份存储是否正常                                                        |
|     | 连接 session 数过高。当前 session 连接数为%s, 超出阈值%s。%s         | 检查虚拟机的业务 session 是否正常, 尝试调整 session 阈值                            |
|     | 虚拟机的 CPU 利用率持续过高                                    | 检查虚拟机的性能优化工具是否正常。<br>尝试扩容虚拟机的 vCPU 配置。                            |
|     | 虚拟机镜像文件损坏                                           | 检查虚拟机的是否能够正常启动, 如无法启动可联系深信服技术支持解决。                                |
|     | 虚拟机的内存不足。                                           | 检查虚拟机的性能优化工具是否正常。<br>尝试扩容虚拟机的内存配置。                                |
|     | 虚拟机连接的物理出口没有桥接该虚拟机所在主机的网口, 这会导致虚拟机与外部               | 将主机的业务网口桥接到物理出口上。                                                 |

|  |                                                  |                                     |  |
|--|--------------------------------------------------|-------------------------------------|--|
|  | 网络不通。                                            |                                     |  |
|  | 删除备份时发现虚拟机的备份镜像损坏                                | 如果虚拟机还存在请立即对其进行备份，然后联系深信服技术支持！      |  |
|  | 虚拟机重启 CDP 失败                                     | 请去管理->虚拟机备份与恢复->备份策略页面手动开启 CDP      |  |
|  | 虚拟机开启 CDP 失败                                     | 请去管理->虚拟机备份与恢复->备份策略页面手动开启 CDP      |  |
|  | 虚拟机正在运行，但是其配置的 CDP 策略被禁用，目前数据处于不受保护状态,请调整 CDP 策略 | 请去管理->虚拟机备份与恢复->备份策略页面手动开启 CDP      |  |
|  | 虚拟机无响应/虚拟机故障，已经自动重启恢复                            | 检查虚拟机日志，排查虚拟机无响应原因                  |  |
|  | 虚拟机的 GPU 利用率持续过高                                 | 检查虚拟机 GPU 负载<br>扩容虚拟机 GPU 配置        |  |
|  | 虚拟机的显存不足。当前使                                     | 检查虚拟机 GPU 负载<br>扩容虚拟机 GPU 配置        |  |
|  | 网口的丢包率过高。                                        | 检查虚拟机虚拟网卡配置                         |  |
|  | 虚拟机已使用 IO 日志备份空间超过告警阈值                           | 请调整虚拟机 IO 日志备份空间大小。                 |  |
|  | 虚拟机的探测操作系统类型与配置不符，可能导致报表信息不准确                    | 检查虚拟机的操作系统类型与 HCI 的 web 控制台配置的是否一致。 |  |

### 11.2.2. 周维护

每周维护任务以系统配置备份&检测、一键巡检等任务为主，同时统计本周告警日志及故障处理情况

| 维护项目     | 维护场景                                                  | 具体维护任务                              | 操作入口                    |
|----------|-------------------------------------------------------|-------------------------------------|-------------------------|
| UPS 电量检查 | 当使用 UPS 供电时，要人为检查 UPS 电量是否充足，以防止系统异常掉电而产生数据异常不可恢复的风险。 | 检查 UPS 是否供电充足，如果不足，请及时对超融合系统进行安全下电。 | 参考 UPS 蓄电池使用说明          |
| 系统配置备份检查 | 为确保系统异常时有可用的备份数据，需定时检查备份功能和数据的可用性；                    | 根据系统备份查看备份数据是否存在，如果出现异常，请立即处理。      | HCI 控制台[系统管理/系统配置备份与恢复] |

|            |                                   |                                        |                                     |
|------------|-----------------------------------|----------------------------------------|-------------------------------------|
| 系统配置备份     | 为了确保系统彻底异常时有可用的备份数据，需定期将系统配置备份至本地 | 备份系统配置到本地                              | HCI 控制台[系统管理/系统配置备份与恢复]，点击备份系统配置到本地 |
| HCI 系统健康检查 | 定期对 HCI 环境进行全面检测，防范于未然。           | 建议每周在 HCI 上对系统进行健康检查；对于存在不合格的检查项，请立即处理 | HCI 控制台首页[一键检测]                     |
| 本周告警处理     | 本周告警处理情况                          | 检查本周紧急告警处理情况以及普通告警处理计划执行情况             |                                     |

11.2.3. 月维护

11.2.3.1. 月度巡检

每月应使用aDeploy工具对平台进行巡检，aDeploy巡检工具能够针对HCI平台做深层次的检查，具体的检查内容包括：

- 平台硬件健康检测
- 平台存储状态检测
- 平台系统关键服务检测
- 平台系统配置检测
- 平台网络状态检测
- 平台预警补丁检测
- 平台安全检测

巡检完成后，对于故障级别的检测项应立即着手进行处理，对于告警级别的检测项应制定整改计划，逐步完成整改。

| 维护项目   | 维护场景                  | 具体维护任务                | 操作入口                                      |
|--------|-----------------------|-----------------------|-------------------------------------------|
| 平台健康检查 | 定期对超融合平台进行全面巡检，防患于未然。 | HCI 平台硬件健康检测、平台运行状态监测 | 参考“ <a href="#">使用 aDeploy 工具进行检测</a> ”章节 |

11.2.3.2. 预警补丁

当产品发现问题后，深信服科技会针对产品问题发布修复补丁，最大程度的降低产

品问题对业务的影响。

接收到产品预警和整改公告后，运维人员可使用aDeploy工具对当前使用的HCI平台进行巡检，确认当前平台是否存在公告中存在的问题。同时运维人员应及时分析当前平台的版本信息及承载业务的实际情况，确认预警对现网平台的影响。并根据评估结果确定是否进行补丁修复操作。

### 11.2.3.3. 可用性管理

平台可用性管理，主要是通过对平台的CPU、内存、存储等资源进行检查，保障业务连续性。

关注超融合平台的CPU使用率，存在以下任意情况应考虑对超融合平台进行扩容：

- CPU 的持续使用率超过 70%
- 普通集群场景 CPU 资源的冗余量不满足坏掉一台或两台（两副本、三副本）主机的情况下支撑业务系统的正常运行。
- 延伸集群场景 CPU 资源的冗余量不满足坏掉一个故障域主机的情况下支撑业务系统的正常运行。

关注超融合平台的内存配置量及内存使用率，存在以下任意情况应考虑对超融合平台进行扩容：

- 内存的持续使用率超过 80%
- 普通集群场景内存资源的冗余量不满足坏掉一台或两台（两副本、三副本）主机的情况下支撑业务系统的正常运行。
- 延伸集群场景内存资源的冗余量不满足坏掉一个故障域主机的情况下支撑业务系统的正常运行。

关注超融合平台的存储容量使用率，存在以下任意情况应考虑对存储进行扩容：

- 存储使用率超过 90%
- 管理员可以通过存储容量的使用趋势预测超融合平台的剩余的存储容量能够支撑业务系统使用的天数，并根据预测数据调整扩容计划。当预测的剩余的存储容量不足以支撑业务系统使用 90 天时就必须要考虑对超融合平台的存储资源进行扩容。

关注超融合平台的存储性能，同时通过对重要虚拟机的IOPS进行分析，评估当前超融合平台的存储性能是否能够满足业务系统的需求。当业务系统的IO时延大于20ms时就需要对超融合平台的存储性能进行扩容。

关注超融合平台的业务系统备份和容灾执行情况，在必要时可挑选部分业务系统执行恢复演练，确保业务系统的备份和容灾数据正常，在极端情况下能够通过备份或

容灾数据来恢复业务。

具体关注的指标参考下表：

| 维护项目      | 关注指标                                                                                                    | 具体维护任务                        |
|-----------|---------------------------------------------------------------------------------------------------------|-------------------------------|
| CPU 使用率   | CPU 持续使用率不超过 70%                                                                                        | 查看 CPU 最近一个月的峰值使用率和持续使用率      |
| CPU 资源冗余量 | 普通集群场景 CPU 资源的冗余量不满足坏掉一台或两台（两副本、三副本）主机的情况下支撑业务系统的正常运行。<br>延伸集群场景 CPU 资源的冗余量不满足坏掉一个故障域主机的情况下支撑业务系统的正常运行。 | 计算当前 CPU 资源的冗余量是否满足要求         |
| 内存使用率     | 内存持续使用率不超过 80%                                                                                          | 查看内存最近一个月的峰值使用率和持续使用率         |
| 内存资源冗余量   | 普通集群场景内存资源的冗余量不满足坏掉一台或两台（两副本、三副本）主机的情况下支撑业务系统的正常运行。<br>延伸集群场景内存资源的冗余量不满足坏掉一个故障域主机的情况下支撑业务系统的正常运行。       | 计算当前内存资源的冗余量是否能够满足要求          |
| 存储使用率     | 存储使用率不超过 90%，预测的剩余的存储容量足以支撑业务系统使用 90 天以上。                                                               | 查看当前存储资源的使用率以及 90 天后容量使用率预测   |
| 业务备份或容灾情况 | 业务备份和容灾任务执行正常。<br>恢复演练正常                                                                                | 查看业务备份和容灾的任务执行情况<br>执行业务的恢复演练 |

11.2.3.4. 安全管理

超融合平台的安全至关重要，每月应针对超融合平台的安全进行检查，包括以下项目：

| 维护项目    | 维护场景              | 具体维护任务               | 操作入口                      |
|---------|-------------------|----------------------|---------------------------|
| 允许登录的范围 | 检查当前平台用户允许登录范围的配置 | 检查当前平台用户是否开启了登录允许的范围 | [系统管理/管理员与权限管理]-用户编辑-登录限制 |
| 密码有效期   | 检查当前的密码有效期的配置     | 检查当前的密码有效期是否在六个月及以内  | [系统管理/管理员与权限管理]-登录与密码策略   |

|           |               |                                |                         |
|-----------|---------------|--------------------------------|-------------------------|
| 密码输入错误次数  | 检查密码输入错误次数的配置 | 检查密码输入错误次数是否在 10 次以内           | [系统管理/管理员与权限管理]-登录与密码策略 |
| 端口管理      | 检查平台开放的端口     | 检查平台是否开启了没有在使用的端口，并关闭当前没有使用的端口 | [系统管理/端口管理]             |
| 补丁服务连通性检测 | 检查补丁服务器的连通性   | 检查补丁服务的连通性，保障补丁服务连通正常          | [系统管理/补丁升级]-补丁设置        |

### 11.3. 基础业务变更

#### 11.3.1. 系统上下电

##### 11.3.1.1. 单台主机上下电

###### 场景说明

硬件维护场景，当管理员需要对单主机进行下电操作前，可以使用主机维护模式，启动维护模式后系统会先将平台上的业务迁移到其它主机上，确保替换过程中不对业务造成影响。

###### 注意事项

1. 主控不支持进入单主机维护模式，如果需要维护主控请先切换其他主机为主控。
2. 环境上有主机离线不能进入单主机维护模式。
3. 待维护主机上有任务在进行暂时不能进入单主机维护模式，需要等待任务完成后方可进入。
4. 目前仅允许同时有一台主机进入单主机维护模式。

###### 前提条件

无

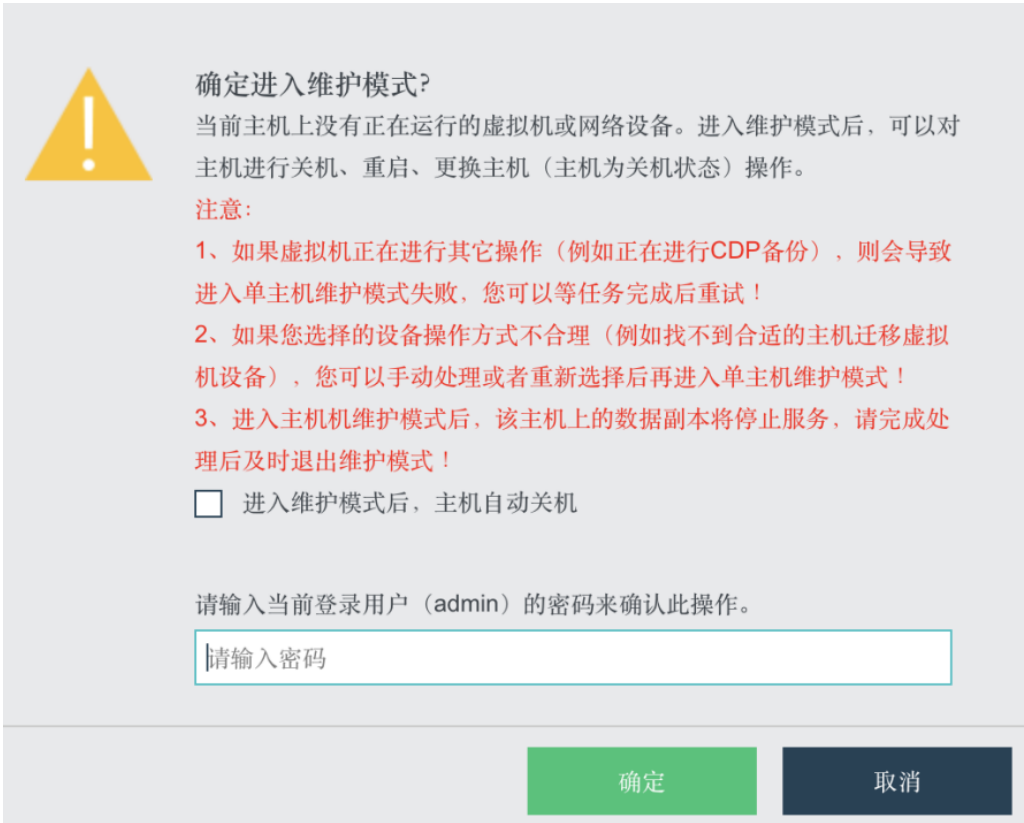
###### 操作步骤

1. 在[实体机/更多]，选择进入单主机维护模式。





2. 输入密码后选择<确定>进入主机维护模式，此时系统会将主机进行隔离处理。这一步骤也可勾选“进入维护模式后，主机自动关机”。



3. 主机进入维护模式成功，可以在web控制台点击关闭电源，对主机执行下电操作。



4. 维护完毕后，将服务器开机并等待完全启动后，将主机退出单主机维护模式。



5. 等待虚拟存储数据同步完毕后，可将其他主机上的虚拟机迁移到该主机运行

11.3.1.2. 超融合集群上下电

场景说明

当机房进行例行维护（例行停电）或搬迁时，就需要对超融合集群执行下电和上电的操作。为了充分保障业务系统的可用性，避免下电过程对用户的业务数据造成影响。应在下电前先手动关闭业务服务，然后对虚拟机执行关机操作，最后再对超融合集群执行关机操作。

注意事项

- 1. 超融合集群执行下电操作前保障整个集群没有其他任务在执行。
- 2. 虚拟机的关机操作应使用超融合web控制台的关机功能或虚拟机内部的关机功能，禁止使用超融合web控制台的关闭电源功能。
- 3. 服务器的关机操作应在超融合web控制台的主机页面执行，禁止直接拔电源或长按服务器关机键执行关机操作。
- 4. 集群下电过程应遵循先停业务，再关闭虚拟机，再关闭服务器，最后关闭网络设备的顺序。
- 5. 集群上电过程应遵循上开启网络设备，再开启服务器，再开启虚拟机，最后开启业务服务的顺序。

操作步骤

集群下电过程

- 1. 登录超融合web控制台，检查超融合平台的任务列表是否有任务在执行。如果有

任务在执行，则等待任务执行完毕后在继续进行操作。



- 2. 手动关闭业务系统的服务（可选）
- 3. 在[虚拟机]页面，勾选全部虚拟机，选择关机操作，确保所有虚拟机处于关机状态。



4. 在[网络与安全/网络拓扑]页面，点击设备列表，进入设备列表页面。



5. 勾选所有设备，点击关机，将虚拟网络设备执行关机操作。



6. 等待关闭完毕后，可使用步骤1的方法检查任务列表是否有任务在执行，如果有任务在执行则需要所有任务执行完毕后再进行操作。

7. 打开[实体机/物理主机]页面，逐个选择非主控主机，点击更多-关闭电源执行关机操作，最后在选择主控主机点击更多-关闭电源执行关机操作。



8. 确认服务器关闭完毕后，再对关联的网络设备执行关机操作。

集群上电过程

1. 将网络设备加电启动，并进行网络测试，确保网络正常。
2. 将服务器加电启动，确保服务器的所有电源正常运行。
3. 服务器正常启动后，等待10-20分钟，登录超融合控制台，在首页进行一键检测，确保一键检测分数为100分。



4. 检查超融合平台的任务列表是否有任务在执行，如果有任务再执行则需要等待任务执行完毕后再继续进行操作。



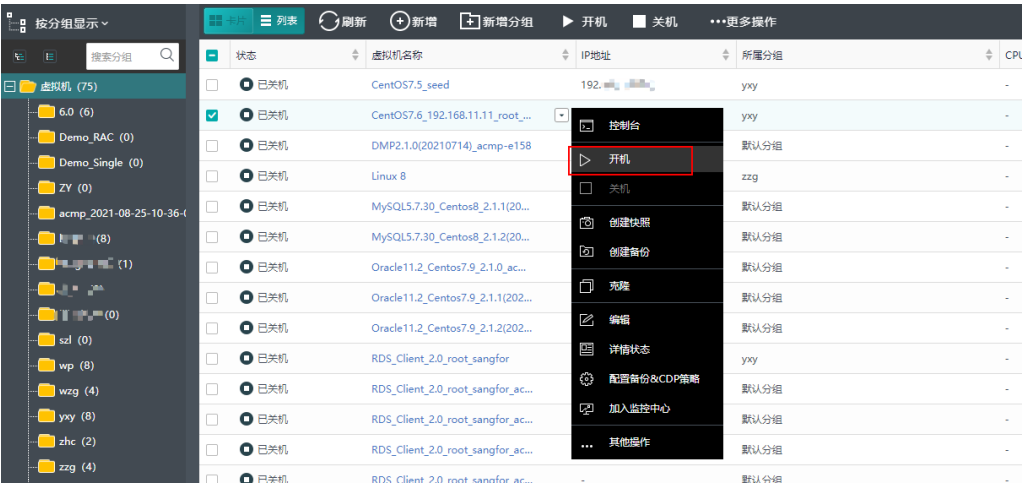
5. 在[网络与安全/网络拓扑]页面，点击<设备列表>，进入设备列表页面。



6. 勾选所有设备，点击开机，将虚拟网络设备执行开机操作。



7. 在[虚拟机]页面对虚拟机逐步执行开机操作，并在虚拟机内部启用业务系统的服务。开机和启用服务的顺序应遵循先开机数据库虚拟机，等数据库服务正常后再开机应用虚拟机。



8. 开机过程中应逐个验证业务系统是否正常，当前业务系统正常后再往下开机其他的业务系统。

### 11.3.2. 平台版本及补丁包升级

升级指导请参见 [《深信服超融合 HCI&SCP 升级方案》](#)。

### 11.3.3. HCI 平台网络设置与变更

当用户的网络规划变更时就涉及到HCI平台相关的网络配置变化，HCI平台的共划分4个网络平面：管理网络、存储私网、VXLAN网络以及业务网络，这四个网络平面的变更指导可参考下表的内容：

| 场景 | 运维指导 |
|----|------|
|----|------|



|           |                           |
|-----------|---------------------------|
| 管理网络变更    | <a href="#">修改集群管理网络</a>  |
| 存储私网变更    | <a href="#">存储私网变更</a>    |
| 数据通信口配置修改 | <a href="#">数据通信口配置修改</a> |
| 物理出口的配置修改 | <a href="#">物理出口的配置修改</a> |

### 11.3.4. 虚拟网络设置与运维

参考“[虚拟网络配置指导](#)”章节

### 11.3.5. 虚拟存储设置与运维

参考“[虚拟存储配置指导](#)”章节

### 11.3.6. 扩容变更

当HCI平台资源不足时，运维管理员就需要对集群的资源进行扩容，当前扩容变更主要包括两个层面，主机扩容和磁盘扩容。

#### 11.3.6.1. 主机扩容

##### 功能说明

当集群资源紧张匮乏时，可以通过横向扩展的方式进行资源扩容。

##### 注意事项

1. 主机扩容会触发数据平衡，建议在业务空闲时段进行操作。
2. 如果是两主机集群，扩容至三主机集群时需要关闭集群内所有虚拟机和NFV设备。
3. 如果集群主机 $\geq 3$ 台，此时进行主机扩容无需停止业务。
4. 确保扩容后平台的授权足够。
5. 如果添加集群时报“当前集群为企业版序列号，不支持添加测试设备到集群，如有需要请联系深信服客服”，这种情况是当前的主机没有打测试设备的签名，待添加的主机是打过签名，导致两台设备不一致。解决方法：联系深信服技术支持将未打测试设备签名的设备进行签名后，重新扫码申请序列号。

## 前提条件

1. 规划好扩容主机的各个网络平面的IP地址。
2. 扩容主机已安装好aSV软件且与原版本一致（包括补丁），并设置好管理IP。
3. 扩容主机的管理口、数据通信口、业务口、存储口已经正确接入到网络中。

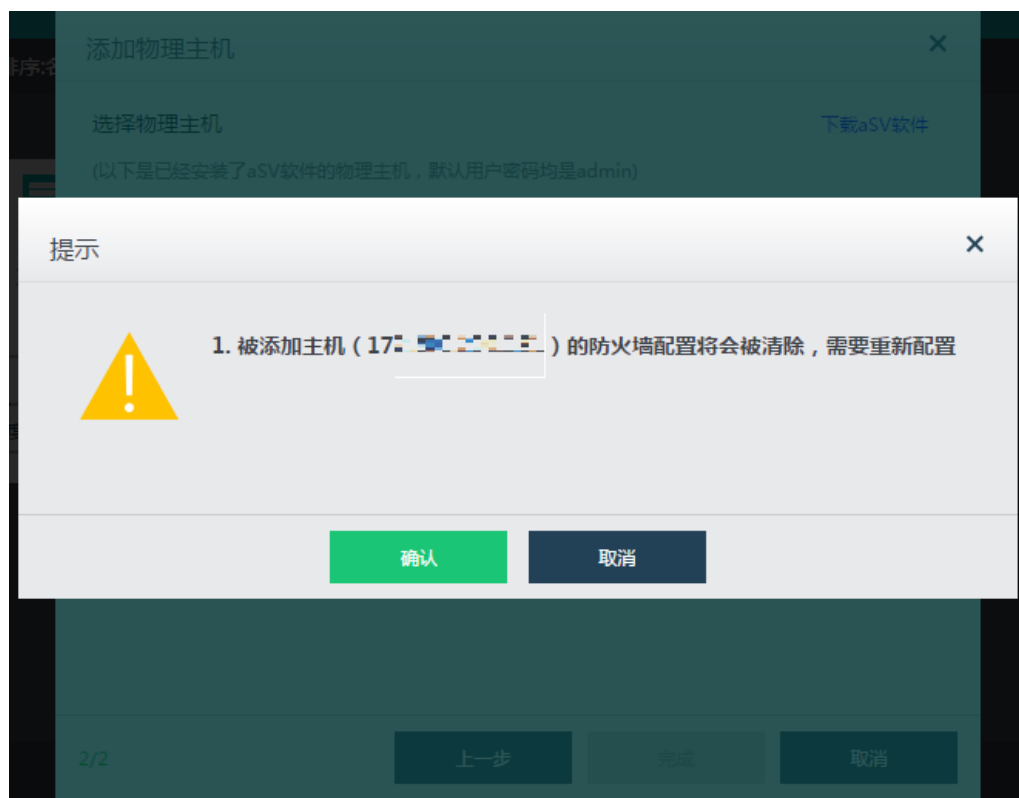
## 操作步骤

1. 在[实体机/物理主机]中点击<添加主机>。

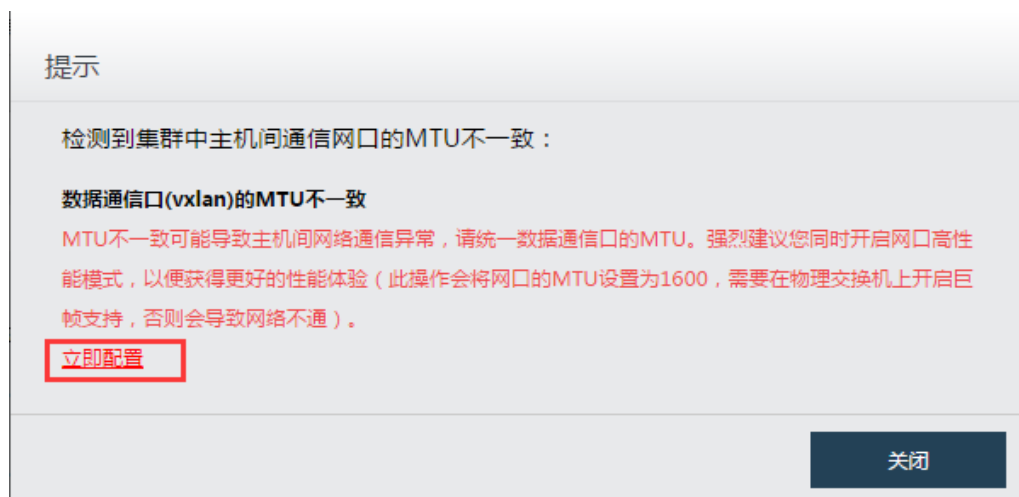


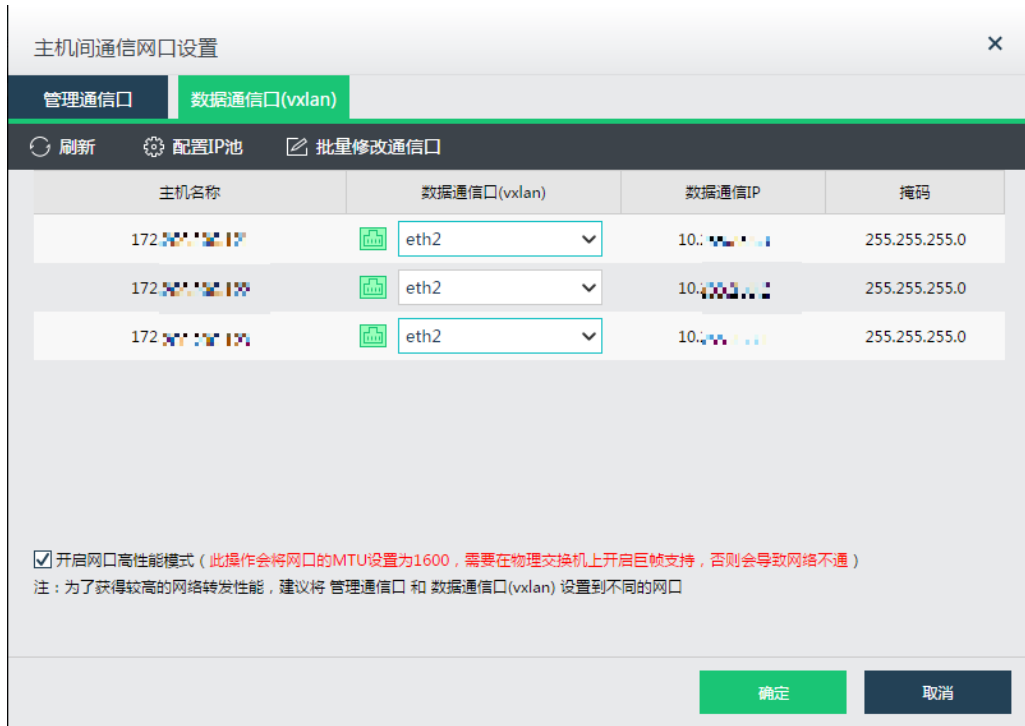
2. 选择需要添加的主机，如果需要添加的主机不在列表中，点击<+>进行添加。提示将清除防火墙配置，点击<确认>。





3. 若提示检测到主机间数据通信口之间的MTU不一致, 点击[立即配置], 勾选“开启网口高性能模式”; 可根据实际网络环境调整数据通信口网口。

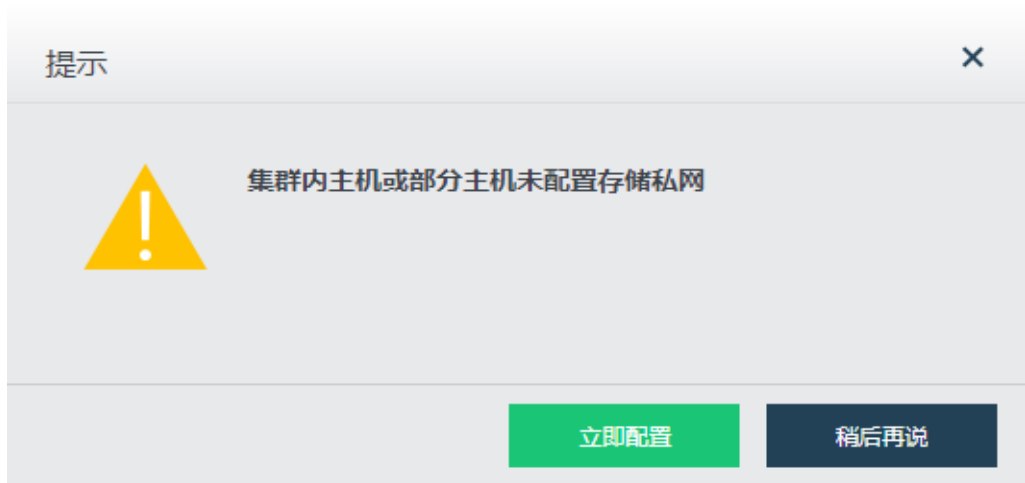




4. 点击[存储/虚拟存储/扩容]。



5. 根据实际网络，选择虚拟存储通信网络部署模式。





6. 选择合适的存储网口，并配置IP。



7. 再次点击<扩容>，选择需要进行主机扩容的存储卷；点击[主机扩容]，确认存储卷的扩容方式为主机扩容。

扩容

1 选择存储卷

2 确认扩容方式

3 配置硬盘

4 确认配置

请选择需要扩容的存储卷

|                                  | 名称        | 总容量     | 剩余容量       | 主机数 | 已用硬盘数 | 可用硬盘数 |
|----------------------------------|-----------|---------|------------|-----|-------|-------|
| <input checked="" type="radio"/> | 虚拟存储(2副本) | 5.41 TB | 1019.01 GB | 3   | 10    | 0     |

虚拟存储(2副本卷)

下一步取消

扩容

选择存储卷

2 确认扩容方式

3 配置硬盘

4 确认配置

扩容方式：

☒ 主机扩容 ☐ 硬盘扩容

发现有下列可扩容的物理主机，请选择要加入存储卷“虚拟存储(2副本卷)”的主机：已选择0台主机

| <input type="checkbox"/> | 主机名称         | 主机IP         | 固态硬盘总数 | 机械硬盘总数 |
|--------------------------|--------------|--------------|--------|--------|
| <input type="checkbox"/> | 172.17.0.101 | 172.17.0.101 | 0      | 4      |
| <input type="checkbox"/> | 172.17.0.102 | 172.17.0.102 | 0      | 2      |
| <input type="checkbox"/> | 172.17.0.103 | 172.17.0.103 | 0      | 2      |

上一步下一步取消

8. 进行磁盘的配置，建议SSD作为缓存盘，HDD作为数据盘和热备盘。



说明：

5.8.7R1 版本设置 HDD 为热备盘时，需先将 HDD 从硬盘组中移除，再单独设置为热备盘。



9. 输入要扩容存储卷的名称、admin管理员密码，进行配置确认。



10. 扩容后进行一键检测，确认集群正常运行。

## 11.3.6.2. 硬盘扩容

### 功能说明

当存储卷容量空间不足时，HCI主机还有空余磁盘插槽时，可以通过添加磁盘的方式对存储卷进行扩容。

### 注意事项

1. 替换磁盘后涉及数据重建与平衡，会对业务有影响，建议在业务空闲时操作。
2. 若一体机设备的RAID卡是JBOD模式，此时磁盘支持热插拔，支持在服务器不关机的情况下插上磁盘。
3. 若一体机设备的RAID卡是RAID 0模式，此时磁盘不支持热插拔，需将服务器关机下电后再插上新盘。对新盘进行单盘设置为RAID 0操作，再进行前台页面操作。
4. 扩容后需要满足下列条件：
  - 主机之间的数据盘容量总和，最高和最低的相差不能超过 50%。
  - 主机之间的数据盘个数总和，最高和最低相差不能超过 3 个。
  - 每台主机的缓存盘容量和数据盘容量的比例，不能低于 5%，且各主机之间这一比例的差值不能超过 5%。
  - 每台主机内缓存盘和机械盘的个数比例大于等于 1: 6。
  - 两主机的情况下，容量必须一致。
  - 如果是单独添加缓存盘，则在界面上添加完毕后，需要联系深信服技术支持进行操作。

### 前提条件

1. 新磁盘已经插入到主机上，并且能够被平台识别到。
2. 确保虚拟存储的任务执行页面没有任务在运行。

### 操作步骤

1. 在[存储/虚拟存储]中点击扩容，选择需要扩容的卷。





2. 选择“硬盘扩容”，进入配置磁盘，选择新发现磁盘的用途：数据盘、缓存盘、热备盘、不加入到虚拟存储。





3. 确认配置后，请输入要扩容的存储卷名称和admin管理员密码，点击<确定>，磁盘扩容完毕。



4. 磁盘扩容后，进行一键检测，确认平台运行稳定。

## 11.4. 平台硬件维护

### 11.4.1. 硬件巡检

定期使用信服云智能交付工具aDeploy对超融合平台的硬件进行巡检，提前发现超融合平台存在的硬件风险并及时进行处理，是保障超融合平台和业务稳定的关键举措。信服云智能交付工具已全面覆盖硬件相关的问题和风险，针对硬件的巡检内容如下表：

| 序号 | 巡检项目               | 说明 |
|----|--------------------|----|
| 1  | 主机在线检测             |    |
| 2  | 主机 CPU 检测          |    |
| 3  | 主机内存检测             |    |
| 4  | 平台主机网口检测           |    |
| 5  | 平台机械盘健康检测          |    |
| 6  | 平台 SSD 健康检测        |    |
| 7  | 系统盘检测              |    |
| 8  | 平台 RAID 卡健康状态检测    |    |
| 9  | 平台 RAID 卡兼容性检测     |    |
| 10 | 平台集群资源使用率检测        |    |
| 11 | 主机 VXLAN 网口高性能模式检测 |    |
| 12 | 磁盘 SMART 信息检测      |    |
| 13 | 平台 IMPI 检测         |    |
| 14 | 系统异常重启检测           |    |

### 11.4.2. 硬件告警查看

定期查看服务器面板指示灯状态及IMPI管理界面的日志，可以从主机层面观测服务器硬件的运行情况。

11.4.2.1. 面板指示灯判断【9C、9S、9T、9D 均指服务器 SN 码编号的开头】

1. 9C（SN码）面板指示灯样例及硬盘状态指示灯

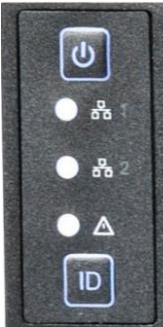


| 编号 | 模块名称               | 正常情况                    | 异常情况                                                  |
|----|--------------------|-------------------------|-------------------------------------------------------|
| 1  | 服务器开关按键            | NA                      | NA                                                    |
| 2  | ID 灯及按键            | NA                      | NA                                                    |
| 3  | Rset 键             | NA                      | NA                                                    |
| 4  | LCD 液晶管理模块接口       | NA                      | NA                                                    |
| 5  | 系统故障指示灯            | 不亮                      | 发生故障时，常亮红色<br>发生警告时，红色闪烁                              |
| 6  | 内存故障指示灯            | 不亮                      | 发生故障时，常亮红色<br>发生警告时，红色闪烁                              |
| 7  | 风扇故障指示灯            | 不亮                      | 发生故障时，常亮红色<br>发生警告时，红色闪烁                              |
| 8  | 电源故障指示灯            | 不亮                      | 发生故障时，常亮红色<br>发生警告时，红色闪烁                              |
| 9  | 系统过热指示灯            | 不亮                      | CPU/MEM 过热，常亮红色                                       |
| 10 | 网络状态指示灯（eth0 eth1） | 插网线亮                    | -                                                     |
| 11 | 硬盘活动状态指示灯          | 绿色<br>绿色闪烁：<br>硬盘进行读写活动 | NA                                                    |
| 12 | 硬盘故障报警指示灯          | 不亮                      | 常亮红色：硬盘出现故障故障<br>常亮蓝色：硬盘定位<br>常亮紫色：配合 RAID Rebuilding |

2. 9S（SN码）面板指示灯样例及硬盘状态指示灯



| 按键    | 符号  | 功能说明                               |
|-------|-----|------------------------------------|
| 电源按键  |     | 短按电源键：开机或向操作系统发送关机指令<br>长按电源键：强制关机 |
| ID 按键 | ID  | 打开或关闭蓝色 ID 灯，用于服务器识别               |
| 复位键   | Rst | 按下复位键可以重启服务器                       |



| LED 指示灯       | 符号 | 功能说明                      |
|---------------|----|---------------------------|
| 电源指示灯         |    | 安装在电源键上，亮：服务器运行中；灭：服务器未启动 |
| NIC1/NIC2 指示灯 |    | 亮：板载 LAN 工作；灭：板载 LAN 无活动  |
| 系统故障指示灯       |    | 亮：服务器系统出现故障或异常；灭：服务器工作正常  |
| ID 指示灯        |    | 安装在 ID 键上，蓝灯亮，用户将该服务器标记识别 |

备注：系统故障指示灯（黄色表示通常为设备硬件有告警或故障）

硬盘架指示灯状态及详细功能说明。



| Active | Locate/ERR | 功能说明           |
|--------|------------|----------------|
| 灭      | 灭          | 不在位或故障         |
| 绿色常亮   | 灭          | 工作正常无数据读写      |
| 绿色闪烁   | 灭          | 工作正常有数据读写      |
| 绿色常亮   | 蓝色常亮       | 被定位            |
| 绿色闪烁   | 黄色闪烁 1Hz   | 所在 RAID 组在进行重构 |
| 绿色常亮   | 黄色闪烁 4Hz   | 即将故障           |
| 绿色常亮   | 黄色常亮       | 硬盘故障           |

3. 9T（SN码）面板指示灯样例及硬盘状态指示灯



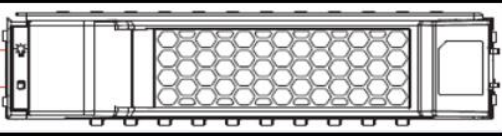
| LED 灯号       | 图示 | 显示 | 说明       |
|--------------|----|----|----------|
| 电源指示灯        |    | 常亮 | 已开机      |
|              |    | 熄灭 | 已关机      |
| Location 指示灯 | ID | 常亮 | 选中此机台    |
|              |    | 熄灭 | 未选中此机台   |
| 系统报警灯        |    | 闪烁 | 系统存在异常报警 |
|              |    | 熄灭 | 系统工作正常   |

备注：

系统报警灯：指示灯慢闪（告警）、指示灯快闪（严重错误）

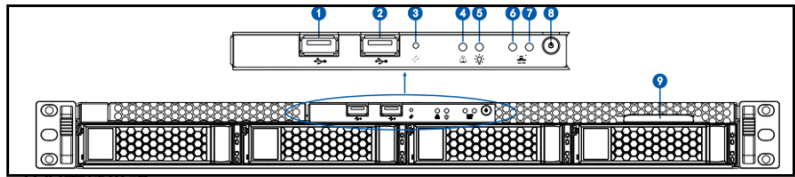
硬盘架指示灯状态及详细功能说明。

硬盘绿色指示灯  
硬盘黄色指示灯



|       |                                                                                                                                                                        |      |              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------|
| 硬盘指示灯 | <br> | 绿灯常亮 | 硬盘在位         |
|       |                                                                                                                                                                        | 绿灯闪烁 | 硬盘处于读写状态     |
|       |                                                                                                                                                                        | 绿灯熄灭 | 硬盘不在位或系统无电   |
|       |                                                                                                                                                                        | 黄灯常亮 | 硬盘坏掉         |
|       |                                                                                                                                                                        | 黄灯闪烁 | 硬盘处于raid重组状态 |
|       |                                                                                                                                                                        | 黄灯熄灭 | 硬盘正常工作       |

4. 9D（SN码）面板指示灯样例及硬盘状态指示灯



控制面板说明：

① USB2.0 ② USB2.0 ③ 重启键 ④ 警告灯 ⑤ 系统状态灯  
⑥ 网口1指示灯 ⑦ 网口2指示灯 ⑧ 开机键 ⑨ 服务器信息标签

注：图片为参考式样，规格及设计以实物为准。

控制面板指示灯说明：

| 名称     | 颜色 | 状态 | 说明         |
|--------|----|----|------------|
| 系统状态灯  | 蓝色 | 亮  | 服务器处于开机状态  |
| 网络1指示灯 | 绿色 | 亮  | 网络连接正常     |
|        | 绿色 | 闪烁 | 板载网络1有数据传输 |
| 网络2指示灯 | 绿色 | 亮  | 网络连接正常     |
|        | 绿色 | 闪烁 | 板载网络2有数据传输 |
| 警告灯    | 黄色 | 闪烁 | 服务器处于异常状态  |

备注：告警指示灯（黄色）的两种情况1.内存告警 2.传感器告警

硬盘架指示灯状态及详细功能说明。



| Active | Locate/ERR | 功能说明      |
|--------|------------|-----------|
| 灭      | 灭          | 不在位或故障    |
| 绿色常亮   | 灭          | 工作正常无数据读写 |
| 绿色闪烁   | 灭          | 工作正常有数据读写 |

11.4.2.2. IPMI 信息判断

当面板指示灯出现异常情况时，需要进一步确定问题，则需要通过IPMI查看详细的事件日志定位问题；日常处理方法如下：

### 1. 电源故障类建议处理方法

- 先进IPMI查看事件日志，确认是CPU过热还是MEM过热；
- 查看发过部件是瞬间的通常是环境温度过热导致，会自行恢复；持续过热则需要关机断电确认；
- 持续过热且无法降温，需要联系400专家确认是否返修。

### 2. 内存故障类建议处理方法

- 先进IPMI查看事件日志，确认异常内存的具体槽位；
- 故障类，如，内存设备禁用，插槽无法识别出容量，先做插拔仍无法解决返修；不可修正ECC，直接返修对应内存；
- 告警类，通常是（可修正ECC）数量少，且不是连续多天持续报，可进行清理日志，重启BMC，解决；若持续报数量大，则返修对应内存。

### 3. 风扇故障类建议处理方法

- 先进IPMI查看事件日志和查看传感器值；
- 风扇转速值高于或低于BMC设定阈值会告警,通常能自行恢复不反复发生不用理会；
- 显示风扇故障，且传感器显示风扇无值，插拔风扇无用后直接返修风扇。

### 4. 系统故障类建议处理方法

- 先进IPMI查看事件日志（通常是子系统健康故障）；
- 结合IPMI事件日志确认系统是否引导异常，若异常重启设备通常能解决；
- 重启无效需要联系专家确认是否返修。

### 5. 硬盘故障类建议处理方法

- 重新插拔raid卡；
- 确认BIOS 内是否识别 raid卡；
- 确认raid卡上是否有硬盘；
- JBOD磁盘，可做插拔，无效，返修磁盘。

## 11.4.3. 服务器拆机规范

### 防静电处理

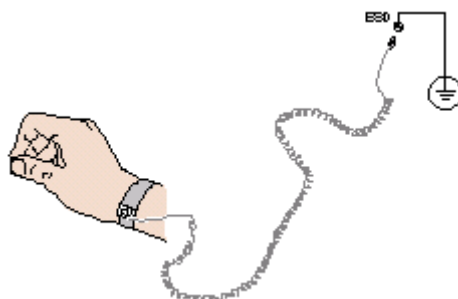
天气干燥时，人体与衣服摩擦，容易产生静电，这些静电可能会对集成电路上的芯片造成损伤，所以在直接接触电路板或者相关板卡时，需要释放人体所带静电。在

接触设备前，应当穿上防静电工作服、佩戴防静电手套或防静电腕带、去除身体上携带的易导电物体（如首饰、手表等），如图所示，以免被电击或灼伤。



佩戴防静电腕带的方法如图所示。

1. 将手伸进防静电腕带。
2. 拉紧锁扣，确认防静电腕带与皮肤接触良好。
3. 将防静电腕带的接地端插入机柜或机箱（已接地）上的防静电腕带插孔。



## 防液体溅入电路板

电路板如有液体，容易引起电路板短路及腐蚀，在操作时，应避免液体溅入电路板。因此要求如下：

1. 尽量避免操作范围有液体，如有液体，尽量盖好密封盖，并且请勿摆放在设备附近。
2. 环境温度高时，需注意人体排汗，避免头上汗水滴落，手上汗水沾湿板卡。

## 不可暴力拆装

通常部件组装或者拆卸，都是经过设计的，不会出现强力拆装的要求。如发现某个部件装不到预安装位置，或无法正常取下，通常是有结构控制件，需要注意拆装优先级，不要暴力拆装部件。通常建议：

1. 严格按照产品操作指导说明来实施。
2. 可以向有拆装经验者咨询。
3. 操作过程中，需对工具使用特别注意，切勿因未注意力道而划伤电路板。

## 避免杂物掉落



通常电子部件，相对脆弱，千万注意不要在操作过程中，有重物掉落，砸中电路板，导致大概率元器件损伤，也不要有小部件导电体掉落到主板或者板卡上，当通电时这些小部件物料也可能导致短路，所以也需注意异物掉落。通常建议：

1. 将拆装设备，放置工作台或者桌面操作。
2. 拆装过程，部件需要拿稳，谨防掉落。
3. 螺丝等小配件物件，集中放置在设备以外的地方。
4. 安装完后整理布线，同时确认设备内部未遗留杂物。

## 断电操作

涉及在主板上操作的部件，如内存、CPU、PCIE扩展卡等一定要断电操作，不仅要关机，还需要拔掉电源线。个别部件，如可以热插拔的硬盘、冗余模块等，是可以在设备工作状态下直接更换的。

## 11.4.4. 硬件故障处理

### 11.4.4.1. 主机替换

#### 功能说明

当集群中某台主机由于物理故障离线时，需要用一台新主机进行替换。

#### 注意事项

1. 主机替换会触发数据重建，会占用IO，建议和客户商议，在业务空闲时段进行操作。
2. 要求新主机的CPU主频、内存的大小和频率、硬盘容量不能低于原故障主机。
3. 如果新主机的硬盘数量大于原故障主机，主机替换完成之后要进行扩容。
4. 建议新主机的单块磁盘的容量和原故障主机的一致。
5. 要求新主机的管理IP地址不能和原故障主机的相同。

#### 前提条件

1. 新主机的各个网络平面的IP地址已规划好。
2. 新主机已安装好aSV软件且与原版本一致（包括补丁），设置好管理IP。
3. 新主机的管理口、VXLAN口、数据通信口、存储口已正确接入到网络中。

#### 操作步骤

1. 在[实体机/物理主机]中找到故障主机，点击<更换主机>。



2. 确认新主机配置不低于原故障主机，并正确安装好aSV软件后，勾选“我已准备完成”，点击<下一步>。



3. 选择新发现的主机，点击<下一步>，将主机添加到集群之后，进行替换。



4. 配置网络，选择存储通信口，并配置通信网口IP。



5. 确认配置：选择是否参照旧主机的磁盘配置模式，并勾选“我确定要更换物理主机”，点击<完成>。



6. 显示检测通过, 点击<确认>, 在任务中心中就可以看到更换主机的进度, 等待主机更换完成。



任务列表

| 状态            | 动作       | 对象           | 开始时间                | 结束时间                | 操作人                    | 操作                                    |
|---------------|----------|--------------|---------------------|---------------------|------------------------|---------------------------------------|
| <div>0%</div> | 替换主机     | 主机           | 2017-05-18 17:39:30 |                     | admin( 192.168.1.100 ) | <a href="#">查看</a> <a href="#">取消</a> |
| 完成            | 添加主机前置检测 | 主机           | 2017-05-18 17:38:56 | 2017-05-18 17:39:10 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 添加主机前置检测 | 主机           | 2017-05-18 17:38:42 | 2017-05-18 17:38:50 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 添加主机前置检测 | 主机           | 2017-05-18 17:38:29 | 2017-05-18 17:38:39 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 添加主机前置检测 | 主机           | 2017-05-18 17:37:56 | 2017-05-18 17:38:11 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 添加主机     | 172.16.1.100 | 2017-05-18 17:34:02 | 2017-05-18 17:35:07 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 编辑网口     | eth3         | 2017-05-18 17:31:05 | 2017-05-18 17:31:08 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 编辑网口     | eth2         | 2017-05-18 17:30:58 | 2017-05-18 17:31:00 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 编辑网口     | eth1         | 2017-05-18 17:30:51 | 2017-05-18 17:30:54 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 登录       | admin        | 2017-05-18 17:30:19 | 2017-05-18 17:30:19 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 更改主节点    | 172.16.1.100 | 2017-05-18 17:29:35 | 2017-05-18 17:29:35 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 登录       | admin        | 2017-05-18 17:28:43 | 2017-05-18 17:28:43 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 登录       | admin        | 2017-05-18 17:27:32 | 2017-05-18 17:27:32 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 登录       | admin        | 2017-05-18 17:26:02 | 2017-05-18 17:26:02 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 登录       | admin        | 2017-05-18 17:22:41 | 2017-05-18 17:22:41 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |
| 完成            | 登录       | admin        | 2017-05-18 17:13:49 | 2017-05-18 17:13:49 | admin( 192.168.1.100 ) | <a href="#">查看</a>                    |

[查看历史操作日志](#)

关闭

7. 等待数据重建完成后，进行一键自检，确认平台运行正常。

11.4.4.2. 系统盘替换

功能说明

系统盘发生故障导致主机离线，或者系统盘被检测为亚健康盘时，可进行安全的系统盘更换。

注意事项

1. 不支持组RAID的系统盘进行替换磁盘操作，请联系深信服技术支持。
2. 不支持同步进行多个主机同时替换系统盘。
3. 不支持集群内有任务时进行更换系统盘。
4. 不支持替换主控系统盘，如需替换需要切换主控进行更换。
5. 仲裁节点不支持系统盘替换功能。
6. 替换系统盘前后，禁止物理网卡发生变动。
7. 系统盘更换成功后，不会立即退出维护模式，需要等待1分钟主机服务重启完毕，再手动退出维护模式。
8. 系统盘如果空间不足，会导致系统盘配置备份失败。
9. 替换系统盘之前需要进入单主机维护模式，切勿勾选“进入维护模式后，主机自动关机”。
10. 系统会每天自动备份系统盘数据到其他主机上，支持在系统盘故障导致主机离

线情况下替换系统盘。

前提条件

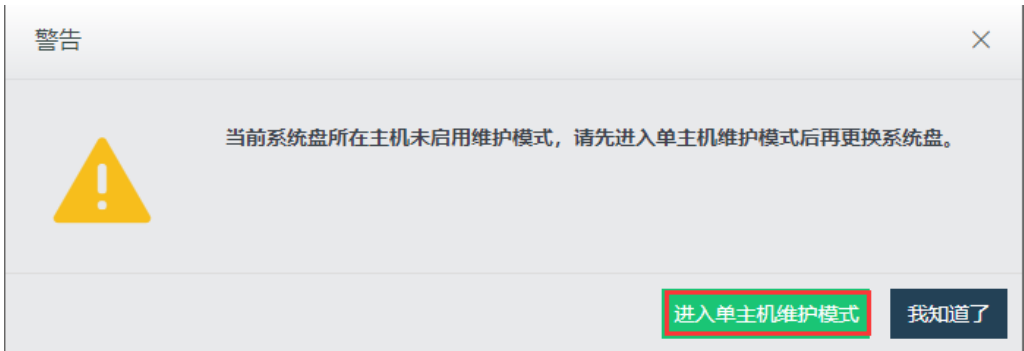
无

操作步骤

1. 在[实体机/系统盘]中找到相应的主机。



2. 点击[更换系统盘]，进入单主机维护模式。



3. 在进入单主机维护模式时，切勿勾选“进入维护模式后，主机自动关机”，关机造成主机系统盘数据无法备份。



4. 启用单主机维护模式需要将该主机上运行的虚拟机和虚拟设备进行迁移或者关机处理。



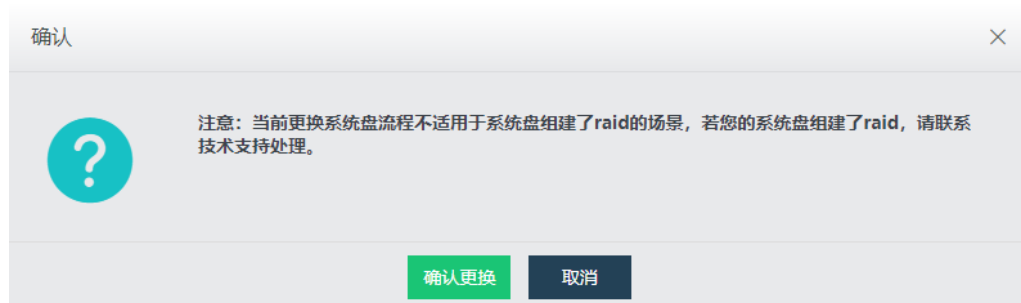


5. 确认虚拟机处理之后，点击<下一步>，提示输入管理员密码。



6. 主机进入维护模式，提示不适用于系统盘组建RAID场景。





7. 点击<确认更换>，进入系统备份界面。



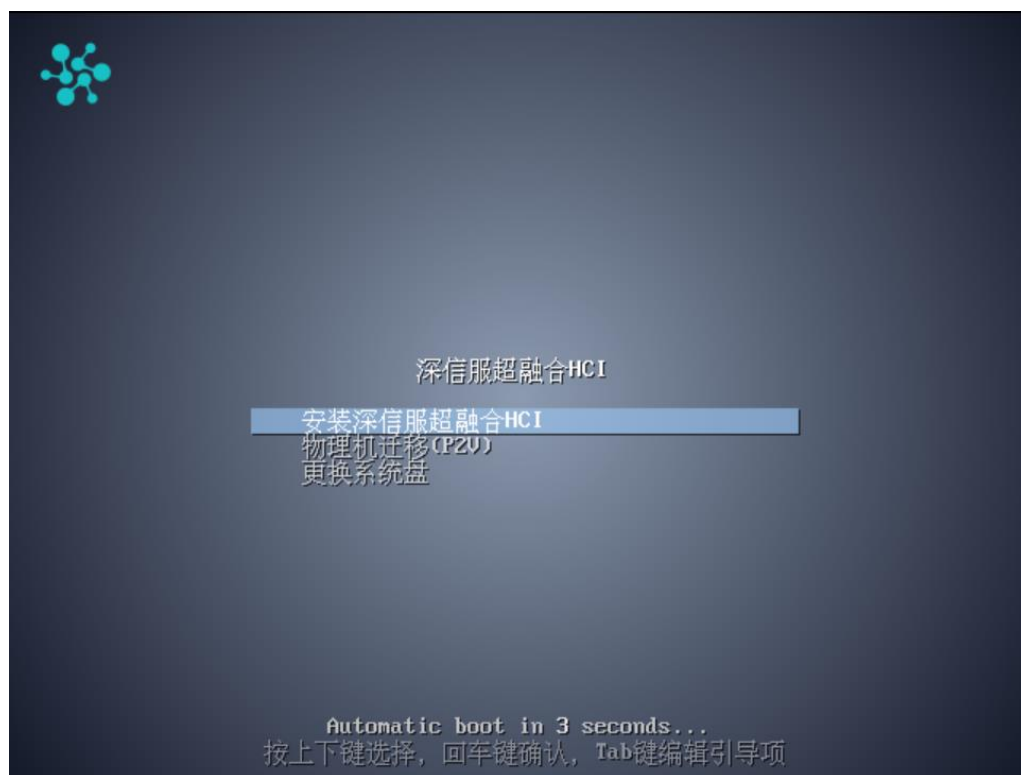
8. 点击<开始备份>，会将需要更换的主机系统盘配置信息备份到其他主机上。



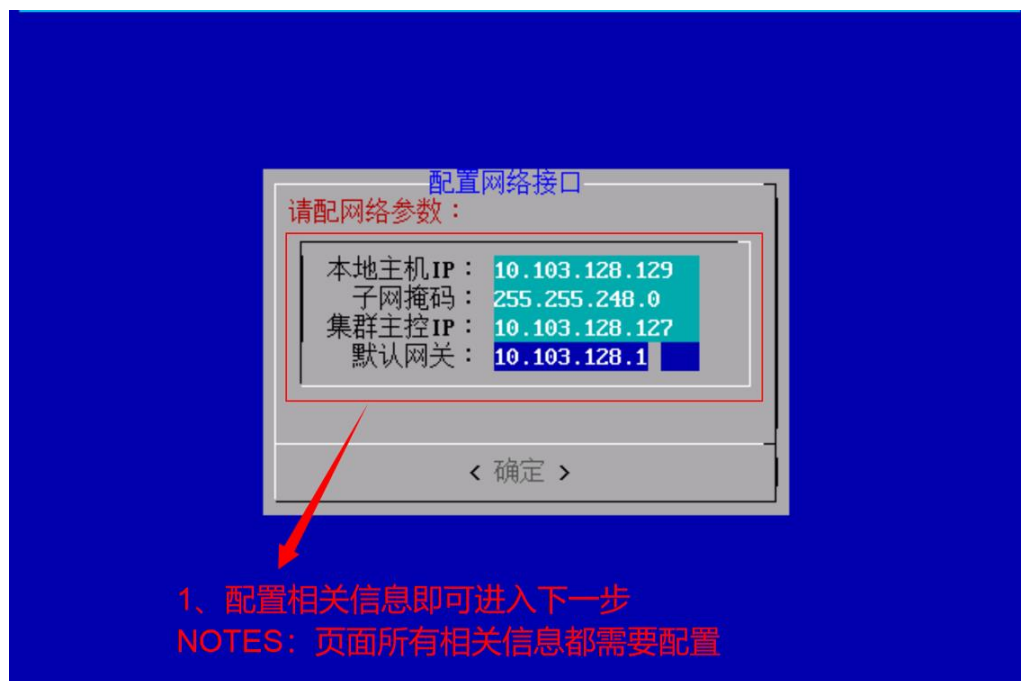
9. 备份完成之后，界面出现替换系统盘流程指引。



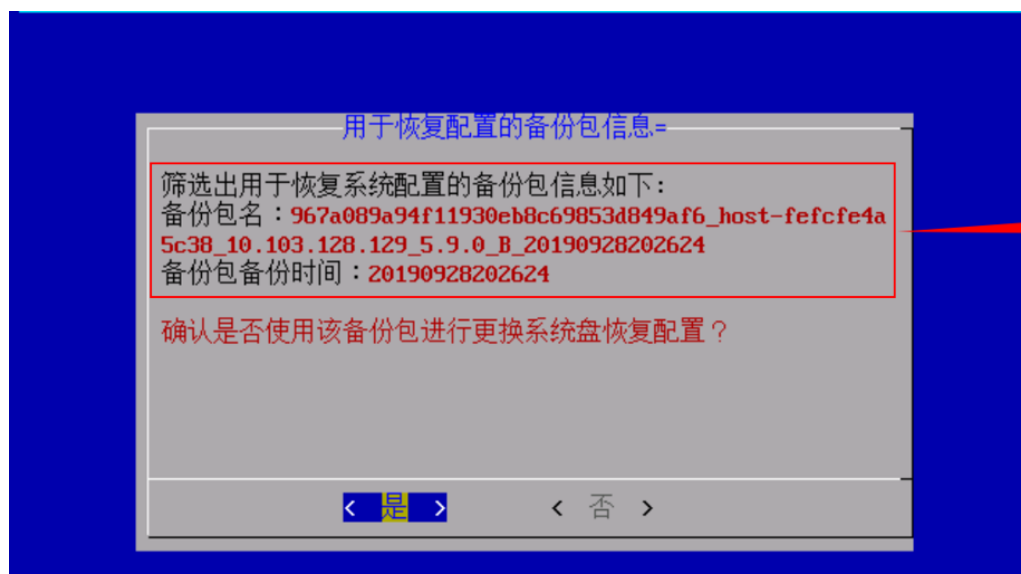
10. 拔出原系统盘之后，插入新的系统盘。通过同版本的安装光盘/u盘启动物理主机，选择更换系统盘，进入新系统盘安装向导，选择更换系统盘。



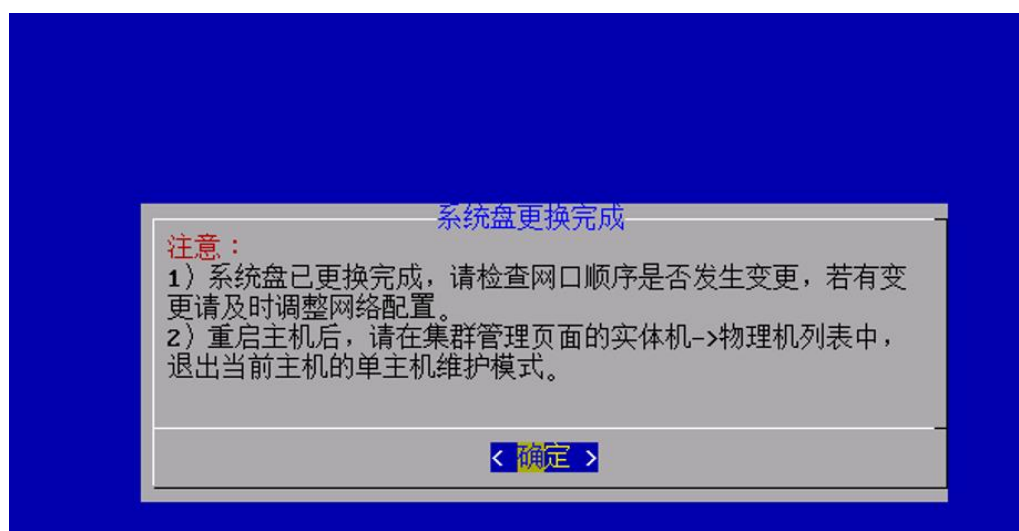
11. 进入配置网络接口页面，本地主机IP写所要恢复的主机IP。



12. 系统会根据填写的IP，自动获取到最新的系统盘数据备份，用于恢复。



13. 等待恢复完成，提示重启主机。



14. 手动更换完系统盘之后, 点击<完成>, 等一分钟之后关闭单主机维护模式。



### 11.4.4.3. 磁盘替换

#### 功能说明

当集群中主机有磁盘故障时, 需要用新的磁盘进行替换。(支持数据盘、缓存盘替换)。

#### 注意事项

1. 替换磁盘后会触发数据重建, 对业务有影响, 建议在业务空闲时操作。
2. 若一体机设备的RAID卡是JBOD模式, 此时磁盘支持热插拔, 支持在服务器不关机的情况下将故障磁盘拔下, 再插上新磁盘。
3. 若一体机设备的RAID卡是RAID 0模式, 此时磁盘不支持热插拔, 需将服务器关

机下电后再换盘。对新盘进行单盘设置为RAID 0操作，再进行前台页面操作。

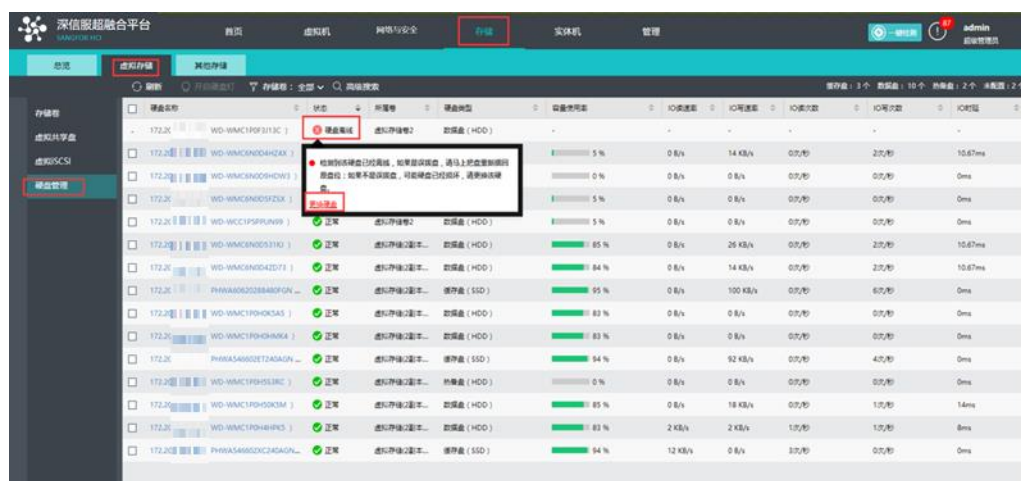
- 一体机磁盘故障后必须购买深信服的磁盘才可以进行磁盘替换，非深信服磁盘虚拟存储识别不到。
- 新磁盘的位置必须和故障磁盘在同一台主机上，推荐使用原盘位。
- aCloud 5.8.6 及之前版本在进行缓存盘前，需联系深信服技术协助回刷缓存数据。

## 前提条件

- 新磁盘的容量大小要和故障磁盘的大小一致（严禁替换磁盘容量小于故障磁盘容量）。
- 确保虚拟存储的任务执行页面没有任务在运行。

## 操作步骤

- 在[存储/虚拟存储/硬盘管理]中找到故障磁盘，点击[更换硬盘]。



- 先将故障磁盘拔出，再插入新磁盘，勾选“我已准备完成”。



3. 选择新磁盘，点击<下一步>。



4. 确认新磁盘及故障磁盘的信息，勾选“我确定要更换磁盘”，点击<完成>后平台开始执行更换磁盘的操作。



5. 更换完成后可以在平台的配置界面看到已经没有离线的磁盘。



6. 替换完成后，进行一键检测，确认平台运行稳定。

### 11.4.4.4. 内存替换

#### 功能说明

1. 当集群内有主机内存发生故障时，可以手动更换故障内存。
2. 当集群中内存资源不足时，可以手动对集群内主机进行内存扩容。
3. 非一体机需联系服务器厂商，由相应厂商人员操作维护，禁止深信服员工直接操作。

#### 注意事项

1. 可以在不停止客户业务的情况下进行扩容，扩容需逐台关机，建议在业务非高峰时段进行。
2. 扩容前需确认集群当前无虚拟存储任务在运行（数据重建、数据同步、数据平衡）。
3. 每扩容一台主机后，需等待虚拟存储任务执行完毕后再进行下一台主机的扩容。
4. 硬件拆箱操作请严格遵守服务器厂商提供的操作规划。

## 前提条件

1. 确认内存的厂家和型号，保证硬件兼容性，内存扩容或更换时，务必保存是深信服内存，且参数与原机器上的一模一样，公司禁止第三方配件。
2. 确认集群当前无虚拟存储任务执行。

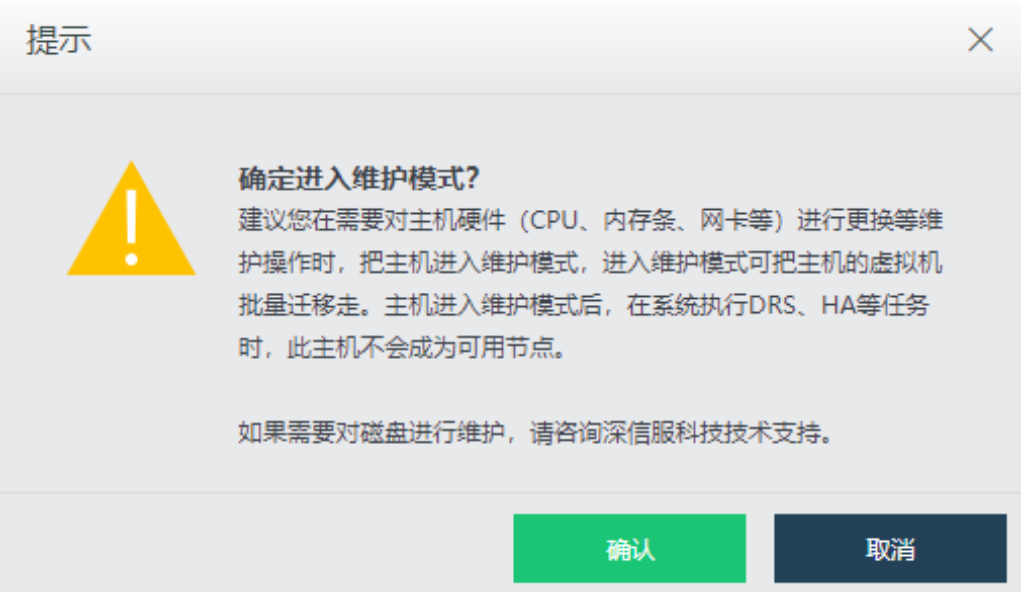
## 操作步骤

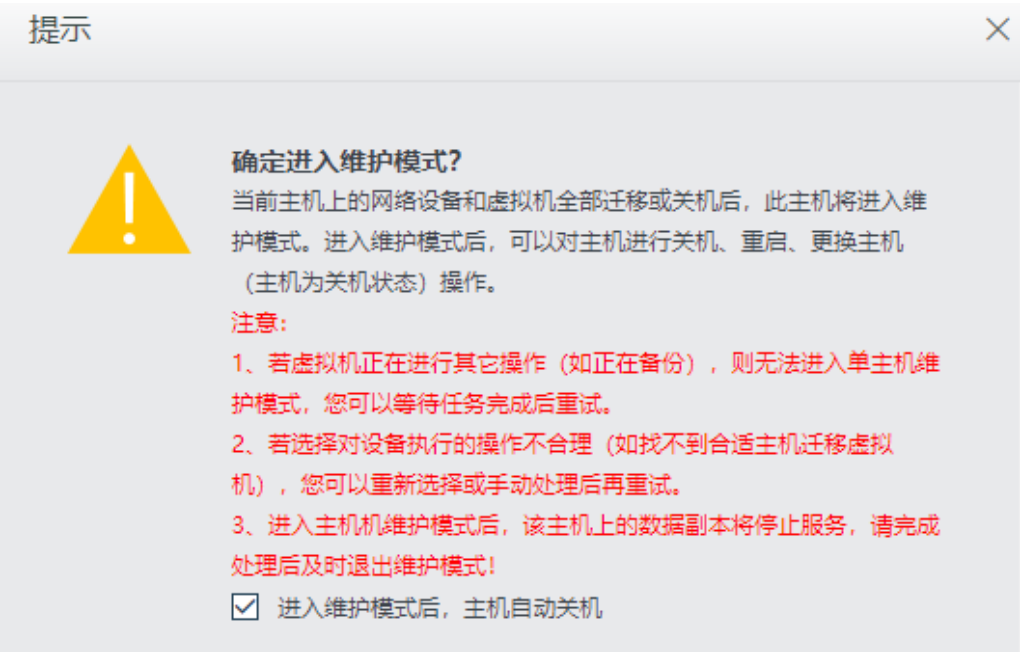
1. 点击[存储/总览]，查看当前虚拟存储是否有其他任务在执行，如果有任务在执行，请等待任务执行完毕后再进行维护操作。



2. 将需要维护的主机开启<单主机维护模式>，将需要不停机的虚拟机和NFV设备迁移至其他主机，勾选“进入维护模式后，主机自动关机”。







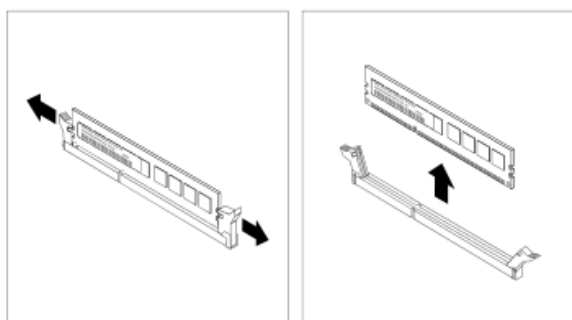
- 3. 确认主机关机后，将主机下架，进行开箱扩容，详细操作请参考下文硬件操作指南。
- 4. 硬件扩容完毕后，将主机重新上架，加入原集群。等待虚拟存储任务执行完毕后，进行一键检查（一定要勾选虚拟存储数据检查）。



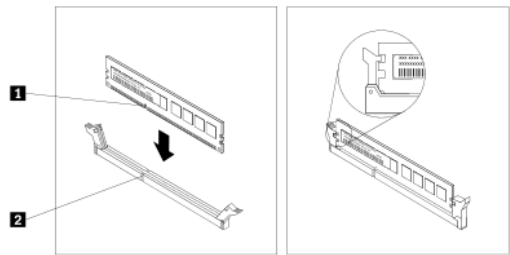


## 硬件操作指南

1. 确认设备断电后，并拔掉该设备电源连接线，取下服务器，平放在平稳平台上，打开机箱上盖。
2. 阅读内存安插顺序，并记住内存安装槽位，确认设备本身是否有内存安插错误。
3. 向下按内存左右固定夹，使其向左右打开，弹出内存。



4. 使装有新内存条的防静电包装接触服务器外侧表面上任意未涂油漆的地方。然后，从包装中取出内存条（注：抓住内存条边缘，小心操作内存条）。
5. 确认内存型号正确。
6. 将新内存条放置在内存插槽上。确保新内存条上的槽口与内存插槽上的凸起对齐，然后将新内存条笔直向下按入内存插槽，直到固定夹合上且新内存条咬合到位。



7. 检测没有其它杂物遗留在机箱内，封盖还原。

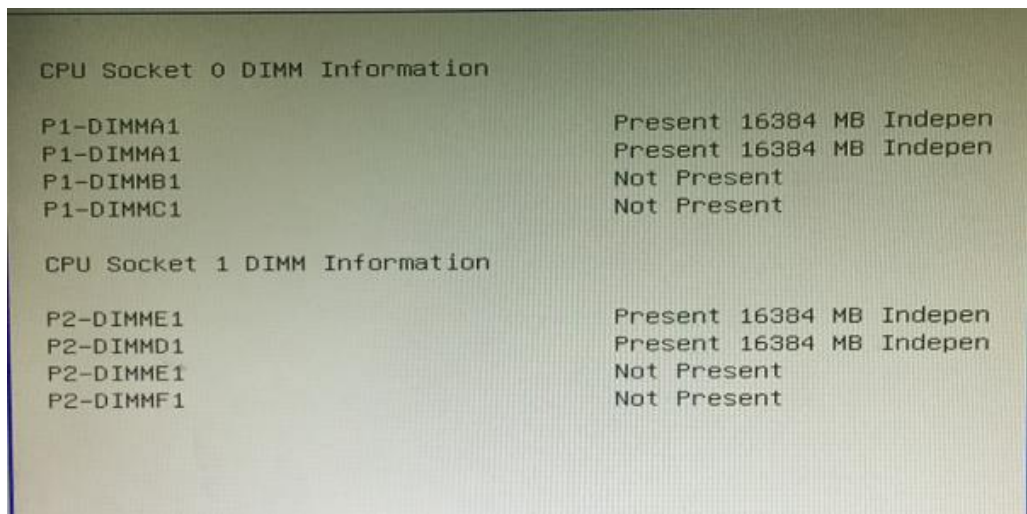
8. 替换后检测：

正常启动后需要进BIOS或进系统确认设备是否认全所有内存。

BIOS确认方法如下：

- 在 Main 查看 Total Memory 值是否等于所有内置总容量。
- 如 65536=64G、131072=128G。
- 在 Advanced 查看 ChIPset Configuation -- North Bridge -- DIMM Configuration -- DIMM Information。

下图为显示每个内存槽使用情况。



进系统后可通过指令查看内存使用情况来判断，是否识别完全。

使用命令较多，不一一例举，如下：

- Cat /proc/meminfo
- free -m

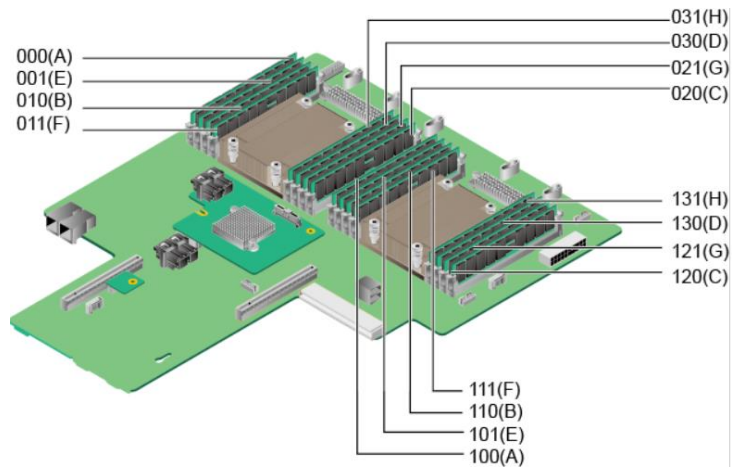
## 附：内存槽位插法

9S开头设备，内存插法如下表所示。

| 配置内存数量 | CPU0 内存插槽 |    |    |    |    |    |    |    |    |    |    |    | CPU1 内存插槽 |    |    |    |    |    |    |    |    |    |    |    |
|--------|-----------|----|----|----|----|----|----|----|----|----|----|----|-----------|----|----|----|----|----|----|----|----|----|----|----|
|        | A0        | A1 | A2 | B0 | B1 | B2 | C0 | C1 | C2 | D0 | D1 | D2 | E0        | E1 | E2 | F0 | F1 | F2 | G0 | G1 | G2 | H0 | H1 | H2 |
| 1条     | ✓         |    |    |    |    |    |    |    |    |    |    |    | ✓         |    |    |    |    |    |    |    |    |    |    |    |
| 2条     | ✓         |    |    |    |    |    |    |    |    |    |    |    | ✓         |    |    |    |    |    |    |    |    |    |    |    |
| 4条     | ✓         |    |    |    |    |    | ✓  |    |    |    |    |    | ✓         |    |    |    |    |    | ✓  |    |    |    |    |    |
| 6条     | ✓         |    |    | ✓  |    |    | ✓  |    |    |    |    |    | ✓         |    |    | ✓  |    |    | ✓  |    |    |    |    |    |
| 8条     | ✓         |    |    | ✓  |    |    | ✓  |    |    | ✓  |    |    | ✓         |    |    | ✓  |    |    | ✓  |    |    | ✓  |    |    |
| 10条    | ✓         | ✓  |    | ✓  |    |    | ✓  |    |    | ✓  |    |    | ✓         | ✓  |    | ✓  |    |    | ✓  |    |    | ✓  |    |    |
| 12条    | ✓         | ✓  |    | ✓  | ✓  |    | ✓  |    |    | ✓  |    |    | ✓         | ✓  |    | ✓  |    |    | ✓  | ✓  |    |    |    |    |
| 14条    | ✓         | ✓  |    | ✓  | ✓  |    | ✓  | ✓  |    | ✓  |    |    | ✓         | ✓  |    | ✓  | ✓  |    | ✓  | ✓  |    |    |    |    |
| 16条    | ✓         | ✓  |    | ✓  | ✓  |    | ✓  | ✓  |    | ✓  | ✓  |    | ✓         | ✓  |    | ✓  | ✓  |    | ✓  | ✓  |    |    |    |    |
| 18条    | ✓         | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  |    |    | ✓         | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  |
| 21条    | ✓         | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓         | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  |
| 24条    | ✓         | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓         | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  |

- ⚠ 注意:
1. 表格中✓代表此内存槽安装内存，空白代表没有安装内存。

2. 将服务器上盖卸下，可以看到主板内存插槽旁有标记，参考下图。当只要插一根内存时，将内存插入 A0 插槽上；当要插入 4 条内存时，将内存插入 A0、C0、E0、G0 插槽上；以此类推。



9T开头设备，内存插法如下表。

| Two CPU. |   | CPU0      |    |    |           |    |    |           |    |    |           |    |    | CPU1      |    |    |           |    |    |           |    |    |           |    |    |
|----------|---|-----------|----|----|-----------|----|----|-----------|----|----|-----------|----|----|-----------|----|----|-----------|----|----|-----------|----|----|-----------|----|----|
|          |   | Channel 0 |    |    | Channel 1 |    |    | Channel 2 |    |    | Channel 3 |    |    | Channel 4 |    |    | Channel 5 |    |    | Channel 0 |    |    | Channel 1 |    |    |
|          |   | A0        | A1 | B0 | B1        | C0 | C1 | D0        | D1 | E0 | E1        | F0 | F1 | G0        | G1 | H0 | H1        | J0 | J1 | K0        | K1 | L0 | L1        | M0 | M1 |
| 1 DIMM   | V |           |    |    |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 2 DIMM   | V |           |    |    |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 3 DIMM   | V |           |    |    |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 4 DIMM   | V |           |    |    |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 5 DIMM   | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 6 DIMM   | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 7 DIMM   | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 8 DIMM   | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 9 DIMM   | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 10 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 11 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 12 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 13 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 14 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 15 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 16 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 17 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 18 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 19 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 20 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 21 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 22 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 23 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |
| 24 DIMM  | V |           |    | V  |           |    |    |           |    |    |           |    |    | V         |    |    |           |    |    |           |    |    |           |    |    |

| One CPU:  |    |           |    |           |    |           |    |           |    |           |    |   |
|-----------|----|-----------|----|-----------|----|-----------|----|-----------|----|-----------|----|---|
| CPU0      |    |           |    |           |    |           |    |           |    |           |    |   |
| Channel 0 |    | Channel 1 |    | Channel 2 |    | Channel 3 |    | Channel 4 |    | Channel 5 |    |   |
| A0        | A1 | B0        | B1 | C0        | C1 | D0        | D1 | E0        | E1 | F0        | F1 |   |
| 1 DIMM    | V  |           |    |           |    |           |    |           |    |           |    |   |
| 2 DIMM    | V  |           |    |           |    | V         |    |           |    |           |    |   |
| 3 DIMM    | V  |           | V  |           |    | V         |    |           |    |           |    |   |
| 4 DIMM    | V  |           | V  |           |    | V         |    | V         |    |           |    |   |
| 5 DIMM    | V  |           | V  |           | V  | V         |    | V         |    |           |    |   |
| 6 DIMM    | V  |           | V  |           | V  | V         |    | V         |    |           | V  |   |
| 7 DIMM    | V  | V         | V  |           | V  | V         |    | V         |    | V         |    |   |
| 8 DIMM    | V  | V         | V  |           | V  | V         | V  | V         |    | V         |    |   |
| 9 DIMM    | V  | V         | V  | V         | V  | V         | V  | V         |    | V         |    |   |
| 10 DIMM   | V  | V         | V  | V         | V  | V         | V  | V         | V  | V         |    |   |
| 11 DIMM   | V  | V         | V  | V         | V  | V         | V  | V         | V  | V         | V  |   |
| 12 DIMM   | V  | V         | V  | V         | V  | V         | V  | V         | V  | V         | V  | V |

11.4.4.5. 网卡替换

功能说明

- 1. 当深信服一体机网卡需要升级替换（千兆网卡升级为万兆网卡）。
- 2. 当深信服一体机现有网卡数量较少，不满足最佳实践，需要增加网卡。
- 3. 当深信服一体机网卡出现故障，需要替换网卡。
- 4. 非一体机需联系服务器厂商，由相应厂商人员操作维护，禁止深信服员工直接操作。

注意事项

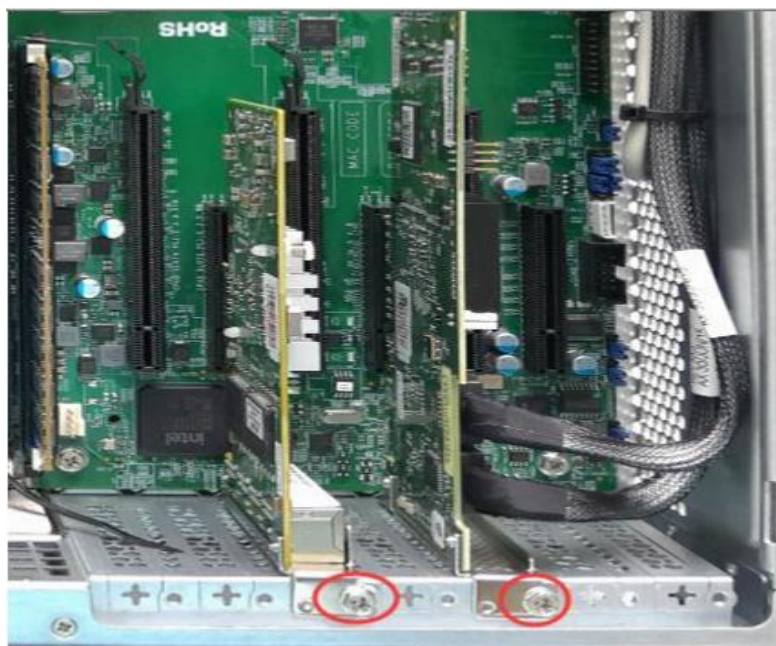
- 1. 升级网卡、增加网卡请确认网卡在兼容性列表中。
- 2. 替换网卡推荐使用和原网卡型号参数一致的网卡。

前提条件

- 1. 确认网卡兼容性无问题，无法确定的情况下请联系深信服技术支持进行评估。
- 2. 确认需要升级、增加、替换网卡的主机，并将运行在该主机上的虚拟机和虚拟设备迁移至集群其他主机，保证业务不中断。

操作步骤

- 1. 确认设备断电后，拆卸所有外部线缆，如电源线缆、网线等。
- 2. 从机柜上将服务器拆卸下架，水平放置在平稳桌面上。
- 3. 打开机箱上盖，卸下网卡固定螺丝。
- 4. 双手拿住网卡两边，缓慢向上拔出网卡。



5. 确认网卡型号无误。
6. 双手拿住新网卡两边，插入对应插槽。
7. 上螺丝固定。
8. 检测没有其它杂物遗留在机箱内，封盖还原。
9. 进行一键检测，确认平台运行正常。

#### 11.4.4.6. RAID 卡替换

##### 功能说明

1. 当深信服一体机RAID卡出现故障，需要在不停止业务的情况下进行替换。
2. 非深信服一体机需联系服务器厂商，由相应厂商人员操作维护，禁止深信服员工直接操作。

##### 注意事项

确认服务器型号、RAID卡型号，推荐使用和原RAID卡参数一致的进行替换，保证兼容性。

##### 前提条件

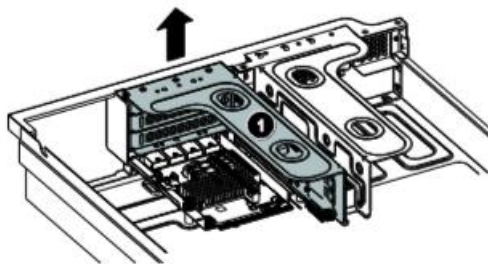
1. 确认新RAID卡与服务器兼容性无问题，且支持JBOD模式。
2. 将需要硬件维护的主机进入单主机维护模式，将该主机上运行的虚拟机迁移至集群内其他主机上，保证业务不中断。



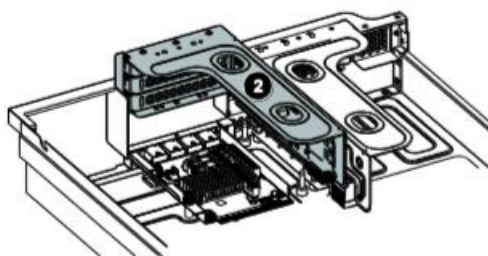
## 操作步骤

### 1. 9S开头设备

- 确认设备断电后，并拔掉该设备电源连接线，取下服务器，平放在平稳平台上，打开机箱上盖。
- 取下 PCI-E 转接卡。



- 拔掉 2 根连接在阵列卡上的 RAID 线，记住接线顺序（按下压片，向外拔出）。
- 拧下 RAID 卡的固定螺丝，握住 RAID 卡边缘，取下 RAID 卡。
- 确认阵列卡型号正确。
- 将阵列卡放在 PCI-E 插槽附近。然后，小心地将该阵列卡直着按入插槽，直至其牢固就位。确保阵列卡支架被转接卡支架固定。
- 上固定螺丝，并按顺序接回 RAID 线。
- 将转接卡装回机箱。

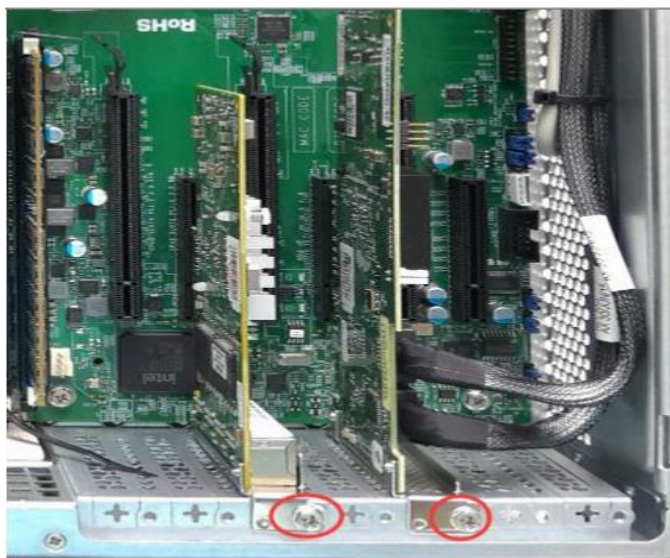


- 检测没有其它杂物遗留在机箱内，封盖还原。

### 2. 9W开头设备

- 确认设备断电后，并拔掉该设备电源连接线，取下服务器，平放在平稳平台上，打开机箱上盖，卸下导风罩。
- 拔掉 2 根连接在阵列卡上的，RAID 线，注意 2 根线是有顺序的（按下压片，向外拔出）。
- 卸下固定螺丝。
- 拿住阵列卡 2 边，向上拔出阵列卡。

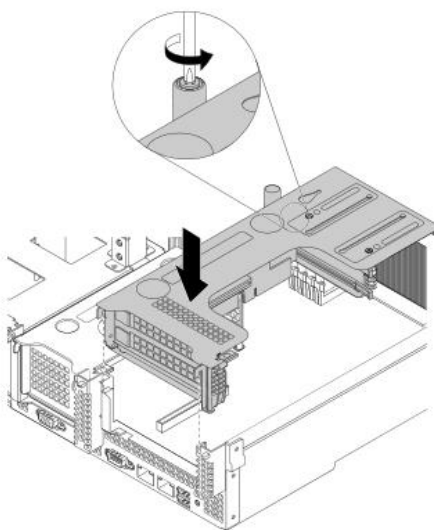




- 确认阵列卡型号。
- 拿住新阵列卡两边，插入对应插槽。
- 上螺丝固定，接口 RAID 线（此处注意 2 根线需要按原顺序插回）。
- 检测没有其它杂物遗留在机箱内，封盖还原。

### 3. 9L 开头设备

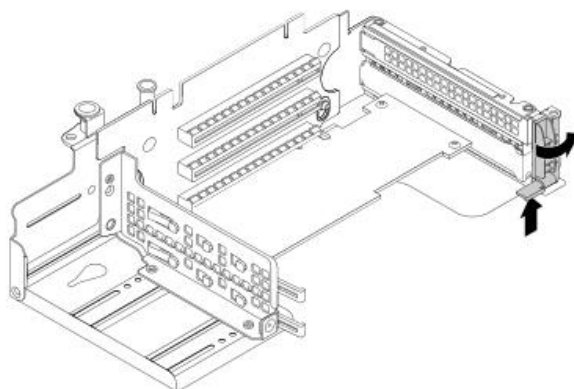
- 确认设备断电后，并拔掉该设备电源连接线，取下服务器，平放在平稳平台上，打开机箱上盖。
- 拧松固定转接卡组合件的螺钉。然后，握住组合件的边缘，然后小心地直着向上从机箱中取出整个固定架。



#### 注意:

此固定架内如有其它 PCIE 卡，请优先去掉各连接线。

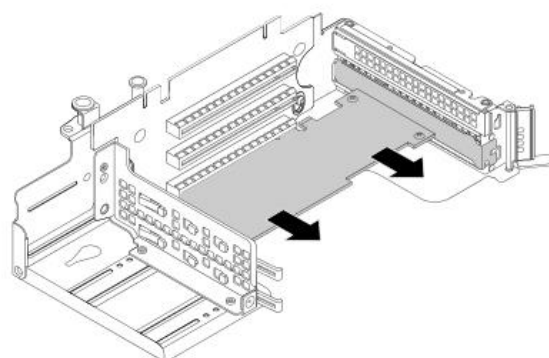
- 拔掉 2 根连接在阵列卡上的，RAID 线（按下压片，向外拔出）。
- 找到要卸下的 PCIE 卡，然后，按卡舌以将卡栓旋转至打开位置。



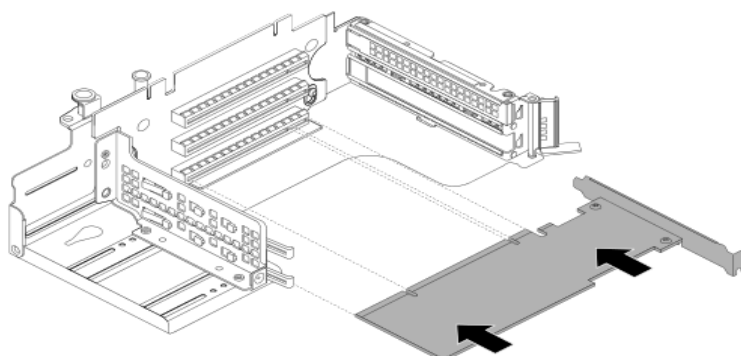
- 握住阵列卡的边缘，小心地从 PCIE 插槽中抽出它。

### ⚠ 注意:

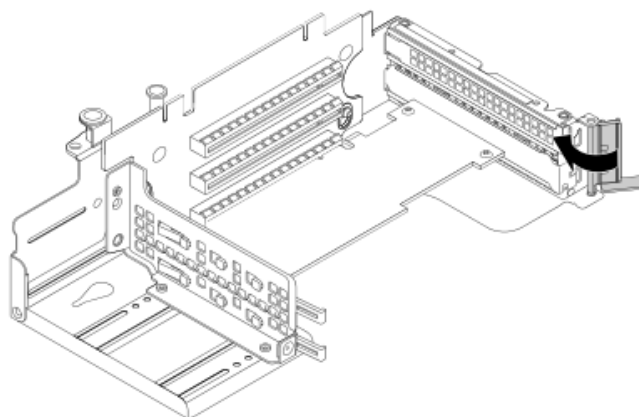
阵列卡可能紧紧地固定在 PCIE 插槽中。如有必要，请交替地少许、均匀地移动阵列卡的两侧，直至从插槽中将其卸下。也可通过固定架 2 个圆孔位置，将阵列卡向外推出。



- 确认阵列卡型号正确。
- 将阵列卡放在 PCIE 插槽附近。然后，小心地将该阵列卡直着按入插槽，直至其牢固就位，确保阵列卡支架被转接卡支架固定。



- 将卡栓旋转至闭合位置以将该阵列卡固定到位。



- 将 RAID 线接回阵列卡，注意 2 根线是有顺序的，RAID 卡上 0 口接 0-3RAID 线。1 口接 4-7RAID 线。
  - 将整个固定架，装回机箱。反方向选择固定好组件螺钉。
  - 检测没有其它杂物遗留在机箱内，封盖还原。
4. 替换后检查
- 确认 bios boot 选项中有阵列卡。
  - 确认阵列卡内硬盘识别，且模式为 JBOD 模式。
  - 进行一键检查，确认平台运行正常。

### 11.4.4.7. 电源替换

#### 功能说明

1. 当深信服一体机电源模块出现故障时，需要对电源进行替换。
2. 非深信服一体机需联系服务器厂商，由相应厂商人员操作维护，禁止深信服员工直接操作。

#### 注意事项

1. 当服务器配置双电源模块，其中一块出现故障另一块正常运行时，可以不中断业务进行替换。
2. 当服务器配置单电源模块，电源出现故障时，若主机还未断电停机，可以不中断业务进行替换；若主机已断电停机，直接操作进行替换。
3. 替换的电源模块型号与参数需与原故障电源模块保持一致。

#### 前提条件

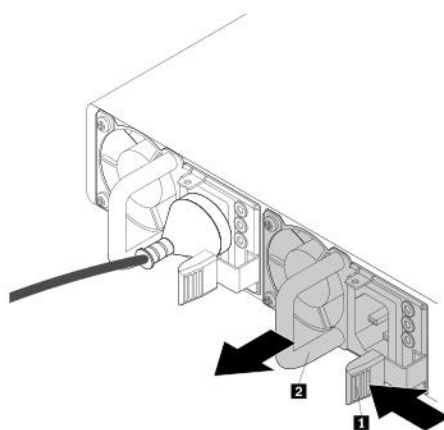
确认服务器配置单电源模块还是双电源模块，制定替换计划。

## 操作步骤

本操作步骤以服务器配置双电源模块，其中一块出现故障为例，进行替换。

当服务器配置单电源模块，电源出现故障，主机还未断电停机时，可以将该主机上的虚拟机和虚拟设备迁移至其他主机上，保证业务不中断。再进行服务器下电，进行替换电源模块。

1. 拔掉故障电源连接线，如图方向按松开卡舌，同时小心地拉动手柄，从机箱中抽出故障的电源。



2. 再次确认新电源型号与设备匹配。
3. 将新电源模块推入机箱，直至其咔嗒一声固定到位，接上电源线。
4. 替换后检测
  - 观察电源指示灯情况是否正常。
  - 观察设备上电情况是否正常，能否正常运行。
  - 进 IPMI 查看电源电压输出状态是否正常（通常在资产信息或部件信息下的电源选项里）。
  - 进行一键检测，确认平台正常运行。

## 11.5. 平台高危操作

### 11.5.1. 界面配置高危操作

#### 11.5.1.1. 更改存储通信网口

##### 功能说明

管理员需要更改在[虚拟机存储/配置/高级配置]中修改存储通信网口配置匹配新的通信方式。

### 风险说明

1. 更改存储网口通信口会导致虚拟机通信异常，业务中断等风险。
2. 目前平台已经对更改存储通信进行了限制，必须关闭所有虚拟机才能更改，防止虚拟机运行异常。

### 正确处理方式

关闭所有运行虚拟机，再更改集群存储网口。

## 11.5.1.2. 格式化集群

### 功能说明

管理员在[系统管理/系统配置备份与恢复]中恢复出厂设置。

### 风险说明

集群内包含的虚拟机、备份、虚拟网络设备等所有数据都将被格式化，恢复出厂状态。

### 正确处理方式

确认当前集群内没有可用数据，如果需要相关虚拟机，请采用导出镜像方式保存，其他操作需拨打深信服400电话技术支持。

## 11.5.1.3. 集群备份恢复

### 功能说明

管理员平台无法使用，需要在[系统管理/系统配置备份与恢复]中恢复到某个时间点的备份。

### 风险说明

恢复备份会导致从恢复时间点到目前时间点的数据丢失。

### 正确处理方式

请确认当前没有其他方式处理可以处理，保存相关数据进行备份恢复。

### 11.5.1.4. 清空回收站

#### 功能说明

在[系统管理/回收站]对平台回收站的数据进行清空。

#### 风险说明

清空回收站会导致回收站数据被清空，数据无法恢复。

#### 正确处理方式

清空回收站前确认无需要使用的数据。

### 11.5.2. 硬件高危操作

#### 11.5.2.1. 未加入超融合集群的服务器重装系统

##### 功能说明

重装未加入深信服超融合系统所在深信服一体机。

##### 风险说明

重装系统会导致丢失一体机签名，导致该服务器无法加入深信服超融合集群。

##### 正确处理方式

用户重装前后需拨打深信服400电话技术支持。

#### 11.5.2.2. 已加入超融合集群的服务器重装系统

##### 功能说明

重装已经加入深信服超融合系统所在深信服一体机或者第三方服务器。

##### 风险说明

1. 导致运行在该服务器上的虚拟机无法使用。
2. 导致丢失一体机签名，致该服务器无法加入深信服超融合集群。

##### 正确处理方式

1. 用户应避免此类操作。

2. 出现该问题后需拨打深信服400电话技术支持。

### 11.5.2.3. 变更物理网络

#### 功能说明

在业务运行过程中变更网络，如更改超融合平台使用交换机端口VLAN、IGMP snooping、MTU、STP协议；拔插服务器网线；更换服务器网卡等。

#### 风险说明

1. 可能导致业务异常甚至无法访问。
2. 存储网络变更可能导致虚拟机迁移甚至数据丢失。

#### 正确处理方式

1. 用户应避免此类操作。
2. 必须做此类操作时需拨打深信服400电话技术支持。

### 11.5.2.4. 随意拔插服务器磁盘

#### 功能说明

随意拔插已加入深信服超融合服务器的磁盘。

#### 风险说明

1. 随意拔插磁盘会导致分布式副本之间出现不一致。
2. 可能导致分布式存储数据丢失。

#### 正确处理方式

用户应禁止此类操作。

### 11.5.2.5. 格式化服务器磁盘

#### 功能说明

格式化已加入深信服超融合集群的服务器磁盘或者外置存储磁盘。

#### 风险说明

导致存储数据丢失，严重的可能导致整个平台虚拟机无法使用。

正确处理方式

用户应禁止此类操作。

11.5.2.6. iSCSI 存储重新扫描或重新发现目标

功能说明

对于正在运行的业务虚拟机，并且该虚拟机的存储位置在连接上HCI的iSCSI服务器上，在[存储/其他存储]的“iSCSI服务器连接配置”中，执行“重新扫描”或“发现目标”的操作。

风险说明

会触发iSCSI连接更新中断重连，导致正在进行的IO异常，从而影响业务系统的正常访问，导致业务中断。

正确处理方式

在执行此类操作前务必确认该iSCSI存储上的业务系统能够停机。

11.6. 通信矩阵

| 源设备   | 源端口 | 目的设备 | 目的端口        | 协议      | 端口说明                                    |
|-------|-----|------|-------------|---------|-----------------------------------------|
| 管理员终端 | any | HCI  | 80          | http    | HCI web 控制台跳转到 443 端口                   |
| 管理员终端 | any | HCI  | 443         | https   | HCI web 控制台登录端口                         |
| HCI   | any | HCI  | 4099        | UDP     | 用于发现安装了 HCI 的物理主机                       |
| HCI   | any | HCI  | 7001-7019   | TCP     | 用于集群内、跨集群虚拟机迁移；当集群被云管平台纳管后此端口将自动开启      |
| 待迁移主机 | any | HCI  | 4000-4010   | TCP/UDP | 使用 converter 或 ISO 执行 p2v 任务时，发现主机使用的端口 |
| 待迁移主机 | any | HCI  | 10809-10900 | TCP/UDP | 使用 converter 或 ISO 执行 p2v 任务时，拷贝磁盘使用的端口 |
| 管理员终端 | any | HCI  | 139,445     | TCP     | Samba 共享目录管理服务，提供文件共享功能                 |
| 第三方设备 | any | HCI  | 4433        | TCP     | 用于提供 API 接口给第三方调用（SCMT 使用此端             |



|        |     |     |      |     |                                        |
|--------|-----|-----|------|-----|----------------------------------------|
|        |     |     |      |     | 口)                                     |
| 监控管理设备 | any | HCI | 161  | UDP | 通过 <b>SNMP</b> 服务可帮助管理员了解运行时的物理资源使用情况。 |
| HCI    | any | HCI | 22   | TCP | 用于主机扩容、主机替换、巡检时连接主机                    |
| 管理员终端  | any | HCI | 4480 | TCP | 访问 NFV 设备的 web 控制台                     |

## 12. 术语表

| 名词            | 英文全称                             | 解释                                                                                                                  |
|---------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------|
| 持续数据保护        | CDP (Continuous Data Protection) | CDP 即持续数据保护，它能够记录虚拟机中业务系统对磁盘的每一个 IO，可以将虚拟机恢复到任意时刻的状态，也可以直接查看并下载某个时刻的文件，对于文件误删、病毒、系统崩溃、数据损坏等故障有十分明显的价值，做到 RPO 接近于 0。 |
| 超级管理员         | N/A                              | 超级管理员（又称 admin 用户）具有超融合平台所有权限，是整个深信服超融合资源池中权限最大的用户。                                                                 |
| 动态资源调度        | DRS                              | 动态资源调度将虚拟机从 CPU 或者内存利用率比较高的主机迁移到利用率比较低的主机上，将负载过高的主机的利用率降到阈值以下。                                                      |
| 动态资源扩展        | DRX                              | 动态资源扩展在业务高峰期间，虚拟机自动的添加 CPU 和内存的资源，以保障业务系统的正常使用。                                                                     |
| 深信服计算虚拟化组件    | aSV                              | 通过 VMM (Virtual Machine Monitor，虚拟机监视器)对 CPU、内存以及 IO 设备进行虚拟化。                                                       |
| 深信服存储虚拟化组件    | aSAN                             | 深信服自研的分布式存储系统，融合分布式缓存、SSD 缓存加速、全局应用交付以及多重数据保护等诸多存储技术，能够满足关键业务的需求，保证客户业务高效稳定运行。                                      |
| 深信服网路虚拟化组件    | aNET                             | 深信服自研的网络虚拟化层，提供所画即所得的业务逻辑呈现，支持虚拟路由器、虚拟交换机、虚拟网络安全设备的部署。                                                              |
| 深信服虚拟安全组件     | aSEC                             | 深信服虚拟安全组件包括防火墙（AF）、上网行为管理（AC）、应用交付（AD）SSL VPN 等。                                                                    |
| 深信服 SCP 云计算平台 | SCP                              | 深信服云管平台，可以纳管管理 HCI、VMware 以及其他云资源池。                                                                                 |
| 深信服超融合智能交付工具  | aDeploy                          | 深信服超融合智能交付工具，具有 HCI 及 SCP 智能巡检，网口乱序调整，序列号收集，兼容性列表查询等功能，是深信服云计算项目交付必不可少的工具。                                          |
| 深信服一体机        | aServer                          | 深信服一体机，深信服自己的服务器，出产已内置超融合软件，部署快捷，兼容性好。                                                                              |

|         |                |                                                                                                                                                                                      |
|---------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HA      | High Available | 高可用性集群，通常需要两个或者两个以上的主机节点组成集群，当启用了 HA 功能的虚拟机所在节点发生意外（主机掉电、断网等）时，集群心跳机制侦测到后，将选择一台资源充足的节点自动重启该虚拟机，从而实现业务的不中断或短暂中断。深信服超融合提供高可用的主机服务，当发现异常并持续时长达到客户设置的故障检测敏感度时（比如 5 分钟），切换 HA 虚拟机到其他主机运行。 |
| 回收站     | N/A            | 用于临时存放删除的虚拟机、网络设备、虚拟共享盘资源，可以对存放的资源进行回收和还原。                                                                                                                                           |
| 虚拟网络设备  | NFV            | NFV 是指虚拟网络设备，例如：vSSL、vAC、vAF、vAD 等。                                                                                                                                                  |
| 克隆      | N/A            | 通过克隆的操作生成一个完全相同的虚拟机，提高业务部署效率。                                                                                                                                                        |
| 快照      | N/A            | 数据存储的某一时刻的状态记录，深信服超融合通过对 qcow2 打快照，将快照时刻 qcow2 的状态记录下来，即当时 qcow2 文件所描述的数据位置。可以通过该时刻快照进行虚拟机的数据恢复。                                                                                     |
| 模板派生    | N/A            | 以当前某个虚拟机为主体，将其转换为模板（关机和锁定状态）进而派生出 N 个与当前模板状态一致的虚拟机，派生虚拟机的镜像文件引用模板镜像文件以及自己的增量镜像，并且可以配置数据盘。                                                                                            |
| 异构虚拟化管理 | aHM            | HCI 可添加 VMware vCenter 并对其进行纳管，实现双平台的集中管理。VMware vCenter 和 HCI 之间的虚拟机可以实现支持双向迁移。                                                                                                     |



## 13. 缩略语

|            | 英文全称                                     | 中文全称              |
|------------|------------------------------------------|-------------------|
| aXXX       | Advanced XXX                             | 深信服云计算授权命名方式      |
| ACL        | Access Control Lists                     | 访问控制列表            |
| aDeploy    | Deploy                                   | 深信服超融合智能交付工具      |
| aNET       | Network                                  | 深信服虚拟网络           |
| aSAN       | Storage Area Network                     | 深信服虚拟存储（虚拟存储区域网络） |
| aSEC       | Security                                 | 深信服虚拟安全组件         |
| aServer    | Server                                   | 深信服一体机            |
| aSV        | Server Virtualization                    | 深信服虚拟服务器          |
| ATS        | Atomic Test and Set                      | 一种硬件辅助的锁定机制       |
| BIOS       | Basic Input Output System                | 基本输入输出系统          |
| BMC        | Baseboard Manager Controller             | 基板管理控制器           |
| CDP        | Continuous Data Protection               | 持续数据保护            |
| COW        | Copy On Write                            | 写时复制              |
| DHCP       | Dynamic Host Configuration Protocol      | 动态主机配置协议          |
| DNS        | Domain Name System                       | 域名系统              |
| DRS        | Dynamic Resource Scheduling              | 动态资源调度            |
| DRX        | Dynamic Resource eXtension               | 动态资源扩展            |
| DWPD       | Drive Writes Per Day                     | 每日全盘写入次数          |
| FC         | Fibre Channel                            | 网状通道协议            |
| Google OTP | Google One Time Password                 | 谷歌一次性密码           |
| GPT        | GUID Partition Table                     | 磁盘类型的一种           |
| GUI        | Graphical User Interface                 | 图形用户界面            |
| HA         | High Available                           | 高可用               |
| HBA        | Host Bus Adapter                         | 主机总线适配器           |
| HCI        | Hyper-Converged Infrastructure           | 超融合基础设施           |
| iDRAC      | Integrated Dell Remote Access Controller | 集成戴尔远程控制卡         |

|        |                                           |                   |
|--------|-------------------------------------------|-------------------|
| IOMMU  | Input/Output Memory Management Unit       | 内存管理单元            |
| IOPS   | Input/Output per second                   | 每秒读写速率            |
| IPMI   | Intelligent Platform Management Interface | 智能平台管理接口          |
| IPSAN  | Internet Protocol Storage Area Network    | 基于IP协议的存储区域网络     |
| IQN    | iSCSI Qualified Name                      | iSCSI存储的识别码       |
| iSCSI  | internet Small Computer System Interface  | Internet小型计算机系统接口 |
| JBOD   | Just a Bunch Of Disks                     | 磁盘簇               |
| LVM    | Logical Volume Manager                    | 逻辑卷管理             |
| LUN    | Logical Unit Number                       | 逻辑单元号             |
| MBR    | Master Boot Record                        | 主引导记录             |
| M-LAG  | Multichassis Link Aggregation Group       | 跨交换机链路聚合          |
| MTU    | Maximum Transmission Unit                 | 最大传输单元            |
| NAT    | Network Address Translation               | 网络地址转换            |
| NFS    | Network File System                       | 网络文件系统            |
| NFV    | Network Functions Virtualization          | 网络功能虚拟化           |
| NM     | N/A                                       | 希捷NM企业级硬盘         |
| NTFS   | New Technology File System                | windows的一种文件系统    |
| NTP    | Network Time Protocol                     | 网络时间协议            |
| NUMA   | Non-Uniform Memory Access                 | 非一致性内存访问          |
| OTP    | One Time Password                         | 一次性密码             |
| PCIe   | Peripheral Component Interconnect Express | 高速串行计算机扩展总线标准     |
| PVID   | Port-base VLAN ID                         | 端口的缺省VLAN ID      |
| RAID   | Redundant Arrays of Independent Disks     | 独立硬盘冗余阵列          |
| ROW    | Redirect On Write                         | 写时重定向             |
| RPO    | Recovery Point Objective                  | 恢复点目标             |
| RTO    | Recovery Time Objective                   | 恢复时间目标            |
| SCP    | Sangfor Cloud Platform                    | 深信服云计算平台          |
| SR-IOV | Single Root I/O Virtualization            | 一种设备接口虚拟化技术       |

|          |                                                         |                   |
|----------|---------------------------------------------------------|-------------------|
| STP      | Spanning Tree Protocol                                  | 生成树协议             |
| TPM      | Trust Platform Module                                   | 数据库的可信平台模块        |
| UEFI     | Unified Extensible Firmware Interface                   | 统一可扩展固件接口         |
| UPS      | Uninterruptible Power System                            | 不间断电源             |
| URL      | Uniform Resource Locator                                | 统一资源定位符           |
| UUID     | Universally Unique Identifier                           | 通用唯一识别码           |
| VAAI     | The vStorage API for Array Integration                  | 阵列集成存储API         |
| vAC      | Virtual Access Control                                  | 深信服虚拟上网行为管理       |
| vAD      | Virtual Application Delivery                            | 深信服虚拟应用负载均衡       |
| vAF      | Virtual Next General Application Firewall               | 深信服虚拟下一代防火墙       |
| vCS      | Virtual Compute Server                                  | 英伟达的一种vGPU授权      |
| vDAS     | Virtual Database audit system                           | 深信服虚拟数据库审计系统      |
| vDWS     | Virtual Data Warehouse Service                          | 深信服虚拟数据仓库服务       |
| VMM      | Virtual Machine Monitor                                 | 虚拟机监视器            |
| VMX      | Virtual Machine Extension                               | Intel CPU支持虚拟化的技术 |
| vSSL     | Virtual Secure Sockets Layer                            | 深信服虚拟SSL          |
| vSSL VPN | Virtual Secure Sockets Layer<br>Virtual Private Network | 深信服虚拟SSL VPN      |
| VT-x     | Virtualization Technology - x                           | Intel CPU支持虚拟化的技术 |
| vWOC     | Virtual WAN Optimization Controller                     | 深信服虚拟广域网优化控制器     |
| VXLAN    | Virtual eXtensible Local Area Network                   | 虚拟扩展局域网           |