**HEDU智能协作系统**

——安全白皮书

**2020年10月**

**青岛华师智慧科技有限公司**

**目 录**

[第 1 章 概况 5](#_Toc54891100)

[第 2 章 安全责任共担 6](#_Toc54891101)

[2.1 华师安全责任 6](#_Toc54891102)

[2.2 天翼云安全责任 7](#_Toc54891103)

[第 3 章 HEDU智能协作系统安全 8](#_Toc54891104)

[3.1 个人信息保护 8](#_Toc54891105)

[3.2 基础架构 8](#_Toc54891106)

[3.3 客户端安全 8](#_Toc54891107)

[3.4 会议安全 9](#_Toc54891108)

[3.5 管理控制 9](#_Toc54891109)

[3.6 特殊的安全特性/API 10](#_Toc54891110)

[第 4 章 HEDU智能协作系统基础设施 11](#_Toc54891111)

[第 5 章 云安全架构 12](#_Toc54891112)

[5.1 数据存储的持久性 12](#_Toc54891113)

[5.2 数据可销毁性 12](#_Toc54891114)

[5.3 数据可迁移性 13](#_Toc54891115)

[5.4 数据私密性 16](#_Toc54891116)

[5.5 数据知情权 17](#_Toc54891117)

[5.6 服务可审查性 17](#_Toc54891118)

[5.7 服务功能 17](#_Toc54891119)

[5.8 服务的可用性 18](#_Toc54891120)

[5.9 服务资源调度能力 20](#_Toc54891121)

[5.10 故障恢复能力 21](#_Toc54891122)

[5.11 网络接入性能 22](#_Toc54891123)

[5.12 服务计量准确性 22](#_Toc54891124)

[5.13 服务安全性 22](#_Toc54891125)

[5.13.1 身份认证 22](#_Toc54891126)

[5.13.2 用户授权 22](#_Toc54891127)

[5.13.3 密码管理 23](#_Toc54891128)

[5.13.4 软件代码漏洞 23](#_Toc54891129)

[5.13.5 数据传输加密 23](#_Toc54891130)

[5.13.6 数据存储加密 23](#_Toc54891131)

[5.13.7 数据备份 24](#_Toc54891132)

[5.13.8 数据删除保护 24](#_Toc54891133)

**文 档 信 息**

|  |  |
| --- | --- |
| **文档名称** | **HEDU智能协作系统安全白皮书** |
| **文档编号** |  |
| **文档类别** | 技术文档 ■ 服务文档 □ 其他 □ |
| **当前版本** | 1.0 |
| **创建日期** | 2020-10 |
| **文档作者** | 刘兴华 |
| **联系方式** | Liuxh@hsjc.com.cn |

# 概况

HEDU智能协作系统数据安全和用户隐私是华师最重要的原则。华师致力于打造公共、开放、安全的智能协作平台。HEDU视频会议，在线会议，群消息，在一个易于使用的平台上提供软件定义会议解决方案。HEDU智能协作系统可以在Windows、Mac、iOS、Android终端上提供最佳的视频、音频、无线分享自己电脑桌面。

HEDU智能协作系统在公有云部署当中，始终将安全性放在最高优先级。HEDU智能协作系统致力于不断提供健壮的安全特性来满足企业的安全合作需求。

而天翼云作为HEDU智能协作系统基础架构；竭诚为HEDU智能协作系统提供稳定、可靠、安全、合规的云计算基础服务，保护系统及数据的机密性、完整性、和可用性。

# 安全责任共担

基于天翼云的HEDU智能协作系统，其安全责任由双方共同承担:天翼云要保障云平台自身安全并提供安全产品和能力给云上HEDU智能协作系统;华师负责基于天翼云服务构建的应用系统的安全。

天翼云负责基础设施(包括跨地域、多可用区部署的数据中心，以及天翼云骨干传输网络)和物理设备(包括计算、存储和网络设备)的物理和硬件安全，并负责运行分布式云操作系统之上的虚拟化层和云产品层的安全。同时，天翼云负责平台侧的身份管理和访问控制、 监控和运营，从而为客户提供高可用和高安全的云服务平台。

HEDU智能协作系统负责以安全的方式配置和使用各种云上产品，并基于这些云产品的安全能力以安全可控的方式构建自己的云上应用和业务，保障云上安全。天翼云基于电信多年攻防技术 积累，为客户提供云安全服务，保护客户的云上业务和应用系统。天翼云建议客户选择使用云安全服务的安全产品为其云上应用和业务系统提供全面的安全防护。

安全责任共担模式之下，天翼云保障云平台层面的安全并提供一方集成的云产品安全能力

给客户使用，让客户降低对安全性的顾虑，更专注于核心业务发展。

## 华师安全责任

华师基于天翼云提供的服务构建自己的云端应用系统，综合运用天翼云产品的安全功能、 云安全服务以及安全生态提供的第三方安全产品保护自己的业务系统。

华师应对云上产品进行安全配置管理，保障云上业务的基础安全和数据安全。请注意，华师在天翼云上如果使用的是基础类服务(例如，天翼云提供的云主机(ECS))，那么相关服务实例完全由华师控制，华师对管理实例进行了安全配置，并应加固租用的云服务器操作系统、升级补丁、配置安全组防火墙进行网络访问控制。

华师使用天翼云产品的原生加密能力或云加密服务对敏感数据进行加密，并对加密密钥进行妥善管理。

华师天翼云上的应用和业务系统已通过使用云安全服务以及安全生态提供的第三方安全产品来保护。并使用云安全服务对云上应用和业务系统，包括云上资源进行有效的安全监控和运营。在账户安全层面，华师保护天翼云账户认证凭证，并在账号设置上遵循最小权限原则，通过如群组授权等手段实现职责分离。

## 天翼云安全责任

天翼云负责基础设施、物理设备、分布式云操作系统及云服务产品安全，并为HEDU智能协作系统提供保护云端应用及数据的技术手段。

天翼云保障云平台自身安全，包括但不限于:

⚫  保障云数据中心物理安全。

⚫  保障云平台硬件、软件和网络安全，包括操作系统及数据库的补丁管理、网络访问控制、DDoS 防护、灾难恢复等。

⚫  及时发现云平台的安全漏洞并修复，修复漏洞过程不影响HEDU智能协作系统业务可用性。

⚫  通过与外部第三方独立安全监管与审计机构合作，对天翼云进行安全合规与审计评估。

天翼云为HEDU智能协作系统提供保护云端信息系统的技术手段，包括但不限于:

⚫  提供多地域、多可用区分布的云数据中心以及多线 BGP 接入网络，利用天翼云基础设施构建跨机房高可用的云端应用。

⚫  提供安全的硬件基础设施和设备。

⚫  提供云上账户安全管理能力，包括但不限于云账号支持主子账号、多因素认证、

分组授权、细粒度授权、临时授权等账户安全管控手段。

⚫  提供安全监控和运营能力，包括安全审计手段。

⚫  提供数据加密手段。

⚫ 提供各类安全服务。

# HEDU智能协作系统安全

## 个人信息保护

长期以来，华师坚持致力于保护每位用户的个人信息，保证用户对所有提供给HEDU智能协作系统的个人信息拥有所有权和控制权。与此同时，华师积极响应国家监管部门对企业承担个人信息保护责任的号召，持续完善内部的个人信息管理和保护体系。华师设置了专业的个人信息保护团队，在隐私权政策、用户权利保障等方面持续优化，建立了内部整体的数据安全管理体系， 落地数据安全保护的核心技术，为用户个人信息提供了全生命周期的安全可靠的保护能力。

华师将持续建设个人信息保护管理体系，除了关注华师作为控制者角色时云平台自身的个人信息保护能力之外，会进一步投入力量建设作为数据处理者的角色时个人信息保护能力。

HEDU智能协作系统的隐私权政策可以在HEDU官网查看，有任何隐私相关的问题都可以通过邮件support@hsedugroup.com或电话客服进行反馈。

## 基础架构

HEDU智能协作系统是一个专有的网络,提供高质量沟通体验。HEDU智能协作系统实时媒体服务器放置于天翼云。

在HEDU智能协作系统基础设施拥有一套低延迟的分布式网络多媒体路由器(软件)。使用这些低延迟多媒体路由器，所有来自主机设备和到达参与者设备的会话动态切换。

客户端与云端服务器通过https（443端口/TLS）建立连接。

## 客户端安全

基于角色的用户安全（端到端加密）；

* 开启端到端加密会议
* 使用标准的用户名和密码或SAML单点登录
* 密码保护的会议
* 可预约一场密码保护的会议

有选择性邀请参会者；

会议详细信息存储在HEDU智能协作系统安全数据库；

高级加密标准（AES256）位算法加密所有的演讲内容；

使用加密标准（AES256）位加密聊天会话；

## 会议安全

* 基于角色的用户安全；

会议主持人拥有以下安全功能：

* 驱逐一个参与者或所有参与者
* 结束一场会议
* 锁定一场会议
* 与参与者或所有参与者聊天
* 静音/不静音一个参与者或所有参与者
* 启用/禁用一个参与者或所有参与者记录
* 当打开一个新窗口，临时暂停分享电脑屏幕

会议的参与者拥有以下安全功能：

* 静音/不静音
* 开/关视频
* 开放或拥有密码的会议；
* 编辑或删除会议；
* 会议中的安全；

使用AES256加密标准加密所有屏幕共享内容

使用256位TLS加密标准加密网络连接

* 客户端和会议服务器使用256位传输层TLS加密隧道

## 管理控制

以下是提供给管理员的安全功能：

-安全使用标准的用户名和密码登录选项或SAML单点登录。

-添加用户和管理员账户

-用户订阅级别升级或降级

-删除用户账户

-审查报告

## 特殊的安全特性/API

* 会议服务器

会议服务器位于中国境内云端，服务器不记录、不向其他目标位置转发任何会议信息。

* 网络研讨会

可以使用HEDU智能协作系统召开500人的高清视频会议

记录存储

HEDU智能协作系统为我们客户提供记录和分享他们的会议。录音可以存储在本地。

* HEDU智能协作系统只有存储基本信息

。

# HEDU智能协作系统基础设施

HEDU智能协作系统是基于天翼云云主机方式部署;采用多线 BGP 网络提高网络访问体验;分布式云操作系统为所有云产品提供高可用基础架构和多副本数据冗余;全球领先的热升级技术使得产品升级、漏洞修复都不会影响客户业务;高度自动化的运维及安全，相关权威机构的认可的合规性;高可用、安全、可信的云计算基础设施。

# 云安全架构

## 数据存储的持久性

除天翼云提供的数据存储持久性保障外，HEDU智能协作系统还制定了合理的数据备份策略定期备份、虚拟机快照等方式提高数据存储持久性。

合同期内每月云主机和块存储的用户应用和用户的内容文件持久性为99.99%，意为每月用户10000个存储的文件，合同期内每月数据不丢失的概率为99.99%，即每月只有1个文件丢失的可能性。

## 数据可销毁性

**安全擦除**

HEDU智能协作系统建立了对设备全生命周期(包含接收、保存、安置、维护、转移以及重用或报废)的安全管理。设备的访问控制和运行状况监控有着严格管理，并定期进行设备维护和盘点。建立废弃介质上数据安全擦除流程，处置数据资产前，检查含有敏感数据和正版授权软件的媒介是否已被覆写、消磁或折弯等数据清除处理，且不能被取证工具恢复。当因业务或法律原因，不再需要某些硬拷贝材料时，将其物理破坏，或取得数据处理第三方的损坏证明，以确保数据无法重建。

**云服务数据处置**

华师在终止为云服务客户提供服务时，及时删除云服务客户数据资产或根据相关协议要求返还其数据资产。基于天翼云数据清除技术满足行业标准，清除操作留有完整记录，确保数据不被未授权访问。

运维人员未经客户许可，不得以任意方式访问客户未经公开的数据内容。遵循生产数据不出生产集群的原则，从技术上控制了生产数据流出生产集群的通道，防止运维人员从生产系统拷贝数据。

**设备报废方法**

第一，数据质量远比数据的数量重要，要注重有效数据的处理。所以任由数据量增长下去，数据中心会很快不断扩容，结果数据中心的规模越来越大，而数据中心业务并没有实质增长。数据切不可成为数据中心的负担，该清理时就清理，该销毁时就销毁。

第二，我们对数据进行销毁，这就要从数据产生的源头做起。管理这些数据是非常复杂的，涉及到数据辨识、清理、优化等等，而这些工作又是周期性，需要花费时间和一定的人力资源，且不会带来明显的收益，常常被忽视。其实，数据的有效存储工作将对数据中心的业务产生长期和正面的收益，且越早行动收益越明显。

第三，数据的销毁并不是简单的删除清空这样简单，销毁的手段也有几种，分为软销毁和硬销毁两种。软销毁是通过数据覆盖等软件方法数据销毁或者数据擦除。硬盘数据销毁中的硬销毁则通过采用物理、化学方法直接销毁存储介质，以达到彻底的硬盘数据销毁的目的。软销毁一般只是将数据文件进行销毁，并不能真正将磁盘区数据擦除，操作系统由于考虑到操作者操作习惯或者误操作，数据销毁后各种非常情况等诸多方面因素，用户所使用的删除命令，只是将文件目录项做一个删除标记，把它们在文件分配表中所占用的簇标记为空簇，并没有对数据区进行任何改变也就是没有对这些信息做任何数据擦除、数据销毁的操作，这样数据其实依然占用存储空间，没有达到节省存储空间的目的。所以数据中心的数据销毁都采用硬销毁的方式，真正将存储空间释放出来，用来存放更有意义的数据。硬销毁常用的方法有：格式化硬盘、硬盘分区、文件粉碎软件。还有一种硬销毁是采用专用的消磁硬盘机或者折弯机来彻底销毁数据，不管是直接对硬盘进行消磁，还是对硬盘进行折弯，都是破坏性的行为，硬盘将被损坏，不仅数据不能再还原，硬盘也无法再进行使用，这种硬销毁往往是用来对已经故障的硬盘进行处理，避免故障硬盘里存着的数据被外人还原出来，拿着数据去做坏事。

及时对数据中心中的无用数据进行销毁，不仅可以节省硬盘存储空间，还可以提升安全性，避免一些数据泄露，给数据中心带来安全隐患。所以对于无用数据要进行彻底销毁，不让任何人有可乘之机，更不能让人有机会再还原出来利用。

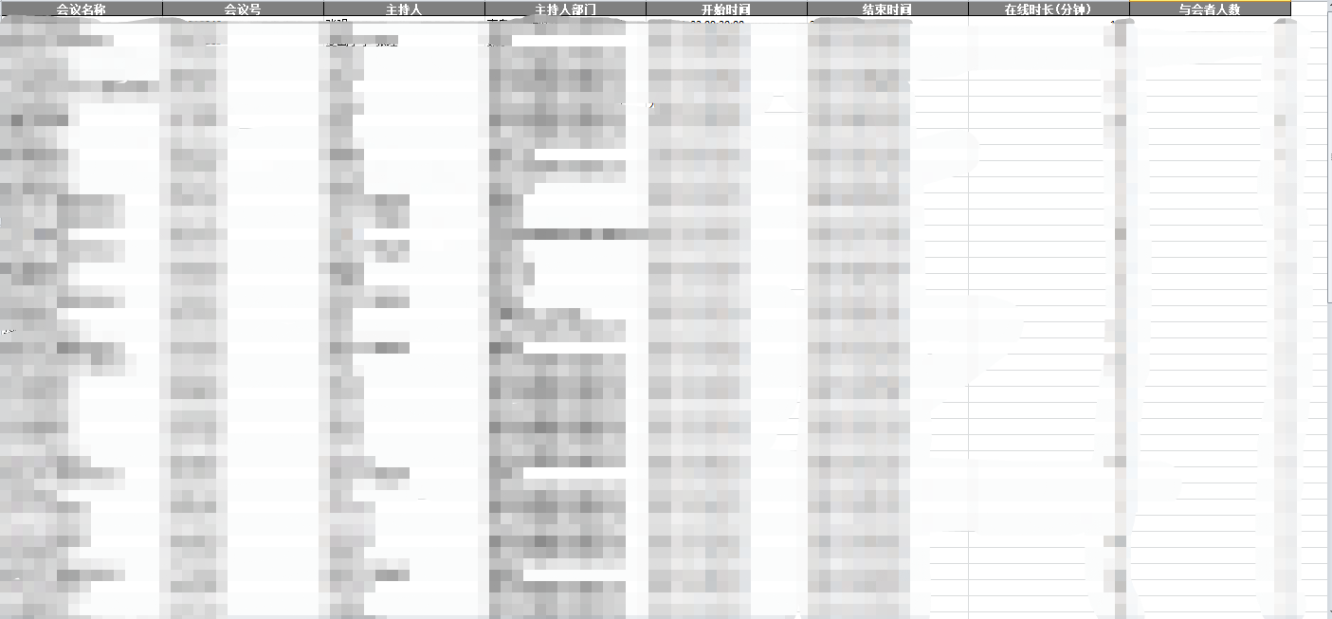
在用户要求删除数据或设备在弃置、转售前服务商将采取高级清零操作彻底删除用户所有数据，并无法复原，硬盘报废时将消磁。

## 数据可迁移性

HEDU智能协作系统基于天翼云主机搭建的软件应用，不管从软件层面或者是硬件层面，都能保证启用或弃用该云服务时，数据能迁入和迁出。

用户数据以报表的形式在管理后台呈现，同时支持数据以Excel表格的形式导入导出，

且HEDU在预约会议时支持所有格式的文件上传，预约完成后可以在会议信息中下载已上传的文件。



另外,天翼云云主机、云数据库产品和服务获得可信云服务认证，对数据可销毁性、数据可迁移性、数据私密性、 数据知情权等进行了规范。

天翼云主机承诺用户能够控制数据的迁移，保证启用或弃用云服务时，数据能迁入和迁出。

## 数据私密性

HEDU智能协作系统使用加密和安全组隔离等手段保证同一会议资源池用户数据互不可见，其中安全组通过一系列数据链路层、网络层访问控制技术实现对不同用户会议资源的隔离。用户会议媒体流通过SSL协议加密传输，保证媒体流在互联网上传输的安全性。

另外，HEDU智能协作系统基于天翼云主机搭建的软件应用，天翼云云主机、云数据库、内容分发等多款产品和服务获得可信云服务认证，对数据可销毁性、数据可迁移性、数据私密性、 数据知情权等进行了规范。

云主机隔离

天翼云主机底层使用KVM、xenServer提供虚拟化服务，每一台云主机之间相互独立，无法通过系统层面相互访问，实现了云主机之间的隔离。

磁盘隔离

天翼云主机系统采用块存储方式，用户数据以虚拟磁盘文件的格式存储于底层存储介质上。不同虚拟磁盘文件各自独立，无法相互访问数据，实现了磁盘隔离。

## 数据知情权

HEDU智能协作系统基于天翼云主机搭建的软件应用,部署于天翼云青岛-青岛节点，中心机房地址位于：山东省青岛市城阳区锦汇路蓝湾创业园电信E3机楼。天翼云云主机、对象存储、云数据库、内容分发等多款产品和服务获得可信云服务认证，对数据可销毁性、数据可迁移性、数据私密性、数据知情权等进行了规范。

## 服务可审查性

HEUD智能协助系统承诺用户在必要的条件下，由于合规或是安全取证调查等原因，可以提供相关的信息。

**数据可审查性的条件**

对于面向政府的用户，应遵守国家相应的法律法规，配合政府监管部门的监管审查。

对于普通的个人用户，应遵守国家相应的法律法规，配合政府公安部门的监管审查。

**提供的相关信息**

提供的相关信息包括：关键组件的运行日志、运维人员的操作记录。

## 服务功能

华师承诺用户提供如下功能：

* 会议前基本功能

固定ID修改

安排会议

设置主持人入会前，参会者可提前入会

* 会议中基本功能

主持人清除并将所有注释

会议通知（邮件、链接、QQ、微信）

本地录制

远程控制

会议中聊天、保存记录

一键静音

共享屏幕

多人屏幕共享

主持人控制

举手功能

分组讨论

在等候室允许所有参会者进入

会议中文件传输

* IM收发消息

单聊发送/接收文本、消息；

* 音视频会议-分别用音频、视频测试会议

具体操作说明-参考HEDU智能协作系统操作手册

## 服务的可用性

华师承诺用户服务可用性：不低于99.968%。计算方式如下：

|  |  |  |
| --- | --- | --- |
| **服务可用性计算方法**  **参评单位：青岛华师智慧科技有限公司 参评服务名称：HEDU智能协作系统** | | |
| **一、服务可用性计算方法**  服务可用性 = 机房可用性 \* 服务器可用性 \* 网络可用性 \* 软件可用性 | | |
| 1.1  机房可用性=机房级别 | **机房级别[T# 或 #星]：五星** | |
| 机房物理位置及具体名称：山东省青岛市城阳区锦汇路蓝湾创业园电信E3机楼 | |
| 机房类型 [运营商或第三方]：第三方 | |
| 机房类别 [自建或租用]：租用 | |
| 环境要求 | 主机房温度：22℃ |
| 主机房相对湿度：45%-55% |
| 建筑结构 | 抗震设防分类：八级防震抗震标准 |
| 屋面防水等级：1级 |
| 耐火等级：1级 |
| 空调 | 机房专用空调冗余：模块n+1 |
| 电力 | 供电公司承诺可用性： |
| 供电电源：双路一类市电 |
| 变压器冗余：2N |
| 后备柴油发电机系统：三菱 |
| 柴油发电机燃料储备量：12小时 |
| 不间断电源系统配置：2N |
| 不间断电源系统电池备用时间：30分钟 |
| 市电供电条件： 一类 |
| 消防 | 报警系统：烟温感 |
| 灭火系统：七氟丙烷 |
| 监控 | 巡检机制：一次/三小时 |
| 人员监控：门禁、人脸、摄像头 |
| 设备监控：网络监控系统、机房24小时人员值守 |
| 人员 | 人员素质：大学本科 |
| 换班机制：8人轮班，7\*24小时 |
| 1.2  服务器可用性=1-单台服务器故障率（冗余备份） | 服务器型号：华为 2288H V5 | |
| 供应商承诺单台服务器可用性：99.99% | |
| 实际运行单台服务器可用性：99.95% | |
| 系统架构说明：  云服务系统采用典型的二层组网方式，服务器通过接入交换机直连核心交换机，层级架构简单方案成熟，可靠性高。公网业务通过防火墙过滤和负载均衡分流到前端服务器集群，前端服务器调用后端存储集群服务器提供存储能力。存储采用服务器分布式存储系统分散所有单点故障风险。 | |
| 1.3  网络可用性 = 外网可用性\*(1-单台交换机故障率（冗余备份）) | 外网可用性：100% | |
| 交换机型号：接入交换机 CE6851  核心交换机 S6730S-H24X6C-A  防火墙 USG6530 | |
| 供应商承诺单台交换机可用性：  核心交换机 99.99%  接入交换机 99.99%  防护墙 99.9% | |
| 实际运行单台交换机可用性：  BGP故障业务故障响应5分钟，一年可用性=525595/525600=99.999%  系统bug响应15分钟，一年可用性=525585/525600=99.997%  网络可用性=99.999%\*（1-99.997%²）=99.998999% | |
| 网络架构说明：  IDC机房物理链路对于每一个外边接入点均采用双路双上联，并拥有两个以上地域分散链路独立部署的接入点、接入网络层与核心网络层采用交换机双机冗余、采用双机热备故障自动切换的运行模式。 | |
|  | 网络安全：防病毒软件、堡垒机、防DDOS攻击 | |
| 1.4  软件可用性 =  虚拟化软件可用性 \* 虚拟化管理软件可用性 \* 集群软件可用性 | 软件清单：centos7.6，docker，PostgreSQL，nginx，redis | |
| 软件故障率：0.011% | |
| **服务可用性计算过程** | 服务可用性 = 机房可用性 \* 服务器可用性 \* 网络可用性 \* 软件可用性  服务可用性 = 99.99% \*99.99% \* 99.998999%\* 99.989%=99.968% | |

## 服务资源调度能力

华师承诺用户，可以满足业务资料的30%的并发容量，24小时完成；100%的并发扩容需要2天；每次最大可扩容100%容量，最小100方并发参会者容量。

另外天翼云对云资源也有相关规范：天翼云主机向用户提供按需的资源弹性扩展，包括计算资源（vCPU和内存）的弹性扩展和弹性缩减，存储资源（含系统存储和额外存储）的弹性扩充，以及网络资源（含IP和带宽）的弹性扩充和缩减。

1. **高扩展性**
2. 计算资源扩展

天翼云主机可以根据客户实际使用需求，对已开通计算资源进行弹性扩展和弹性缩减，调整vCPU和内存的大小，从而实现计算资源的扩展。

1. 存储资源扩展

天翼云主机可以根据客户实际使用需求，添加或卸载块存储，从而实现存储资源的扩展。

1. 网络资源扩展

天翼云主机可以根据客户实际使用需求，增加或退订IP，扩大或缩减带宽，从而实现网络资源的扩展。

1. **可扩展资源**

vCPU：单位：个，可满足以最小单位1个进行扩展。需要重新启动云主机，在10分钟内完成扩展。

内存：G，可满足以最小单位1G进行扩展。需要重新启动云主机，在10分钟内完成扩展。

存储：G，可满足以最小单位10G进行扩展。可以通过自服务门户订购块存储，并挂载到云主机。实现实时动态扩展。

IP：个，可满足以最小单位1个进行扩展。可以通过自服务门户订购IP，并映射到云主机。实现实时动态扩展。

带宽：Mbps，可满足以最小单位1Mbps进行扩展。可以通过自服务门户变更带宽。实现实时动态扩展。

## 故障恢复能力

HEDU智能协作系统运营中心提供7×24小时的运行维护，并以在线申请和电话报障等方式提供技术支持，服务方式通过邮件、电话、远程或现场进行故障处理；具备完善的故障监控、自动告警、快速定位、快速恢复等一系列故障应急响应机制。

|  |  |  |  |
| --- | --- | --- | --- |
| **要求** | **说明** | **服务指标** | **备注** |
| 一级故障 | 客户虚拟会议室发生中断，所有会议软硬件终端无法注册登录。 | 实时响应，故障恢复时限2小时。 | 优先级：高 |
| 二级故障 | 客户虚拟会议室视频质量有所降低，但是不影响正常的视频会议。 | 实时响应，故障恢复时限4小时。 | 优先级：高 |
| 三级故障 | 客户的个别视频终端质量差或无法正常注册使用。 | 实时响应，故障恢复时限24小时。 | 优先级：中 |
| 四级故障 | 客户需要关于云服务的功能介绍、终端配置修改咨询、会管操作培训或者其他帮助。云服务业务根本不受影响。 | 实时响应，故障恢复时限48小时。 | 优先级：低 |

天翼云主机承诺用户，系统的可用性为99.95%，若出现故障，天翼云主机会立即采取行动，及时进行故障恢复。

1. **故障监控系统**
2. 监控平台部署情况

统一监控平台，对主机、网络等进行监控，发现故障立即报警。

监控工具对云主机服务进行监控，发现故障立即报警。

1. 监控岗位配置

* 一线现场值班人员
* 二线云主机平台监控人员
* 三线云主机后台支持人员

1. **故障发现及处理流程**

自发现故障：故障发生后5秒内会通过邮件、短信方式告知一线现场值班人员和云主机平台监控人员，1分钟中判断是主机网络类故障还是云主机平台故障；主机网络类故障交由运营部处理，云主机平台故障交由云主机平台人员处理，故障处理时间要求在5分钟内；5分钟内处理不了，要求云主机后台人员加入处理。

客户发现故障：一线现场值班人员接到客户故障报告后，5秒内定位故障并通知云主机平台监控人员，1分钟中判断是主机网络类故障还是云主机平台故障；主机网络类故障交由运营部处理，云主机平台故障交由云主机平台人员处理，故障处理时间要求在5分钟内；5分钟内处理不了，要求云主机后台人员加入处理。

## 网络接入性能

HEDU智能协作系统目前使用的是天翼云的的共享带宽包的方式，可根据业务的情况动态扩容；目前HEDU智能协作系统出口总计使用带宽是10Gbps左右。

## 服务计量准确性

线下付费方式，主要是根据用户沟通的会议并发方式100方、300方、500方视频会议来计算费用，按年计费 。

## 服务安全性

### **身份认证**

身份认证是指通过凭证信息认证用户的真实身份。它通常是指通过登录密码或访问密钥来进行认证。请注意，用于身份认证的凭证信息对于用户来讲是秘密 信息，用户必须妥善保护好身份凭证信息的安全。

系统后台支持设置多种认证方式，分别有：默认账号密码、LDAP、CAS、OAUTH2、SAML等认证方式。

### **用户授权**

系统提供了多种权限分配方式，用来帮助用户在各种情况下授权资源的使用权力，并可以根据最小权限原则为不同用户分配最小的工作权限，从而降低用户的信息安全管理风险。

### **密码管理**

HEDU智能协作系统遵循一人一账号原则，每个账号都有明确的持有者，同时，支持账号密码登录、单点登录等多种认证登录方式，会议中**可对会议进行加锁、设置密码方式来确保与会人员的信息安全。**

### **软件代码漏洞**

通过在服务器端安装轻量级的代理进行安全检测和防护，监测数据由天翼云专业安全团队以报告的形式定期发送给客户，避免入侵等高危情况进行实时邮件通知，从而客户可以及时全面的了解服务器的安全状态，将安全从传统的安全事件防护变成一项持续的安全响应和处理过程。功能涵盖弱口令检测，软件突破检测，防暴力破解，网站后门，外壳检测等多个维度，实现服务器安全的持续纵深保护。

### **数据传输加密**

HEDU只能协作系统传输加密是指为客户端与云端服务器提供了 SSL/TLS 协议来保证数据传输的安全。

例如，实际是在网络层（传输层）通过TLS进行加密，因此数据只有在通过网络发送前才会进行加密，保证在传输期间即使被截获数据，也无法读取里面的有效信息。

简单来说，音、视频数据从客户端发送到后台服务器这个过程是加密的。数据到达后台服务器后，只会向后台提供音、视频的质量信息（比如延迟、丢包、接入地区等信息），以便于在出现故障时运维人员进行排查。而会议中的音、视频流（实际的声音及图像信息），系统设计时没有预留任何接口让运维人员去获取这些音、视频流，因此HEDU网络会议无法获取用户的会议信息。

### **数据存储加密**

HEDU智能协作系统依托于天翼云的云主机、云存储、云数据库等技术，另外,天翼云云主机、云数据库产品和服务获得可信云服务认证，对数据存储加密进行了规范。

### **数据备份**

数据库备份策略, 一周中的每天凌晨4点进行备份, 保留最近7天; 1个月中每周的周天凌晨3点进行备份, 保留最近4周备份; 6个月中每个月的1号凌晨2点进行备份, 保留最近6个月的备份。

### **数据删除保护**

**数据删除**

在用户进行删除操作后，释放的存储空间由文件系统回收，禁止任何用户访问，同时进行内容擦除，最大限度保证用户的数据安全性。

华师在终止为云服务客户提供服务时，及时删除云服务客户数据资产或根据相关协议要求返还其数据资产。基于天翼云数据清除技术满足行业标准，清除操作留有完整记录，确保数据不被未授权访问。

运维人员未经客户许可，不得以任意方式访问客户未经公开的数据内容。遵循生产数据不出生产集群的原则，从技术上控制了生产数据流出生产集群的通道，防止运维人员从生产系统拷贝数据。