新华三集团

公安部网络安全等级保护中心

**新华三集团**

北京总部
北京市朝阳区广顺南大街8号院 利星行中心1号楼
邮编:100102

杭州总部
杭州市滨江区长河路466号
邮编:310052

www.h3c.com


**CN-173X30-20190909-BR-HZ-V1.0**

公安部信息安全等级保护评估中心

地址：北京市海淀区阜成路58号新洲商务大厦703室
邮编：100142

版本：V1.0
新华三云计算安全等级保护2.0合规能力白皮书
编号：20191001

公安部信息安全等级保护评估中心

紫光集团 核心企业 | H3C 数字化解决方案领导者

# 新华三云计算安全等级保护2.0合规能力白皮书

编号：20191001
版本：V1.0

# 总 述

《新华三云计算安全等级保护 2.0 合规能力白皮书》从等保能力验证技术架构、新华三云计算安全能力等保 2.0 合规状况及白皮书使用建议等方面做了详细阐述。借助白皮书，客户能够快速获取多交付场景下新华三云计算安全合规防护能力，同时结合客户侧的应用、安全管理、物理环境等方面的保护措施，共同构筑满足等保和客户需求的信息系统整体安全防御体系。

**白皮书共分为四个部分，各部分内容具体安排如下：**

第一部分主要介绍云计算的基础知识及云安全概述，主要包括云计算定义；云计算安全、云计算服务模式以及云安全责任分担模型，并简要概述新华三云计算平台部署模式。

第二部分描述了合规白皮书与规范体系架构的关系，基于云平台保护对象，对新华三云计算平台的安全措施及安全能力进行识别分析，构建了新华三云计算安全等保 2.0 合规能力模型，为云服务商和云服务客户的安全能力改进提供方向和指引，并简要介绍了云计算等保 2.0 合规能力安全评估方法。

第三部分介绍了新华三云计算安全，对新华三云计算安全架构进行了阐述，梳理了新华三云计算安全各安全层面的防护架构，对新华三云计算各安全组件（服务）进行详细介绍；此外，分别从网络安全等级保护 2.0 第三级和第四级通用要求和云计算扩展要求对新华三云计算安全等保 2.0 合规能力进行了分析、评估。

第四部分从行业应用角度对《新华三云计算安全等级保护 2.0 合规能力白皮书》的应用价值进行了介绍，阐述了白皮书的指导作用，并分别针对用户和等级保护测评机构的应用方法进行了详细的介绍，为用户在技术选型、规划设计和等级测评等方面提供不同程度的指导。

最后，在附录部分提供了新华三云计算安全在不同的交付模式下应该满足的等级保护 2.0 测评指标及新华三云计算安全等级保护安全合规能力。

本白皮书力求全面、深入浅出的分析新华三云计算安全的安全合规能力，通过分析新华三云计算平台的安全能力，构建云计算（新华三云计算安全）等保 2.0 合规能力模型，分析了新华三云计算安全等级保护 2.0 安全合规状况的详细报告。

公安部信息安全等级保护评估中心　　新华三技术有限公司

# 声 明

《新华三云计算安全等级保护 2.0 合规能力白皮书》是在中国云计算安全等级保护合规能力规范体系技术社区指导下，依据《云计算安全等级保护合规能力框架》，由公安部信息安全等级保护评估中心和新华三技术有限公司共同编制。新华三技术有限公司提醒您在阅读或使用本文档之前仔细阅读、充分理解下列各条款的内容：

1. 通过新华三技术有限公司提供的正规授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动，本文档的内容视为新华三技术有限公司的保密信息，应严格遵守保密义务；
2. 由于产品版本升级、调整或其他原因，本文档内容有可能变更，新华三技术有限公司保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在新华三技术有限公司授权通道中不时发布更新后的用户文档，应实时关注用户文档的版本变更并通过新华三授权渠道下载、获取最新版的用户文档；
3. 新华三技术有限公司已尽最大努力确保本文档内容准确可靠，但不提供任何形式的担保，任何情况下，新华三技术有限公司均不对（包括但不限于）最终用户或任何第三方因使用本文档而造成的直接或间接的损失或损害负责。
4. 本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其它相关权利均由公安部信息安全等级保护评估中心和新华三技术有限公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。新华三技术有限公司保留对本文档及本声明的最终解释权和修改权，非经新华三技术有限公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播，本文档中的信息可能变动，恕不另行通知；且不得以任何理由使用、公布或复制本白皮书中公安部信息安全等级保护评估中心的名称（图案标示、标识）；
5. 限于编制时间仓促，编制组水平有限，书中难免疏漏和不足，诚望不吝赐教、斧正，以便后续改进和完善，期望能够给本白皮书的阅读者提供有用的参考，任何意见或建议，敬请联系 yang.hongqi@h3c.com。


**主要撰稿人**

张振峰 （公安部信息安全等级保护评估中心）
张志文 （公安部信息安全等级保护评估中心）
杨洪起 （新华三技术有限公司）
张 野 （新华三技术有限公司）
刘姝麟 （新华三技术有限公司）
于子洲 （新华三技术有限公司）
董 伟 （新华三技术有限公司）
贾 楠 （新华三技术有限公司）
赵新珂 （新华三技术有限公司）
韩 超 （新华三技术有限公司）
王 乐 （新华三技术有限公司）
史翔宇 （新华三技术有限公司）



**特别感谢**

张宇翔 （公安部信息安全等级保护评估中心）
李 明 （公安部信息安全等级保护评估中心）
张 力 （新华三技术有限公司）
刘云峰 （新华三技术有限公司）
孙松儿 （新华三技术有限公司）
涂 尧 （新华三技术有限公司）


# 目 录

# 第 1 章 云计算概述

## 1.1 云计算基本概念

云计算是一种资源利用模式，它是一种无处不在的、便捷的、按需的，基于网络访问的，共享使用的，可配置的计算资源（如：网络、服务器、存储、应用和服务），可以通过最少的管理工作或与服务提供商的互动来快速置备并发布。云计算将计算、网络、存储、数据等资源集中在资源池中，并以服务的形式提供给用户，这些服务可以快速构建、准备、部署和退出，并且可迅速扩充或缩减规模。该定义描述了云计算的三种服务模式，四种部署模式以及五个基本特征。

云计算服务的五个基本特征：按需自助、无所不在的网络访问、资源池化、快速弹性和可度量的服务。

云计算基于交付方式可以划分为三种服务模式：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。

基础设施即服务 (Infrastructure-as-a-Service)，云服务商主要提供一些基础资源，包括服务器、网络、存储等服务，由自动化的、可靠的、扩展性强的动态计算资源构成。云服务客户能够部署和运行任意软件，包括操作系统和应用程序，无需管理或控制任何云计算基础设施，但能控制操作系统的选择、存储空间、部署的应用，也有可能获得网络组件的控制。

平台及服务 (Platfrom-as-a-Service)，主要作用是将一个开发和运行平台作为服务提供给用户，能够提供定制化研发的中间件平台、数据库和大数据应用等。

软件即服务 (Software-as-a-Service)，通过网络为最终用户提供应用服务，绝大多数 SaaS 应用都是直接在浏览器中运行，不需要用户下载安装任何程序，由服务商管理和托管的完整应用软件。云服务客户可以通过 web 浏览器、移动应用或轻量级客户端应用来访问它。

根据使用云计算平台的客户范围不同，可以将云计算分成私有云、公有云、社区云和混合云。

## 1.2 云计算安全

随着云计算的普及，安全问题已成为制约其发展的关键要素之一，与传统信息系统安全相比，云计算具有按需服务、泛在接入、多租户和资源池、快速弹性、可度量性五大特有属性，在安全方面，云计算也具有一些新的特征，如传统的安全边界消失、服务安全保障模式改变、数据安全保护强度提高，技术标准和政策法规缺失。鉴于云计算的新特性，传统的安全防护措施无法有效的保证云计算的完整性、可用性和保密性，云计算的安全性受到严重挑战。传统信息技术所面临的安全风险依然威胁着云计算安全，云计算新特性也带来一些新的风险，如数据泄露、数据丢失、数据劫持、共享技术漏洞、不安全 API 接口及滥用云服务等。基于云计算新增的安全威胁、防护手段及“一个中心，三重防御”的纵深防御思想，《GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求》中进行了扩展，形成了云计算安全扩展要求，网络安全等级保护制度在 2.0 时代着重于全方位的主动防御、动态防御、精准防护和整体防控的安全防护体系，将云计算平台 / 系统的安全问题主要分为物理环境安全、通信网络安全、区域边界安全、计算环境安全、管理中心安全以及云计算安全管理方面的安全问题。

### 1.2.1 物理环境安全

云计算依赖于强大可靠的虚拟化和分布式计算技术，其依赖于由计算、存储、网络等云基础设施设备构成的物理机房。物理环境安全是系统安全的前提，信息系统所处物理环境安全的优劣对信息系统的安全有着直接的影响，物理环境安全主要包括两个方面：一方面是指保护云计算平台免遭地震、水灾、火灾等自然灾害以及人为行为导致的破坏，预防措施主要包括场地安全、防火、防水、防静电、防雷击、电磁防护及线路安全等；另一方面是指云服务商部署基础设施的数据中心安全设计和运维运行管理，以及建立严格的管理规章制度。

### 1.2.2 通信网络安全

云计算的主要特征泛在接入凸显了网络是云计算的重要基石，网络安全是云计算安全的重要一环。对于大多数的云计算而言，网络的性能决定云计算的性能。通信网络安全一方面是边界内部的局域网网络架构以及虚拟网络架构设计的安全性，整个网络资源分布、架构合理是在网络上实现各种技术功能以达到通信网络保护目的为前提；另一方面是网络传输数据的安全性，通信数据在传输过程中的安全性是保障网络环境安全运行的根基，保障通信网络的安全性，可有效地防止数据在通信传输中被篡改或泄露，确保在网络中传输数据的保密性、完整性和可用性等。

### 1.2.3 区域边界安全

云与外部网络互联互通过程中也存在着较大的安全隐患，尽管云计算具有无边界化、分布式的特性，但对于每一个云数据中心，其服务器仍然是局部规模化集中部署的。通过对每个云数据中心分别进行安全防护，来实现云基础设施边界安全，并在云计算服务的关键节点和服务入口处实施重点防护，实现局部到整体的严密联防。网络边界防护是云计算环境安全防御的第二道防线。在不同的网络间实现互联互通的同时，在网络边界采取必要的安全接入、访问控制、入侵防范、安全审计等措施是实现内部计算环境安全防御的必要手段。

### 1.2.4 计算环境安全

除对传统系统的服务器操作系统、数据库、业务应用及数据的安全性要求外，等保 2.0 还对镜像和快照安全、虚拟化安全、网络安全设备等方面提出了相关的要求。云计算操作系统基于虚拟化技术实现计算资源池化、动态配置以及资源编排，为应对虚拟化技术自身安全性，对云计算平台提出了一层额外的安全要求。针对虚拟机在使用和迁移过程中可能引起风险，增加的安全性要求还有虚拟服务管理平台（Hypervisor，VMM）安全、虚拟资源隔离、虚拟机镜像安全等。

### 1.2.5 安全管理中心

“安全管理中心”是纵深防御体系的“大脑”，通过“安全管理中心”实现技术层面的系统管理、审计管理和安全管理，同时通过“安全管理中心”实现整个云计算环境的集中管控。“安全管理中心”并非一个机构，也并非一个产品，是一个技术管控枢纽，通过一个技术工具或多个技术工具实现一定程度上的集中管理，便于云计算资源进行调度、管理以及监控，同时能够对统一身份、认证、授权及密钥进行管理。

### 1.2.6 安全管理

安全管理包括安全运维管理、安全建设管理、安全管理人员、安全管理机构、安全管理制度。任何一个组织机构应制定符合国家需求和自己机构内部需求的安全管理制度体系，构建从单位最高管理层到执行层以及具体业务运营层的组织体系，明确各个岗位的安全职责，对参与系统建设、管理、运维等人员实施科学、完善的管理，保证系统建设的进度、质量和安全以及系统运维有效、完善的运行。

## 1.3 云安全责任分担模型

任何一个云服务的参与者都应承担起相应的职责，不同角色的参与者通常会承担实施和管理不同部分的责任。因此，云安全的责任由云服务不同的参与者分担。云平台一般提供基础设施即服务、平台即服务和软件即服务的各类云服务资源，云服务安全责任主要涉及的角色有云服务商和云服务客户。

云服务商的主要安全责任是研发和运维云平台，保障云平台基础设施的安全，同时提供各项基础设施服务以及各项服务内置的安全功能。云服务商在不同的服务模式下承担的安全责任不同（图 1.1），在基础设施即服务（IaaS）模式下，云服务商需确保基础设施无漏洞，云服务商基础设施包括支撑云服务的物理环境、云服务商自研的软硬件以及运维运营包括计算、存储、数据库以及虚拟机镜像等各项云服务的系统设施，同时云服务商还需负责底层基础设施和虚拟化技术免遭外部攻击和内部滥用的安全防护责任，并与云服务客户共同分担网络访问控制策略的防护；在平台即服务（PaaS）模式下，云服务商还需负责底层基础设施和虚拟化技术免遭外部攻击和内部滥用的安全防护责任，并与云服务客户共同分担网络访问控制策略的防护；在平台即服务（PaaS）模式下，云服务商除防护底层基础设施安全外，还需对其提供的虚拟机、云应用开发平台及网络访问控制等进行安全防护，并对其提供的数据库、中间件进行基础的安全加固；在软件即服务（SaaS）模式下，云服务商需对整个云计算环境提供安全防护责任。

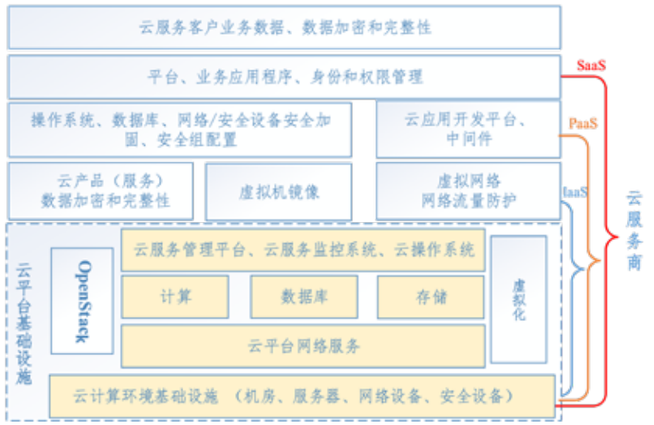



图 1.1 云安全责任分担模型—云服务商安全责任


图 1.2 云安全责任分担模型—云服务客户安全责任

各类可控的资源进行安全配置，对其云平台的相关账户进行安全策略配置，对运维人员实施权限管理及职责分离，并对云服务商提供的虚拟机、安全组、高级安全服务以及云服务客户自行部署的安全防护软件进行合理的安全策略配置。此外，对于云服务客户自行部署在云上的业务应用、数据库及中间件等均需云服务客户进行安全管理，云服务客户始终是云上业务数据的所有者和控制者，云服务客户需对数据的保密性、可用性、完整性以及数据访问验证、授权进行安全管理；在平台即服务（PaaS）模式下，云服务客户需保证其部署在云平台上的业务应用和数据的安全性，并对云服务商提供的各项服务进行安全配置，各类账户进行安全管理，防止自身业务应用受到非授权的破坏，导致数据泄露或丢失；在软件即服务（SaaS）模式下，云服务客户需对其选用的应用进行安全配置，并对自身业务数据做好安全防护工作。

无论哪种云服务模式，云服务商都应为客户提供数据保护手段，并实现数据保护的相关功能，但是云服务商绝不允许运维人员在未经授权的情况下私自访问云服务客户数据；云服务客户对其业务数据拥有所有权和控制权，需负责各项具体的数据安全配置，云计算平台提供的数据传输、存储完整性和保密性的安全功能决定着用户数据安全防护措施是否能实现。

## 1.4 新华三云计算平台部署模式

新华三云计算部署场景可以是私有云部署、公有云部署或者是混合云部署，在不同的云计算部署场景中，新华三提供的安全能力各有侧重。新华三云计算聚焦行业云和城市云，为百城百业提供全栈式服务和全产业链云生态。新华三为政务、高校、融媒、工业、金融、党建等多行业提供的云计算涉及 IaaS 和 PaaS 两种服务模式，云计算基础设施相关软件、硬件部署在客户提供的数据中心本地或者是私有云云计算平台的数据中心。新华三云计算平台融合 H3C CloudOS 云操作系统、H3C CAS 虚拟化平台、H3C VCFC 及 H3C SecCloud OMP 云安全管理平台，且兼容基于 OpenStack 的第三方云架构，为每个云服务客户提供完善的安全防护解决方案，并为数据中心的边界安全提供防护。


图 1.3　云计算服务模式

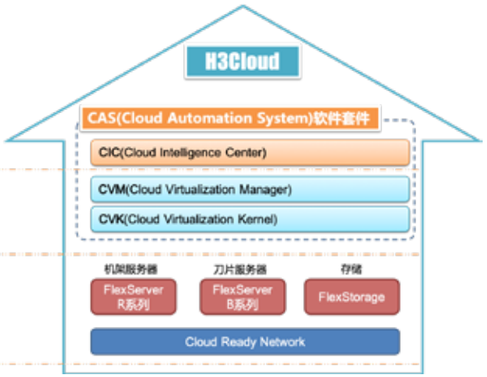



图 1.4　新华三云计算基础设施架构

H3C CAS 虚拟化平台采用满足电信级性能及可靠性要求的虚拟化内核，支持融合交付计算、存储、网络、安全虚拟化资源，H3C CAS 虚拟化平台由 CVK 虚拟化内核系统、CVM 虚拟化管理平台和 CIC 云业务管理中心三个组件构成，能够提供强大的数据中心虚拟化及管理能力，将基础架构资源及相关策略整合成弹性数据资源池，云服务客户可通过自服务门户（H3C CloudOS）按需使用资源。H3C CloudOS 实现对数据中心资源的统一管理和智能调度，为上层的 XaaS 提供对应的能力支持，基于稳定可靠的 IaaS 服务能力，有效拉通数据中心基础设施资源，并通过运营运维一体化门户自动交付。

H3C CloudOS 云操作系统将 IT 资源抽象为各种各样的云服务，用户根据需要按需申请、使用。目前，H3C CloudOS 云操作系统提供 X86 虚拟机、PowerVM 虚拟机、云硬盘、云网盘、云网络、云防火墙、裸金属服务器等 IaaS 服务，应用仓库、应用管理、镜像仓库、流水线等 PaaS 服务，还提供一些开发测试服务及大数据和 AI 服务等。

H3C SecCloud OMP 与 H3C CloudOS 集成部署（图 1.5），为新华三云计算平台提供丰富的安全服务目录，保障云平台高效运行。

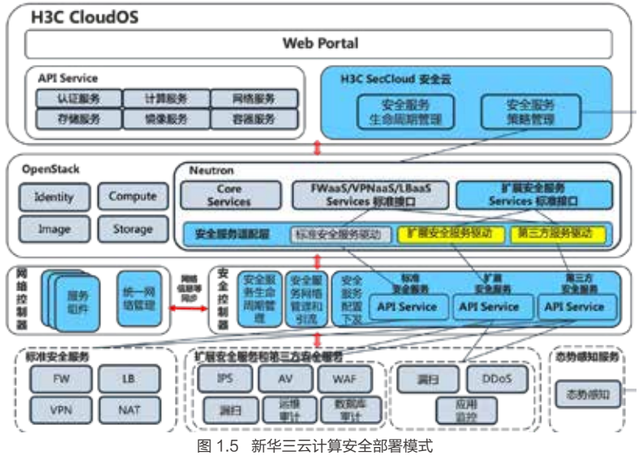



图 1.5　新华三云计算安全部署模式

- H3C SecCloud OMP 作为安全服务组件集成到 CloudOS 页面中，提供：
  安全服务生命周期管理（对接 VCFC）；
  安全服务策略配置管理；
  安全服务订单管理等功能；
- H3C CloudOS 提供 WEB portal 页面，提供：
  安全服务生命周期管理页面；
  安全服务编排页面。
- H3C VCFC，提供：
  安全服务生命周期管理（对接设备）；
  安全服务策略配置对接；
  网络部署；
  业务引流。





# 第 2 章　云计算等保 2.0 合规能力技术架构

## 2.1　合规白皮书与规范体系框架的关系

云计算平台由设施、硬件、资源抽象控制层、虚拟化计算资源等组成。区别于传统的信息系统，在云计算不同的服务模式中，云服务商和云服务客户对计算资源拥有不同的控制范围（图 2.1），在基础设施即服务模式 (IaaS) 下，云计算平台 / 系统由设施、硬件、资源抽象控制层组成；在平台即服务模式 (PaaS) 下，云计算平台 / 系统包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在软件即服务模式 (SaaS) 下，云计算平台 / 系统包括设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件。对计算资源的控制范围决定了安全责任的边界，云计算环境中通常有一个或多个安全责任主体，各安全责任主体根据管理权限的范围划分安全责任边界。云计算环境中多个安全责任主体的安全保护能力之和共同构成了整个云计算环境的安全防护能力。当“云服务商”与“云服务客户”为同一类实体机构或自然人时，云计算环境的安全责任只有一个，就是该系统的建设运行使用单位或个人。

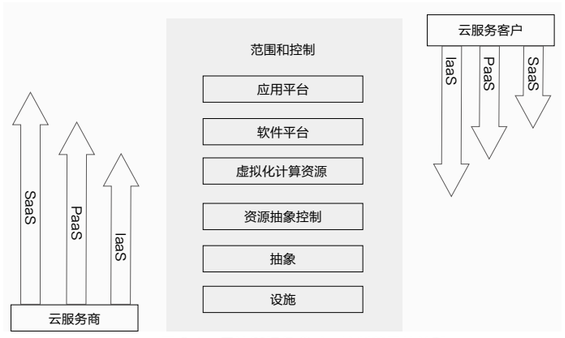



图 2.1　云计算服务模式与控制范围的关系

云计算环境中可能承载一种或多种云服务模式，每种云服务模式下提供了不同的云计算服务及相应的安全防护措施，在对云计算系统安全评估时，应仅关注每种特定云服务模式下，与其提供的云服务相对应的安全防护措施有效性。

不同的云服务模式下，云服务商与云服务客户的责任边界会发生变化（如图 2.1），在确定具体的安全责任时，应根据系统的实际运行情况而定。在明确云计算平台保护等级的情况下，按照等级保护对象在云计算环境中的角色、云计算的服务模式、云计算环境中的责任主体以及云计算实现方式对测评指标选取的影响四个步骤对等级保护对象和等级测评指标进行选取。四个步骤充分的体现了云计算系统等保合规的两大基本原则：责任分担原则和云服务模式适用性原则。

合规白皮书是严格按照合规能力规范体系框架封装的方法，呈现了云计算环境等保 2.0 的合规能力模型，明确了云计算环境的保护对象、安全措施以及安全防护能力，并对云计算环境的等保 2.0 的合规状况进行分析、认定。

## 2.2　新华三云计算安全等保 2.0 合规能力模型

### 2.2.1　新华三云计算安全等级保护对象

新华三云计算平台由设施、硬件、资源抽象控制层、虚拟化计算资源等组成。面向各行业主要提供平台即服务（PaaS）、基础设施即服务（IaaS）的云计算服务模式。在不同的服务模式中，云服务商和云服务客户对计算资源拥有不同的控制范围，控制范围则决定了安全责任的边界。在基础设施即服务模式下，云计算平台 / 系统由设施、硬件、资源抽象控制层组成；在平台即服务模式下，云计算平台 / 系统包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台。不同服务模式下云服务商和云服务客户的安全管理责任有所不同，同时保护对象也随之发生变化。基于《信息安全技术—网络安全等级保护云计算测评指引》对不同云计算服务模式下云计算平台测评对象的选取方法，综合考虑新华三云计算平台组网情况，确定新华三云计算平台的安全保护对象如图 2.2。

### 2.2.2 新华三云计算安全措施

区别于传统的信息系统，在云计算环境中，边界可信日益削弱，源自不同平面的攻击也日趋增多。传统分层面单层防御体系对确保云计算系统安全性显得尤为困难，基于等级保护 2.0“一个中心，三重防护”的纵深防护思想，即从通信网络到区域边界再到计算环境进行重重防护，通过安全管理中心进行集中监控、调度和管理，构建云计算安全措施，如图 2.3 所示。

用户通过安全的通信网络跨越安全的区域边界以网络直接访问、API 接口访问或 Web 服务访问等方式访问安全的云计算环境。云计算环境安全包括基础架构层安全、云服务层安全以及业务应用和数据安全，其中基础架构层包括云计算硬件设备和虚拟化计算资源，云服务层包含云产品以及资源抽象控制等。云计算环境的系统管理、安全管理和安全审计由安全管理中心统一管控。


图 2.2 新华三云计算平台安全保护对象

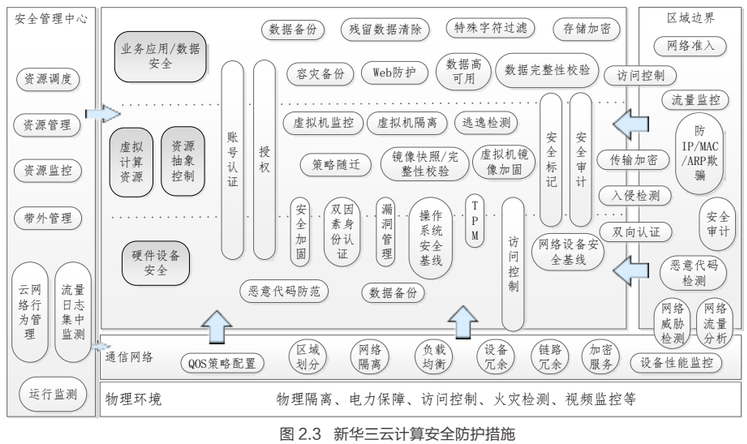



图 2.3 新华三云计算安全防护措施

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》在安全计算环境方面，主要增加了虚拟化安全、镜像和快照安全等云计算相关的控制点，安全的云计算环境应提供安全加固（操作系统、镜像）、虚拟机隔离、双因素身份认证以及访问控制、安全审计等安全措施；在安全区域边界方面，除了传统物理区域的边界安全外，增加了虚拟网络区域边界、虚拟机与宿主机之间的区域边界等防护安全要求，安全的云计算环境区域边界应提供网络隔离、流量监控、虚拟机隔离等安全措施；在安全通信网络方面，在物理通信网络基础上增加了虚拟网络通信的安全保护要求，安全的通信网络应提供区域划分（物理网、虚拟网）、入侵检测、设备性能（物理网络设备、虚拟网络设备）监控、东西向及南北向流量安全防护等安全措施；在安全管理中心方面应提供资源的统一调度、监控、管理以及全网审计日志集中收集（分析）、时间同步等安全措施。

基于 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》，详细的新华三云计算安全措施与实现安全措施的产品 / 方法如表 1。

表 1 实现安全措施的产品 / 方法

| 安全层面 | 安全措施 | 实现安全措施的安全产品方法 | |
|---|---|---|---|
| | | 平台侧 | 云服务 客户侧 |
| 安全通信网络 | 网络设备性能监控、带宽监控 | IMC、态势感知、性能监控 | 态势感知 |
| | 负载均衡 | 负载均衡设备（SLB、LLB） | 负载均衡设备 – 虚机 |
| | 网络隔离 | VPC、vrouter | 虚拟防火墙、VPC |
| | 安全域划分 | 防火墙 –– 安全域 | 防火墙虚机 –– 安全域 |
| | 访问控制 | 下一代防火墙、虚拟防火墙 | 虚拟防火墙 |
| | 网路设备双活部署、链路冗余 | 设备堆叠、链路冗余、智能 DNS | 负载均衡 |
| | QOS 策略配置 | 网络设备配置 QoS 策略 | 网络设备配置 QoS 策略 |
| 安全区域边界 | 传输加密 | IIPsec、HTTPS | 通过堡垒机管理 |
| | 证书双向认证 | CloudOS 证书、Https | —— |
| | 加密服务 | 虚拟机密钥对 | —— |
| | IP/MAC 绑定 | 防火墙、交换机 IP/MAC 绑定策略 | 防火墙、交换机 IP/MAC 绑定策略 |
| | 网络准入 | SDN 控制器、服务器安全监测、态势感知（资产管理）、IPS、防火墙、ACG、IP/MAC 绑定 | 桌面准入（EAD）、服务器安全监测 |
| | 流量监控 | 态势感知平台 | 态势感知平台 |
| | 入侵检测 | 服务器安全监测、态势感知、IDS | 防火墙 –IPS |
| | 安全审计 | 态势感知平台、日志审计 | 日志审计 |
| | 恶意代码检测 | 防火墙（防病毒模块） | 虚拟防火墙（防病毒模块） |
| 安全计算环境 | 账号认证 | 堡垒机 + 第三方认证 | 堡垒机 + 第三方认证 |
| | 网络设备加固 | 安全基线 | 安全基线 |
| | 镜像 / 系统安全加固 | 机安全加固、安全基线 | 机安全加固、安全基线 |
| | 传输加密 | HTTPS 协议 | HTTPS 协议 |
| | 双因素身份认证 | 堡垒机 + 第三方认证 | 堡垒机 + 第三方认证 |
| | 授权 | 三权分立 | —— |
| | 安全审计 | 态势感知、日志审计、数据库审计、堡垒机 | 态势感知、日志审计、数据库审计、堡垒机 |
| | 登录地址限制 | CloudOS、堡垒机、虚拟防火墙 | 堡垒机、虚拟防火墙 |
| | 特殊字符过滤 | 安全测试、防火墙 ––IPS、WAF | 防火墙 ––IPS、WAF |
| | 漏洞管理 | 云漏洞扫描系统 | 云漏洞扫描系统 |
| | 恶意代码检测 / 防范 | 防火墙 ––IPS、亚信安全服务器深度安全防护系统 | 防火墙 ––IPS、亚信安全服务器深度安全防护系统 |
| | 可信计算 | TPM | —— |
| | 数据完整性校验 | MD5、虚拟机分布式存储，三副本完整性校验 | 虚拟机分布式存储，通过三副本实现完整性校验 |
| | 数据备份 | ONEStor、CAS 备份功能 | 分布式存储 |
| | 数据冗余、高可用 | 虚拟机、负载均衡 | 虚拟机、负载均衡 |
| | 容灾备份 | ONEStor | —— |
| | 残留数据清除 | 写零机制 | 写零机制 |
| | 虚拟机迁移 | 迁移工具 Move sure | —— |
| | 镜像 / 快照完整性 | 磁盘机密、CAS 完整性校验 | —— |
| 安全管理中心 | 带外管理 | 带外管理网络 | —— |
| | 运行监测 | 态势感知、H3C CAS、H3C CloudOS | 态势感知、H3C CloudOS |
| | 策略集中管控 | H3C SecCloud OMP | H3C Cloud |

### 2.2.3 新华三云计算安全能力

安全技术能力是云计算系统安全措施作用于保护对象上形成的抵抗外部攻击的一种防护能力，云安全措施是根据广泛的经验和学识为对抗云计算系统面临的威胁而采取的防护措施，有的安全措施是由云计算平台原生，有些则是云服务商为应对威胁而自研或由云生态合作伙伴提供。新华三云计算安全基于 OpenStack 接口，提供整体的安全能力集合，采用归一化标准接口，与多种场景无缝适配，为华三云平台或第三方云平台提供丰富的安全服务。不同侧的安全措施作用于保护对象后形成了不同的安全技术能力，在此，引入安全能力定量和变量的定义，即：定量是指云服务商不依赖于用户选择而原生提供的安全能力，如 VCFC、安全组防火墙等。

变量是指云服务商依据用户需求，为应对系统威胁而选择性提供的安全能力，该能力既可由云服务商提供，也可由云服务生态合作伙伴提供，如第三方硬件加密机。

**1）安全物理环境**

云机房物理环境安全措施，主要包括但不限于火灾检测、双路供电、访问控制、视频监控、机房热备等。

安全措施：火灾检测

安全能力：云数据中心机房配备火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等，能够对于火灾发生的部位以声、光或电的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。

安全措施：双路供电

安全能力：云数据中心机房的每一个负载均由两个电源供电，两个电源之间可以进行切换。若电源发生故障，在其中一个电源失电的情况下可以投切到另一个电源供电，保障业务 7*24 小时持续运行。

安全措施：访问控制

安全能力：云数据中心的物理设备和机房的访问要具备访问控制，包括机房的进出访问控制，例如，对于进出机房或者携带设备进出机房，物理设备的配置、启动、关机、故障恢复等，均需具备相应的访问控制策略。

安全措施：视频监控

安全能力：云数据中心机房装设视频监控系统或者有专人 24 小时值守，对通道等重要部位进行监视。例如，对出入通道进行视频监控，同时报警设备应该能与视频监控系统或者出入口控制设备联动，实现对于监控点的有效监视。

新华三云计算部分安全措施作用于保护对象后形成的安全能力：

**2）安全通信方面**

安全措施：智能 DNS、设备高可用

安全能力：网络架构从接入层到汇聚层，实现节点冗余和链路 LLB 负载分担，在满足带宽收敛和保证业务性能同时满足整个业务系统的高可用；H3C 云计算在组网时防火墙通过堆叠的形式，交换机通过 M-LAG 的方式，服务器通过集群的方式，保证基础设施设备高可用；负载均衡设备提供智能 DNS 服务，保证网路链路、系统的高可用。

安全措施：网络隔离

安全能力：H3C 云计算环境专有网络（Virtual Private Cloud）VPC 采用隧道技术，帮助用户构建出一个隔离的网络环境，实现不同云服务客户间的网络资源的隔离；同一 VPC 内通过虚拟防火墙进行安全域隔离；不同 VPC 间部署虚拟防火墙，通过 VRF 进行路由隔离，部署虚拟防火墙进行访问控制，实现不同 VPC 间隔离；虚拟防火墙能够帮助用户实现云计算环境中东西向流量的隔离。

**3）安全区域边界**

安全措施：流量监控、入侵检测

安全能力：H3C 态势感知服务系统在云平台关键节点处部署流量探针，对整个云平台的全流量包进行深度解析，实时地检测出各种攻击和异常行为；旁路部署 IDS 硬件设备，对云平台的所有流量进行检测；H3C 云计算环境出口防火墙开启 IPS 功能，对进出流量进行监测；服务器端安装新华三服务器安全监测系统进行安全加固，防止对内部的网络攻击行为。

**4）安全计算环境**

安全措施：双因素身份认证

安全能力：H3C CloudOS、H3C CAS、H3C SecCloud OMP 等管理平台的鉴别方式有用户名、口令 + 短信验证码、邮件验证码两种身份鉴别方式；新华三云计算系列产品均允许被堡垒机接管，且可配置仅允许堡垒机访问，在堡垒机侧通过用户名、口令 +USB Key 的认证方式，实现用户双因素身份鉴别。

安全措施：镜像加固

安全能力：H3C 能够为用户提供主流的操作系统镜像，对镜像基于安全基线进行加固，安装防恶意代码软件、服务器安全监测系统，保证镜像的安全性。

安全措施：数据处理系统冗余、高可用

安全能力：新华三云计算环境中防火墙采用堆叠的形式、交换机通过 M-LAG 的形式、服务器侧采用虚拟机、存储侧为分布式存储系统，还有负载均衡等均可保证数据处理系统的冗余。

**5）安全管理中心**

安全措施：资源监控

安全能力：H3C 态势感知系统支持全网全流量的监测，能够对所有的网络设备、安全设备、服务器、虚拟机进行集中监测；H3C Cloud 、H3C SecCloud OMP 管理平台为云平台侧和云服务客户侧分别分配账户，可对两侧各自部分的资源进行集中监测。

### 2.2.4 能力矩阵模型

安全技术能力是云计算系统安全措施作用于保护对象上形成的抵抗外部攻击的一种防护能力，构建 SMO（safety measure -object）矩阵模型：

| | 保护对象 1 | 保护对象 1 | …… | 保护对象 m |
|---|---|---|---|---|
| 安全措施 1 | √ | N/A | √ | N/A |
| 安全措施 3 | √ | √ | N/A | √ |
| …… | N/A | √ | √ | √ |
| 安全措施 n | √ | N/A | √ | √ |

其中，“√”表示安全措施在保护对象上能够起到相应的安全作用；

N/A 表示安全措施无法作用于保护对象或作用在保护对象时无法起到相应的安全作用。

根据不同的安全措施作用于不同的保护对象形成的安全能力，构建 SCMO（safety capability& measure -object）矩阵模型：

| | 保护对象 1 | 保护对象 1 | …… | 保护对象 m |
|---|---|---|---|---|
| 安全措施 1 | 1 | — | 0 | — |
| 安全措施 3 | -1 | 0 | — | -1 |
| …… | — | 1 | 1 | 0 |
| 安全措施 n | 0 | — | -1 | -1 |

其中，“0”表示云平台原生安全措施作用于保护对象后提供的安全能力，在云平台交付时，默认交付；“1”表示云平台提供的安全能力，在云平台交付时，用户根据业务需求，考虑系统所面临的威胁，需按需购买，“-1”表示根据业务需求，用户自行部署安全产品或安全加固后所形成的安全能力；此处 0 为定量，1 和 -1 为变量，“—”表示安全措施无法作用于保护对象或作用后未形成安全能力。

### 2.2.5 新华三云计算等保 2.0 合规能力模型

**1. 模型建立**

H3C 云计算平台融合 H3C SecCloud OMP 安全云管理平台，H3C SecCloud OMP 除为新华三云计算平台提供安全防护措施外，还能够为云客户业务系统提供 SeCaaS 服务。首先，明确新华三云计算环境保护对象，其次依据 SMO 模型分析新华三云计算平台所拥有的原生安全措施以及为应对可能面临的威胁而建设的安全防护措施，并根据 SCMO 模型分析安全云安全措施作用于保护对象之后所形成的安全技术能力，最后对标安全云云平台安全技术能力与《网络安全等级

保护 2.0 基本要求》间的差距，分析安全云云平台的合规情况，构建安全云等保 2.0 合规能力模型（图 2.4）。

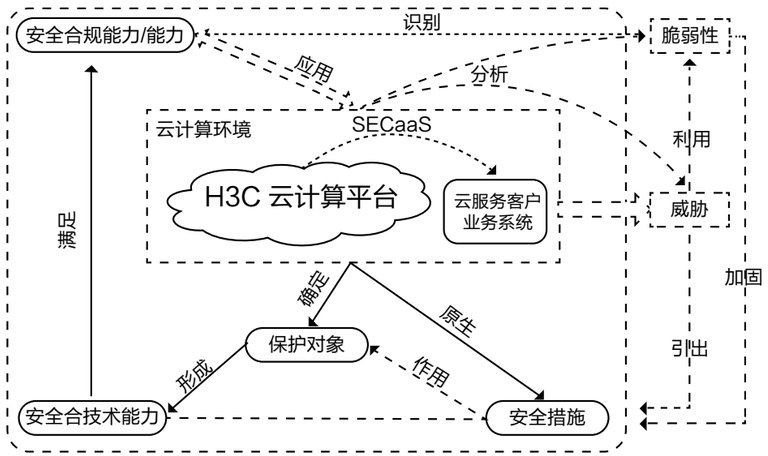



图 2.4　新华三云计算安全网络安全等级保护 2.0 合规模型

此外，通过合规能力模型的评估，可识别当前安全云和云计算平台 / 系统所面临的脆弱性，便于对整个云计算环境进行加固，强化安全防护措施，以提升安全云平台的安全防护能力。

**2. 新华三云计算等保 2.0 评估方法**

根据模型，识别保护对象、安全措施，分析得到安全云安全技术能力，对标网络安全等级保护 2.0 基本要求测评项，进行安全合规性评估，如图 2.5，对于不符合项，可识别安全云云平台脆弱性，及时作出相应的加固，增强抵御风险的防护能力。

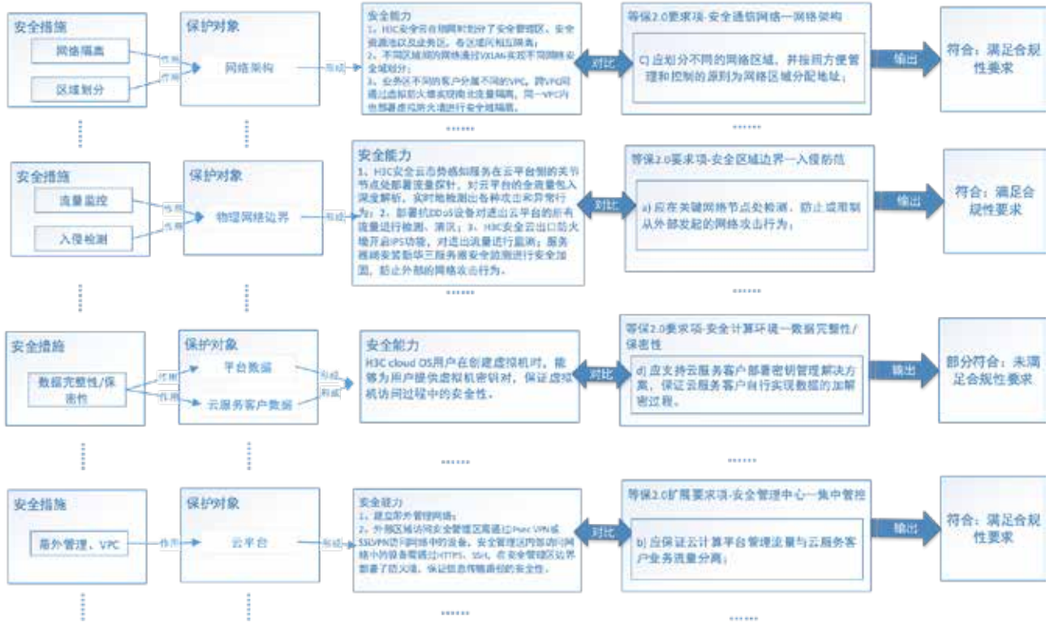



图 2.5　新华三云计算平台网络安全等级保护 2.0 评估方法





# 第 3 章　新华三云计算安全等级保护 2.0 合规状况

## 3.1　新华三云计算安全概述

### 3.1.1　新华三云计算安全背景概述

数字经济浪潮席卷全球，企业和国家需要对其所在的行业数字化转型需求进行洞察与实践。中国数字化时代充满机遇和挑战，科技革新和消费者的需求倾向转变正在改变着每个行业并影响着我们的工作方式和商业模式。在此过程中，我们对数字化的依赖越来越强，同时，数字化转型也对网络安全架构提出了更高的要求。在数字化转型的过程中，IT 架构也正在发生着巨大的变化，云计算、大数据、物联网、人工智能等新技术的涌现，让割裂分散的传统 IT 架构向集中统一的新兴 IT 架构快速转型。网络边界的模糊以及业务资源的整合与再分配都对网络安全架构提出了新的挑战。

传统烟囱式的建设模式，每个业务系统拥有独立的安全防护设备，业务系统规模较小，网络结构简单，各个系统间边界清晰，资源独立，安全运维也相对简单。在数字化时代，数据大集中带来业务系统规模的激增，云计算技术的大规模应用以及租户的出现，使得网络边界完全被打破，业务资源池化，原有碎片化的安全架构已完全不能够适应业务架构的融合与扩张。海量业务在上线过程中，安全系统的部署会由于访问量和应用的多样性成为最大的瓶颈。企业如何差异化实现业务系统的安全，也成为数字化转型过程中的重要课题。

云计算成为近十年来成长最快的一种 IT 技术，但是随之而来的也有很多问题，比如安全问题。对于企业来说，安全是个不可逃避的话题。随着云计算技术的大规模应用，使得网络边界完全被打破，呈现出网络虚拟化、服务资源池化、服务位置可迁移、服务资源按需获取、服务能力弹性可扩展等特点。传统的网络安全架构已不能完全适应这种新的业务架构。

云计算场景下，如何有效部署安全系统成为各企业数字化转型过程中的重要课题。云计算网络安全体系的三个核心需求：安全能力的快速部署、安全能力的差异化部署及安全状态的可视化。其根本是降低云计算网络安全运维的复杂度，提高安全服务弹性伸缩能力以及差异化安全能力交付的问题。

为了解决上述问题，H3C 推出了一款全新设计的适用于云计算网络的云安全服务管理平台—H3C SecCloud OMP 安全云管理平台（简称：安全云管平台）。安全云管平台从逻辑控制层的角度出发，屏蔽底层技术细节，将繁琐的安全业务重新进行定义，基于用户业务角度为其提供抽象的各类安全能力的服务化配置和管理。安全云管平台基于 OpenStack 架构，与 H3C CloudOS、H3C CAS 虚拟化平台、VCFC 完美融合，为用户提供高效的安全资源管理能力，同时为用户业务应用系统云上部署及运行提供完善的一体化解决方案。

### 3.1.2　新华三云计算安全特点

**1. 极简的配置逻辑**

安全云管平台从用户出发，提供一套极简的配置逻辑，防护对象一次配置，多种安全服务均可引用，仅通过简单操作便能完成安全服务的购买与开通。对使用者而言，不仅逻辑更加清晰，更大大了降低了配置难度，真正的节约了客户时间。

**2. 丰富的服务目录**

安全云管平台可以为用户提供丰富的安全服务目录，用户可以根据自身需求定制安全服务列表，包括安全服务类型、服务内容、服务规格、服务周期等内容。安全云管平台从用户业务角度出发，屏蔽安全服务底层技术细节，为用户提供简便快捷的配置界面，安全云管平台目前可以提供的安全服务包括：

- 防火墙服务
- 入侵检测服务（IPS）
- 病毒防护服务
- 抗 DDoS 服务
- WEB 应用防护服务
- 负载均衡服务
- 地址转换服务（NAT）
- VPN 服务
- 应用监控服务
- 漏洞扫描服务
- 态势感知服务
- 运维审计服务
- 数据库审计服务

**3. 统一化配置界面**

统一的界面，各安全服务风格统一，真正的做到所见即所得，各安全服务的开通配置具有共通性，之间没有壁垒，用户操作简单，易于上手。

**4. 自动化业务部署**

业务部署编排的自动化，实现端到端的业务自动化部署，当用户创建安全服务时，安全云管平台会自动分析云环境中各相关组件信息，自动关联业务地址，做到租户对网络部署无感知，仅需要点击开通安全服务，而无需再登录到各设备上做复杂的配置操作，在设备上自动下发相应的配置，大大加快了部署时间和效率。

**5. 智能化运维管理**

为了简化系统运维，提高运维效率，安全云管平台采用大数据分析技术，从不同角度、不同维度向用户展示云计算网络云安全服务信息，包括服务状态统计、服务资源统计、告警事件统计、用户账户信息、服务费用统计、工单统计、安全态势信息等，并提供各种可视化的操作界面，使得管理员轻松运维管理云计算网络云安全服务，及时清晰掌握云安全服务状况和云计算网络安全态势风险，及时应对各类安全事件。

**6. 可视化运营分析**

安全云管平台同时也是一个安全资源的运营平台，在分发安全资源同时，提供了强大的运营管理功能，管理员通过运营分析能够对安全服务运营情况了如指掌，不仅可以了解每个月的营收和各安全服务收入情况，还可看到各租户详细的消费情况，从而达到协助管理员合理申请服务资源，针对性制定运营策略，达到精细化运营。

**7. 订单化服务管理**

为了满足云计算“按使用量付费的模式”特性，安全云管平台开发了订单管理系统，以方便用户快捷的开通云安全服务，享受到云计算平台提供的安全服务能力，真正实现了用户自助服务，按需申请，即买即用。

**8. 标准化流程管理**

安全云管平台通过流程化管理，帮助云管理员建立标准的、系统化的云安全服务运营管理流程，保障云服务提供商为云租户提供高效流转、快捷有序的云安全服务。

- 订单服务流程化管理：云租户在线申请订购云安全服务，系统管理员后台在线审批及维护安全服务订单；
- 云安全服务功能流程化管理：云租户在线申请云安全服务功能，系统管理员后台在线审批及维护安全服务；
- 安全云管平台工单运维流程化管理：云租户在线提交工单，系统管理员后台在线解决工单问题；
- 安全云管平台－消息流程化管理：云管理员在线发布消息，云租户实时获取通知。

**9. 归一化标准接口**

安全云管平台不仅支持 OpenStack Neutron 组件定义的 FWaaS、LBaaS、VPNaaS、NAT 标准接口对接安全服务，同时还创新性的拓展了 Neutron 组件支持的安全服务的范围，率先基于 OpenStack 标准定义了更多应用安全服务接口，包括：DDoSaaS、IPSaaS、AVaaS、 SSLVPNaaS、WAFaaS、OAaaS、SCANaaS、DBAaaS，未来还会根据云计算网络安全需求继续更新和扩展新的安全服务接口。通过支持 OpenStack 标准的和扩展的安全服务接口，安全云管平台不仅可以和 H3C 自有的安全产品对接，还可以和第三方安全产品对接，极大地提高了安全云管平台的服务能力和适用场景，同时也可以最大限度保护用户现有投资。

安全云管平台基于 OpenStack 标准提供北向 API 接口，不仅可以和 H3C CloudOS 深度集成，也可以与第三方云平台对接，提供完整的云计算安全防护能力。





## 3.2 新华三云计算架构

### 3.2.1 新华三云计算整体架构

新华三云计算平台以自研的H3C CloudOS云操作系统、H3C CAS虚拟化平台、H3C SecCloud OMP安全云管平台、分布式存储产品为基础，一套体系支撑所有服务，提供完整的云计算平台，具备完善的电信级服务特性、完善的灾备解决方案和完全自主可控的能力。

通过将物理服务器以及网络设备虚拟化成虚拟计算、分布式存储和软件定义网络，并在此基础上提供云数据库、云防火墙、云负载均衡、镜像仓库、大数据、AI 服务，为用户的应用系统提供 IT 基础服务的支撑能力，同时可以和用户现有的账号体系、监控运维系统进行对接。

新华三云计算系统架构（图 3.1）主要分为：

- 基础设施层：主要包括用于云计算的物理机房、服务器、网络等硬件设施。
- 虚拟化层：基于新华三自研的虚拟化和云计算管理软件 H3C CAS，满足电信级性能及可靠性要求的虚拟化内核，支持融合交付计算、存储、网络、安全虚拟化资源，包括 CVK 虚拟化内核系统、CVM 虚拟化管理平台。
- 云管理层：为上层应用或服务等提供统一的调度，包括 H3C CloudOS、H3C CIC 云业务管理中心及 H3C SecCloud OMP，并提供统一的运营和运维管理入口，通过融合的服务节点管理，对虚拟机和物理机提供统一管理和运维，实现云服务客户对安全资源的按需申请、直接纳管、集中管理等。
- 云服务与接口层：通过开放的 API 平台，统一接口并支持定制化开发。
- 全栈的安全支撑、可靠性和业务持续性的保障（H3C CloudOS 安全组和 H3C SecCloud OMP）。

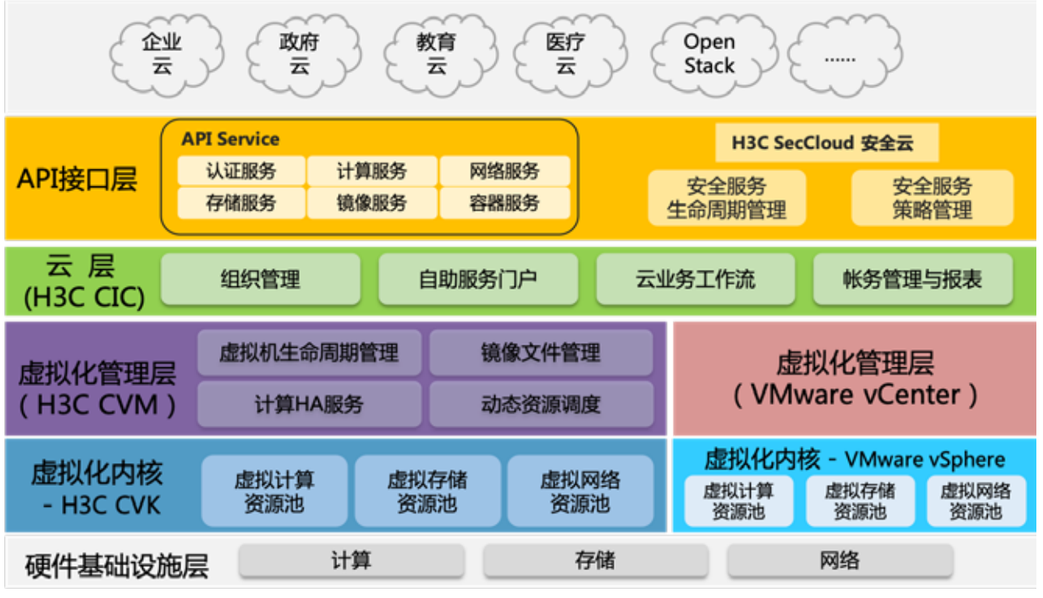



图 3.1 新华三云计算平台基础架构

### 3.2.2 新华三云计算网络基础架构

基于“云网安一体化”的建设思路，打造具备完善安全能力云平台的理念，新华三云计算组网将基础硬件设备与云平台、SDN 控制器、虚拟化平台等深度融合，同时结合实际业务提供智能化运维和场景化运营等视角，并在云平台上呈现唯一用户接口，灵活、高效，实现云安全的整体交付。新华三云计算平台网络架构定义了互联网接入区、业务服务区、安全管理区域、安全资源池四个逻辑区域：

互联网接入区：业务服务区的外延网络，提供用户管理、用户自有网络、互联网访问云计算网络的通道。

业务服务区：该区域提供所有云业务的网络承载，各个云服务客户业务系统的内部流量交互在该区域内完成，此部分是新华三云计算网络的核心必选区域。

安全管理区域：新华三云计算管理流量与业务流量分离，单独划分独立的管理网络，部署各类平台管理软件和安全管理产品。

安全资源池区：该区域包括安全防护资源池和安全检测资源池。

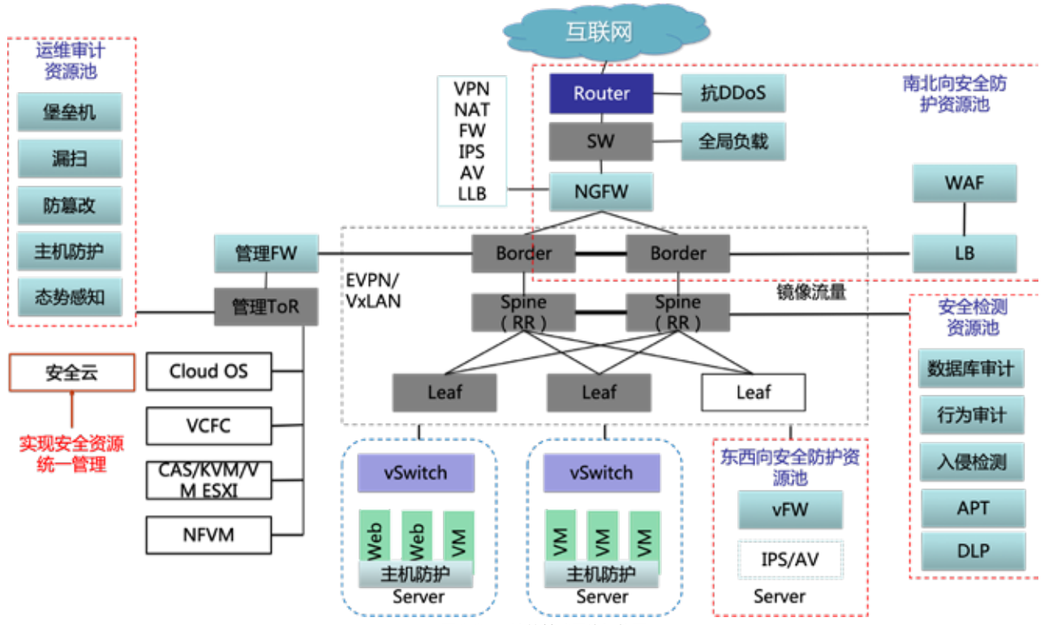



图 3.2 云计算基础网络拓扑图

H3C SecCloud OMP 云安全管理平台是云管理平台的扩展组件，可直接部署于云管理平台环境中，实现云管理平台对安全资源纳管能力的扩展。通过安全云组件可对租户的安全能力进行按需分配和策略管理，同时安全云还可以结合高效运维，智能运营等业务场景，帮助用户全方位的掌控云内安全情况。配备安全防护资源池、安全检查资源池、安全管理资源池等多种资源池，可以为业务云平台提供安全服务。安全防护资源池主要有中高端硬件防火墙和负载均衡设备形成硬件虚拟化资源池，以及硬件或 NFV 形态的 Web 应用防护产品形成 WAF 资源池提供南北向的安全防护和东西向的防护。安全检测资源池：以 NFV 形态为主的数据库审计、数据防泄漏系统、流量分析引擎、APT 产品组成深度检测资源池，提供应用及数据安全的防护。安全管理资源池主要包含主机加固、漏洞扫描、堡垒机、综合审计等，以软件或 NFV 形态提供服务，与业务云的管理网对接，实现虚拟主机的安全加固、防护以及全网安全管理。

**1. 安全管理资源池**

1）安全运维审计

基于云平台的内部管理机制存在的风险、管理员权限没有约束机制，存在内部人员越权看数据、偷数据、毁数据的风险，方案设计在核心交换层面，以硬件设备或平台组件的形式，提供运维安全管控系统，通过引入基于 4A 认证机制的运维安全建设体系，做到从内部控制、规范运维流程，划分来自平台运维人员、第三方厂商运维人员的访问管理权限，提高对运维人员的行为审计力度与精细程度，对于重要数据和服务需要有双人共管、二次授权等访问模式，避免由于部分设备认证方式弱、安全审计不足等风险引起的运维安全风险。运维安全管控系统解决方案如图 3.3 所示。运维安全管控系统部署在提供运维服务设备的访问路径上，通过路由器或者交换机的访问控制策略限定只能由其直接访问设备的远程维护端口（如果采用平台组件形式：通过引流方式将运维人员对各类 IT 资产的管理流量牵引至云平台的运维审计组件中）。运维人员进行运维工作时，首先以 WEB 方式登录运维管理员管控系统，然后通过系统展现的运维访问资源列表。

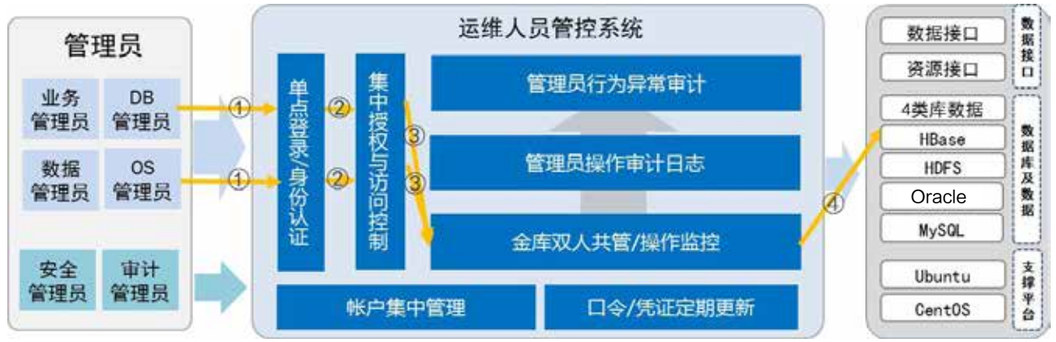



图 3.3 运维安全管控模块设计

2）脆弱性管理

通过漏洞扫描系统，实现各业务系统或主机脆弱性的统一管理。漏洞扫描主要包括系统漏扫、web 漏扫和数据库漏扫，其中 web 漏扫主要面向对 web 服务器漏洞进行发现和扫描，系统漏扫和数据库漏扫主要针对内部服务器区的重要应用和数据库进行安全检查与风险评估。

3）主机安全防护

部署主机加固系统，同时在业务云虚拟主机上安装管理插件。实现主机级的安全防护，进而进行东西向流量的安全管控。具体实现如下功能：

主机级入侵检测：增加主机侧检测维度，填补仅流量检测的空白，主机层面与流量层面的联合监控，高精准，低误报；将检测的点覆盖到每一台服务器，由点到面展开，可有效检测内部横向蔓延；自内而外基于真实环境的恶意行为检测，比沙箱检测更有效。

主机侧风险感知：主机安全解决方案会主动、持续性地监控所有主机上的软件漏洞、弱密码、应用风险、资产暴露性风险等，并结合资产的重要程度进行风险分析，准确定位最急需处理的风险。为决策者动态展示主机安全指标变化、安全走势分析，使安全状况的改进清晰可衡量；为安全运维人员实时展示风险分析结果、风险处理进度，提供专业可视化的风险分析报告，使安全管理人员的工作价值得到可视化呈现。主机安全解决方案将视角从了解黑客的攻击方式，转化成对内在指标的持续监控和分析，无论多么高级的黑客其攻击行为都会触发内部的异常变化，从而被迅速发现并处理。

主机安全基线：主机安全基线管理解决方案通过自动化检查，节省传统的手动单点安全配置检查的时间，并避免传统人工检查方式所带来的失误风险，同时能够出具详细的检测报告。支持自定义基线配置，可灵活添加系统基线或应用基线；支持基线一键检测可用于等级保护等合规性检查：在等级保护检查、测评、整改工作过程中，对服务器系统进行对应级别的安全风险检查是运营人员的必要工作。新华三专家对国家等级保护规范进行了细化整理，把相关技术要求落实到合规基线（等保合规）模块中，可进行对应级别的安全配置检查，对合规情况进行等保符合性报告，保证系统建设符合等保要求、促使等保监督检查工作高效执行。

资产清点：通过安装 Agent 从正在运行的环境中，反向自动化构建主机业务资产结构，上报中央管控平台，集中统一管理；独特的主机发现系统，随时发现网络环境内没有纳入安全保护的主机，确保安全覆盖无死角。系统将保持对资产持续监控，保证监控数据与实际业务数据一致。一些需要特殊关注的敏感资产（如：账号、进程、端口，数据库，Web 站点等）发生变化时，将提供实时或定时通知，实现资产动态保护和通用安全检查规范与安全事件的数据需求，形成细粒度资产清点体系，利用多维度的视图，引导用户轻松获得需要的资产信息，借助多角度的搜索工具，帮助用户快速定位关键资产信息。

恶意文件检测：僵木蠕的感染与传播过程往往依赖于对业务主机的漏洞利用，主机安全僵木蠕检测系统通过安全补丁，漏洞检测等功能实现补丁漏洞管理，降低业务主机感染僵木蠕的可能性。同时，入侵检测产品针对网络内部的僵尸、木马、蠕虫等攻击行为进行有效检测和告警。对僵尸进程、webshell、系统后门进行监测，并通过各种渠道收集到新型攻击样本，如 2009 年的特种木马，将规则融入到入侵检测系统。通过特征、沙箱，正则等不同技术手段发现恶意进程和文件。动态蜜罐功能通过开放钓鱼端口，对全网攻击事件、内网渗透扫描进行发现预警。

与传统的被动扫描相比，主机层面的检测是主动的监控进程创建行为。再通过主机级别威胁情报联动，文件、dns、ip 多维度关联，能通过威胁情报直接定位恶意进程，使得查杀更加快捷有效。

4）态势感知系统

a) 安全事件分析

- 基于策略的事件分析

系统可为用户在进行安全事件的实时分析和历史分析的时候提供基于策略的安全事件分析过程。用户可以通过事件分析策略对全网的安全事件进行全方位、多视角、大跨度、细粒度的实时监测、统计分析、查询、调查、追溯、地图定位、可视化分析展示。

- 事件关联分析

系统支持建立单事件规则和多事件规则，实现单事件关联和多事件关联，单事件关联：通过单事件关联，系统可以对符合单一规则的事件流进行规则匹配；多事件关联：通过多事件关联，系统可以对符合多个规则（称作组合规则）的事件流进行复杂事件规则匹配。实时关联和历史关联，实时关联：对当前正在发生的事件进行规则关联分析；历史关联：对已经发生的事件进行规则关联分析。

- 流安全分析

系统的智能化流安全分析主要体现在以下几个方面：

流分布可视化分析：通过对流信息的统计分析，以可视化的方式展示特定网络访问关系下的流量信息，譬如重要业务系统或者服务器的进出流量、各协议流量分布和流量趋势，以及重要资产的业务流量可视化等等。

流行为轮廓建模：借助创新的 vFlow 流描述语言，采用基于行为的分析算法，对流信息建立行为轮廓模型，为后续的流行为合规分析和异常检测奠定基础。

流行为合规性分析：系统采用基于黑白灰规则集的模式进行流行为合规性分析，帮助用户识别违规流行为。流行为可以看作网络中 IP/ 业务系统 / 安全域之间，一段时间内的相互网络连接关系的集合。流行为合规分析就是判定网络节点间的连接关系（包括端点 IP/ 端口、时间、协议、流量等）是否合规。

流行为异常检测：通过对流行为轮廓的分析，有助于实现对未知攻击行为的辅助研判。系统可以帮助用户识别网络中的异常行为，例如在一台应用服务器上发现 FTP 服务且有大量数据外传、某台 HTTP 服务器的 404 错误骤增、来自罕见源地址的访问、罕见的访问协议、超量的 SSH2 数据外传、隐藏 IP 使用，等等。此外，通过对海量的、大时间跨度的流信息进行数据挖掘分析，还可以帮助感知未知安全威胁。





流与安全事件的协同分析：通过将流安全分析技术与安全事件分析技术有机地整合到一起，系统能够实现从关联告警事件到原始事件的钻取，再到原始事件发生时段的原始流信息的回溯分析，甚至到原始包数据的回溯，譬如僵尸网络心跳连接、DNS 异常，等等。

b) 安全事件展示

通过各类引擎将全网镜像复制的流量进行统一汇总和分析后，各检测引擎将检测结果发送到态势感知平台进行各类事件的汇总和分析，并统一进行结果展示。在本次项目中，态势感知可为云平台的安全管理提供如下功能：

- 风险情报管理

对来自于网络、安全、操作系统、数据库、存储等设施的安全信息与事件进行分析，采用数据挖掘技术，发现隐藏的安全问题，使安全运维人员有效聚焦安全威胁，通过丰富的分析报表全方位检视网内安全状况，通过信息丰富的定位溯源，为业务风险管理及安全响应控制提供有效支持。

- 安全资源管控

可针对下一代防火墙、IPS、负载均衡等网络设备实现应用安全风险的精细化管理，同时支持实时风险联动策略，能够根据预先制定的策略快速自动响应，使管理员能够轻松应对突发安全事件，保障业务系统安全运行

- 业务风险可视化

通过业务建模，形成对在网业务的健康度、繁忙度、风险的立体监控；

整网安全态势实时监控，动态展示最新发生的攻击行为，提供业务风险雷达，将各个业务面临的风险状况实时展现；

提供端到端攻击路径拓扑展示，结合详细的上下文信息实现攻击溯源，协助管理员做出有效管控措施。

c) 安全资产维护

支持新增、修改、删除、导出资产类型。资产类型支持树状结构，增加资产类型时，可以指定父类型、资产类型名称、编号、缺省值等信息。

支持服务器、网络、安全、应用等类型资产的信息录入和维护，资产信息包含服务器的位置、序列号、软硬件版本、维保信息、联系人等。

在手工增加或者自动发现网络设备的时候，将自动创建资产信息。

d) 应用状态监控

监视各类应用的性能和可用性相关的关键指标，比如，针对 Oracle 数据库，支持查询端口状态、数据库版本、可用性等等监控内容。

应用监控是作为安全监控的辅助，可以提供应用健康状态的监控，如健康状态欠佳，则可以查看根因。有别于 IT 运维管理，安全管理中对应用的监控是重在与安全风险的关系上：监控数据除了可关联到业务风险监控中，也可用于事件级的关联分析计算（即关联分析中的资产状态关联）。

具体支持的应用类型包括：

- Windows 服务器
- Unix 服务器（AIX、Solaris、MacOS、HP-UX、FreeBSD 等）
- Linux 服务器（Redhat、CentOS、Suse 等）

- 数据库（Oracle、MS-SQL、MYSQL、Sybase、DB2、PostgreSQL、Informix、达梦数据库等）
- 应用服务器（.Net、Jboss、Tomcat、WebLogic、WebSphere、GlassFish、Jetty）
- Web 服务器（Apache、IIS 等）
- 邮件服务器（Exchange 等）
- 中间件（Office SharePoint、WebSphere MQ、Active MQ、Tonglink/Q）
- Lotus Domino、LDAP、SAP、Lync
- 虚拟化软件（VMware、Hyper-V、KVM、Xen）

e) 实时攻击分析

- 实时威胁监控

动态展示最新发生的攻击事件以及攻击行为，并统计攻击源、攻击目的 TOP N 信息。通过该页面使企业面临的攻击威胁状况得以可视化展示，便于采取相应动作来削弱企业所面临的风险。

- 整网安全态势实时监控

列出整网安全评分，最近一小时内的攻击状态，提供针对攻击目的 IP、攻击源 IP、攻击协议、安全威胁整体趋势等信息。同时提供业务风险雷达，将各个业务面临的风险状况在雷达中体现出来。整网安全态势实时监控用来帮助管理员直观地了解到网内最新的安全状况，及时采取必要的行动。

- 实时事件列表

实时事件列表列出了最近一小时内的攻击事件，详细展示了最近一小时内的攻击事件，详细给出了事件包含的具体内容，包括日志级别、时间、源 IP/ 用户、目的 IP/ 用户、协议、攻击类型、事件数和设备名称。同时，提供了基于设备名称、协议、源用户、源 IP、目的用户、目的 IP 的查询条件，方便管理员快速的查询到需要的攻击事件信息。另外，该页面支持自动刷新功能，实时地刷新页面，管理员可以根据需要设置页面刷新的时间间隔。

- 攻击拓扑溯源

基于强大的拓扑引擎，计算攻击源到目的端到端路径，对攻击进行网络路径角度的可视化呈现，管理员可参考并实施针对性管理动作（为确保展现效果，相应设备应加入到管理中）。该功能用来协助操作员作出判断，可以对攻击源进行下线、走工单流程等处理动作，也可以参考着变更安全规则的部署。

**2. 安全防护资源池**

1）南北向访问控制与网络隔离

在云计算平台边界进行多层防御，采用防火墙硬件设备实现服务器区和网络接入区域的边界隔离，以帮助保护网络边界面临的外部攻击；在区域边界，只允许被授权的服务和协议传输，未经授权的数据包将被自动丢弃，依据最小化访问控制权限为原则，实现边界隔离和来自边界以外的流量访问控制，安全策略设计主要包括以下内容：

- 控制网络流量和边界，使用标准的网络 ACL 技术对网络进行隔离；
- 网络 ACL 策略的管理包括变更管理、同行业审计和自动测试；
- 通过自定义的前端服务器定向所有外部流量的路由，可帮助检测和禁止恶意的请求。

2）网络入侵防御





依托平台内的硬件防火墙和虚拟防火墙组件，实现对南北向、东西向网络入侵事件的检测，并通过与访问控制策略与流量控制策略联动，实现符合国家规定的安全检测机制，实现网络层面上针对平台业务区的自动入侵防御和分析，提高系统整体安全性。

通过监控网络中存在的现象来判定网络是否存在异常，如果存在异常则及时报警。采用的是自主智能学习模式的方式，是一种检测未知威胁的新型技术，通过不断收集历史流量数据，建立流量和行为模型的一种“动态检测”技术，有别于基于特征检测的防火墙只能检测到库文件中已有威胁的“静态检测”。

网络入侵防御模块内置统计智能学习算法，对新建连接数、并发连接数、流量等数据智能学习；监控对象包括：源 IP、目的 IP，地址对象支持主机地址、子网地址、范围地址等。对新型威胁做出判断和预警，在其发生破坏之前阻断或者控制它。异常行为分析技术的出现可以很好地弥补这一“传统设备”的缺陷，对阻断和防范新型威胁发生有效的作用。云平台的网络防病毒与云主机的防病毒软件不同，主要是用来分析由外部进入网络的数据包，对其中的恶意代码进行查杀，使得病毒在未感染到云主机时，就可以过滤掉这些攻击数据包，从而防止病毒在网络及云平台内部传播。

云平台的防火墙系统建设中，内置防病毒模块，可以从流量上对 SMTP、POP3、IMAP、HTTP 和 FTP 等应用协议进行病毒扫描和过滤，并同恶意代码特征库进行匹配，对符合规则的病毒、木马、蠕虫以及移动代码进行过滤、清除或隔离，拦截在云平台的处理区域之外。

3）攻击防护

云攻击目前主要是指利用云平台通过虚拟化技术定义出的网络、操作系统、应用存在的漏洞和安全缺陷对网络资源的硬件、软件及其系统中的数据进行的攻击，通过边界的硬件防火墙及平台内部的虚拟防火墙组件，可构建的防攻击能力：

- 非法报文攻击及统计型报文攻击；
- 基于 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议的 DDOS 攻击防护；
- 内置 11 大类，超过 4000 条入侵防御实时规则库并支持自定义规则、规则集；
- 支持根据威胁事件、攻击来源、受威胁主机查询攻击；

4）VPN 远程安全访问

云平台的通信安全应部署 VPN 服务，以便和远程接入设备建立安全连接，建立加密通道保障通信过程中的数据安全，并建立身份验证机制，实现接入认证。

5）安全应用交付

随着云平台内各业务系统规模变大，各部门资源信息的整合，来自于公共侧的访问压力越来越大，需要云平台内部各业务区具备一定的高并发、高业务连续性的应用交付能力。在如今越来越大的访问压力下，关键业务交付能力迟迟无法同步提升。同时，多运营商链路接入问题，也是作为平台业务系统无法顺利交付应用服务的主要原因。

因此，本方案设计采用基于智能 DNS 的多运营商链路接入设计，通过链路负载均衡，实现提供足够的网络带宽并且充分利用互联网带宽资源，保障各业务系统用户访问的高效性和可靠性。同时，在云管理平台部署负载均衡和应用交付组件，实现来自于对各业务区应用负载均衡服务的弹性扩展和动态调配。

主要实现目标具体如下：

- 保证 WEB 网站不间断服务，保证应用的可靠性；
- 通过负载均衡设备，把访问 web 服务器的流量转发到多台应用服务器上，对流量进行合理优化，减少单点故障的问题，提高系统效率；

● 通过链路负载均衡，保证各业务系统用户能够快速访问互联网查询资料；

● 提供有效的健康检查机制，可以及时发现有问题的应用服务器，并及时屏蔽流量，当有问题的应用服务器恢复正常时，可以自动重新对请求进行响应。

6）Web 应用防护

部署 web 应用防火墙，提供 web 应用安全防护能力，防止 web 服务攻击。主要针对 Web 服务器进行 HTTP/HTTPS 流量分析，防护以 Web 应用程序漏洞为目标的攻击，并针对 Web 应用访问各方面进行优化，以提高 Web 或网络协议应用的可用性、性能和安全性，确保 Web 业务应用能够快速、安全、可靠地交付。

7）东西向访问控制与网络隔离

通过防火墙与 SDN 控制器的深度融合，形成东西向安全服务链，可对 VPC 内部业务进行区域划分和网络隔离，同时东西向防火墙具备入侵检测和病毒检测的功能，对东西向业务流量进行安全防护。

**3. 安全检测资源池**

1）安全流量采集

基于安全检测需求，配置高性能的 TAP 产品对重要的网络节点镜像的流量进行采集和复制，同时针对多个万兆的入向流量进行 HASH 分流，把流量均衡分散到多个出接口，转发送入后台的各类安全引擎，维持同源同宿，保证用户数据和会话的完整性。通过五元组过滤规则以及特征码过滤规则对某项业务流量或协议进行数据包的过滤和多重复制，分发到不同的安全检测引擎当中。

2）数据库安全审计

数据库审计系统通过全面记录对数据库服务器的连接情况，记录会话相关的各种信息和原始 SQL 语句。如：来源计算机名称、IP 地址、MAC 地址、端口号、日期时间、通信量大小以及违规数量，从而支持一切对数据库的访问协议的审计。其中包括标准 TCP/IP 协议、本地环回 TCP/IP 协议、通过 SSH、TELNET 远程连接数据库进行的数据库操作。

通过设计审计系统开启双向审计的功能，不仅可以审计应用服务器对数据库服务器的访问流量，对数据库服务器针对于应用服务器的访问返回的结果也能进行审计，比如“select * from a;”，若表 a 不存在，则会审计到数据库返回错误的信息，若表 a 存在，则可审计到查询表具体的条目数。

通过数据库审计系统提供实时的事前 + 事中 + 事后的连接监控功能，能够实时的监控所有到数据库的连接情况。监控信息包括连接建立时间、IP、各业务系统用户名、非法操作（越权访问等）次数统计。而对于非法连接或有非法行为的连接，管理员可以立即断开指定的可疑连接。确保数据库安全性不受进一步威胁。

数据库安全审计可以对不同的风险设置不同的风险报警方案，同时可以针对不同风险、新 SQL、访问规则违规、数据库服务器状态异常、审计系统服务器状态异常、缓冲区溢出攻击、SQL 注入攻击等报警，报警方式有：短信、邮件、FTP、SYSLOG、SNMP 等报警方式。

3）数据泄漏防护

以深度内容识别技术为核心，提供完整的数据防泄漏防护，全面保障云平台在数据传输和使用过程中，发现并监控敏感数据，确保敏感数据的合规使用，防止主动或意外的数据泄漏。并通过对敏感数据的使用行为、安全事件、策略执行记录等内容的审计分析，为数据安全管理工作提供技术支持。达到敏感数据利用的事前、事中、事后完整保护，实现数据的合规使用，同时检测主动或意外的数据泄漏，保障单位数据资产可控、可信、可充分利用。

4）未知威胁检测





未知威胁检测系统利用大数据技术结合威胁情报针对高级威胁攻击进行检测，通过建立本地重点流量采集、存储、分析平台，结合云端威胁情报，全面监测单位发生高级威胁事件，并对未知攻击事件进行溯源。利用威胁情报，能够对网络中的威胁事件进行发现和告警，可从威胁事件视图、受害主机视图、受害服务器视图或受害用户视图的角度分别展示高级威胁攻击态势，对整体攻击有全面性的认识。同时，针对高级威胁事件可以展示威胁发生时间、攻击类型、受害 IP、攻击 IP、资产状态、攻击组织、威胁等级等信息。支持对 DNS 异常行为分析、SSL 通信异常、web 行为异常、ARP 行为异常等感知；深度木马网络回连行为报警、特种木马网络通联行为报警、未知病毒与木马心跳挖掘、时间行为异常分析、内外通联行为异常分析等。支持从 IP 或攻击组织的维度对高级威胁事件进行快速检索，能够支持查看高级威胁告警的攻击详情。基于态势感知，利用数据追溯功能对发现的未知攻击进行溯源包括攻击来源、攻击过程以及攻击手段等进行分析，对攻击目标、攻击目的、影响范围等形成报告。

5）流量分析引擎

依据方案设计，针对云平台网络访问应具备透明化，对访问云数据中心的行为进行细粒度的审计，包含应用访问、流量分析、共享协议、高危行为等，可以及时掌握到云数据中心的使用情况，形成用户行为画像。

### 3.2.3 新华三云计算安全架构

**1. H3C SecCloud OMP 安全云管理平台基础架构**

新华三云计算平台组件 H3C SecCloud OMP 安全云管理平台基于 OpenStack 架构，定义各类标准安全服务，并关联 OpenStack 所标识的租户边界”网关”节点，实现租户流量的牵引与安全能力编排，同时，针对第三方安全控制器及安全设备也可通过标准接口进行适配，纳入到云计算的安全能力体系中。通过对认证模块的调用及虚拟机列表的读取，完成云管理平台到云计算的平滑单点登录及对象操作，重新定义面向数字化转型的安全能力。云计算通过实现安全资源抽象、统一逻辑配置，将安全能力按需分配，使原本碎片化的安全能力集中管理，提供基础设施、边界和云业务的一体化安全能力集合。

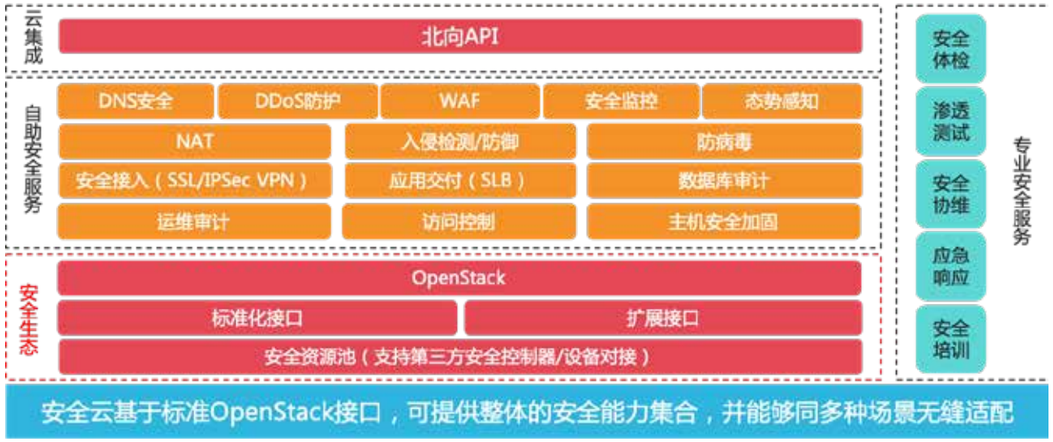



图 3.4 新华三云计算平台安全架构

H3C SecCloud OMP 从逻辑控制层的角度出发，屏蔽底层技术细节，将各类安全能力从单纯的产品配置转变为服务化配置，将繁琐的安全业务重新进行定义，从用户业务的角度出发，抽象为必要的实现逻辑。新华三云计算可提供包括监测服务、清洗服务、态势感知服务、云代维服务等四大类服务，并且还将进一步推出新的服务类型；同时提供丰富的安全服务目录。

**2. 防护类安全能力架构**

防护类安全设备采用硬件资源池的方式进行部署，虚拟化微服务通过 Docker 方式部署，Docker 之间通过开放 API 接口进行通信，能够使每个租户独享安全能力。每个 Docker 具备有独立的日志发送、独立的策略配置、独立的硬件资源，即使在单独重启后也不互相干扰。防护类安全能力通过同租户在 OpenStack 架构中的网关（OpenStack 称之为“路由器”）关联，保证业务流量能够对应到租户专属的安全能力。

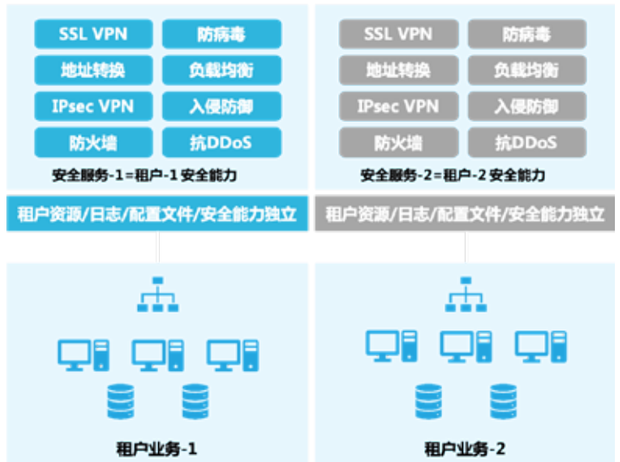



图 3.5　防护类安全能力架构

### 3. 检测类安全能力架构

检测类能力采用基于租户标签的流量分发方式，实现对不同租户的独立审计及检测。在云架构中，可以采用 VLAN 或 VxLAN 的方式为不同的租户划分独立的 VPC。检测类能力需要根据不同的 VPC，将流量对应到不同的检测设备上。通过汇聚分流平台将镜像流量进行 M:N 的复制分发和智能过滤，一次性接收云架构内的全部流量，随后，基于标签实现不同租户的流量分发。最后，将检测结果反馈到多租户模式下的态势感知平台上，针对每个租户进行呈现。在此架构下，不需要检测类设备支持虚拟化技术部署，就可以使安全检测能力得到弹性化扩展，同时不改变网络架构或增加流量镜像的配置，就可以使每个租户拥有专享的安全威胁展示空间。

### 4. 审计类安全能力架构

如何实现租户内的日志审计，包括操作运维日志的审计以及业务系统的集中审计是《信息安全技术 网络安全等级保护基本要求》中所强调的技术重点。传统技术无法对租户的日志进行区分，采用物理设备的审计技术，也不能保证各个租户间的审计独立性，存在较大的合规风险。在云计算审计架构中，提供虚拟带外管理网，与业务网段完全分开，专门用于运维操作登录以及业务系统日志的收集。业务网段通过访问控制策略的配置，不允许进行运维操作，如 Telnet，SSH，管理网段的 HTTP/HTTPS 连接。

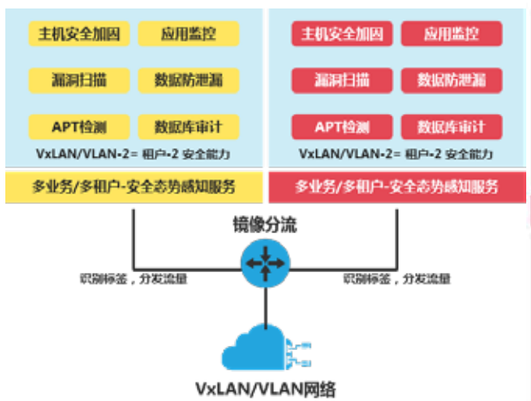



图 3.6　检测类安全能力架构

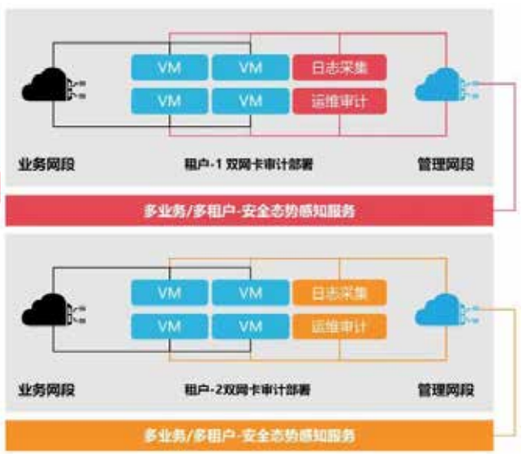



图 3.7　审计类安全能力架构

## 3.3　新华三云计算安全技术能力

### 3.3.1　新华三云计算安全能力

新华三云计算安全架构如图 3.8 所示，主要包括了物理安全，硬件安全，虚拟化安全、多租户安全、云产品自身安全五个重要组成部分。其中物理安全由 IDC 运营方保障。

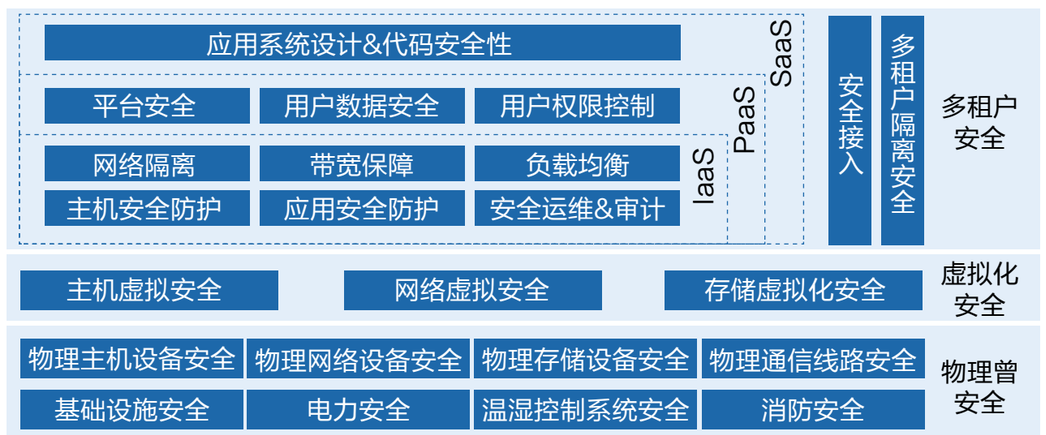



图 3.8　新华三安全云安全架构图

### 1. 物理层安全

云计算面临的物理层安全风险与传统数据中心基本相同，物理层安全主要是指由于网络、计算、存储等设备故障的原因造成所承载的应用不可用的问题。问题产生的原因主要包括自然灾害、电磁辐射、三防（防火、防水、防尘）及人为破坏等方面，通过下列防范措施可以避免物理层的伤害：抗干扰系统、物理隔离、防辐射系统、供电系统的冗余设计和可靠性备份等。

### 2. 硬件安全

安全集群框架高可靠性技术通过将两台设备虚拟化为一台逻辑设备，实现了管理和控制上的统一，同时组网部署更加简单，有效利用链路带宽，提高系统稳定性，大幅减少故障点带来的业务切换冲击。

为解决传统双机备份“故障出发点多”及“切换粒度粗”带来的业务冲击及性能损失问题，安全集群架构引入了引擎级备份技术。引擎级备份技术通过将主机进行安全集群，对外通过跨设备链路捆绑或者提供等价路由节点进行互联，有效利用链路带宽。对内在业务引擎之间实现备份，从而将主控、接口和业务引擎的故障解耦，可以最大程度地减少各节点故障带来的业务冲击。单台物理设备受限于自身 CPU 处理能力、内存容量、硬件槽位等多方面因素，整体处理能力存在上限。传统 IT 部署模式下，为了满足未来三到五年的业务流量需求，通常会购买远超实际需求的高端设备，导致资源利用率低下和投资浪费。安全集群架构基于 Scale-out 弹性扩展方式实现多台机框的集群，实现系统性能的弹性增长。同时支持异构集群，可以将两台不同性能的设备进行集群，便于企业按需采购和部署，保护投资。多框集群的另外一个应用场景就是双活数据中心，通过跨数据中心部署多设备集群，并且在跨数据中心的两台设备之间开启会话备份，实现业务故障、业务迁移、数据中心故障等多种场景下的可靠性。

### 3. 虚拟化资源层安全

虚拟化是现阶段云计算数据中心实施最为广泛的技术之一，基于服务器的虚拟化技术可以将单台物理服务器虚拟出多台虚拟机，从而有效提升服务器自身的利用率。但是虚拟化技术也带来了一些安全风险，比较典型的有基于虚拟化所衍生的一些安全漏洞，以及针对 VM-VM 虚拟机流量交换的安全问题。

虚拟化应用程序（hypervisor、虚拟化管理软件）本身可能存在的安全漏洞将影响到整个物理主机的安全。攻击者在利用漏洞入侵到主机系统之后，可以对整个主机上的虚拟机进行任意的配置破坏，从而导致系统不可用，或者窃取相关数据。如果攻击者侵入了虚拟机管理程序，则会直接影响到其管理的全部虚拟机的安全。

在虚拟化环境下，单台物理服务器上的各虚拟机之间可能存在二层流量交换，而这部分流量对于管理员来说是不可见的。在这种情况下，管理员需要判断 VM 虚拟机之间的访问是否符合预定的安全策略，或者需要考虑如何设置策略以便实现对 VM 之间流量的访问控制。

针对虚拟化的资源安全防护手段主要从两个方面入手，一方面通过漏洞扫描设备周期性的扫描主机及操作系统存在的漏洞，从而进行相应的安全调整加固；另一方面，通过在网络中部署东西向安全资源池，通过服务链技术把流量引出来引到安全资源池中进行安全防护。

新华三安全云虚拟化架构采用基于容器的虚拟化方案，是一种轻量级的虚拟化技术，在一个安全引擎内，通过唯一的 OS 内核对系统硬件资源进行管理，每个虚拟防火墙作为一个容器实例运行在同一个内核之上。

采用容器化技术，虚拟防火墙有独立的进程上下文运行空间，容器与容器之间的运行空间完全隔离，天然具备了虚拟化特性。攻击者无法从一个虚拟墙进入另一个虚拟墙或者获取另一个虚拟墙的数据。相比传统的 VRF 隔离，具有更好的数据安全性。在一个容器中，运行了完整的防火墙业务系统（包括管理平面、控制平面、数据平面），从功能角度看虚拟化后的系统和非虚拟化系统的功能是一致的（整机重启、存储格式化、集群配置等全局系统配置只能由系统管理执行）。同时进程空间的隔离实现了虚拟墙的故障隔离。

另外，由于多个虚拟墙共享统一的 OS 内核，可以从调度入口灵活分配每个虚拟墙的处理能力比如吞吐、并发、新建等，也可以在线动态地增加资源。最后，基于容器的虚拟化实现在容器中并不需要运行完整的操作系统，减少了由于完全虚拟化带来的内存开销，每个 VFW 可以直接通过内核和物理硬件交互，避免了和虚拟设备交互代理的性能损耗，所以可以支持更多的虚拟防火墙实例，而不会对系统性能造成实质影响。

**4．多租户安全**

多租户环境下的基础安全服务主要体现在 IaaS 服务层。IaaS 作为云计算的重要组成部分，其将基础设施包括网络、存储、计算等资源进行虚拟化等处理，能够为每个用户提供相对独立的服务器计算资源、存储资源以及在承载网上设定专有的数据转发通道。

在云安全平台的建设过程中，基于 IaaS 模型下的各种安全服务体系的建设是重点所在，根据现阶段的需求来看，这部分服务主要包括针对云计算防火墙服务、云计算负载均衡业务。不同的租户可以根据自身的业务需求，合理的选择部署云安全防火墙服务或者是防火墙叠加负载均衡业务。部署该安全服务后，每个租户可以获得逻辑上完全属于自己的防火墙和负载均衡。租户可以根据自身需求，设定自身的各种安全防护策略，生成自身独有的安全日志分析报告。同时对于部分需要负载均衡的业务，也可以设置独立的负载均衡的算法，以保证业务的可靠性运行。当然，考虑到应用层的安全风险一直是互联网的重点防护对象之一，各种基于 web 应用层的安全攻击会导致用户业务系统的权限被窃取以及关键数据的泄露，也可以考虑增加一些新的诸如 WAF、IPS 入侵检测等增值服务，用户可以根据自身业务系统的安全级别合理选择是否租用该漏洞防护服务等。

在云安全体系的建设过程中，PaaS 和 SaaS 的安全建设也非常重要。和 IaaS 的建设思路不同，PaaS 的安全建设，其关键在于平台开放的思想下，开发者应用平台及数据库系统对于多开发者数据安全的适配。典型问题包括针对开发者的用户身份认证，开发者的平台和数据库的访问使用权限控制，不同开发者数据的安全隔离、及操作行为审计等内容。为此需要在数据库的开发及平台应用环境开发过程中考虑到上述安全风险的防护。而在 SaaS 模型下，应用系统级的多租户共享涉及到的应用层安全问题，除了多租户身份认证和权限控制及数据库安全隔离等需求外，还需要考虑针对应用环境的代码级的安全审计等问题，确保提供给租户的应用程序本身的安全具备很高的水平，不会轻易被黑客等攻击者利用其内在的各种安全漏洞。





**5．云产品自身安全**

1）H3C CloudOS 安全

● 快速自动化安装部署

H3C CloudOS 云操作系统通过 Openstack 这个中间层对下层的虚拟化软件进行管理，H3C CloudOS 云操作系统并不直接与虚拟化软件进行任何通讯，所有操作都是调用 Openstack 的标准 API 来完成，Openstack 再调用虚拟化软件完成相应的动作。

H3C CloudOS 云操作系统对各种组件和服务进行了重新打包，将其纳入到 H3C CloudOS 云操作系统的统一安装框架中，实现基于 Docker 容器的自动化的安装部署，对用户屏蔽了各种组件安装的复杂性，整个 H3C CloudOS 云操作系统，包括 CentOS 操作系统、Openstack 以及各种组件服务在内，整体可以在 1 小时内部署完成。

实现基于 Docker 容器的自动化的安装部署，将 H3C CloudOS、Openstack 以及各种组件打包在一起，形成一个一体化的可启动安装盘，内置 Cent-OS 操作系统、PostgreSQL 数据库和各种组件服务，因此这些物理服务器不需要预先安装任何操作系统，通过此光盘启动服务器，会自动进入 Cent-OS 操作系统的安装界面，然后按照向导的步骤操作选择安装节点即可安装完成，安装节点完成后选择需要安装的服务，能极大地提高部署效率，减少部署工作量和人为差错。

● 灵活的系统参数设置

H3C CloudOS 云操作系统提供灵活的系统参数设置，通过对业务功能参数、高级特性配置参数等的设置，可以灵活适应不同局点云基础设施的部署情况。

● 灵活的分权分域管理

H3C CloudOS 云操作系统支持多种用户角色和分级的多租户管理，二者结合为用户提供灵活的分权分域管理。

● 多种用户角色

云管理员：负责整个云平台的管理，进行全局资源配置，计费策略、资源规格定义，划分组织和配额，分配组织管理员，统一监控全局资源的使用情况、计费统计、运维健康状态等（Admin 账号是默认的云管理员）；

组织管理员：通过租户服务台操作，可以创建下属组织，为下属组织分配资源配额，创建本组织的普通用户以及下级组织的管理员和普通用户；为本组织申请网络、防火墙等资源；查看组织及下属组织的资源使用状况、费用统计等；

普通用户：通过租户服务台操作，可以申请云主机、云硬盘等资源服务，并对已申请的资源进行监控和管理；可以查看自己的资源使用状况、费用信息等；

审计员：可以查看云平台中审计信息，包括各类管理人员和用户的身份鉴别记录、操作记录、以及访问受保护资源的行为记录等；

自定义权限分组：支持基于上述四种角色，进一步定制用户权限，可以控制到操作菜单粒度；通过自定义权限分组，可以实现定制服务目录。

● 多层次的租户组织结构

H3C CloudOS 云操作系统支持灵活的多租户管理，每个租户对应一个组织，按组织进行资源配额和计费，组织内自主管理（子组织创建、业务审批等），满足政府、企业、高校等用户的复杂分权管理需求。

每个组织有自己独立的资源配额，组织管理员可以自由的创建子组织，为子组织创建组织管理员和用户账号，从组织的配额内划分资源作为子组织的配额。父组织可以统一查看各子组织的资源使用情况和费用统计。

父组织和子组织之间的关系是一种行政从属关系，两者的网络是互相隔离的，各自拥有自己的私有网络。

这种多层次的组织结构非常灵活，实际运用中可以应对各种用户需求。例如用户需要将自己的资源分为测试和生产两个互相隔离的环境，二者互不干扰，但需要统一监控和计费。这时就可以在用户的组织下面，再创建两个子组织，各分配一部分资源，分别用作生产环境和测试环境；两个子组织之间的网络是隔离的，互不干扰；计费可以统一由父组织出口。

● 可自定义的业务审批流程

H3C CloudOS 云操作系统支持多级云服务审批，使用业务流程控制手段，对行为的过程和结果进行有效监管和控制，并在事后提供行为审计的能力。云管理员和组织管理员申请资源是不需要走审批流程的；普通用户申请资源则需要走审批流程进行审批，审批的流程环节可以按用户的需求进行定制，H3C CloudOS 云操作系统支持通过流程设计器定制个性化的流程模板。

2）H3C CAS 安全

H3C CAS 云计算软件将一组服务器主机合并为一个具有共享资源池的集群，并持续对集群内所有的服务器主机与虚拟机运行状况进行检测，一旦某台服务器主机或虚拟机发生故障，H3C CAS HA 软件模块会立即响应并在集群内另一台服务器主机上重启所有受影响的虚拟机。当物理服务器发生硬件故障时，所有运行于该服务器的虚拟机可以自动切换到其它的可用服务器上，相对传统的双机容错方案，H3C CAS HA 可以最大程度减少因硬件故障造成的服务器故障和服务中断时间。不同于其它 HA 的双机热备方式，所有参与 HA 的物理服务器都在运行生产系统，充分利用现有硬件资源。同时，对众多的操作系统和应用程序，H3C CAS 提供统一的 HA 解决方案，避免了针对不同操作系统或者应用，采用不同的 HA 方案带来的额外开销和复杂性。

在虚拟化和云计算环境中，一旦客户将服务器整合到资源较少的物理主机上，虚拟机的资源需求往往会成为意想不到的瓶颈，全部资源需求很有可能超过主机的可用资源。H3C CAS 云计算软件提供的动态负载均衡特性引入一个自动化机制，通过持续地平衡容量，将虚拟机迁移到有更多可用资源的主机上，确保每个虚拟机在任何节点都能及时地调用相应的资源。即便大量运行 SQL Server 的虚拟机，只要开启了动态资源调整功能，就不必再对 CPU 和内存的瓶颈进行一一监测。全自动化的资源分配和负载平衡功能，也可以显著地降低数据中心的成本与运营费用。

H3C CAS 管理台定期（默认 1 分钟）轮询集群内所有的物理服务器主机，对 CPU 和内存等关键计算资源的利用率进行检测，并根据用户自定义的规则来判断是否需要为物理服务器主机在集群内寻找有更多可用资源的主机，以将该主机上的虚拟机迁移到另外一台具有更多合适资源的服务器上，或者将该服务器上其它的虚拟机迁移出去，从而为某个虚拟机腾出更多的“空间”。

● 自动侦测物理服务器和虚拟机失效

H3C CAS 会自动的监测物理服务器和虚拟机的运行状态，如果发现服务器或虚拟机出现故障，会在其它的服务器上重新启动故障机上所有虚拟机，这个过程无需任何人为干预。

● 资源预留

H3C CAS 永远会保证资源池里有足够的资源提供给虚拟机，当物理服务器宕机后，这部分资源可以保证虚拟机能够顺利的重新启动。

● 虚拟机自动重新启动

通过在其它的物理服务器上重新启动虚拟机， HA 可以保护任何应用程序不会因为硬件失效而中断服务。

● 智能选择物理服务器

当与 H3C CAS 动态负载均衡功能共同使用时，H3C CAS HA 可以根据资源的使用情况，为失效物理服务器上的虚拟机选择能获得最佳运行效果的物理服务器。

● 动态资源调整

H3C CAS 云计算软件提供的动态负载均衡特性引入一个自动化机制，通过持续地平衡容量，将虚拟机迁移到有更多可用资源的主机上，确保每个虚拟机在任何节点都能及时地调用相应的资源。

3）服务链技术

H3C SDN 服务链，基于网络的核心控制部件 SDN 控制器——VCFC（Virtual Converged Framework Controller）进行部署。VCFC 根据租户需求，定义、创建服务链，并部署服务链上每个节点的业务逻辑。VCFC 将需要进入服务链处理的用户报文特征，下发到接入软件 / 硬件 VTEP，从而将数据报文引入服务链。

H3C SDN 服务链中具有如下角色：

● 流分类节点 (Classification)：也是原始数据报文的接入节点。按照定义的流分类规则匹配数据报文，对报文做服务链的 Overlay 封装 , 并将其转发到服务链中处理。

● 服务节点（Service Function）：服务节点作为资源被分配使用，它的物理位置可以是任意的，分散的，通过 SDN 对服务链的定义和引流串联，完成预定义的工作。服务节点可以是防火墙（FireWalls）、负载均衡（LoadBalance）、入侵检测（Intrusion Prevention System）等资源 / 资源池。

● 代理节点（Proxy Node）：对于不支持服务链封装的服务节点，需要通过代理节点剥离服务链封装，将业务策略信息转换成 VLAN 等，转交给服务节点处理。

● 控制平面（Control Plane）：负责管理服务链域内的设备，创建服务链，将服务节点的配置定义，下发到各个相关节点上。在 H3C SDN 网络中，通过 VCFC 实现。

服务链的典型示意图：

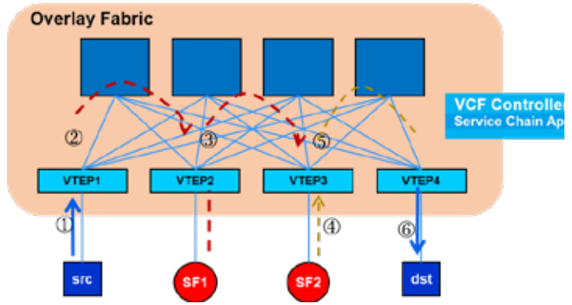



图 3.9 服务链示意图

其中各对应角色及其处理为：

● VCFC：H3C SDN 控制器。作为网络资源池的唯一控制点，VCFC 控制了虚拟化网络，并且通过对虚拟网络进行抽象和编排，定义服务链特征；VTEP 和服务节点上的转发策略都由控制器下发。

● 服务链流分类节点（VTEP1）：原始报文通过 VTEP1 接入 VxLAN 网络，并直接进行流分类，以确定报文是否需要进入服务链：如果需要进入服务链，则将报文做 VxLAN+ 服务链 ID 的封装，转到服务链首节点处理。

● 服务链首节点（SF1）：进行服务处理后，将数据报文继续做服务链封装，交给服务链下一个服务节点。

● 服务链尾节点（SF2）：进行服务处理后，服务链尾节点需要删除服务链封装，将报文做普通 VxLAN 封装，并转发给目的 VTEP。如果 SF2 不具备根据用户报文寻址能力，则需要将用户报文送到网关 (VTEP3)，VTEP3 再查询目的 VTEP 进行转发。

报文转发说明如下：

● ①⑥ Native 以太报文，IP(src)----->IP(dst)
● ② VxLAN+ 业务链报文，外层 : IP(VTEP1)----->IP(SF1)
● ③ VxLAN+ 业务链报文，外层 : IP(SF1)----->IP(SF2)
● ④ VxLAN 报文，外层 : IP(SF2)----->IP(VTEP3)
● ⑤ VxLAN 报文，外层 : IP(VTEP3)----->IP(VTEP4)

具体的匹配转发流程描述如下：

- VM 首包上送控制器处理时，在 VCFC 上解析 packet in 报文，根据报文目的地址确定是虚拟网络内的东西向流量还是通往传统网络的南北向流量，对于南北向流量则将报文转发到网关设备，报文后续的处理由网关设备负责；
- 对于东西向流量，从收到的 packet in 报文中提取源端口，并根据源端口确定源 subnet、network、router 信息；并根据 packet in 报文的目的 IP 获取目的 VM 连接的目的端口，并根据目的端口确定目的 subnet、network、router 信息；
- 对于东西向流量，根据报文特征进行服务链匹配，首先使用源端口和目的端口的属性与服务链配置进行匹配，如果找到匹配的服务链，则下发导流流表；如果没找到匹配的服务链，就下发东西向卸载的流表项（即非服务链转发）；
- 如果存在匹配的服务链，确定服务链所在 VTEP 的 VTEP IP，VCFC 向 VTEP 和后续处理节点下发流表项，流表项格式如下：

• Match：port & vlan & 五元组

普通报文进入服务链或 tunnel & vni & 五元组、VxLAN 报文进入服务链

• Action：vni & service chain id & order counter & tunnel，指向服务链首节点所在的服务节点，order counter =1。

- 当匹配到多条服务链时，按照最精确匹配的原则确定实际使用的服务链配置。上述 4 种维度按照精确程度从低到高排序依次为：Routers, Networks, Subnets, Ports。

4）安全云管理平台

H3C SecCloud 云计算技术在设计之初即包含了灵活、扩展性、成本节约等特性，所有云平台的安全能力亦应该延续这样的理念：安全能力的按需获取，也就是“SecAAS 安全即服务”。租户在建设 vDC 网络时通过我司安全云管理平台，自行选择必要的安全能力，实现细粒度的精准防护。

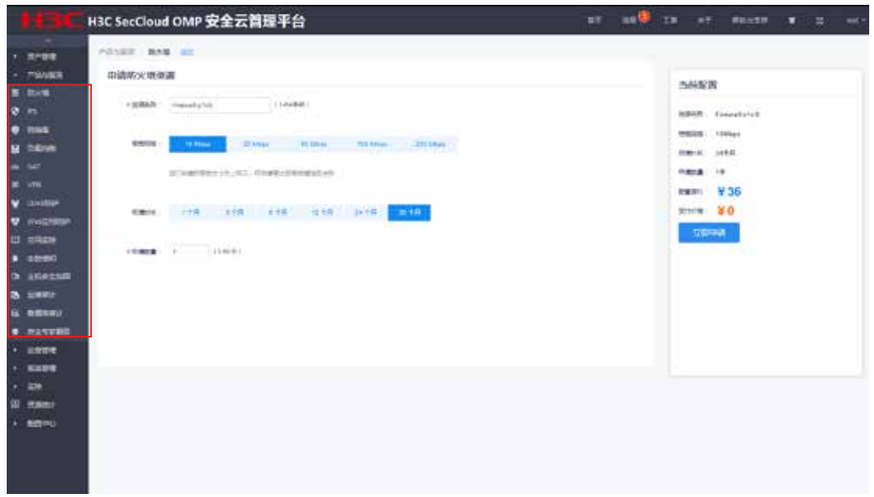



图 3.10　安全云管平台的服务目录

H3C SecCloud OMP 安全云管理平台能够为租户提供丰富的安全服务目录，用户可以根据自身需求定制安全服务列表，包括安全服务类型、服务内容、服务规格、服务周期等内容。安全云系统从用户业务角度出发，屏蔽安全服务底层技术细节，为用户提供简便快捷的配置界面

- SecAAS 安全能力

安全 SaaS 云架构可以提供丰富的安全服务目录，包括但不仅限于如下安全能力：

| 服务项目 | 描述 | 分配方式 |
|---|---|---|
| SSL VPN 服务 | 提供 SSL VPN 远程接入能力 | 每账号 |
| IPsec VPN 服务 | 提供 IPsec VPN 远程接入能力 | 每链路 |
| Web 应用防火墙服务 | 提供 WAF 防护能力，针对 Web 应用进行精细化防护 | 每 DNS |
| 防火墙服务 | VPC 边界，每租户提供独立日志审计 | 每 VPC |
| 入侵防御 / 检测服务 | 提供对恶意代码防护的能力，每租户提供独立日志审计 | 每 VPC |
| 负载均衡服务 | 提供租户内业务的服务器负载均衡能力，包括 4 层和 7 层 | 每 IP 地址 |
| 网络防病毒服务 | 提供租户内网络防病毒能力，每租户提供独立日志审计 | 每 VPC |
| 运维审计服务 | 提供租户内资源的操作审计能力，每租户提供独立日志审计 | 每 VPC |
| 抗 DDoS 服务 | 提供边界出口 DDoS 防护能力，采用检测 + 清洗模式 | 每 IP 地址 |
| 应用监控服务 | 提供对业务应用可用性的监控能力，持续监控与告警 | 每 IP 地址 |
| 漏洞扫描服务 | 提供数据库、Web、业务系统扫描能力，独立输出报告 | 每 IP 地址 |
| 安全态势展示服务 | 提供图形化的界面对现有安全态势进行全局直观展示 | 每 VPC |
| 数据库审计服务 | 提供数据安全审计能力，记录数据操作过程，独立输出报告 | 每 IP 地址 |
| 态势感知服务 | 提供基于日志、流量和状态的智能分析系统 | 每 VPC |

SecAAS 性能规划：H3C SecCloud OMP 云安全管理平台以 32 个 VPC 为一组多虚拟资源单元，整体安全性能网络层以 200G 为最低处理单位，如云安全防护能力需求超过 200G，则需要额外扩容安全 SaaS 云中的安全资源池组件，追加 200G 的性能单位。

- 自动化部署

业务部署编排的自动化，实现端到端的业务自动化部署，当用户创建安全服务时，安全云管理平台会自动分析云环境中各相关组件信息，做到用户侧无感知，仅需要点击开通安全服务，而无需再登陆到各设备上做复杂的配置操作，在设备上自动下发相应的配置，大大加快了部署时间和效率。

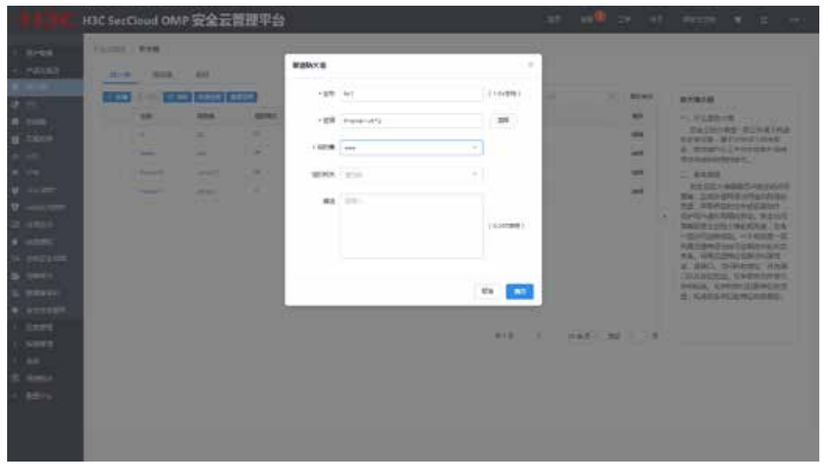



图 3.11　通过安全云管平台部署防火墙

- 智能化运维

为了简化系统运维，提高运维效率，安全云管理平台基于大数据分析系统，从不同角色、不同维度向用户展示云计算网络云安全服务信息，包括服务状态统计、服务资源统计、告警事件统计、用户账户信息、服务费用统计、工单统计、安全态势信息等，并提供各种可视化的操作界面，使得管理员轻松运维管理云计算网络云安全服务，及时清晰掌握云安全服务状况和云计算网络安全态势风险，及时应对各类安全事件。


图 3.12　安全云管平台的运维展示

- 可视化运营

安全云管理平台同时也是一个安全资源的运营平台，在分发安全资源同时，提供了强大的运营管理功能，管理员通过运营分析能够对安全服务运营情况了如指掌，不仅可以了解每个月的营收和各安全服务收入情况，还看到各租户详细的消费情况，从而达到协助管理员合理申请服务资源，针对性制定运营策略，达到精细化运营。


图 3.13　安全云管平台的运营展示

### 3.3.2 安全组件

**1. 云防火墙**

H3C CloudOS 云操作系统提供基于 M9000 物理设备的高性能、高可靠性的云防火墙服务。M9000 通过 Context 技术将一台物理设备划分为互相隔离的多云防火墙，每个组织分配一个专有的云防火墙，为组织专属的网络提供安全保护，租户管理员可以根据实际业务为防火墙设置规则，实现内网与公网的访问控制以及内网的应用安全防范。

H3C CloudOS 云操作系统云防火墙服务包括云防火墙创建、查询、删除和修改等服务内容；并为租户管理员提供防火墙规则集的定义、规则创建、修改、明细查询等功能。

**2. 安全组**

安全组是一种东西向防火墙，通过 OVS 实现，可以实现同一个 VLAN 内的 VM 之间的访问控制和安全防护。安全组功能由 Openstack 与虚拟化软件配合完成，不依赖物理安全设备。

启用安全组服务后，任何一个虚拟机都必须属于一个或多个安全组。一个安全组可包含多个虚拟机。用户可以创建自定义的安全组，如果用户在创建虚拟机时没有指定自定义安全组，云平台将为该虚拟机自动生成并分配一个默认安全组。用户可以通过添加或删除安全规则的方式修改用户自有安全组和默认安全组的安全策略。

**3. 云防病毒**

H3C CloudOS 云操作系统与安全产品 M9000、F5000 配合，提供高性能、高可靠性的云防病毒服务。能够有效对文件传输、邮件和 WEB 应用等进行保护，防止病毒对系统的传染和破坏。

**4. 云 IPS**

入侵防御系统（IPS：Instrusion Prevention System）是计算机网络安全设施，是对防病毒和防火墙的有益补充，是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够即时中断、调整或隔离一些不正常或具有伤害性的网络资料传输行为。H3C CloudOS 云操作系统与安全产品 M9000、F5000 配合，提供高效、可靠的云 IPS 服务，能够对操作系统、网络设备、服务器和办公软件等进行有效保护。

**5. 云负载均衡**

H3C CloudOS 云操作系统提供基于 L5000 物理设备的高性能、高可靠性的云负载均衡服务。H3C CloudOS 云操作系统可以为组织和租户提供云负载均衡申请服务，可以将外部的访问流量根据负载均衡算法分发到多台提供后端服务的主机上，并且支持自动检测和隔离不可用的主机，提高了服务的可用性和处理能力。

H3C CloudOS 云操作系统云负载均衡服务包括云负载均衡设备的申请，进行吞吐量定义及防火墙设备选取；负载均衡监听器的配置，支持虚 IP 配置以及监听协议及 LB 算法的定义；在负载均衡列表中可以进行负载均衡设备的启动、关闭、修改及删除等功能。

**6. 服务器安全监测**

H3C 服务器安全监测系统采用 Agent-Server-Web Browser（执行 – 控制 – 展示）三层模型的分布式计算架构，采用 C/S 管理模式，由 Server 对 Agent 进行统一管理，是一款专注于服务端主机的安全防护软件，通过资产清点、风险分析、入侵诊断等安全功能提供持续的安全监控、分析和快速响应能力，能够在公有云、私有云、混合云、物理机、虚拟机等各种业务环境下实现安全的统一策略管理和快速的入侵响应能力。

**7. 漏洞扫描**

- 丰富的漏洞知识库

漏洞规则涵盖对各种主流操作系统、数据库、网络设备、应用程序的检测。漏洞知识库数量国内领先，每周至少升级一次。漏洞信息、漏洞描述全中文支持，兼容 CVE 国际标准。全面支持 OWASP TOP 10 检测，支持对当前各种主流的 WEB 应用、操作系统、数据库、应用服务、国内外主流 CMS 及各类第三方组件等漏洞检测。漏洞修复建议清晰、详细，可操作性强。

● 智能引擎调度

采用智能的调度算法和多引擎分离技术，引擎包含任务调度、业务调度引擎、爬虫引擎和漏洞检测引擎，各引擎实现相互独立，根据引擎资源的使用情况，进行动态调整和智能的任务调度，在保证准确率的前提下大幅提高了检测的速度。

● 领先的扫描技术

自主研发高效稳定的核心扫描引擎，基于 B/S 结构，采用智能页面爬取和手动页面抓取相结合实现立体式页面抓取、资源动态调节、代理缓存机制和实时任务调度等领先技术，实现了对大规模网站的快速、稳定的扫描。产品会自动获取网站包含的相关信息，并全面模拟网站访问的各种行为，比如按钮点击、鼠标移动、表单复杂填充等，通过内建的“安全模型”全面、深度、准确地检测 Web 应用系统潜在的各种应用弱点，有助于提高主动防御能力。

**8. 应用监控**

能监测网站的 HTTP、DNS、PING 响应，提供自定义的安全阀值，从而为网站快速诊断提供帮助，能计量服务器掉线等安全事件发生的频率、时间段同时提供报警操作。

● HTTP 监控

网站应用监控通过监听指定的 TCP 端口，来获取客户端浏览器的访问请求，通过对监控网站的 URL 发起 HTTP 请求，计算从监控节点打开网站所需实际时间。结合预设值的阈值，如果在达到阈值时还无法得到响应，平台将会放弃请求，判定网站服务不可用，得到 HTTP 响应报文的 200 状态码作为是否可用的判断标准，并支持对包括使用 301、302、307 等等状态码进行重定向的网站进行监测，支持自定义匹配网站响应内容。

● DNS 监控

当提供域名解析服务的 DNS 服务器出现故障，会导致使用该服务器作为域名解析地址的客户端，无法正常通过域名访问网站的情况，亦可能是由于网络线路故障导致的网络不可达，或者是由于域名已经失效过期等原因。DNS 应用监控可向指定的 DNS 服务器发送被监测网站的 DNS 请求报文，通过预设的阈值，并计算实际 DNS 的响应时间，以及域名解析结果，来判断网站的域名解析服务是否可用。

● PING 监控

如果网站未禁止 PING，应用监控可通过发送 ICMP 请求报文至监测网站，通过预设的阈值，并计算实际 ICMP 响应报文的响应时间，如果在达到阈值时还无法得到响应，则判断哪个网络不可达。

**9. DDOS 攻击防范**

● 云端清洗大流量攻击

依靠 DNS 智能牵引技术将大流量的攻击牵引至云端，清洗后再将干净流量回注给客户以保障业务的稳定性，其强大的 T 级清洗能力可完美防御 SYN Flood、ACK Flood、UDP Flood、NTP Flood、ICMP Flood、DNS Flood、HTTP Flood、CC 攻击等 DDOS 攻击。

● 精确智能的攻击检测及防护

对 SYN Flood、UDP Flood、ICMP Flood、IGMP Flood、ACK Flood、DNS Query Flood、Ping Sweep 等流量型攻击，HTTP Proxy Flood、HTTP Get Flood、CC Proxy Flood、Connection Exhausted 等连接型攻击和 Smurf、Land-based、Teardrop、Fragment Flood、Red Code 等漏洞型攻击，及其他各种常见的攻击行为均可有效识别，并能实时对这些攻击流量进行阻断处理，保障业务系统正常运行。

● 自动生成策略高效清洗





凭借业界内领先的检测防御算法使 H3C DDOS 清洗服务拥有超过 99.99%的检测准确率，并能在自动检测出攻击时秒级响应，针对不同种类的攻击特征采用不同的算法识别，自动生成多种匹配的防御策略，在短时间内完成高效的清洗。

**10. WEB 应用防火墙**

● 扫描引擎性能优化技术

H3C 安全云管平台研发团队充分考虑内容应用网关的特点，在内容扫描检测匹配上，着重于大量应用数据与特征的并行扫描匹配，从而进一步优化其 Web 应用防火墙的性能。首先通过 Engine Initializer 创建一个共享的 Scan Engine 环境，每个进程可以自由的利用该环境系统，在 WAF 扫描检测过程中，每个进程都可以共享的、独立的访问 Scan Engine 的环境资源，并行扫描，这样不仅充分支持多进程的攻击检测扫描，而且减少了不必要的进程切换，减少了 I/0 Block 操作，从而使得引擎的扫描性能随之同等级的提升。

● 双向多重检测规则

WEB 应用防火墙作为 Web 客户端与服务器端请求与响应的中间人，避免 Web 服务器直接暴露在互联网上，检测过滤 HTTP/HTTPS 双向交互流量数据，对其中的恶意成分进行实时在线清洗过滤。通过对 HTTP/HTTPS 协议进行深入的解析，精确的识别出协议中的各种要素，比如 Cookie、Get 参数、Post 表单等，并对这些数据进行必要的解码，以还原原始信息，根据这些解码后的原始信息，准确检测识别是否包含攻击内容。

● 协议安全＆内容安全

从协议合规及传输内容安全的角度出发，除了常规的特征库检测手段之外还包括 HTTP 协议内容长度检查、请求及行为方法控制、溢出检查、cookie 过滤、上传 / 下载类型检测、URL 访问控制、盗链防护、网站隐身、敏感信息过滤等多项可控安全功能，全方位覆盖 OWASP TOP10 威胁内容。从而有效防护各类 SQL 注入、XSS 跨站脚本、网页木马上传、WebShell、扫描器扫描、敏感信息泄露、盗链行为、第三方漏洞攻击等攻击。并能通过大数据智能分析结合多种特征匹配策略来判断用户是否存在异常行为，并可定制化设置不同的访问频率规则，有效减小误报率的同时杜绝 CC 攻击对 WEB 网站的影响，打造安全网站环境。

**11. 数据库审计**

● 高适用的数据库审计

全面支持 Oracle，Microsoft SQL Server，DB2，Sybase, Informix、MySQL、人大金仓（Kingbase）、达梦 (DM)、Caché、Teradata、MongoDB 等，可准确分析出这些数据库的协议；支持对多种不同类型和不同版本的数据库的同时审计。

● 数据库操作审计

数据库操作审计主要包括语句的解析、操作类型、操作字段和操作表名等的分析。

• 支持语句操作响应时间的审计，支持语句操作返回行数的审计，支持数据库操作成功、失败的审计；

• 支持数据库绑定变量审计，支持访问数据库的源主机名、源主机用户的审计；可审计操作的客户端名称；

• 可进行语句语法解析，分析语句的操作类型，操作对象等信息。

• 支持数据采集规则定义，对于不关心的数据可以不采集，有效保证系统审计的稳定性与针对性。

● 细粒度审计

数据库审计服务完整记录对数据库的所有操作，通过实时监测并智能地分析、还原各种数据库操作，解析数据库操作，还原 SQL 操作语句；跟踪数据库访问过程中的所有细节，提供数据库操作行为、应用服务器行为、终端录像，为追踪、惩罚犯罪分子提供强有力的证据。

• 全方位的数据库活动审计：实时监控来自各个层面的所有数据库活动以及活动的内容。

• 潜在危险活动重要审计：提供对 DDL 类操作、DML 类操作的重要审计功能，重要审计规则的审计要素可以包括：用户、源 IP 地址、操作时间、使用的 SQL 操作类型。当某个数据库活动匹配了事先定义的重要审计规则时，一条告警将被记录以进行审计。

• 支持对数据库 SQL 操作语句的细粒度审计，可完整解析协议的所有 17 个字段。

• 支持正常请求信息的解析，同时支持对返回值行列结果全解析和全记录。

• 敏感信息细粒度审计：对业务系统的重要信息，提供精确到字段及记录内容的细粒度审计功能。

• 支持超长 SQL 语句、注释内容、多嵌套语句、绑定变量、RPC 的审计。

• SQL 模版管理与敏感数据

数据库审计服务通过 SQL 语法分析，自动识别并抽取数据库句式语义相同但参数不同的语句，实现了 SQL 语句的归类及合并，构建 SQL 模版。对于一个每天都重复着同样操作的被审计监控的业务系统，被原始 SQL 语句占据的空间就大大减少，节省了大量的存储空间。同时，数据查询效率大幅度提升。

通过 SQL 模版管理，可协助管理员对审计数据进行处理，将大量的、常见的语句设置为安全规则或过滤规则，大大增加了规则的准确度，优化系统识别事件规则库，形成安全语句和敏感语句管理，对信任语句正常执行，对敏感语句进行及时告警。

**12. 运维审计**

● 全面的系统兼容性，满足不同场景的应用需求

运维审计服务全面兼容当前主流浏览器及操作系统，以满足不同场景的应用需求。

• 支持 IE、Google、Firefox、Safrai 等主流浏览器；

• 支持 Windows、Mac 操作系统；

• 支持 Mstsc、SecureCRT、Xshell、Filezilla 等客户端运维工具。

● 便捷的运维模式，提高运维工作效率

支持多种访问维护方式，降低系统上线后对运维人员原有操作模式的影响，帮助用户提高工作效率。

• 支持 Web、RDP 直连、SSH Client 直连、SFTP Client 直连多种访问方式；

• 支持会话批量启动功能；

• 会话共享，运维人员可以邀请其他人员参与到当前会话中进行远程协助操作。

● 细粒度的访问控制，增强权限管控力度

借助访问控制、命令权限控制、工单动态权限审批等机制明确运维人员的操作权限，确保只有合法的人才能够合法的访问资源，降低越权操作、违规操作等权限管理风险。

• 支持访问规则一键克隆，降低规则部署复杂度；

• 支持基于用户、用户组、设备、设备组、系统账号、来源 ip、时间、告警规则、操作指令的细粒度权限控制；

• 具备工单申请、审批、撤销的动态权限管理机制；





• 可实现磁盘映射、剪切板文字上下行、剪切板文件上下行的权限管理；

• 针对操作指令支持命令黑名单、白名单、命令批复等模式。

● 完整详细的审计信息，明确操作者的操作行为

安全云管平台运维审计服务能够完整记录用户的操作行为，便于在事故发生时能够快速还原操作过程。

1）命令操作审计

文本方式记录，通过命令的精准识别技术，确保对各种常规和非常规操作行为的准确记录。

• 通过在 Web 界面直接回放操作过程；

• 智能输入输出分离，展现在用户面前的只是输入命令，展开后可查看命令输出结果；

• 支持任意指令操作回放；

• 支持“上下箭头”、“TAB 命令补全”“VI 编辑”等输入操作回放。

2）图形操作审计

通过对 RDP 协议的深度解析，实现对用户操作行为的完整记录。

• 通过深度压缩技术，降低审计日志大小；

• 支持文字智能识别功能：可自动识别图形会话中键盘、窗口标题、URL 链接，同时支持以文本方式进行检索定位；

• 具备空闲会话检测机制，无操作时自动过滤相应画面，减少审计日志大小；

• 具备会话缩略图定位功能，可通过缩略图定位用户相关操作。

3）文件传输审计

完整记录用户的操作过程，包括对文件的上传、下载、删除、修改权限等等。并能通过时间、用户、服务、类型、结果等条件进行筛选搜索。同时通过审计系统进行传输的文件，可以在 web 页面直接下载一份到本地进行查看甄别。

## 3.4 新华三云计算等保 2.0 合规性分析

### 3.4.1 等保 2.0 下新华三云计算环境安全评估

综合 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》及章节 2.2.5 中新华三云计算等保 2.0 合规能力模型，对新华三云计算平台等保 2.0 安全合规性评估，分析新华三云计算平台安全措施、保护对象以及安全技术能力。

**1. 新华三云计算平台三级等保 2.0 合规性状况**

**安全通用要求**

1) 安全物理环境

安全物理环境依据用户业务系统建设需求，选择相应安全等级的基础设施以满足下列安全物理环境合规要求。

① 物理位置选择

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

② 物理访问控制

a) 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

③ 防盗窃和防破坏

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；

b) 应将通信线缆铺设在隐蔽安全处；

c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。

④ 防雷击

a） 应将各类机柜、设施和设备等通过接地系统安全接地；

b） 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

⑤ 防火

a） 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c） 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

⑥ 防水和防潮

a） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

c） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

⑦ 防静电

a） 应采用防静电地板或地面并采用必要的接地防静电措施；

b） 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

⑧ 温湿度控制

a） 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

⑨ 电力供应

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；

c） 应设置冗余或并行的电力电缆线路为计算机系统供电。

⑩ 电磁防护

a） 电源线和通信线缆应隔离铺设，避免互相干扰；

b） 应对关键设备实施电磁屏蔽。

2) 安全通信网络

① 网络架构

a）应保证网络设备的业务处理能力满足业务高峰期需要；

安全措施：网络设备性能监控

保护对象：出口路由器、核心交换机、接入交换机、负载均衡

安全能力：

（1）H3C 云计算环境组网时，根据业务需求可供用户选择高中低档网络设备以满足业务处理能力；

（2）新华三提供的网络设备、安全设备支持 SOP、SCF 横向扩展，业务高峰期设备资源可按需扩展；





（3）H3C 态势感知系统对设备日志进行分析告警，保证设备业务处理能力出现异常时，实时响应；

（4）新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对设备性能进行监控，发现异常时进行报警提示。

合规性情况：符合。

b） 应保证网络各个部分的带宽满足业务高峰期需要；

安全措施：带宽监控、负载均衡

保护对象：出口路由器、核心交换机、接入交换机、负载均衡、网络链路

安全能力：

（1）H3C 态势感知服务系统支持对网络链路进行实时监控告警；

（2）新华三 LLB 负载均衡设备能够对多出口链路进行合理的流量分担， SLB 负载均衡设备可以将客户对数据中心服务的访问请求合理地分发到数据中心的各台服务器上，以此来保证各部分业务带宽的高可用；

（3）新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对网络链路的能力进行监控、告警。

合规性情况：符合。

c） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

安全措施：网络隔离、安全域划分

保护对象：网络架构、云平台内部 VPC

安全能力：

（1）H3C 云计算环境在组网时划分了安全管理区、安全资源池以及业务区，各区域间相互隔离；

（2）不同区域间的网络通过防火墙实现不同网络安全域的划分。

合规性情况：符合

d） 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

安全措施：网络隔离、访问控制

保护对象：网络架构、云平台、业务应用系统

安全能力：

（1）H3C 云计算环境部署出口防火墙；

（2）安全管理区边界部署独立的防火墙，安全资源池部署虚拟防火墙实现不同安全域的隔离，业务区每个客户出口部署虚拟防火墙，每个客户通过 VRF 进行路由隔离；

（3）跨 VPC 间通过虚拟防火墙实现南北向流量隔离，同一 VPC 内也部署虚拟防火墙进行安全域隔离。

合规性情况：符合

e） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

安全措施：网络设备双活部署、链路冗余

保护对象：出口路由器、核心交换机、接入交换机、负载均衡、数据链路

安全能力：

（1）网络架构从接入层到汇聚层，实现节点冗余和链路 LLB 负载分担，在满足带宽收敛和保证业务性能同时满足整个业务系统的高可用；

（2）H3C 云计算环境在组网时防火墙通过堆叠的形式，交换机通过 M-LAG 的方式，服务器通过集群的方式，以保证设备可用；

（3）负载均衡设备提供智能 DNS 服务，保证链路、系统的高可用。

合规性情况：符合

② 通信传输

a） 应采用校验技术或密码技术保证通信过程中数据的完整性；

安全措施：传输加密

保护对象：平台数据：鉴别信息、业务数据、存储数据、配置信息、镜像文件；

租户数据：业务应用数据

安全能力：

（1）数据链路采用 IPsec VPN，用户远程访问使用 SSL VPN，保障通信链路中数据的完整性；

（2）云平台内部管理通过 HTTPS 的访问方式，保证数据在通信过程中的完整性。

合规性情况：符合

b） 应采用密码技术保证通信过程中数据的保密性。

安全措施：传输加密

保护对象：平台数据：鉴别信息、业务数据、存储数据、配置信息、镜像文件；

租户数据：业务应用数据

安全能力：

（1）数据链路采用 IPsec VPN，用户远程访问使用 SSL VPN，保障通信链路中数据的保密性；

（2）云平台内部管理通过 HTTPS 的访问方式，保证数据在通信过程中的保密性。

合规性情况：符合

③ 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

安全能力：

该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信已在测试阶段。

3) 安全区域边界

① 边界防护

a） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；

安全措施：访问控制

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境外部的流量访问时需通过出口防火墙，仅允许通过受控的接口进行通信；

（2）业务区域边界部署虚拟防火墙、安全管理区边界部署独立防火墙、 安全资源池部署虚拟防火墙，在防火墙侧设置 ACL，保证跨边界的访问有效性 ；

（3）虚拟防火墙对跨 VPC 的访问流量进行检测和控制；





（4）同一 VPC 内部的流量访问需通过虚拟防火墙；

（5）VPC 内部基于安全服务链进行自动化编排，实现灵活的访问控制规则，仅允许通过受控的接口进行通信。

合规性情况：符合

b） 应能够对非授权设备私自联到内部网络的行为进行检查或限制；

安全措施：IP/MAC 绑定

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境面向终端和安全设备在接入交换机配置 IP/MAC 地址绑定，并指定端口；对访问内部网络需要安全网关进行身份认证；

（2）H3C 云计算环境 SDN 控制器能够对非法接入的设备进行自动感知，实时更新拓扑，便于及时发现未授权设备的非法接入；

（3）H3C 云计算环境底层基础设施硬件设备的所有空闲端口全部关闭；

（4）H3C 服务器安全监测系统可实时监测非授权的接入；

（5）H3C 云计算环境态势感知服务的资产管理模块可监控非法用户的接入。

合规性情况：符合

c） 应能够对内部用户非授权联到外部网络的行为进行检查或限制；

安全措施：网络准入

保护对象：物理网络边界

安全能力：

（1）H3C 云计算环境 SDN 控制器能够对非法的设备进行自动感知，实时更新拓扑，便于及时发现未授权设备的非法外联；

（2）H3C 云计算环境底层基础设施硬件设备的所有空闲端口全部关闭；

（3）H3C 云计算环境态势感知服务的资产管理模块可监控非法外联；

（4）互联网出口审计设备 IPS、防火墙、ACG（应用流量审计）可以对非法外联行为进行分析、阻断。

合规性情况：符合

d） 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

安全措施：网络准入

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境组网不会涉及无线网络接入，无线网络的使用按照客户需求和具体应用场景而定。

合规性情况：符合

② 访问控制

a） 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境在出口防火墙、虚拟防火墙以及业务负载均衡等设备通过五元组设置访问控制 ACL 规则进行访问控制，最后存在一条 deny all 的配置。

合规性情况：符合

b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）新华三防火墙产品能够对配置的 ACL 规则进行有效检查，帮助用户进行多余策略的实时检查。

合规性情况：符合

c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许 / 拒绝数据包进出；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境组网中的所有防火墙基于五元组，即源地址、目的地址、源端口、目的端口和协议，进行访问控制 ACL 规则的设定，来控制进出防火墙的数据包。

合规性情况：符合

d） 应能根据会话状态信息为进出数据流提供明确的允许 / 拒绝访问的能力；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）新华三下一代防火墙能够对数据会话状态信息进行过滤，提供明确的允许、拒绝访问的能力；

（2）H3C 云计算环境态势感知服务支持全网网络流量可视，识别威胁、监测，可通过联动其他安全设备的方式进行阻断。

合规性情况：符合

e） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）新华三下一代防火墙提供对第七层应用协议和应用内容的访问控制功能，下一代防火墙中包括了 IPS、WAF、AV 杀毒等多个安全模块。

合规性情况：符合

③ 入侵防范

a） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

安全措施：流量监控、入侵检测

保护对象：物理网络边界





安全能力：

（1）H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量包进行深度解析，实时地检测出各种攻击和异常行为；

（2）部署抗 DDoS 设备对进出云平台的所有流量进行检测、清洗；

（3）H3C 云计算环境出口防火墙开启 IPS 功能，对进出流量进行监测系统；

（4）服务器端安装新华三服务器安全监测进行安全加固，防止外部的网络攻击行为。

合规性情况：符合

b） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；

安全措施：流量监控、入侵检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量包进行深度解析，实时地检测出各种攻击和异常行为；

（2）旁路部署 IDS 硬件设备，对云平台的所有流量进行检测；

（3）H3C 云计算环境出口防火墙开启 IPS 功能，对进出流量进行监测系统；

（4）服务器端安装新华三服务器安全监测进行安全加固，防止内部的网络攻击行为。

合规性情况：符合

c） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

安全措施：流量监控、入侵检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境态势感知服务对全网流量进行监测，完成全流量网络行为画像，并通过与云端情报中心联动感知实现对新型网络攻击的分析。

合规性情况：符合

d） 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

安全措施：流量监控、入侵检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境态势感知服务对全网流量进行监测，检测到攻击行为时，能够记录的信息包括：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等，可通过邮件、Web 界面的形式进行告警，并且支持细粒度事件分析展示。

合规性情况：符合

④ 恶意代码和垃圾邮件防范

a） 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

安全措施：流量监控、入侵检测、恶意代码检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境出口防火墙开启防病毒、IPS 等功能，能够对互联网出口的恶意代码进行检测，恶意代码库支持自动更新、手动更新及定期更新；

（2）虚拟防火墙开启防病毒功能，在业务区提供 WAF ，可实现各节点处的恶意代码检测和清除，恶意代码库支持自动更新、手动更新及定期更新。

合规性情况：符合

b） 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

安全措施：入侵检测、恶意代码检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境能够为客户提供反垃圾邮件网关、邮件 DLP（数据防泄漏）、沙箱等方式对垃圾邮件进行检测和防护，用户可根据业务需求选择相应的安全技术。

（2）云服务客户侧根据业务需求，部署第三方邮件防护软件。

合规性情况：符合

⑤ 安全审计

a） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

安全措施：安全审计

保护对象：物理网络边界、虚拟网络边界、网络设备、堡垒机

安全能力：

（1）H3C 云计算环境态势感知服务能够收集全网的日志和流量，日志能够覆盖到全网的所有用户；

（2）H3C 云计算环境日志审计服务，能够提供部署日志审计服务器，收集各设备、节点处的日志信息；

（3）堡垒机能够对租户侧操作行为进行审计。

合规性情况：符合

b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

安全措施：安全审计

保护对象：物理网络边界、虚拟网络边界、网络设备、堡垒机

安全能力：

（1）H3C 云计算环境态势感知服务对收集的全网日志可进行细粒度的分析展示，包括的信息有：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等；

（2）H3C 堡垒机提供录像式日志回放功能，并且可通过关键信息进行定位回放；

（3）第三方堡垒机审计日志类型包含事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

合规性情况：符合

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

安全措施：数据备份、访问控制

保护对象：物理网络边界、虚拟网络边界、网络设备、堡垒机

安全能力：





（1）态势感知通过集群的方式部署，客户可根据实际业务需求情况调整存储空间，且提供定期的备份机制，保证审计数据的可用性；

（2）第三方堡垒机审计日志可存在堡垒机本地，也可保存在云存储上，至少保存 6 个月以上。

合规性情况：符合

d） 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

保护对象：物理网络边界、虚拟网络边界、网络设备、堡垒机

安全能力：

（1）H3C 云计算环境态势感知服务能对远程访问（如 SSLVPN 接入）的用户行为，访问互联网的用户行为（EAD 准入、互联网审计）等单独进行行为审计和分析。

合规性情况：符合

⑥ 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

安全能力：

（1）该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信功能已在测试阶段。

4) 安全计算环境

① 身份鉴别

a） 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

安全措施：网络设备加固、系统加固、账号认证

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品本地均可设置用户口令复杂度、最小口令长度以及口令有效期；

（2）新华三云计算系列产品均允许被堡垒机接管，堡垒机侧可设置强制的口令复杂度策略。

合规性情况：符合

b） 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

安全措施：网络设备加固、系统加固

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品本地均可设置登录失败次数以及限制超时时长；

（2）新华三云计算系列产品均允许被堡垒机接管，堡垒机侧可设置登录失败次数以及限制超时时长。

合规性情况：符合

c） 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

安全措施：传输加密

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）云平台内部访问通过 HTTPS 的方式进行远程连接，通信过程中信息加密传输；

（2）新华三云计算系列产品被堡垒机接管后，可设置访问策略，保证信息在传输过程中的完整性和保密性。

合规性情况：符合

d） 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

安全措施：双因素身份认证

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）H3C CloudOS、H3C CAS、H3C SecCloud OMP 等管理平台的鉴别方式有用户名、口令 + 短信验证码、邮件验证码两种身份鉴别方式；

（2）新华三云计算系列产品均允许被堡垒机接管，且仅允许堡垒机访问，在堡垒机侧通过用户名、口令 +USB Key 的认证方式，实现用户双因素身份鉴别。

合规性情况：符合

② 访问控制

a） 应对登录的用户分配账户和权限；

安全措施：授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品基于三权分立原则，默认分配系统管理员、安全管理员、审计管理员，如 H3C CloudOS 基于用户角色分配账户，角色分为组织管理员（租户）、普通用户、审计员、云管理员（平台侧）。

合规性情况：符合

b） 应重命名或删除默认账户，修改默认账户的默认口令；

安全措施：网络设备加固、系统加固

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统





安全能力：

（1）新华三云计算系列产品 admin、administrator 等默认账户在交付时，默认禁用，且会对所有用户的默认口令进行更改。

合规性情况：符合

c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

安全措施：网络设备加固、系统加固

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品会对账户资源情况进行展示，确定账户无资源使用时，可删除多余账户。

合规性情况：符合

d） 应授予管理用户所需的最小权限，实现管理用户的权限分离；

安全措施：授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品根据用户所属组织架构角色，为其分配权限，且遵循最小授权原则。

合规性情况：符合

e） 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

安全措施：授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品基于用户角色分配权限，限制用户对功能模块的访问。

合规性情况：符合

f） 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

安全措施：授权

保护对象：平台侧：物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品主体到用户级，客体为功能模块、文件或数据库表。

合规性情况：符合

g） 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

安全措施：授权、安全标记

保护对象：平台侧：物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

该项能力 H3C 云计算环境正在建设中。

合规性情况：不符合

③ 安全审计

a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

安全措施：安全审计

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品自身均有操作日志审计模块，默认开启，且覆盖到系统所有用户；

（2）新华三云计算系列产品均允许被堡垒机接管，堡垒机通过录屏和记录的方式审计所有用户的行为；

（3）新华三态势感知、日志审计产品支持全网日志收集，日志审计支持网络设备、安全设备、服务器等云上各类组件的安全审计，态势感知支持安全日志、网络审计日志、数据库审计日志、SSLVPN 日志、DLP 审计日志、运维日志、流量日志等。

合规性情况：符合

b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

安全措施：安全审计

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品审计记录包括登录名称、IP 地址、操作、资源、操作时间、级别、结果等；

（2）堡垒机侧的审计记录内容包括：时间、IP、用户账户、操作类型、影响内容、结果、操作；

（3）日志审计的日志类型包括操作日志、审计日志、流量日志、威胁日志、系统日志、安全控制日志、用户接入日志等，态势感知的审计内容包括日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等。

合规性情况：符合

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

安全措施：审计数据转存 / 备份、访问控制

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品审计记录支持导出；

（2）堡垒机支持审计报表生成，并支持审计记录导出；

（3）日志审计、态势感知支持审计报表生成，并支持审计记录导出。

合规性情况：符合

d） 应对审计进程进行保护，防止未经授权的中断。

安全措施：安全审计、授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品均可设置审计员，并对审计进程进行保护。

合规性情况：符合

④ 入侵防范

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；

安全措施：主机安全加固、服务器安全监测

保护对象：平台侧：物理服务器、虚拟机镜像

云服务客户侧：虚拟机

安全能力：

（1）物理机、虚拟机侧均最小安装，且经主机安全加固，仅安装必要的组件和应用程序。

合规性情况：符合

b） 应关闭不需要的系统服务、默认共享和高危端口；

安全措施：主机安全加固、服务器安全监测

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、宿主机

云服务客户侧：虚拟机、数据库

安全能力：

（1）新华三云计算平台对所有网络设备、镜像和系统均进行了安全检测，删减危险的第三方组件，关闭了不需要的系统服务、默认共享和高危端口；

（2）云服务客户侧在使用过程中，关闭不必要的服务、默认共享及高危端口。

合规性情况：符合

c） 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

安全措施：网络隔离、访问控制、登录地址限制

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品可设置终端接入方式，如堡垒机、基于 LDAP 认证或者特定地址范围。

合规性情况：符合

d） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

安全措施：特殊字符过滤

保护对象：平台侧：H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台

云服务客户侧：业务应用系统

安全能力：

（1）新华三云计算平台所有系统在上线前均会进行安全测试，对输入数据的有效性进行验证，过滤特殊字符。

合规性情况：符合

e） 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

安全措施：漏洞管理

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）H3C 云漏洞扫描系统提供 Web 漏洞扫描、数据库漏洞扫描、系统漏洞扫描，会提供漏扫报告，发现漏洞，提供升级服务。

合规性情况：符合

f） 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

安全措施：入侵检测

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）主机层面安装亚信安全服务器深度安全防护系统，支持入侵防御；

（2）网络层面防火墙包含 IPS 模块，在各区域边界节点处部署服务器，能够对入侵行为进行检测，并提供报警机制；

（3）新华三态势感知系统对全网流量进行监测分析，并能够与 IDS、IPS、防火墙等进行联动，对入侵行为进行检测，并提供报警功能。

合规性情况：符合

⑤ 恶意代码防范

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

安全措施：恶意代码检测





保护对象：平台侧：物理服务器、虚拟机镜像、宿主机

云服务客户侧：虚拟机、数据库

安全能力：

（1）主机层面安装亚信安全服务器深度安全防护系统，支持防恶意软件、防火墙、入侵防御、完整性监控、日志审查，并支持病毒查杀功能。

合规性情况：符合

⑥ 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

安全措施：TPM

保护对象：平台侧：宿主机、云产品

安全能力：

该项能力 H3C 云计算安全正在建设中，目前网络设备侧的安全可信功能已在测试阶段。

合规性情况：部分符合

⑦ 数据完整性

a） 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

安全措施：传输加密

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）云平台内部访问时通过 HTTPS 访问，数据上传时会进行完整性校验；

（2）关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证在加载到存储过程中数据的完整性。

合规性情况：符合

b） 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

安全措施：数据完整性校验

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证数据存储过程中的完整性。

合规性情况：符合

⑧ 数据保密性

a） 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

安全措施：传输加密

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）云平台内部访问时通过 HTTPS 访问，可保证数据在传输过程中的保密性。

合规性情况：符合

b） 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

安全措施：存储加密

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证数据存储过程中的保密性。

合规性情况：符合

⑨ 数据备份恢复

a） 应提供重要数据的本地数据备份与恢复功能；

安全措施：数据备份

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式。

合规性情况：符合

b） 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

安全措施：数据备份

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式。

合规性情况：符合

c） 应提供重要数据处理系统的热冗余，保证系统的高可用性。

安全措施：数据处理系统冗余、高可用

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、宿主机

云服务客户侧：虚拟机、虚拟防火墙（东西向）

安全能力：

（1）新华三云计算环境中防火墙采用堆叠的形式、交换机通过 M-LAG 的形式、服务器侧采用虚拟机、存储侧为分布式存储系统，还有负载均衡等可保证数据处理系统的冗余。





合规性情况：符合

⑩ 剩余信息保护

a） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

安全措施：残留数据清除

保护对象：平台侧：云平台管理系统

云服务客户侧：虚拟机、业务应用系统

安全能力：

（1）数据的存储空间删除后，底层存储会进行写零回收，可有效的防止剩余信息残留。

合规性情况：符合

b） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

安全措施：残留数据清除

保护对象：平台侧：云平台管理系统

云服务客户侧：虚拟机、业务应用系统

安全能力：

（1）数据的存储空间删除后，底层存储会进行写零回收，数据只有在被写零后才能重新分配。

合规性情况：符合

⑪ 个人信息保护

a） 应仅采集和保存业务必需的用户个人信息；

安全能力：

（1）由云服务客户侧根据部署的应用系统功能建设相应的个人信息清除机制。

合规性情况：该条款不适用

b） 应禁止未授权访问和非法使用用户个人信息。

安全能力：

（1）由云服务客户侧根据部署的应用系统功能建设相应的个人信息清除机制。

合规性情况：该条款不适用

5) 安全管理中心

① 系统管理

a） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

安全措施：权限划分、账号认证、授权、安全审计

保护对象：云计算环境

安全能力：

（1）设备层默认分配系统管理员、审计管理员、安全管理员，堡垒机侧默认分配系统管理员、安全审计员、运维人员；

（2）系统管理员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，系统管理员的操作均可被堡垒机审计。

合规性情况：符合

b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、

系统运行的异常处理、数据和设备的备份与恢复等。

安全措施：权限划分、授权

保护对象：云计算环境

安全能力：

（1）设备层的系统管理员的权限主要包括系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；

（2）堡垒机侧系统管理员主要分配运维人员、安全审计员的账户和权限。

合规性情况：符合

② 审计管理

a） 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

安全措施：权限划分、账号认证、授权、安全审计

保护对象：云平台

安全能力：

（1）设备侧的审计管理员、堡垒机侧的审计管理员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，且所有的操作被堡垒机实时审计，系统管理员可查看审计管理员的操作行为。

合规性情况：符合

b） 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

安全措施：审计分析

保护对象：云平台

安全能力：

（1）审计管理员对设备、系统的审计记录进行分析、统计，审计策略由审计管理员制定，审计记录的存储、管理、查询工作均由审计管理员在堡垒机侧进行操作。

合规性情况：符合

③ 安全管理

a） 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

安全措施：权限划分、账号认证、授权、安全审计

保护对象：云计算环境

安全能力：

（1）设备侧的安全管理员、堡垒机侧的运维人员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，且所有的操作被堡垒机实时审计。

合规性情况：符合

b） 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

安全措施：授权、安全标记

保护对象：云计算环境





安全能力：

（1）安全管理员主要对安全业务功能配置、安全业务状态监控。

合规性情况：符合

④ 集中管控

a） 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

安全措施：安全域划分

保护对象：网络架构

安全能力：

（1）划分了安全管理区，安全管理区部署了堡垒机、H3C SecCloud OMP 管理平台，能够对所有的设备进行管控；

（2）第三方安全管理设备可根据用户需求，部署在安全管理区。

合规性情况：符合

b） 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

安全措施：带外管理

保护对象：云计算环境

安全能力：

（1）新华三云计算平台网络架构中独立建设带外管理（OOB）网络，对业务网络中的安全设备或安全组件进行管理；

（2）外部区域访问安全管理区需通过 IPsec VPN 或 SSLVPN 访问网络中的设备，安全管理区内部访问网络中的设备需通过 HTTPS、SSH，在安全管理区边界部署了防火墙，保证信息传输路径的安全性。

合规性情况：符合

c） 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

安全措施：运行监测

保护对象：云计算环境

安全能力：

（1）H3C 云计算环境态势感知服务能够对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

（2）H3C CloudOS 管理平台可集中对网络设备、安全设备、服务器的运行情况进行监测；

（3）H3C SecCloud OMP 管理平台能够对安全资源的运行状况、资源使用情况进行监测；

（4）H3C 服务器集中监测能够对服务器运行状况、资源使用情况进行监测；

（5）SDN 控制器运维模块包括物理网络、逻辑网络、拓扑映射、网络健康监控、流量监控。

（6）新华三 IMC 能够对网络链路、网络设备、安全设备的运行状况和资源使用情况进行集中监测，云服务客户可根据业务需求选择性部署。

合规性情况：符合

d） 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

安全措施：安全审计

保护对象：云计算环境

安全能力：

（1）H3C 态势感知系统能够收集全网日志，对日志进行集中分析，并进行细粒度展示，态势感知集群部署，至少保存 6 个月以上，可手动或自动转存至第三方设备；

（2）日志审计支持收集全网日志，可作为态势感知探针使用，与态势感知进行二次联动，进行细粒度展示。

合规性情况：符合

e） 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

安全措施：策略集中管控

保护对象：云计算环境

安全能力：

（1）态势感知、集中式漏扫、H3C SecCloud OMP 管理平台、服务器安全监测能够对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

（2）H3C SecCloud OMP 管理平台支持安全策略统一下发。

合规性情况：符合

f） 应能对网络中发生的各类安全事件进行识别、报警和分析。

安全措施：流量监控、入侵检测

保护对象：云计算环境

安全能力：

（1）态势感知、日志审计对全网的日志流量、日志进行集中监测，支持各类安全事件的分类、识别、分析、报警。

合规性情况：符合

6) 安全管理制度

云服务客户根据业务系统等级制定相应的安全管理制度及要求。

① 安全策略

a） 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

② 管理制度

a） 应对安全管理活动中的各类管理内容建立安全管理制度；

b） 应对管理人员或操作人员执行的日常管理操作建立操作规程；

c） 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

③ 制定和发布

a） 应指定或授权专门的部门或人员负责安全管理制度的制定；

b） 安全管理制度应通过正式、有效的方式发布，并进行版本控制。

④ 评审和修订

a） 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

7) 安全管理机构

① 岗位设置

a） 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；

b） 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c） 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

② 人员配备

a） 应配备一定数量的系统管理员、审计管理员和安全管理员等；

b） 应配备专职安全管理员，不可兼任。

③ 授权和审批

a） 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

b） 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c） 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

④ 沟通和合作

a） 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；

b） 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

c） 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

⑤ 审核和检查

a） 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

b） 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

c） 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

8) 安全管理人员

① 人员录用

a） 应指定或授权专门的部门或人员负责人员录用；

b） 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；

c） 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

② 人员离岗

a） 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

b） 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

③ 安全意识教育和培训

a） 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b） 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；

c） 应定期对不同岗位的人员进行技能考核。

④ 外部人员访问管理

a） 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

b） 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

c） 外部人员离场后应及时清除其所有的访问权限；

d） 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

9) 安全建设管理

① 定级和备案

a） 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b） 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c） 应保证定级结果经过相关部门的批准；

d） 应将备案材料报主管部门和相应公安机关备案。

② 安全方案设计

a） 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b） 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

c） 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

③ 产品采购和使用

a） 应确保网络安全产品采购和使用符合国家的有关规定；

b） 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；

c） 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

④ 自行软件开发

a） 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

c） 应制定代码编写安全规范，要求开发人员参照规范编写代码；

d） 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

e） 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；

f） 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

g） 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

⑤ 外包软件开发

a） 应在软件交付前检测其中可能存在的恶意代码；

b） 应保证开发单位提供软件设计文档和使用指南；

c） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

⑥ 工程实施

a） 应指定或授权专门的部门或人员负责工程实施过程的管理；

b） 应制定安全工程实施方案控制工程实施过程；

c） 应通过第三方工程监理控制项目的实施过程。

⑦ 测试验收

a） 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；





b） 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

⑧ 系统交付

a） 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b） 应对负责运行维护的技术人员进行相应的技能培训；

c） 应提供建设过程文档和运行维护文档。

⑨ 等级测评

a） 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；

b） 应在发生重大变更或级别发生变化时进行等级测评；

c） 应确保测评机构的选择符合国家有关规定。

⑩ 服务供应商选择

a） 应确保服务供应商的选择符合国家的有关规定；

b） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；

c） 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

10) 安全运维管理

① 环境管理

a） 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b） 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；

c） 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

② 资产管理

a） 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b） 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

c） 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

③ 介质管理

a） 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

b） 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

④ 设备维护管理

a） 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

b） 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

c） 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；

d） 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

⑤ 漏洞和风险管理

a） 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

b） 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

⑥ 网络和系统安全管理

a） 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b） 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

c） 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；

d） 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

e） 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

f） 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

g） 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

h） 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；

i） 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

j） 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

⑦ 恶意代码防范管理

a） 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；

b） 应定期验证防范恶意代码攻击的技术措施的有效性。

⑧ 配置管理

a） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

b） 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

⑨ 密码管理

a） 应遵循密码相关国家标准和行业标准；

b） 应使用国家密码管理主管部门认证核准的密码技术和产品。

⑩ 变更管理

a） 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

b） 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

c） 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

⑪ 备份与恢复管理

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

c） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

⑫ 安全事件处置

a） 应及时向安全管理部门报告所发现的安全弱点和可疑事件；





b） 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c） 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

d） 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

⑬ 应急预案管理

a） 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b） 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

c） 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

d） 应定期对原有的应急预案重新评估，修订完善。

⑭ 外包运维管理

a） 应确保外包运维服务商的选择符合国家的有关规定；

b） 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

c） 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

d） 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

**云计算安全扩展要求**

1) 安全物理环境

① 基础设施位置

a） 应保证云计算基础设施位于中国境内。

安全措施：物理位置选择

保护对象：办公场地、机房和平台建设方案

安全能力：

（1）H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，部署在用户内部或租用运营商机房。

合规性情况：符合

2) 安全通信网络

① 网络架构

a） 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

安全措施：平台安全能力

保护对象：云平台

安全能力：

（1）H3C 云计算环境通过等级保护安全性评估具有承载四级应用系统的安全防护能力。

合规性情况：符合

b） 应实现不同云服务客户虚拟网络之间的隔离；

安全措施：网络隔离

保护对象：网络架构

安全能力：

（1）H3C 云计算环境专有网络（Virtual Private Cloud）VPC 采用隧道技术，帮助用户构建出一个隔离的网络环境，实现不同云服务客户间的网络资源的隔离；

（2）同一 VPC 内通过虚拟防火墙进行安全域隔离；

（3）不同 VPC 间通过 VRF 进行路由隔离，在云端部署虚拟防火墙，划分网络安全域，实现不同 VPC 间的访问控制。

（4）虚拟防火墙能够帮助用户实现云计算环境中东西向流量的隔离。

合规性情况：符合

c） 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；

安全措施：传输加密、访问控制、流量监控、web 攻击防护

保护对象：网络架构

安全能力：

（1）H3C 云计算环境在通信传输层面为云服务客户提供 IPsec VPN、SSL VPN 服务，云平台内部所有通讯访问均通过 https 实现，保证了传输过程中的保密性；

（2）在边界防护层面，部署出口防火墙，各安全域边界处部署防火墙，对常见的 Web 应用攻击进行通过 WAF 拦截旁路阻断；

（3）H3C 下一代防火墙包含 IPS 模块，提供入侵防范功能，态势感知服务对全网流量进行监测；

（4）基于虚拟防火墙实现灵活的访问控制规则。

合规性情况：符合

d） 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；

安全措施：自主设置安全策略的能力

保护对象：网络架构

安全能力：

（1）H3C 云计算环境所有安全产品（服务）均支持云服务客户根据业务需求，自主定义安全访问路径，设置安全组策略，自主选择使用各种安全组件。

合规性情况：符合

e） 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

安全措施：开放接口或服务

保护对象：网络架构

安全能力：

（1）H3C 云计算环境提供开放的 API 接口；

（2）第三方安全产品（服务）如防火墙、漏扫、安全审计、负载均衡等，接入到云平台后，H3C 云计算环境可通过纳管的方式管理第三方安全产品或服务，如绿盟、山石、F5。

合规性情况：符合

3) 安全区域边界

① 访问控制





a） 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

（1）虚拟网络边界处部署虚拟防火墙，业务区内跨 VPC 的访问需通过虚拟防火墙，可根据业务实际情况在防火墙上配置访问控制规则；

（2）虚拟网络东西向流量需通过安全服务链控制 VPC 内部流量走向，并在防火墙上配置访问控制规则。

合规性情况：符合

b） 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

安全措施：访问控制

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境在不同的安全域边界部署了防火墙，如出口防火墙、虚拟防火墙；

（2）同一 VPC 内通过虚拟防火墙进行访问控制，并根据需求设置访问控制规则；

（3）在安全管理区域部署了单独的物理防火墙。安全资源池、业务区部署虚拟防火墙，云平台侧和云服务客户侧可以根据业务实际情况独立设置访问控制规则。

合规性情况：符合

② 入侵防范

a） 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

安全措施：流量监控、入侵检测

保护对象：云平台

安全能力：

（1）H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量深度解析，实时地检测出各种攻击和异常行为，记录的主要内容有：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等；

（2）各安全域边界处部署的防火墙能够对跨区域的攻击行为进行检测、记录，记录的内容有：时间、威胁类型、威胁 ID、威胁名称、源安全区域、目的区域、源 IP 地址、目的 IP 地址、应用、协议、内容安全策略等。

合规性情况：符合

b） 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

安全措施：流量监控、安全审计

保护对象：云平台

安全能力：

（1）各安全域虚拟网络边界处部署的防火墙能够对跨区域的攻击行为进行检测、记录，记录的内容有：时间、威胁类型、威胁 ID、威胁名称、源安全区域、目的区域、源 IP 地址、目的 IP 地址、应用、协议、内容安全策略等。

（2）跨 VPC 的攻击行为可通过虚拟防火墙（IPS 模块）对攻击行为进行检测；

（3）同一 VPC 内的攻击行为可通过虚拟防火墙（IPS 模块）对攻击行为进行检测。

合规性情况：符合

c） 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

安全措施：流量监控、访问控制

保护对象：云平台

安全能力：

（1）虚拟机与宿主机分属不同的网段，默认不通，从虚拟机到宿主机的异常流量会通过态势感知流量探针进行监测，联动防火墙 IPS 进行检测；

（2）宿主机服务器部署新华三服务器监测系统对虚机与宿主机间的流量进行监测；

（3）跨 VPC 的虚拟机间的访问流量需通过虚拟防火墙，虚拟防火墙 IPS 模块可对流量进行检测；

（4）同一 VPC 内不同网段的虚拟机间流量通过虚拟机防火墙 IPS 模块进行流量检测；

（5）同一 VPC 内同一网段的虚拟机间访问需通过 VSwitch，VSwitch 可以对流量进行重定向，将流量定向至态势感知探针、IPS 等工具，对异常流量进行检测。

合规性情况：符合

d） 应在检测到网络攻击行为、异常流量情况时进行告警。

安全措施：流量监控、入侵检测

保护对象：云平台

安全能力：

（1）态势感知与 IPS、IDS 进行联动，能够对异常的攻击行为进行告警、阻断；

（2）新华三服务器安全监测系统能够对异常流量进行告警。

合规性情况：符合

③ 安全审计

a） 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

安全措施：安全审计

保护对象：云平台

安全能力：

（1）H3C 堡垒机（运维审计系统）能够提供完整的审计回放和权限控制服务，能够记录用户的重要操作；

（2）H3C CloudOS 收集用户的日志，能够查看重要特权的操作，如虚拟机删除、重启等。

合规性情况：符合

b） 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

安全措施：安全审计

保护对象：云平台

安全能力：

（1）H3C 云计算环境能够为用户提供运维审计系统，云服务客户可通过堡垒机审计云服务商的操作。

合规性情况：符合

4) 安全计算环境

① 身份鉴别

a） 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

安全措施：账号认证

保护对象：云平台

安全能力：

（1）管理终端对云计算平台通过 https 访问时，服务器端向终端下发证书，实现客户端对服务器端的认证；

（2）云平台通过用户名密码 + 邮箱或短信的方式实现对终端的认证，CloudOS 也可配置 LDAP 实现对终端的认证；

（3）远程管理时，可设置仅允许通过堡垒机访问云管理平台，堡垒机侧支持双因素身份认证。

合规性情况：符合

② 访问控制

b） 应保证当虚拟机迁移时，访问控制策略随其迁移；

安全措施：策略随迁

保护对象：虚拟机

安全能力：

（1）H3C CloudOS 安全组会随虚拟机的迁移一起迁移；

（2）虚拟机迁移过程中，网络属性不会发生改变，系统属性保证安全策略在虚拟机迁移后仍有效。

合规性情况：符合

c） 应允许云服务客户设置不同虚拟机之间的访问控制策略。

安全措施：访问控制

保护对象：虚拟机

安全能力：

（1）同一 VPC 内的虚拟机、不同 VPC 间的虚拟机访问需通过虚拟防火墙、安全组，云服务客户可在防火墙上配置访问控制策略。

合规性情况：符合

③ 入侵防范

a） 应能检测虚拟机之间的资源隔离失效，并进行告警；

安全措施：虚拟机隔离、虚拟机监控

保护对象：虚拟机

安全能力：

（1）H3C CAS 云计算管理平台对虚拟机的资源、运行情况进行监控，对虚拟机的资源使用率设置阈值，有异常时会告警，可设置邮件告警、短信告警；

（2）H3C CAS 虚拟机开启保密模式后，虚拟机资源独占、不共享，保证资源隔离。

合规性情况：符合

b） 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

安全措施：虚拟机监控

保护对象：虚拟机

安全能力：

（1）H3C CAS 虚拟资源审计模块对虚拟机的所有操作进行审计，包括虚拟机重启、新建；

（2）态势感知系统资产管理模块能够对非授权的虚拟机新建进行告警提示；

（3）H3C CAS 虚拟化拓扑进行实时展示，有异常虚拟机新建时，可通过拓扑进行查看。

合规性情况：符合

c） 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

安全措施：恶意代码检测

保护对象：虚拟机

安全能力：

（1）虚拟机上部署主机安全加固（亚信安全服务器深度安全防护系统），对恶意代码进行查杀，支持报警功能；

（2）虚拟机上部署服务器安全监测系统可实时监测、隔离恶意代码；

（3）态势感知能够对虚机间流量进行分析，可发现恶意代码的攻击，并进行告警。

合规性情况：符合

④ 镜像和快照保护

a） 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；

安全措施：镜像加固

保护对象：虚拟机镜像

安全能力：

（1）H3C 能够为用户提供主流的操作系统镜像，对镜像进行安全基线加固，安装防恶意代码软件、服务器安全监测系统软件等。

合规性情况：符合

b） 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

安全措施：镜像、快照完整性校验

保护对象：虚拟机镜像、快照

安全能力：

（1）H3C CloudOS 对虚拟机镜像、快照进行上传时会进行校验，生成 MD5 值，上传完成后会再次生成 MD5 值，进行校验比对；

（2）H3C CAS 对虚拟机进行迁移前后会进行完整性校验。

合规性情况：符合

c） 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

安全措施：存储加密

保护对象：虚拟机镜像

安全能力：

（1）在 H3C CAS 系统管理处参数配置处启用保密模式后能够对虚拟机、镜像进行保密；





（2）镜像、快照保存在磁盘后会对磁盘进行加密；

（3）H3C CAS 特定版本能够对虚拟机镜像的硬盘进行加密。

合规性情况：符合

⑤ 数据完整性和保密性

a） 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

安全措施：——

保护对象：业务数据、鉴别数据

安全能力：

（1）H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，部署在用户内部或租用运营商机房，均位于中国境内。

合规性情况：符合

b） 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；

安全措施：授权

保护对象：业务数据

安全能力：

（1）H3C 行业云在客户授权云服务商人员后，云服务商才能访问客户资源。

合规性情况：符合

c） 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

安全措施：虚拟机迁移

保护对象：虚拟机

安全能力：

（1）H3C 提供迁移服务，对 P2V、V2V 的迁移会通过 TCP 协议进行校验，保证迁移的完整性。

合规性情况：符合

d） 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

安全措施：存储加密、传输加密

保护对象：业务数据、鉴别数据

安全能力：

（1）H3C CloudOS 用户在创建虚拟机时，能够为用户提供虚拟机密钥对，保证虚拟机访问过程中的安全性。

合规性情况：符合

⑥ 数据备份恢复

a） 云服务客户应在本地保存其业务数据的备份；

安全措施：数据备份

保护对象：业务数据

安全能力：

（1）H3C CAS 与 ONEStor 深度融合，用户可将数据存储在 ONEStor 保证数据高可用；

（2）H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式；

（3）租户根据业务需求，选择适当的方式在本地保存其业务数据。

合规性情况：符合

b） 应提供查询云服务客户数据及备份存储位置的能力；

安全措施：资源监控

保护对象：存储数据

安全能力：

（1）H3C CAS 可查看虚拟机运行状态、存储位置；

（2）云服务客户在创建虚拟机时，可选择存储磁盘的存储池，在存储池中可查看虚拟机对应的存储卷。

合规性情况：符合

c） 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；

安全措施：数据备份

保护对象：存储数据

安全能力：

（1）H3C Unistor 支持多副本存储（2-5），各副本间内容保持一致。

合规性情况：符合

d） 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

安全措施：数据迁移

保护对象：配置文件、业务数据、鉴别信息、存储数据

安全能力：

（1）新华三提供迁移工具 Movesure、迁移服务，支持热迁移、冷迁移。

合规性情况：符合

⑦ 剩余信息保护

a） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

安全措施：残余数据清除

保护对象：配置文件、业务数据、鉴别信息、存储数据

安全能力：

（1）虚拟机所有的内存和存储空间被回收时，用户可根据需求进行选择，H3C CAS 提供彻底销毁数据功能，通过写零的方式进行完全清除；

（2）H3C CAS 提供虚拟回收保存期功能。

合规性情况：符合

b） 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

安全措施：残余数据清除

保护对象：配置文件、业务数据、鉴别信息、存储数据





安全能力：

（1）用户删除数据存储卷的时候，各副本会同步删除。

合规性情况：符合

5） 安全管理中心

① 集中管控

a） 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；

安全措施：资源调度与分配

保护对象：云平台

安全能力：

（1）H3C CloudOS 对物理资源、虚拟资源进行统一调度、分配；

（2）H3C SecCloud OMP 对安全资源进行统一调度、分配。

合规性情况：符合

b） 应保证云计算平台管理流量与云服务客户业务流量分离；

安全措施：带外管理，网络隔离

保护对象：云平台

安全能力：

（1）建立带外管理网，保证管理流量和业务流量分离；

（2）安全管理区和业务区边界部署了防火墙，对跨区域的流量进行策略控制。

合规性情况：符合

c） 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；

安全措施：账号授权、安全审计

保护对象：云平台

安全能力：

（1）云平台侧 H3C 态势感知系统能够收集全网日志，对日志进行集中分析，并进行细粒度展示；

（2）H3C 堡垒机支持云平台侧和云服务客户侧的日志收集。

合规性情况：符合

d） 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

安全措施：资源监控

保护对象：云平台

安全能力：

（1）H3C 态势感知系统支持全网全流量的监测，能够对所有的网络设备、安全设备、服务器、虚拟机进行集中监测；

（2）H3C CloudOS 、H3C SecCloud OMP 管理平台为云平台侧和云服务客户侧分别分配账户，可对两侧各自部分的资源进行集中监测。

合规性情况：符合

6) 安全建设管理

云服务客户应根据业务系统安全建设能力需求，依据下列要求选择合适的云服务商并进行相关约定。

① 云服务商选择

a） 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；

安全措施：——

保护对象：——

安全能力：H3C 云计算环境为云服务提供商，云平台能够承载 4 级业务应用系统所需要的安全防护能力。

b） 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c） 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

d） 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；

e） 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。

② 供应链管理

a） 应确保供应商的选择符合国家有关规定；

安全措施：——

保护对象：——

安全能力：

（1）H3C 云计算环境组网时选用的网络、计算、存储等设备均符合国家相关要求，H3C SecCloud OMP 安全产品准许销售，已获得销售许可证；

（2）云服务客户根据供应商选择要求，确保供应商的选择符合国家有关规定。

合规性情况：符合

b） 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；

安全措施：——

保护对象：——

安全能力：

（1）H3C 云计算环境态势感知服务推送最新的安全事件信息，以保证第一时间传达给云服务客户。

合规性情况：符合

c） 应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

安全措施：——

保护对象：——

安全能力：

（1）H3C 云计算环境的变更会通过 H3C SecCloud OMP 进行公告，以保证第一时间传达；

（2）H3C 云计算环境提供一对一服务，变更的通知会及时送达，提供安全风险的应急响应。

合规性情况：符合

7) 安全运维管理





① 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

安全措施：——

保护对象：——

安全能力：

（1）H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，基本运维地点在中国境内。

合规性情况：符合

**2. 新华三云计算平台四级等保 2.0 合规性状况**

**安全通用要求**

1) 安全物理环境

安全物理环境依据用户业务系统建设需求，选择相应安全等级的基础设施以满足下列安全物理环境合规要求。

① 物理位置选择

a） 机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b） 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

② 物理访问控制

a） 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

③ 防盗窃和防破坏

a） 应将设备或主要部件进行固定，并设置明显的不易除去的标识；

b） 应将通信线缆铺设在隐蔽安全处；

c） 应设置机房防盗报警系统或设置有专人值守的视频监控系统。

④ 防雷击

a） 应将各类机柜、设施和设备等通过接地系统安全接地；

b） 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

⑤ 防火

a） 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c） 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

⑥ 防水和防潮

a） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

c） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

⑦ 防静电

a） 应采用防静电地板或地面并采用必要的接地防静电措施；

b） 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

⑧ 温湿度控制

a） 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

⑨ 电力供应

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；

c） 应设置冗余或并行的电力电缆线路为计算机系统供电。

⑩ 电磁防护

a） 电源线和通信线缆应隔离铺设，避免互相干扰；

b） 应对关键设备实施电磁屏蔽。

2) 安全通信网络

① 网络架构

a） 应保证网络设备的业务处理能力满足业务高峰期需要；

安全措施：网络设备性能监控

保护对象：出口路由器、核心交换机、接入交换机、负载均衡

安全能力：

（1）H3C 云计算环境组网时，根据业务需求可供用户选择高中低档网络设备以满足业务处理能力；

（2）新华三提供的网络设备、安全设备支持 SOP、SCF 横向扩展，业务高峰期设备资源可按需扩展，以此来保证各部分业务带宽的高可用；

（3）H3C 态势感知系统对设备日志进行分析告警，保证设备业务处理能力出现异常时，实时响应；

（4）新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对设备性能进行监控，发现异常时进行报警提示。

合规性情况：符合。

b） 应保证网络各个部分的带宽满足业务高峰期需要；

安全措施：带宽监控、负载均衡

保护对象：出口路由器、核心交换机、接入交换机、负载均衡、网络链路

安全能力：

（1）H3C 态势感知服务系统支持对网络链路进行实时监控告警；

（2）新华三 LLB 负载均衡设备能够对多出口链路进行合理的流量分担， SLB 负载均衡设备可以将客户对数据中心服务的访问请求合理地分发到数据中心的各台服务器上；

（3）新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对网络链路的能力进行监控、告警。

合规性情况：符合。

c） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

安全措施：网络隔离、安全域划分

保护对象：网络架构、云平台内部 VPC

安全能力：

（1）H3C 云计算环境在组网时划分了安全管理区、安全资源池以及业务区，各区域间相互隔离；

（2）不同区域间的网络通过防火墙实现不同网络安全域的划分





合规性情况：符合

d） 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

安全措施：网络隔离、访问控制

保护对象：网络架构、云平台、业务应用系统

安全能力：

（1）H3C 云计算环境部署出口防火墙；

（2）安全管理区边界部署独立的防火墙，安全资源池部署虚拟防火墙实现不同安全域的隔离，业务区每个客户出口部署虚拟防火墙，每个客户通过 VRF 进行路由隔离；

（3）跨 VPC 间通过虚拟防火墙实现南北向流量隔离，同一 VPC 内也部署虚拟防火墙进行安全域隔离。

合规性情况：符合

e） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

安全措施：网路设备双活部署、链路冗余

保护对象：出口路由器、核心交换机、接入交换机、负载均衡、数据链路

安全能力：

（1）网络架构从接入层到汇聚层，实现节点冗余和链路 LLB 负载分担，在满足带宽收敛和保证业务性能同时满足整个业务系统的高可用；

（2）H3C 云计算环境在组网时防火墙通过堆叠的形式，交换机通过 M-LAG 的方式，服务器通过集群的方式，以保证设备可用；

（3）负载均衡设备提供智能 DNS 服务，保证链路、系统的高可用。

合规性情况：符合

f） 应按照业务服务的重要程度分配带宽，优先保障重要业务。

安全措施：网路设备双活部署、链路冗余

保护对象：出口路由器、核心交换机、接入交换机、负载均衡、数据链路

安全能力：

（4）新华三云计算环境中可通过链路负载均衡（LLB）、服务器负载均衡（SLB）保障业务带宽；

（5）新华三云计算环境中的所有路由器、交换机等均可配置 QOS 策略，可根据业务情况进行恰当的 QOS 策略配置，保证重要业务的带宽分配；

（6）SDN 控制器可自动下发 QOS 策略，保证各部分业务的带宽。

合规性情况：符合

② 通信传输

a） 应采用校验技术或密码技术保证通信过程中数据的完整性；

安全措施：传输加密

保护对象：平台数据：鉴别信息、业务数据、存储数据、配置信息、镜像文件；

租户数据：业务应用数据

安全能力：

（1）数据链路采用 IPsec VPN，用户访问使用 SSL VPN，保障通信链路中数据的完整性；

（2）云平台内部管理通过 HTTPS 的访问方式，保证数据在通信过程中的完整性。

合规性情况：符合

b） 应采用密码技术保证通信过程中数据的保密性。

安全措施：传输加密

保护对象：平台数据：鉴别信息、业务数据、存储数据、配置信息、镜像文件；

租户数据：业务应用数据

安全能力：

（1）数据链路采用 IPsec VPN，用户远程访问使用 SSL VPN，保障通信链路中数据的保密性；

（2）云平台内部管理通过 HTTPS 的访问方式，保证数据在通信过程中的保密性。

合规性情况：符合

c） 应在通信前基于密码技术对通信的双方进行验证或认证；

安全措施：传输加密

保护对象：平台数据：鉴别信息、业务数据、存储数据、配置信息、镜像文件；

租户数据：业务应用数据

安全能力：

（1）数据链路采用 IPsec VPN，用户远程访问使用 SSL VPN，保障通信链路中数据的保密性；

合规性情况：符合

d） 应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。

安全措施：传输加密

保护对象：平台数据：鉴别信息、业务数据、存储数据、配置信息、镜像文件；

租户数据：业务应用数据

安全能力：

（1）H3C 路由器产品和防火墙产品均内置硬件加密引擎，支持商用密码；同时也支持安装国密卡；数据链路采用 IPsec VPN，用户访问使用 SSL VPN，保障通信链路中数据的保密性；

（2）新华三云计算平台组网时暂未提供独立的加密机，用户可根据实际业务需求自行部署。

合规性情况：部分符合。

③ 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

安全能力：

该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信已在测试阶段。

3) 安全区域边界

① 边界防护

a） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；





安全措施：访问控制

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境外部的流量访问时需通过出口防火墙，仅允许通过受控的接口进行通信；

（2）业务区域边界部署虚拟防火墙、安全管理区边界部署独立防火墙、 安全资源池部署虚拟防火墙，在防火墙侧设置 ACL，保证跨边界的访问有效性 ；

（3）虚拟防火墙对跨 VPC 的访问流量进行检测和控制；

（4）同一 VPC 内部的流量访问需通过虚拟防火墙；

（5）VPC 内部基于安全服务链进行自动化编排，实现灵活的访问控制规则，仅允许通过受控的接口进行通信。

合规性情况：符合

b） 应能够对非授权设备私自联到内部网络的行为进行检查或限制；

安全措施：IP/MAC 绑定

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境面向终端和安全设备在接入交换机配置 IP/MAC 地址绑定，并指定端口；对访问内部网络需要安全网关进行身份认证；

（2）H3C 云计算环境 SDN 控制器能够对非法接入的设备进行自动感知，实时更新拓扑，便于及时发现未授权设备的非法接入；

（3）H3C 云计算环境底层基础设施硬件设备的所有空闲端口全部关闭；

（4）H3C 服务器安全监测系统可实时监测非授权的接入；

（5）H3C 云计算环境态势感知服务的资产管理模块可监控非法用户的接入。

合规性情况：符合

c） 应能够对内部用户非授权联到外部网络的行为进行检查或限制；

安全措施：网络准入

保护对象：物理网络边界

安全能力：

（1）H3C 云计算环境 SDN 控制器能够对非法的设备进行自动感知，实时更新拓扑，便于及时发现未授权设备的非法外联；

（2）H3C 云计算环境底层基础设施硬件设备的所有空闲端口全部关闭；

（3）H3C 云计算环境态势感知服务的资产管理模块可监控非法外联；

（4）互联网出口审计设备 IPS、防火墙、ACG（应用流量审计）可以对非法外联行为进行分析、阻断。

合规性情况：符合

d） 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

安全措施：网络准入

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境组网不会涉及无线网络接入，无线网络的使用按照客户需求和具体应用场景而定。

合规性情况：符合

e） 应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断；

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C EAD（终端准入控制）方案，能够对终端用户的接入进行身份认证，安全检查及动态授权。若有非授权设备私自联到内部网络，身份认证不通过，会被直接拒绝；若有内部用户非授权连接外网行为，会无法访问未被授权的资源。

（2）H3C 态势感知系统的资产管理模块，实时监测全网的设备，若有未授权设备私自外联或内联，态势感知系统会进行监测，并与其他安全设备联动进行阻断。

合规性情况：符合

f） 应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信功能已在测试阶段。

合规性情况：不符合

② 访问控制

a） 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境在出口防火墙、虚拟防火墙以及业务负载均衡等设备通过五元组进行设置访问控制 ACL 规则进行访问控制，最后存在一条 deny all 的配置。

合规性情况：符合

b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）新华三防火墙产品能够对配置的 ACL 规则进行冗余检查，帮助用户进行多余策略的实时检查。

合规性情况：符合

c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许 / 拒绝数据包进出；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境组网中的所有防火墙基于五元组，即源地址、目的地址、源端口、目的端口和协议，进行访问控制 ACL 规则的设定，来控制进出防火墙的数据包。





合规性情况：符合

d） 应能根据会话状态信息为进出数据流提供明确的允许 / 拒绝访问的能力；

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）新华三下一代防火墙能够对数据会话状态信息进行过滤，提供明确的允许、拒绝访问的能力；

（2）H3C 云计算环境态势感知服务支持全网网络流量可视，识别威胁、监测，可通过联动其他安全设备的方式进行阻断。

合规性情况：符合

e） 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。

安全措施：访问控制策略

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）新华三云计算环境中部署安全数据交换系统可实现不同安全域之间的数据隔离、交换。

合规性情况：符合

③ 入侵防范

a） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

安全措施：流量监控、入侵检测

保护对象：物理网络边界

安全能力：

（1）H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量包进行深度解析，实时地检测出各种攻击和异常行为；

（2）部署抗 DDoS 设备对进出云平台的所有流量进行检测、清洗；

（3）H3C 云计算环境出口防火墙开启 IPS 功能，对进出流量进行监测；

（4）服务器端安装新华三服务器安全监测进行安全加固，防止外部的网络攻击行为。

合规性情况：符合

b） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；

安全措施：流量监控、入侵检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量包进行深度解析，实时地检测出各种攻击和异常行为；

（2）旁路部署 IDS 硬件设备，对云平台的所有流量进行检测；

（3）H3C 云计算环境出口防火墙开启 IPS 功能，对进出流量进行监测；

（4）服务器端安装新华三服务器安全监测进行安全加固，防止内部的网络攻击行为。

合规性情况：符合

c） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

安全措施：流量监控、入侵检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境态势感知服务对全网流量进行监测，完成全流量网络行为画像，并通过与云端情报中心联动感知实现对新型网络攻击的分析。

合规性情况：符合

d） 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

安全措施：流量监控、入侵检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境态势感知服务对全网流量进行监测，检测到攻击行为时，能够记录的信息包括：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等，可通过邮件、Web 界面的形式进行告警，并且支持细粒度事件分析展示。

合规性情况：符合

④ 恶意代码和垃圾邮件防范

a） 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

安全措施：流量监控、入侵检测、恶意代码检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境出口防火墙开启防病毒、IPS 等功能，能够对互联网出口的恶意代码进行检测，恶意代码库支持自动更新、手动更新及定期更新；

（2）虚拟防火墙开启防病毒功能，在业务区提供 WAF ，可实现各节点处的恶意代码检测和清除，恶意代码库支持自动更新、手动更新及定期更新。

合规性情况：符合

b） 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

安全措施：入侵检测、恶意代码检测

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境能够为客户提供反垃圾邮件网关、邮件 DLP（数据防泄漏）、沙箱等方式对垃圾邮件进行检测和防护，用户可根据业务需求选择相应的安全技术。

（2）云服务客户侧根据业务需求，部署第三方邮件防护软件。

合规性情况：符合

⑤ 安全审计

a） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

安全措施：安全审计

保护对象：物理网络边界、虚拟网络边界、网络设备、堡垒机

安全能力：

（1）H3C 云计算环境态势感知服务能够收集全网的日志和流量，日志能够覆盖到全网的所有用户；

（2）H3C 云计算环境日志审计服务，能够提供部署日志审计服务器，收集各设备、节点处的日志信息；

（3）堡垒机能够对租户侧操作行为进行审计。

合规性情况：符合

b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

安全措施：安全审计

保护对象：物理网络边界、虚拟网络边界、网络设备、堡垒机

安全能力：

（1）H3C 云计算环境态势感知服务对收集的全网日志可进行细粒度的分析展示，包括的信息有：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等；

（2）H3C 堡垒机提供录像式日志回放功能，并且可通过关键信息进行定位回放；

（3）第三方堡垒机审计日志类型包含事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

合规性情况：符合

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

安全措施：数据备份、访问控制

保护对象：物理网络边界、虚拟网络边界、网络设备、堡垒机

安全能力：

（1）态势感知通过集群的方式部署，客户可根据实际业务需求情况调整存储空间，且提供定期的备份机制，保证审计数据的可用性；

（2）第三方堡垒机审计日志可存在堡垒机本地，也可保存在云存储上，至少保存 6 个月以上。

合规性情况：符合

⑥ 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

安全能力：该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信已在测试阶段。

4) 安全计算环境

① 身份鉴别

a） 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

安全措施：网络设备加固、系统加固、账号认证

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品本地均可设置用户口令复杂度、最小口令长度以及口令有效期；

（2）新华三云计算系列产品均允许被堡垒机接管，堡垒机侧可设置强制的口令复杂度策略。

合规性情况：符合

b） 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

安全措施：网络设备加固、系统加固

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品本地均可设置登录失败次数以及限制超时时长；

（2）新华三云计算系列产品均允许被堡垒机接管，堡垒机侧可设置登录失败次数以及限制超时时长。

合规性情况：符合

c） 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

安全措施：传输加密

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）H3C CloudOS、H3C CAS、H3C SecCloud OMP 等管理平台的鉴别方式有用户名、口令 + 短信验证码、邮件验证码两种身份鉴别方式；

（2）新华三云计算系列产品均允许被堡垒机接管，且仅允许堡垒机访问，在堡垒机侧通过用户名、口令 +USB Key 的认证方式，实现用户双因素身份鉴别。

合规性情况：符合

d） 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

安全措施：双因素身份认证

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）H3C CloudOS、H3C CAS、H3C SecCloud OMP 等管理平台的鉴别方式有用户名、口令 + 短信验证码、邮件验证码两种身份鉴别方式；

（2）新华三云计算系列产品均允许被堡垒机接管，且仅允许堡垒机访问，在堡垒机侧通过用户名、口令 +USB Key 的认证方式，实现用户双因素身份鉴别。

合规性情况：符合





② 访问控制

a） 应对登录的用户分配账户和权限；

安全措施：授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品基于三权分立原则，默认分配系统管理员、安全管理员、审计管理员，如 H3C CloudOS 基于用户角色分配账户，角色分为组织管理员（租户）、普通用户、审计员、云管理员（平台侧）。

合规性情况：符合

b） 应重命名或删除默认账户，修改默认账户的默认口令；

安全措施：网络设备加固、系统加固

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品 admin、administrator 等默认账户在交付时，默认禁用，且会对所有用户的默认口令进行更改。

合规性情况：符合

c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

安全措施：网络设备加固、系统加固

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品会对账户资源情况进行展示，确定账户无资源使用时，可删除多余账户。

合规性情况：符合

d） 应授予管理用户所需的最小权限，实现管理用户的权限分离；

安全措施：授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品根据用户所属组织架构角色，为其分配权限，且遵循最小授权原则。

合规性情况：符合

e） 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

安全措施：授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品基于用户角色分配权限，限制用户对功能模块的访问。

合规性情况：符合

f） 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

安全措施：授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品主体到用户级，客体为功能模块、文件或数据库表。

合规性情况：符合

g） 应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。

安全措施：授权、安全标记

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

该项能力 H3C 云计算环境正在建设中。

合规性情况：不符合

③ 安全审计

a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

安全措施：安全审计

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品自身均有操作日志审计模块，默认开启，且覆盖到系统所有用户；

（2）新华三云计算系列产品均允许被堡垒机接管，堡垒机通过录屏和记录的方式审计所有用户的行为；

（3）新华三态势感知、日志审计产品支持全网日志收集，日志审计支持网络设备、安全设备、服务器等云上各类组件的安全审计，态势感知支持安全日志、网络审计日志、数据库审计日志、SSLVPN 日志、DLP 审计日志、运维日志、流量日志等。

合规性情况：符合





b） 审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等；

安全措施：安全审计

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品审计记录包括登录名称、IP 地址、操作、资源、操作时间、级别、结果等；

（2）堡垒机侧的审计记录内容包括：时间、IP、用户账户、操作类型、影响内容、结果、操作；

（3）日志审计的日志类型包括操作日志、审计日志、流量日志、威胁日志、系统日志、安全控制日志、用户接入日志等，态势感知的审计内容包括日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等。

合规性情况：符合

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

安全措施：数据备份、访问控制

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品审计记录支持导出；

（2）堡垒机支持审计报表生成，并支持审计记录导出；

（3）日志审计、态势感知支持审计报表生成，并支持审计记录导出。

合规性情况：符合

d） 应对审计进程进行保护，防止未经授权的中断。

安全措施：安全审计、授权

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品均可设置审计员，并对审计进程进行保护。

合规性情况：符合

④ 入侵防范

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；

安全措施：主机安全加固、服务器安全监测

保护对象：平台侧：物理服务器、虚拟机镜像

云服务客户侧：虚拟机

安全能力：

（1）物理机、虚拟机侧均最小安装，且经主机安全加固，仅安装必要的组件和应用程序。

合规性情况：符合

b） 应关闭不需要的系统服务、默认共享和高危端口；

安全措施：主机安全加固、服务器安全监测

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区

域边界防火墙、物理服务器、虚拟机镜像、宿主机

云服务客户侧：虚拟机、数据库

安全能力：

（1）新华三云计算平台对所有网络设备、镜像和系统均进行了安全检测，删减危险的第三方组件，关闭了不需要的系统服务、默认共享和高危端口；

（2）云服务客户侧在使用过程中，关闭不必要的服务、默认共享及高危端口。

合规性情况：符合

c） 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

安全措施：网络隔离、访问控制、登录地址限制

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）新华三云计算系列产品可设置终端接入方式，如堡垒机、LDAP 认证或者特定地址范围。

合规性情况：符合

d） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

安全措施：特殊字符过滤

保护对象：平台侧：H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台

云服务客户侧：业务应用系统

安全能力：

（1）新华三云计算平台所有系统在上线前均会进行安全测试，对输入数据的有效性进行验证，过滤特殊字符。

合规性情况：符合

e） 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

安全措施：漏洞管理

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）H3C 云漏洞扫描系统提供 Web 漏洞扫描、数据库漏洞扫描、系统漏洞扫描，会提供漏扫报告，发现漏洞，提供升级服务。

合规性情况：符合





f） 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

安全措施：入侵检测

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机

云服务客户侧：虚拟机、数据库、业务应用系统

安全能力：

（1）主机层面安装亚信安全服务器深度安全防护系统，支持入侵防御；

（2）网络层面防火墙包含 IPS 模块，在各区域边界节点处部署服务器，能够对入侵行为进行检测，并提供报警机制；

（3）新华三态势感知系统对全网流量进行监测分析，并能够与 IDS、IPS、防火墙等进行联动，对入侵行为进行检测，并提供报警功能。

合规性情况：符合

⑤ 恶意代码防范

应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

安全措施：恶意代码检测

保护对象：平台侧：物理服务器、虚拟机镜像、宿主机

云服务客户侧：虚拟机、数据库

安全能力：

（1）主机层面安装亚信安全服务器深度安全防护系统，支持防恶意软件、防火墙、入侵防御、完整性监控、日志审查，并支持病毒查杀功能。

合规性情况：符合

⑥ 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

安全措施：TPM

保护对象：平台侧：宿主机、云产品

安全能力：

该项能力 H3C 云计算安全正在建设中，目前网络设备侧的安全可信已在测试阶段。

合规性情况：部分符合

⑦ 数据完整性

a） 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

安全措施：传输加密

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）云平台内部访问时通过 HTTPS 访问，数据上传时会进行完整性校验；

（2）关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证在加载到存储过程中数据的完整性。

合规性情况：符合

b） 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

安全措施：数据完整性校验

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证数据存储过程中的完整性。

合规性情况：符合

c） 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

安全措施：数据完整性校验

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）由租户侧根据部署的应用系统功能建设相应的抗抵赖能力。

合规性情况：符合

⑧ 数据保密性

a） 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

安全措施：传输加密

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）云平台内部访问时通过 HTTPS 访问，可保证数据在传输过程中的保密性。

合规性情况：符合

b） 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

安全措施：存储加密

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证数据存储过程中的保密性。

合规性情况：符合

⑨ 数据备份恢复

a） 应提供重要数据的本地数据备份与恢复功能；





安全措施：数据备份

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式。

合规性情况：符合

b） 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

安全措施：数据备份

保护对象：平台侧：配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据

云服务客户侧：个人信息、业务数据

安全能力：

（1）H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式。

合规性情况：符合

c） 应提供重要数据处理系统的热冗余，保证系统的高可用性。

安全措施：数据冗余、高可用

保护对象：平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、宿主机

云服务客户侧：虚拟机、虚拟防火墙（东西向）

安全能力：

（1）新华三云计算环境中防火墙采用堆叠的形式、交换机通过 M-LAG 的形式、服务器侧采用虚拟机、存储侧为分布式存储系统，还有负载均衡等可保证数据处理系统的冗余。

合规性情况：符合

⑩ 剩余信息保护

a） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

安全措施：残留数据清除

保护对象：平台侧：云平台管理系统

云服务客户侧：虚拟机、业务应用系统

安全能力：

（1）数据的存储空间删除后，底层存储会进行写零回收，可有效的防止剩余信息残留。

合规性情况：符合

b） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

安全措施：残留数据清除

保护对象：平台侧：云平台管理系统

云服务客户侧：虚拟机、业务应用系统

安全能力：

（1）数据的存储空间删除后，底层存储会进行写零回收，数据只有在被写零后才能重新分配。

合规性情况：符合

⑪ 个人信息保护

a） 应仅采集和保存业务必需的用户个人信息；

安全能力：

（1）由云服务客户侧根据部署的应用系统功能建设相应的个人信息清除机制。

合规性情况：该条款不适用

b） 应禁止未授权访问和非法使用用户个人信息。

安全能力：

（1）由云服务客户侧根据部署的应用系统功能建设相应的个人信息清除机制。

合规性情况：该条款不适用

5) 安全管理中心

① 系统管理

a） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

安全措施：权限划分、账号认证、授权、安全审计

保护对象：云计算环境

安全能力：

（1）设备层默认分配系统管理员、审计管理员、安全管理员，堡垒机侧默认分配系统管理员、安全审计员、运维人员；

（2）系统管理员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，系统管理员的操作均可被堡垒机审计。

合规性情况：符合

b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

安全措施：权限划分、授权

保护对象：云计算环境

安全能力：

（1）设备层的系统管理员的权限主要包括系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；

（2）堡垒机侧系统管理员主要分配运维人员、安全审计员的账户和权限。

合规性情况：符合

② 审计管理

a） 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

安全措施：权限划分、账号认证、授权、安全审计

保护对象：云平台

安全能力：

（1）设备侧的审计管理员、堡垒机侧的审计管理员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，且所有的操作被堡垒机实时审计，系统管理员可查看审计管理员的操作行为。

合规性情况：符合

b） 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

安全措施：审计分析

保护对象：云平台

安全能力：

（1）审计管理员对设备、系统的审计记录进行分析、统计，审计策略由审计管理员制定，审计记录的存储、管理、查询工作均由审计管理员在堡垒机侧进行操作。

合规性情况：符合

③ 安全管理

a） 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

安全措施：权限划分、账号认证、授权、安全审计

保护对象：云计算环境

安全能力：

（1）设备侧的安全管理员、堡垒机侧的运维人员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，且所有的操作被堡垒机实时审计。

合规性情况：符合

b） 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

安全措施：授权、安全标记

保护对象：云计算环境

安全能力：

（1）安全管理员主要对安全业务功能配置、安全业务状态监控。

合规性情况：符合

④ 集中管控

a） 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

安全措施：安全域划分

保护对象：网络架构

安全能力：

（1）划分了安全管理区，安全管理区部署了堡垒机、H3C SecCloud OMP 管理平台，能够对所有的设备进行管控；

（2）第三方安全管理设备可根据用户需求，部署在安全管理区。

合规性情况：符合

b） 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

安全措施：带外管理

保护对象：云计算环境

安全能力：

（1）新华三云计算平台网络架构中独立建设带外管理（OOB）网络，对业务网络中的安全设备或安全组件进行管理；

（2）外部区域访问安全管理区需通过 IPsec VPN 或 SSLVPN 访问网络中的设备，安全管理区内部访问网络中的设备需通过 HTTPS、SSH，在安全管理区边界部署了防火墙，保证信息传输路径的安全性。

合规性情况：符合

c） 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

安全措施：运行监测

保护对象：云计算环境

安全能力：

（1）H3C 云计算环境态势感知服务能够对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

（2）H3C CloudOS 管理平台可集中对网络设备、安全设备、服务器的运行情况进行监测；

（3）H3C SecCloud OMP 管理平台能够对安全资源的运行状况、资源使用情况进行监测；

（4）H3C 服务器集中监测能够对服务器运行状况、资源使用情况进行监测；

（5）SDN 控制器运维模块包括物理网络、逻辑网络、拓扑映射、网络健康监控、流量监控。

（6）新华三 IMC 能够对网络链路、网络设备、安全设备的运行状况和资源使用情况进行集中监测，云服务客户可根据业务需求选择性部署。

合规性情况：符合

d） 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

安全措施：安全审计

保护对象：云计算环境

安全能力：

（1）H3C 态势感知系统能够收集全网日志，对日志进行集中分析，并进行细粒度展示，态势感知集群部署，至少保存 6 个月以上，可手动或自动转存至第三方设备；

（2）日志审计支持收集全网日志，可作为态势感知探针使用，与态势感知进行二次联动，进行细粒度展示。

合规性情况：符合

e） 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

安全措施：策略集中管控

保护对象：云计算环境

安全能力：

（1）态势感知、集中式漏扫、H3C SecCloud OMP 管理平台、服务器安全监测能够对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

（2）H3C SecCloud OMP 管理平台支持安全策略统一下发。

合规性情况：符合

f） 应能对网络中发生的各类安全事件进行识别、报警和分析。

安全措施：流量监控、入侵检测

保护对象：云计算环境





安全能力：

（1）态势感知、日志审计对全网的日志流量、日志进行集中监测，支持各类安全事件的分类、识别、分析、报警。

合规性情况：符合

g） 应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。

安全措施：时钟同步

保护对象：云计算环境

安全能力：

（1）新华三云技术环境中的所有产品均可通过 ntp 协议，将系统范围内所有设备同步至唯一确定的时钟服务器。

6) 安全管理制度

云服务客户根据业务系统等级制定相应的安全管理制度及要求。

① 安全策略

a） 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

② 管理制度

a） 应对安全管理活动中的各类管理内容建立安全管理制度；

b） 应对管理人员或操作人员执行的日常管理操作建立操作规程；

c） 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

③ 制定和发布

a） 应指定或授权专门的部门或人员负责安全管理制度的制定；

b） 安全管理制度应通过正式、有效的方式发布，并进行版本控制。

④ 评审和修订

a） 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

7) 安全管理机构

① 岗位设置

a） 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；

b） 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c） 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

② 人员配备

a） 应配备一定数量的系统管理员、审计管理员和安全管理员等；

b） 应配备专职安全管理员，不可兼任。

③ 授权和审批

a） 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

b） 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c） 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

④沟通和合作

a） 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；

b） 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

c） 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

⑤ 审核和检查

a） 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

b） 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

c） 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

8) 安全管理人员

① 人员录用

a） 应指定或授权专门的部门或人员负责人员录用；

b） 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；

c） 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

② 人员离岗

a） 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

b） 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

③ 安全意识教育和培训

a） 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b） 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；

c） 应定期对不同岗位的人员进行技能考核。

④ 外部人员访问管理

a） 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

b） 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

c） 外部人员离场后应及时清除其所有的访问权限；

d） 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

9) 安全建设管理

① 定级和备案

a） 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b） 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c） 应保证定级结果经过相关部门的批准；

d） 应将备案材料报主管部门和相应公安机关备案。

② 安全方案设计

a） 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b） 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

c） 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

③ 产品采购和使用

a） 应确保网络安全产品采购和使用符合国家的有关规定；

b） 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；

c） 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

④ 自行软件开发

a） 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

c） 应制定代码编写安全规范，要求开发人员参照规范编写代码；

d） 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

e） 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；

f） 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

g） 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

⑤ 外包软件开发

a） 应在软件交付前检测其中可能存在的恶意代码；

b） 应保证开发单位提供软件设计文档和使用指南；

c） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

⑥ 工程实施

a） 应指定或授权专门的部门或人员负责工程实施过程的管理；

b） 应制定安全工程实施方案控制工程实施过程；

c） 应通过第三方工程监理控制项目的实施过程。

⑦ 测试验收

a） 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

b） 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

⑧ 系统交付

a） 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b） 应对负责运行维护的技术人员进行相应的技能培训；

c） 应提供建设过程文档和运行维护文档。

⑨ 等级测评

a） 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；

b） 应在发生重大变更或级别发生变化时进行等级测评；

c） 应确保测评机构的选择符合国家有关规定。

⑩ 服务供应商选择

a） 应确保服务供应商的选择符合国家的有关规定；

b） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；

c） 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

10) 安全运维管理

① 环境管理

a） 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b） 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；

c） 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

② 资产管理

a） 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b） 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

c） 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

③ 介质管理

a） 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

b） 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

④ 设备维护管理

a） 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

b） 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

c） 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；

d） 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

⑤ 漏洞和风险管理

a） 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

b） 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

⑥ 网络和系统安全管理

a） 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b） 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

c） 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；

d） 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

e） 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

f） 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

g） 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

h） 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；

i） 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

j） 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

⑦ 恶意代码防范管理

a） 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；

b） 应定期验证防范恶意代码攻击的技术措施的有效性。

⑧ 配置管理

a） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

b） 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

⑨ 密码管理

a） 应遵循密码相关国家标准和行业标准；

b） 应使用国家密码管理主管部门认证核准的密码技术和产品。

⑩ 变更管理

a） 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

b） 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

c） 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

⑪ 备份与恢复管理

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

c） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

⑫ 安全事件处置

a） 应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b） 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c） 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

d） 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

⑬ 应急预案管理

a） 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b） 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

c） 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

d） 应定期对原有的应急预案重新评估，修订完善。

14 外包运维管理

a） 应确保外包运维服务商的选择符合国家的有关规定；

b） 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

c） 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

d） 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

**云计算安全扩展要求**

1) 安全物理环境

① 基础设施位置

a） 应保证云计算基础设施位于中国境内。

安全措施：物理位置选择

保护对象：办公场地、机房和平台建设方案

安全能力：

（1）H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，部署在用户内部或租用运营商机房。

合规性情况：符合

2) 安全通信网络

① 网络架构

a） 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

安全措施：平台安全能力

保护对象：云平台

安全能力：

（1）H3C 云计算环境通过等级保护安全性评估具有承载四级应用系统的安全防护能力。

合规性情况：符合

b） 应实现不同云服务客户虚拟网络之间的隔离；

安全措施：网络隔离

保护对象：网络架构

安全能力：

（1）H3C 云计算环境专有网络（Virtual Private Cloud）VPC 采用隧道技术，帮助用户构建出一个隔离的网络环境，实现不同云服务客户间的网络资源的隔离；

（2）同一 VPC 内通过虚拟防火墙进行安全域隔离；

（3）不同 VPC 间通过 VRF 进行路由隔离，在云端部署虚拟防火墙，划分网络安全域，实现不同 VPC 间的访问控制。

（4）虚拟防火墙能够帮助用户实现云计算环境中东西向流量的隔离。

合规性情况：符合

c） 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；

安全措施：传输加密、访问控制、流量监控、web 攻击防护

保护对象：网络架构





安全能力：

（1）H3C 云计算环境在通信传输层面为云服务客户提供 IPsec VPN、SSL VPN 服务，云平台内部所有通讯访问均通过 https 实现，保证了传输过程中的保密性；

（2）在边界防护层面，部署出口防火墙，各安全域边界处部署防火墙，对常见的 Web 应用攻击进行通过 WAF 拦截旁路阻断；

（3）H3C 下一代防火墙包含 IPS 模块，提供入侵防范功能，态势感知服务对全网流量进行监测；

（4）基于虚拟防火墙实现灵活的访问控制规则。

合规性情况：符合

d） 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；

安全措施：自主设置安全策略的能力

保护对象：网络架构

安全能力：

（1）H3C 云计算环境所有安全产品（服务）均支持云服务客户根据业务需求，自主定义安全访问路径，设置安全组策略，自主选择使用各种安全组件。

合规性情况：符合

e） 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

安全措施：开放接口或服务

保护对象：网络架构

安全能力：

（1）H3C 云计算环境提供开放的 API 接口；

（2）第三方安全产品（服务）如防火墙、漏扫、安全审计、负载均衡等，接入到云平台后，H3C 云计算环境可通过纳管的方式管理第三方安全产品或服务，如绿盟、山石、F5。

合规性情况：符合

f） 应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问；

安全措施：安全标记

保护对象：虚拟资源

安全能力：

（1）该项能力新华三云计算环境正在建设中。

合规性情况：不符合

g） 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式；

安全措施：协议转换

保护对象：通信数据

安全能力：

（1）新华三提供安全数据交换系统，能够实现不同安全域间的数据隔离、交换，云服务客户可根据业务需求选择边

界数据交换方式。

合规性情况：符合

h） 应为第四级业务应用系统划分独立的资源池。

安全措施：资源独占

保护对象：业务应用系统

安全能力：

（1）新华三云计算平台为重要业务系统及四级业务系统划分独立的资源池。

合规性情况：符合

3) 安全区域边界

① 访问控制

a） 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

安全措施：访问控制

保护对象：虚拟网络边界

安全能力：

（1）虚拟网络边界处部署虚拟防火墙，业务区内跨 VPC 的访问需通过虚拟防火墙，可根据业务实际情况在防火墙上配置访问控制规则；

（2）虚拟网络东西向流量需通过安全服务链控制 VPC 内部流量走向，并在防火墙上配置访问控制规则。

合规性情况：符合

b） 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

安全措施：访问控制

保护对象：物理网络边界、虚拟网络边界

安全能力：

（1）H3C 云计算环境在不同的安全域边界部署了防火墙，如出口防火墙、虚拟防火墙；

（2）同一 VPC 内通过虚拟防火墙进行访问控制，并根据需求设置访问控制规则；

（3）在安全管理区域部署了单独的物理防火墙。安全资源池、业务区部署虚拟防火墙，云平台侧和云服务客户侧可以根据业务实际情况独立设置访问控制规则。

合规性情况：符合

② 入侵防范

a） 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

安全措施：流量监控、入侵检测

保护对象：云平台

安全能力：

（1）H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量深度解析，实时地检测出各种攻击和异常行为，记录的主要内容有：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等；





（2）各安全域边界处部署的防火墙能够对跨区域的攻击行为进行检测、记录，记录的内容有：时间、威胁类型、威胁 ID、威胁名称、源安全区域、源目的区域、源 IP 地址、目的 IP 地址、应用、协议、内容安全策略等。

合规性情况：符合

b） 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

安全措施：流量监控、安全审计

保护对象：云平台

安全能力：

（1）各安全域虚拟网络边界处部署的防火墙能够对跨区域的攻击行为进行检测、记录，记录的内容有：时间、威胁类型、威胁 ID、威胁名称、源安全区域、目的区域、源 IP 地址、目的 IP 地址、应用、协议、内容安全策略等。

（2）跨 VPC 的攻击行为可通过虚拟防火墙（IPS 模块）对攻击行为进行检测；

（3）同一 VPC 内的攻击行为可通过虚拟防火墙（IPS 模块）对攻击行为进行检测。

合规性情况：符合

c） 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

安全措施：流量监控、访问控制

保护对象：云平台

安全能力：

（1）虚拟机与宿主机分属不同的网段，默认不通，从虚拟机到宿主机的异常流量会通过态势感知流量探针进行监测，联动防火墙 IPS 进行检测；

（2）宿主机服务器部署新华三服务器监测对虚机与宿主机间的流量进行监测系统；

（3）跨 VPC 的虚拟机间的访问流量需通过虚拟防火墙，虚拟防火墙 IPS 模块可对流量进行检测；

（4）同一 VPC 内不同网段的虚拟机间流量通过虚拟机防火墙 IPS 模块进行流量检测；

（5）同一 VPC 内同一网段的虚拟机间访问需通过 VSwitch，VSwitch 可以对流量进行重定向，将流量定向至态势感知探针、IPS 等工具，对异常流量进行检测。

合规性情况：符合

d） 应在检测到网络攻击行为、异常流量情况时进行告警。

安全措施：流量监控、入侵检测

保护对象：云平台

安全能力：

（1）态势感知与 IPS、IDS 进行联动，能够对异常的攻击行为进行告警、阻断；

（2）新华三服务器安全监测系统能够对异常流量进行告警。

合规性情况：符合

③ 安全审计

a） 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

安全措施：安全审计

保护对象：云平台

安全能力：

（1）H3C 堡垒机（运维审计系统）能够提供完整的审计回放和权限控制服务，能够记录用户的重要操作；

（2）H3C CloudOS 收集用户的日志，能够查看重要特权的操作，如虚拟机删除、重启等。

合规性情况：符合

b） 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

安全措施：安全审计

保护对象：云平台

安全能力：

（1）H3C 云计算环境能够为用户提供运维审计系统，云服务客户可通过堡垒机审计云服务商的操作。

合规性情况：符合

4) 安全计算环境

① 身份鉴别

a） 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

安全措施：账号认证

保护对象：云平台

安全能力：

（1）管理终端对云计算平台通过 https 访问时，服务器端向终端下发证书，实现客户端对服务器端的认证；

（2）云平台通过用户名密码 + 邮箱或短信的方式实现 CloudOS 对终端的验证，CloudOS 也可配置 LDAP 实现对终端的认证；

（3）远程管理时，可设置仅允许通过堡垒机访问云管理平台，堡垒机侧支持双因素身份认证。

合规性情况：符合

② 访问控制

a） 应保证当虚拟机迁移时，访问控制策略随其迁移；

安全措施：策略随迁

保护对象：虚拟机

安全能力：

（1）H3C CloudOS 安全组会随虚拟机的迁移一起迁移；

（2）虚拟机迁移过程中，网络属性不会发生改变，系统属性保证安全策略在虚拟机迁移后仍有效。

合规性情况：符合

b） 应允许云服务客户设置不同虚拟机之间的访问控制策略。

安全措施：访问控制

保护对象：虚拟机

安全能力：

（1）同一 VPC 内的虚拟机、不同 VPC 间的虚拟机访问需通过虚拟防火墙，云服务客户可在防火墙上配置访问控制策略。

合规性情况：符合





③ 入侵防范

a） 应能检测虚拟机之间的资源隔离失效，并进行告警；

安全措施：虚拟机隔离、虚拟机监控

保护对象：虚拟机

安全能力：

（1）H3C CAS 云计算管理平台对虚拟机的资源、运行情况进行监控，对虚拟机的资源使用率设置阈值，有异常时会告警，可设置邮件告警、短信告警；

（2）H3C CAS 虚拟机开启保密模式后，虚拟机资源独占、不共享，保证资源隔离。

合规性情况：符合

b） 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

安全措施：虚拟机监控

保护对象：虚拟机

安全能力：

（1）H3C CAS 虚拟资源审计模块对虚拟机的所有操作进行审计，包括虚拟机重启、新建；

（2）态势感知系统资产管理模块能够对非授权的虚拟机新建进行告警提示；

（3）H3C CAS 虚拟化拓扑进行实时展示，有异常虚拟机新建时，可通过拓扑进行查看。

合规性情况：符合

c） 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

安全措施：恶意代码检测

保护对象：虚拟机

安全能力：

（1）虚拟机上部署主机安全加固（亚信安全服务器深度安全防护系统），对恶意代码进行查杀，支持报警功能；

（2）虚拟机上部署服务器安全监测可实时监测、隔离恶意代码；

（3）态势感知能够对虚机间流量进行分析，可发现恶意代码的攻击，并进行告警。

合规性情况：符合

④ 镜像和快照保护

a） 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；

安全措施：镜像加固

保护对象：虚拟机镜像

安全能力：

（1）H3C 能够为用户提供主流的操作系统镜像，对镜像进行安全基线加固，安装防恶意代码软件、服务器安全监测软件等。

合规性情况：符合

b） 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

安全措施：镜像、快照完整性校验

保护对象：虚拟机镜像、快照

安全能力：

（1）H3C CloudOS 对虚拟机镜像、快照进行上传时会进行校验，生成 MD5 值，上传完成后会再次生成 MD5 值，进行校验比对；

（2）H3C CAS 对虚拟机进行迁移前后会进行完整性校验。

合规性情况：符合

c） 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

安全措施：存储加密

保护对象：虚拟机镜像

安全能力：

（1）在 H3C CAS 系统管理处参数配置处启用保密模式后能够对虚拟机、镜像进行保密；

（2）镜像、快照保存在磁盘后会对磁盘进行加密；

（3）H3C CAS 特定版本能够对虚拟机镜像的硬盘进行加密。

合规性情况：符合

⑤ 数据完整性和保密性

a） 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

安全措施：——

保护对象：业务数据、鉴别数据

安全能力：

（1）H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，部署在用户内部或租用运营商机房，均位于中国境内。

合规性情况：符合

b） 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；

安全措施：授权

保护对象：业务数据

安全能力：

（1）H3C 行业云在客户授权云服务商人员后，云服务商才能访问客户资源。

合规性情况：符合

c） 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

安全措施：虚拟机迁移

保护对象：虚拟机

安全能力：

（1）H3C 提供迁移服务，对 P2V、V2V 的迁移会通过 TCP 协议进行校验，保证迁移的完整性。

合规性情况：符合





d） 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

安全措施：存储加密、传输加密

保护对象：业务数据、鉴别数据

安全能力：

（1）H3C CloudOS 用户在创建虚拟机时，能够为用户提供虚拟机密钥对，保证虚拟机访问过程中的安全性。

合规性情况：符合

⑥ 数据备份恢复

a） 云服务客户应在本地保存其业务数据的备份；

安全措施：数据备份

保护对象：业务数据

安全能力：

（1）H3C CAS 与 ONEStor 深度融合，用户可将数据存储在 ONEStor 保证数据高可用；

（2）H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式；

（3）租户根据业务需求，选择适当的方式在本地保存其业务数据。

合规性情况：符合

b） 应提供查询云服务客户数据及备份存储位置的能力；

安全措施：资源监控

保护对象：存储数据

安全能力：

（1）H3C CAS 可查看虚拟机运行状态、存储位置；

（2）云服务客户在创建虚拟机时，可选择存储磁盘的存储池，在存储池中可查看虚拟机对应的存储卷。

合规性情况：符合

c） 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；

安全措施：数据备份

保护对象：存储数据

安全能力：

（1）H3C Unistor 支持多副本存储（2-5），各副本间内容保持一致。

合规性情况：符合

d） 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

安全措施：数据迁移

保护对象：配置文件、业务数据、鉴别信息、存储数据

安全能力：

（1）新华三提供迁移工具 Movesure、迁移服务，支持热迁移、冷迁移。

合规性情况：符合

⑦ 剩余信息保护

a） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

安全措施：残余数据清除

保护对象：配置文件、业务数据、鉴别信息、存储数据

安全能力：

（1）虚拟机所有的内存和存储空间被回收时，用户可根据需求进行选择，H3C CAS 提供彻底销毁数据功能，通过写零的方式进行完全清除；

（2）H3C CAS 提供虚拟回收保存期功能。

合规性情况：符合

b） 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

安全措施：残余数据清除

保护对象：配置文件、业务数据、鉴别信息、存储数据

安全能力：

（1）用户删除数据存储卷的时候，各副本会同步删除。

合规性情况：符合

5) 安全管理中心

① 集中管控

a） 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；

安全措施：资源调度与分配

保护对象：云平台

安全能力：

（1）H3C CloudOS 对物理资源、虚拟资源进行统一调度、分配；

（2）H3C SecCloud OMP 对安全资源进行统一调度、分配。

合规性情况：符合

b） 应保证云计算平台管理流量与云服务客户业务流量分离；

安全措施：带外管理，网络隔离

保护对象：云平台

安全能力：

（1）建立带外管理网，保证管理流量和业务流量分离；

（2）安全管理区和业务区边界部署了防火墙，对跨区域的流量进行策略控制。

合规性情况：符合

c） 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；

安全措施：账号授权、安全审计

保护对象：云平台

安全能力：

（1）云平台侧 H3C 态势感知系统能够收集全网日志，对日志进行集中分析，并进行细粒度展示；





（2）H3C 堡垒机支持云平台侧和云服务客户侧的日志收集。

合规性情况：符合

d） 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

安全措施：资源监控

保护对象：云平台

安全能力：

（1）H3C 态势感知系统支持全网全流量的监测，能够对所有的网络设备、安全设备、服务器、虚拟机进行集中监测；

（2）H3C CloudOS 、H3C SecCloud OMP 管理平台为云平台侧和云服务客户侧分别分配账户，可对两侧各自部分的资源进行集中监测。

合规性情况：符合

6) 安全建设管理

云服务客户应根据业务系统安全建设能力需求，依据下列要求选择合适的云服务商并进行相关约定。

① 云服务商选择

a） 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；

安全措施：——

安全能力：H3C 云计算环境为云服务提供商，云平台能够承载 4 级业务应用系统所需要的安全防护能力。

b） 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c） 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

d） 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；

e） 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。

② 供应链管理

a） 应确保供应商的选择符合国家有关规定；

安全措施：——

保护对象：——

安全能力：

（1）H3C 云计算环境组网时选用的网络、计算、存储等设备均符合国家相关要求，H3C SecCloud OMP 安全产品准许销售，已获得销售许可证；

（2）云服务客户根据供应商选择要求，确保供应商的选择符合国家有关规定。

合规性情况：符合

b） 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；

安全措施：——

保护对象：——

安全能力：

（1）H3C 云计算环境态势感知服务推送最新的安全事件信息，以保证第一时间传达给云服务客户。

合规性情况：符合

c) 应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

安全措施：——

保护对象：——

安全能力：

（1）H3C 云计算环境的变更会通过 H3C SecCloud OMP 进行公告，以保证第一时间传达；

（2）H3C 云计算环境提供一对一服务，变更的通知会及时送达，提供安全风险的应急响应。

合规性情况：符合

7) 安全运维管理

① 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

安全措施：——

保护对象：——

安全能力：

H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，基本运维地点在中国境内。

合规性情况：符合

### 3.4.2 新华三安全云合规性分析

1 安全合规能力汇总分析

新华三云计算平台在网络安全等级保护第四级安全通用要求和云计算扩展要求的测评项指标选取情况如图 3.14，各技术层面（安全类）不同控制点的符合性结果汇总统计如下：

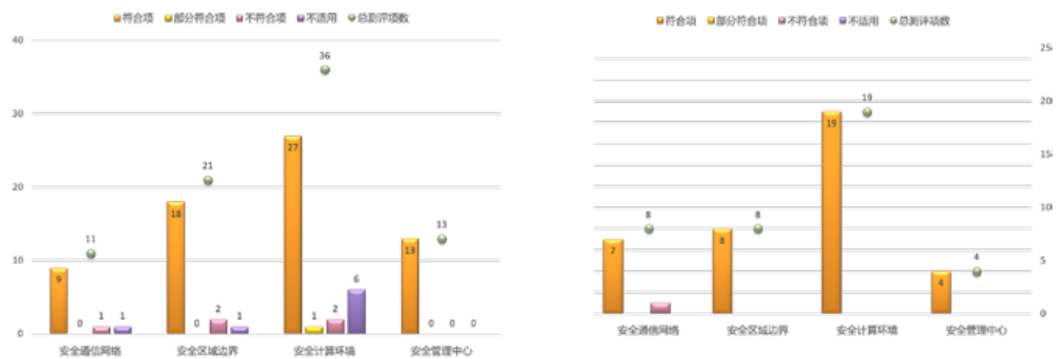
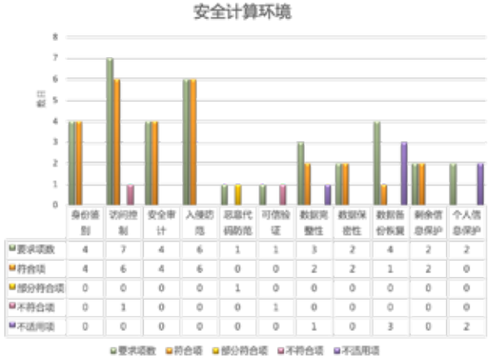



图 3.14 网络安全等级保护基本要求（四级）测评项数



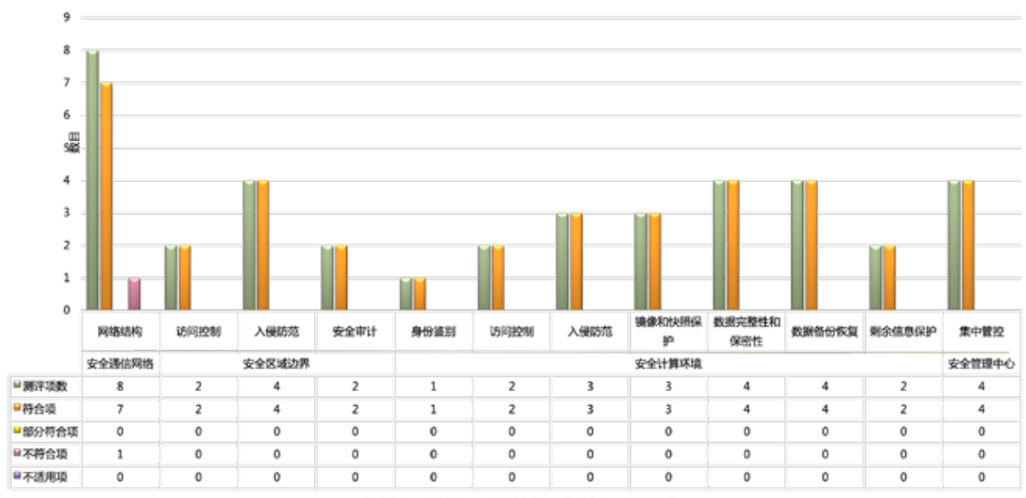








安全扩展要求（云计算）



安全扩展要求（云计算）


| | 基础设施位置 | 云服务商选择 | 供应链管理 | 云计算环境管理 |
|---|---|---|---|---|
| | 安全物理环境 | 安全建设管理 | | 安全运维管理 |
| 测评项数 | 1 | 5 | 3 | 1 |
| 符合项 | 1 | 1 | 3 | 1 |
| 部分符合项 | 0 | 0 | 0 | 0 |
| 不符合项 | 0 | 0 | 0 | 0 |
| 不适用项 | 0 | 4 | 0 | 0 |

2　安全合规性总体分析

公安部信息安全等级保护评估中心对新华三云计算平台实施安全评估，确认由新华三云计算组件 H3C CloudOS（E3106）、H3C CAS（E0530H02）、H3C SDN（E2507）及 H3C SecCloud OMP（E1104）构建的云计算平台基本具备依据 GB/T 22239 −2019《信息安全技术 网络安全等级保护基本要求》制定的云计算平台等级保护 2.0 合规能力规范（第三、四级）要求的安全技术能力：

在安全通信网络方面，新华三云计算平台态势感知系统对全网全流量进行监测分析，可通过部署 IMC 对网络设备的性能进行实时监控，对网络拓扑进行实时展示，H3C SDN 可对云服务客户侧网络拓扑进行实时更新；整个云计算平台的网络架构从接入层到汇聚层，实现了节点冗余和链路 LLB 负载分担，在满足带宽收敛和保证业务性能同时保证整个业务系统的高可用；数据通信传输过程中，数据链路采用 IPsec VPN，用户远程访问采用 SSL VPN，云平台内部管理使用 HTTPS 访问方式，能够保障通信链路中数据的完整性和保密性。

在安全区域边界方面，新华三云计算互联网出口边界部署出口防火墙，业务区域边界部署虚拟防火墙、安全管理区边界部署独立防火墙、安全资源池部署虚拟防火墙，在防火墙侧配置有效的 ACL 策略，对跨边界的访问和数据流进行控制，并对各安全域边界处跨区域的攻击行为进行检测、记录；新华三云计算环境中部署的下一代防火墙含 IPS 模块，支持第七层应用协议和应用内容的访问控制功能；态势感知系统（资产管理）、服务器安全监测系统可以实时对非授权接入的设备进行监测、告警。

在安全计算环境方面，新华三云计算系列产品本地均可设置口令复杂度策略、登录失败次数、用户三权分立、基于用户角色的权限分配及安全审计日志等；新华三态势感知系统、日志审计产品支持全网日志收集，包括网络设备、安全设备、服务器等云上各类组件的安全审计，包括安全日志、网络审计日志、数据库审计日志、SSLVPN 日志、DLP 审计日志、运维日志、流量日志等；主机层面安装亚信安全服务器深度安全防护系统，支持防恶意软件、防火墙、入侵防御、完整性监控、日志审查，并支持病毒查杀功能；新华三云计算为云服务客户提供迁移工具 Movesure、迁移服务，支持热迁移、冷迁移，在用户资源释放时采用写零的数据清除机制，保证残留数据清除；H3C ONEStore 分布式存储，保证所有数据落地到底层存储时都会同步到底层多副本上，无论是新增、修改还是删除数据，均可保障用户数据的可靠性和一致性。

在安全管理中心方面，H3C 云计算环境态势感知服务能够对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测，H3C CloudOS 管理平台集中监测网络设备、安全设备、服务器的运行情况进行监测，H3C SecCloud OMP 管理平台对安全资源的运行状况、资源使用情况进行监测，H3C 服务器集中监测对服务器运行状况、资源使用情况进行监测，SDN 控制器运维模块包括物理网络、逻辑网络、拓扑映射、网络健康监控、流量监控；H3C 态势感知系统、日志审计产品能够收集全网日志，对日志进行集中分析，并进行细粒度展示，态势感知集群部署，至少保存 6 个月以上，可手动或自动转存至第三方设备，支持各类安全事件的分类、识别、分析、报警。





# 第 4 章　新华三云计算安全等保合规白皮书应用价值

## 4.1　应用价值

### 4.1.1　呈现新华三云计算平台云平台等保合规能力

白皮书阐述了新华三云计算平台等保 2.0 合规能力模型、新华三云计算平台的整体架构、网络及安全防护架构和安全技术能力以及新华三云计算平台等保 2.0 合规状况，详细介绍了新华三云计算安全技术能力，包括物理层安全、硬件安全、虚拟化资源层安全、H3C CloudOS、H3C CAS、H3C VCFC、H3C SecCloud OMP 以及安全组件的防护能力。其中，物理安全防护能力由 IDC 运营方负责保障，硬件安全防护能力主要从硬件固件安全方面进行描述，虚拟化安全防护采用容器化技术，虚拟防火墙有独立的进程上下文运行空间，容器与容器之间的运行空间完全隔离，云安全产品防护能力主要是对云防火墙、安全组、态势感知、服务器安全监测系统等产品功能进行描述。

白皮书根据云计算平台等保 2.0 合规模型，呈现新华三云计算平台等保 2.0 合规状况，依据 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》中第三级和第四级安全要求，深入分析了新华三云计算平台安全技术能力与等保 2.0 标准相关要求的匹配度，给出了新华三云计算平台安全技术合规能力状况。

### 4.1.2　识别新华三云计算平台等保测评指标

基于 1.3 节云计算安全责任分担模型，针对新华三云计算为各行业用户交付的 IaaS、PaaS 模式，白皮书识别出两种模式下云服务商和用户的安全责任划分（参见附录 A）。依据 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》中第三级和第四级安全要求，白皮书分析了每个要求项的安全责任归属，主要包括三种情况：一是安全责任归属云服务商，二是安全责任归属用户，三是安全责任由云服务商和用户共担。云服务商和用户可以通过白皮书快速掌握各自的安全责任。

### 4.1.3　为相关用户或机构提供技术参考

针对云计算平台用户，白皮书为其了解、掌握和选择新华三云计算安全解决方案提供了技术参考。白皮书根据云计算平台等保 2.0 合规模型，呈现新华三云计算平台等保 2.0 合规状况，能够帮助用户在选择新华三云计算安全解决方案时获得合规预期。针对云计算环境中安全责任划分往往比较困难的情况，白皮书识别出新华三云计算平台在为各行业用户交付的 IaaS、PaaS 模式下云服务商和云服务客户的安全责任划分，能够帮助云服务客户快速掌握自身的安全责任，同时有助于用户合理选择、配置新华三云计算平台不同保护等级、不同交付模式下属于“变量”的安全能力（附录 B），从而确保云计算平台和云服务客户业务应用系统满足等保合规要求。

针对等级保护测评机构，白皮书为其开展新华三云计算平台等级测评工作提供技术参考。白皮书阐述了新华三云计算平台的整体架构和安全技术能力，可以帮助等级保护测评机构快速了解和掌握新华三云计算平台。白皮书给出了新华三云计算平台为各行业用户交付的 IaaS、PaaS 模式下云服务商和用户各自的安全责任，可以帮助等级保护测评机构科学合理地选择安全测评对象和指标。白皮书深入分析了新华三云计算平台安全技术能力与等保 2.0 标准相关要求的匹配度，给出了新华三云计算平台安全技术合规能力状况，测评机构可以参考新华三云计算平台等保 2.0 合规状况，结合用户业务实际使用情况，对采用新华三云计算技术的云平台及其上业务应用系统开展测评工作。白皮书将新华三云计算平台的安全技术能力分为定量和变量两种，等级保护测评机构应重点关注用户根据业务需求部署的“变量”及用户自行建设的安全技术能力的合规情况。

## 4.2 应用方法

### 4.2.1 新华三云计算用户

**1. 获得新华三云计算平台等保合规预期**

白皮书依据 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》中第三级和第四级安全要求及新华三云计算等保 2.0 合规模型，对新华三云计算平台等保 2.0 安全合规性进行评估，分析新华三云计算平台安全措施、保护对象以及安全技术能力。用户在云平台安全体系建设初期，可参考白皮书第 3 章节 3.4 部分、附录 A 安全责任划分及附录 B 安全合规能力部分，预估新华三云计算平台的安全能力、等保合规状况；用户在新华三云计算平台运营阶段，可参考白皮书附录 A 安全责任划分及附录 B 安全合规能力部分，了解当前云平台的安全能力以及云平台的等保合规情况。本白皮书可帮助用户分析新华三云计算平台的安全技术能力与等级保护合规性要求的匹配度，得出新华三云计算平台等保 2.0 合规状况，帮助用户在选择或运营新华三云计算平台时获得等保合规性预期。以安全通用要求中安全通信网络为例，新华三云平台合规情况如下表所示。

| 等保 2.0 基本要求 | | | 保护对象 | 安全技术能力 | 合规情况 |
|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | |
| 安全通信网络 | 网络架构 | a）应保证网络设备的业务处理能力满足业务高峰期需要； | 出口路由器、核心交换机、接入交换机、负载均衡 | 1、H3C 云计算环境组网时，根据业务需求可供用户选择高中低档网络设备以满足业务处理能力；<br>2、新华三提供的网络设备安全设备支持 SOP、SCF 横向扩展，业务高峰期设备可按需扩展；<br>3、H3C 态势感知服务系统对设备日志进行分析告警，保证设备业务处理能力出现异常时，实时响应；<br>4、新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对设备性能进行监控，发现异常时进行报警提示。 | 符合 |
| | | b）应保证网络各个部分的带宽满足业务高峰期需要； | 出口路由器、核心交换机、接入交换机、负载均衡 | 1、H3C 态势感知服务系统支持对网络链路进行实时监控告警；<br>2、新华三 LLB 负载均衡设备能够对多出口链路进行合理的流量分担， SLB 负载均衡设备可以将客户对数据中心服务的访问请求合理地分发到数据中心的各台服务器上，以此来保证各部分业务带宽的高可用；<br>3、新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对网络链路的能力进行监控、告警。 | 符合 |
| | | c） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | 网络架构、云平台内部 VPC | 1、H3C 云计算环境在组网时划分了安全管理区、安全资源池以及业务区，各区域间相互隔离；<br>2、不同区域间的网络通过防火墙实现不同网络安全域的划分；<br>3、业务区不同的客户分属不同的 VPC，跨 VPC 间通过虚拟防火墙实现南北向流量隔离，同一 VPC 内也部署虚拟防火墙进行安全域隔离。 | 符合 |
| | | d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； | 网络架构、云平台、业务应用系统 | 1、H3C 云计算环境出口部署边界防火墙；<br>2、安全管理区边界部署独立的防火墙，安全资源池部署虚拟防火墙实现不同安全域的隔离，业务区每个客户出口部署虚拟防火墙，每个客户通过 VRF 进行路由隔离；<br>3、跨 VPC 间通过虚拟防火墙实现南北向流量隔离，同一 VPC 内也部署虚拟防火墙进行安全域隔离。 | 符合 |
| | | …… | | | |

**2. 查找新华三云计算平台用户的安全责任**

白皮书构建了云计算安全责任分担模型，基于安全责任分担模型及《网络安全等级保护云计算测评指引》识别出新华三云计算为不同行业用户交付的 IaaS、PaaS 模式下云服务商和用户的安全责任划分，参考白皮书 1.3 云安全责任分担模型及附录 A 安全责任划分的内容，能够帮助用户快速查找到其应该承担的安全责任。以云计算安全扩展要求中安全物理环境、安全通信网络和安全区域边界为例，云服务商和新华三云计算用户的安全责任划分如下表所示。

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全物理环境 | 基础设施位置 | 应保证云计算基础设施位于中国境内。 | | ● | | ● |
| 安全通信网络 | 网络架构 | a）应保证云计算平台不承载高于其安全保护等级的业务应用系统； | | ● | | ● |
| | | b）应实现不同云服务客户虚拟网络之间的隔离； | ● | | ● | |
| | | …… | | | | |
| 安全区域边界 | 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | ● | ● | ● | |
| | | b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | ● | ● | ● | |
| | | …… | | | | |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。

**3. 查找新华三云计算平台用户需实施的安全技术能力**

白皮书附录 B 安全合规能力部分识别了新华三云计算的安全技术能力所涉及的产品，并对安全能力进行了定量和变量的识别，定量是指云平台原生的安全能力或新华三云计算为用户组网时默认提供的安全防护能力，变量是指根据业务需求选择交付或第三方产品提供的安全防护能力。用户在确定云计算平台保护等级后，可以根据白皮书合理选择、配置新华云计算安全能力对应的产品，从而确保用户组网的云计算平台和业务系统满足等保合规要求。以安全通用要求中安全通信网络为例，新华三云计算安全技术能力以及涉及的产品如下表所示。

白皮书应用方法

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全通信网络 | 网络结构 | a) 应保证网络设备的业务处理能力满足业务高峰期需要； | 1、H3C 云计算环境组网时，根据业务需求可供用户选择高中低档网络设备已满足业务处理能力。<br>2、新华三提供的网络设备安全设备支持 SOP、SCF 横向扩展，业务高峰期设备可按需扩展；<br>3、H3C 态势感知服务系统对设备日志进行分析告警，保证设备业务处理能力出现异常时，实时响应；<br>4、新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对设备性能进行监控，发现异常时进行报警提示。 | 高性能网络设备<br>支持 SOP、SCF 的网络设备<br>态势感知<br>IMC | 1、2、3 | 4 |
| | | b) 应保证网络各个部分的带宽满足业务高峰期需要； | 1、H3C 态势感知服务系统支持对网络链路进行实时监控告警；<br>2、新华三 LLB 负载均衡设备能够对外流量链路进行负载， SLB 负载均衡设备可进行内部服务器链路流量负载，以此来保证各部分业务带宽的高可用；<br>3、新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对网络链路的能力进行监控、告警。 | 态势感知<br>IMC<br>负载均衡（SLB、LLB） | 1、2 | 3 |
| | | c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | 1、H3C 云计算环境在组网时划分了安全管理区、安全资源池以及业务区，各区域间相互隔离；<br>2、不同区域间的网络通过防火墙实现不同网络安全域的划分；<br>3、业务区不同的客户分属不同的 VPC，跨 VPC 间通过虚拟防火墙实现南北向流量隔离，同一 VPC 内也部署虚拟防火墙进行安全域隔离。 | VxLAN<br>虚拟防火墙<br>VPC | 1、2 | 3 |
| | | d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； | 1、H3C 云计算环境出口部署边界防火墙；<br>2、安全管理区边界部署独立的防火墙，安全资源池部署虚拟防火墙实现不同安全域的隔离，业务区每个客户出口部署虚拟防火墙，每个客户通过 VRF 进行路由隔离；<br>3、跨 VPC 间通过虚拟防火墙实现南北向流量隔离，同一 VPC 内也部署虚拟防火墙进行安全域隔离。 | 虚拟防火墙<br>出口防火墙 | 1、2、3 | |
| | | e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。 | 1、网络架构从接入层到汇聚层，实现节点冗余和链路 LLB 负载分担，在满足带宽收敛和保证业务性能同时满足整个业务系统的高可用；<br>2、H3C 云计算环境在组网时防火墙通过堆叠的形式，交换机通过 M-LAG 的方式，服务器通过集群的方式，以保证设备可用；<br>3、负载均衡设备提供智能 DNS 服务，保证链路、系统的高可用。 | 负载均衡（SLB、LLB）<br>智能 DNS | 1、2 | 3 |
| | | f) 应按照业务服务的重要程度分配带宽，优先保障重要业务。 | 1、新华三云计算环境中可通过链路负载均衡（LLB）、服务器负载均衡（SLB）保障业务带宽；<br>2、新华三云计算环境中的所有路由器、交换机等均可配置 QOS 策略，可根据业务情况进行恰当的 QOS 策略配置，保证重要业务的带宽分配；<br>3、SDN 控制器可自动下发 QOS 策略，保证各部分业务的带宽。 | 负载均衡（SLB、LLB）<br>SDN 控制器 | 1、2、3 | |
| …… | | | | | | |

### 4.2.2 等保测评机构

1. 掌握云服务商和新华三云计算平台用户的安全责任划分

白皮书针对新华三云计算典型 IaaS、PaaS 模式应用场景，结合云安全责任分担模型以及 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》中第三级和第四级安全要求，明确地给出了云服务商和用户的安全责任划分。本白皮书可给予等级保护测评机构在对新华三云计算平台和云平台上业务应用系统进行等级测评时测评指标选取的指导性建议，参考白皮书 1.3 云安全责任分担模型及附录 A 云安全责任划分的内容，等级保护测评机构可快速筛选哪些要求项是只需要测评新华三云计算平台，哪些要求项是只需要测评云服务客户业务应用系统，哪些安全项是既要测评新华三云计算平台又要测评云服务客户业务应用系统。以云计算安全扩展要求中安全计算环境为例，云服务商和新华三云计算平台用户的安全责任划分如下表所示。

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全计算环境 | 身份鉴别 | 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 | ● | ● | ● | ● |
| | 访问控制 | a）应保证当虚拟机迁移时，访问控制策略随其迁移； | ● | | ● | |
| | | b）应允许云服务客户设置不同虚拟机之间的访问控制策略。 | ● | | ● | |
| | 入侵防范 | a）应能检测虚拟机之间的资源隔离失效，并进行告警； | ● | | ● | |
| | | b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； | ● | | ● | |
| | | c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 | ● | | ● | |
| | …… | …… | | | | |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。

白皮书应用方法

**2. 明确云平台侧和云用户侧所对应的保护对象**

白皮书针对新华三云计算为各行业用户的 IaaS、PaaS 交付模式，结合 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》中第三级和第四级安全要求以及《网络安全等级保护云计算测评指引》中测评对象选取方法，明确了新华三云计算平台的保护对象，并给出了等级保护基本要求中每个测评项在云平台侧和用户侧所对应的测评对象，能够有效指导等级保护测评机构对新华三云计算平台和及云平台上业务应用系统开展等级测评工作。以安全通用要求中安全计算环境为例，平台侧和用户侧所对应的保护对象如下表所示。

| 等保 2.0 基本要求 | | | 保护对象 |
|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | |
| 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机<br>云服务客户侧：虚拟机、数据库、业务应用系统 |
| | | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机<br>云服务客户侧：虚拟机、数据库、业务应用系统 |
| | | c）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机<br>云服务客户侧：虚拟机、数据库、业务应用系统 |
| | | d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 平台侧：出口路由器、核心交换机、接入交换机、出口防火墙、区域边界防火墙、物理服务器、虚拟机镜像、H3C CloudOS、H3C CAS 虚拟化平台、H3C SecCloud OMP 安全云管理平台、宿主机<br>云服务客户侧：虚拟机、数据库、业务应用系统 |
| | | …… | |

**3. 参考新华三云计算等保 2.0 合规状况**

依据 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》中第三级和第四级安全要求，白皮书深入分析了新华三云计算平台安全技术能力与等保 2.0 标准相关要求的匹配度，给出了新华三云计算平台安全技术合规能力状况，测评机构可以参考新华三云计算平台等级保护 2.0 合规状况，结合用户业务实际使用情况，对采用新华三云计算技术的云平台及其上业务应用系统开展测评工作。以云计算安全扩展要求中安全通信网络为例，新华三云计算平台的安全技术能力如下表所示。

| 等保 2.0 基本要求 | | | 安全技术能力 |
|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | |
| 安全通信网络 | 网络架构 | a）应保证云计算平台不承载高于其安全保护等级的业务应用系统； | H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，部署在用户内部或租用运营商机房。 |
| | | b）应实现不同云服务客户虚拟网络之间的隔离； | H3C 云计算环境通过等级保护安全性评估具有承载四级应用系统的安全防护能力。 |
| | | c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； | 1）H3C 云计算环境专有网络（Virtual Private Cloud）VPC 采用隧道技术，帮助用户构建出一个隔离的网络环境，实现不同云服务客户间的网络资源的隔离；<br>2）同一 VPC 内通过虚拟防火墙进行安全域隔离；<br>3）不同 VPC 间通过 VRF 进行路由隔离，在云端部署虚拟防火墙，划分网络安全域，实现不同 VPC 间的访问控制；<br>4）虚拟防火墙能够帮助用户实现云计算环境中东西向流量的隔离。 |
| | | d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； | 1）H3C 安全有云在通信传输层面为云服务客户提供 IPsec VPN、SSL VPN 服务，云平台内部所有通讯访问均通过 https 实现，保证了传输过程中的保密性；<br>2）在边界防护层面，部署出口防火墙，各安全域边界处部署防火墙，对常见的 Web 应用攻击进行通过 WAF 拦截旁路阻断；<br>3）H3C 下一代防火墙包含 IPS 模块，提供入侵防范功能，态势感知服务对全网流量进行监测；<br>4）基于虚拟防火墙实现灵活的访问控制规则。 |
| | | e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务； | H3C 云计算环境所有安全产品（服务）均支持云服务客户根据业务需求，自主定义安全访问路径，设置安全组策略，自主选择使用各种安全组件； |
| | | g) 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式； | 新华三提供安全数据交换系统，能够实现不同安全域间的数据隔离、交换，云服务客户可根据业务需求选择边界数据交换方式。 |
| | | …… | |

## 4.3 新华三云计算平台案例

**1. 项目背景**

AC 省政务云领导小组创新性地提出了 1+N+N+1 的建设模式，即一个云监管平台，多个云服务商平台，多个部门整合平台和一个云灾备平台。基于新华三云计算技术，采用新华三政务云整体解决方案来构建，提供了全面、高效、安全的云服务。

**2. 建设内容**

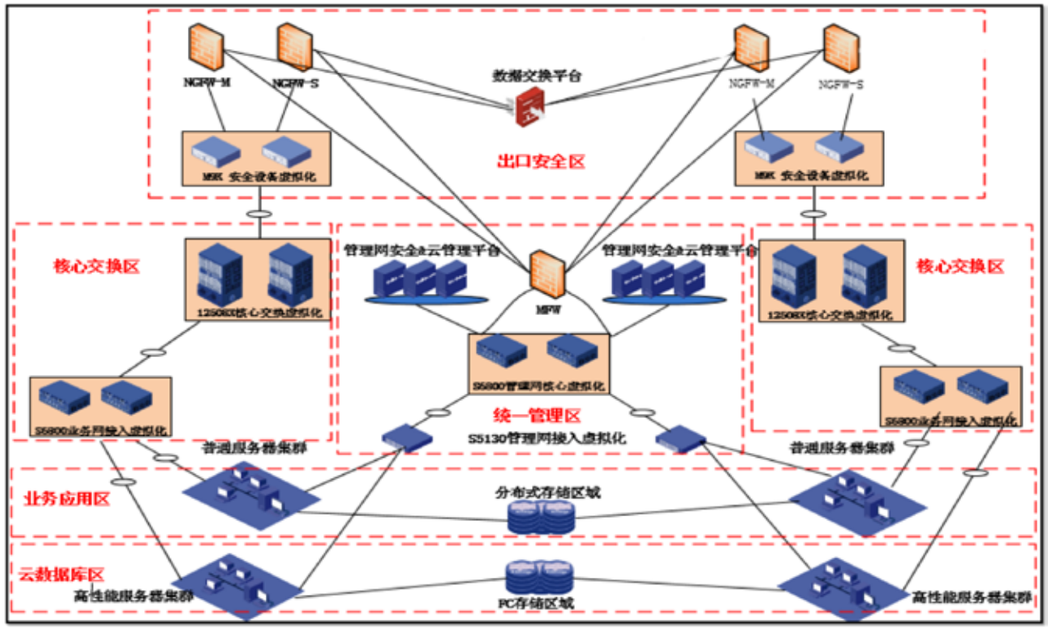
模式创新：1+N+N+1 模式成为国内政务云建设主流模式，被中央网信办作为先进事例在全国电子政务培训会上介绍。

安全可靠：AC 省政务云建设为等保三级，保障了云计算环境下不同安全域间的隔离。

解决方案：基于新华三云计算安全计算，采用新华三政务云安全的整体解决方案。

落地实施：新华三云计算平台是 AC 省政务云第一个正式迁移上线系统的云平台，通过下一代防火墙、综合安全网关、负载均衡、WAF、跨网交换系统做好边界安全防护，再结合态势感知、堡垒机、日志审计、安全管理平台打造可视化云平台安全；通过虚拟防火墙、虚拟负载均衡、虚拟堡垒机、虚拟 WAF、结合虚拟日志审计打造风险可控的云租户安全。

3. 网络拓扑





# 附录 A　安全责任

## A.1　网络安全等级保护通用要求项安全责任

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全物理环境 | 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； | | ● | | ● |
| | | b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 | | ● | | ● |
| | 物理访问控制 | a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员； | | ● | | ● |
| | | b）重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。 | | ● | | ● |
| | 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； | | ● | | ● |
| | | b）应将通信线缆铺设在隐蔽　安全处； | | ● | | ● |
| | | c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。 | | ● | | ● |
| | 防雷击 | a）应将各类机柜、设施和设备等通过接地系统安全接地； | | ● | | ● |
| | | b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 | | ● | | ● |
| | 防火 | a）应将各类机柜、设施和设备等通过接地系统安全接地； | | ● | | ● |
| | | b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； | | ● | | ● |
| | | c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 | | ● | | ● |
| | 防水和防潮 | a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； | | ● | | ● |
| | | b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； | | ● | | ● |
| | | c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 | | ● | | ● |

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全物理环境 | 防静电 | a）应采用防静电地板或地面并采用必要的接地防静电措施； | | ● | | ● |
| | | b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 | | ● | | ● |
| | 温湿度控制 | 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 | | ● | | ● |
| | 电力供应 | a）应在机房供电线路上配置稳压器和过电压防护设备； | | ● | | ● |
| | | b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求； | | ● | | ● |
| | | c）应设置冗余或并行的电力电缆线路为计算机系统供电； | | ● | | ● |
| | | d）应提供应急供电设施。 | | ● | | ● |
| | 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； | | ● | | ● |
| | | b）应对关键设备或关键区域实施电磁屏蔽。 | | ● | | ● |
| 安全通信网络 | 网络架构 | a）应保证网络设备的业务处理能力满足业务高峰期需要； | ● | ● | ● | |
| | | b）应保证网络各个部分的带宽满足业务高峰期需要； | ● | ● | ● | |
| | | c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | ● | ● | ● | |
| | | d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； | ● | ● | ● | |
| | | e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性； | ● | ● | ● | |
| | | f）应可按照业务服务的重要程度分配带宽，优先保障重要业务。 | ● | ● | ● | |
| | 通信传输 | a）应采用密码技术保证通信过程中数据的完整性； | ● | ● | ● | |
| | | b）应采用密码技术保证通信过程中数据的保密性； | ● | ● | ● | |
| | | c）应在通信前基于密码技术对通信的双方进行验证或认证； | ● | ● | ● | |
| | | d）应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。 | ● | ● | ● | |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。





| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全通信网络 | 可信验证 | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。 | ● | ● | ● | |
| 安全区域边界 | 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | ● | ● | ● | |
| | | b）应能够对非授权设备私自联到内部网络的行为进行限制或检查； | ● | ● | ● | |
| | | c）应能够对内部用户非授权联到外部网络的行为进行限制或检查； | ● | ● | ● | |
| | | d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络； | ● | ● | ● | |
| | | e）应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断； | ● | ● | ● | |
| | | f）应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。 | ● | ● | ● | |
| | 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | ● | ● | ● | |
| | | b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | ● | ● | ● | |
| | | c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许 / 拒绝数据包进出； | ● | ● | ● | |
| | | d）应能根据会话状态信息为进出数据流提供明确的允许 / 拒绝访问的能力； | ● | ● | ● | |
| | | e）应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。 | ● | ● | ● | |
| | 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | ● | ● | ● | |

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全区域边界 | 入侵防范 | b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | ● | ● | ● | |
| | | c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | ● | ● | ● | |
| | | d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。 | ● | ● | ● | |
| | 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | ● | ● | ● | |
| | | b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | ● | ● | ● | |
| | 安全审计 | a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | ● | ● | ● | |
| | | b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | ● | ● | ● | |
| | | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 | ● | ● | ● | |
| | 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。 | ● | ● | ● | |
| 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | ● | ● | ● | ● |
| | | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | ● | ● | ● | ● |
| | | c）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | ● | ● | ● | ● |
| | | d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | ● | ● | ● | ● |
| | 访问控制 | a）应对登录的用户分配账户和权限； | ● | ● | ● | ● |
| | | b）应重命名或删除默认账户，修改默认账户的默认口令； | ● | ● | ● | ● |
| | | c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | ● | ● | ● | ● |
| | | d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | ● | ● | ● | ● |
| | | e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | ● | ● | ● | ● |
| | | f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | ● | ● | ● | ● |
| | | g）应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。 | ● | ● | ● | ● |
| | 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | ● | ● | ● | ● |
| | | b）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | ● | ● | ● | ● |
| | | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | ● | ● | ● | ● |
| | | d）应对审计进程进行保护，防止未经授权的中断。 | ● | ● | ● | ● |
| | 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | ● | ● | ● | |
| | | b）应关闭不需要的系统服务、默认共享和高危端口； | ● | ● | ● | |
| | | c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | ● | ● | ● | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全计算环境 | 入侵防范 | d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | ● | ● | ● | ● |
| | | e )应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | ● | ● | ● | ● |
| | | f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | ● | ● | ● | |
| | 恶意代码防范 | 应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | ● | ● | ● | |
| | 可信验证 | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。 | ● | ● | ● | |
| | 数据完整性 | a）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | ● | ● | ● | ● |
| | | b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | ● | ● | ● | ● |
| | | c）在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。 | ● | ● | ● | ● |
| | 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | ● | ● | ● | ● |
| | | b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | ● | ● | ● | ● |
| | 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | ● | ● | ● | ● |
| | | b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | ● | ● | ● | ● |
| | | c）应提供重要数据处理系统的热冗余，保证系统的高可用性； | ● | ● | ● | ● |
| | | d）应建立异地灾难备份中心，提供业务应用的实时切换。 | ● | ● | ● | ● |
| | 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | ● | ● | ● | ● |
| | | b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | ● | ● | ● | ● |
| | 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | ● | ● | ● | ● |
| | | b）应禁止未授权访问和非法使用用户个人信息。 | ● | ● | ● | ● |
| 安全管理中心 | 系统管理 | a )应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； | ● | ● | ● | ● |
| | | b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 | ● | ● | ● | ● |
| | 审计管理 | a )应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； | ● | ● | ● | ● |
| | | b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等 | ● | ● | ● | ● |
| | 安全管理 | a )应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； | ● | ● | ● | ● |
| | | b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 | ● | ● | ● | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全管理中心 | 集中管控 | a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； | ● | ● | ● | |
| | | b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； | ● | ● | ● | |
| | | c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； | ● | ● | ● | |
| | | d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； | ● | ● | ● | ● |
| | | e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； | ● | ● | ● | ● |
| | | f）应能对网络中发生的各类安全事件进行识别、报警和分析； | ● | ● | ● | |
| | | g）应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。 | ● | ● | ● | ● |
| 安全策略和管理制度 | 安全策略 | 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。 | | ● | | ● |
| | 管理制度 | a）应对安全管理活动中的各类管理内容建立安全管理制度； | | ● | | ● |
| | | b）应对要求管理人员或操作人员执行的日常管理操作建立操作规程； | | ● | | ● |
| | | c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系。 | | ● | | ● |
| | 制定和发布 | a）应指定或授权专门的部门或人员负责安全管理制度的制定； | | ● | | ● |
| | | b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。 | | ● | | ● |
| | 评审和修订 | 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 | | ● | | ● |
| 安全管理机构 | 岗位设置 | a）应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权； | | ● | | ● |
| | | b）应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； | | ● | | ● |
| 安全管理机构 | 岗位设置 | c）应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。 | | ● | | ● |
| | 人员配备 | a）应配备一定数量的系统管理员、网络管理员、安全管理员等； | | ● | | ● |
| | | b）应配备专职安全管理员，不可兼任； | | ● | | ● |
| | | c）关键事务岗位应配备多人共同管理。 | | ● | | ● |
| | 授权和审批 | a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； | | ● | | ● |
| | | b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； | | ● | | ● |
| | | c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。 | | ● | | ● |
| | 沟通和合作 | a）应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题； | | ● | | ● |
| | | b）应加强与网络安全管理部门、各类供应商、业界专家及安全组织的合作与沟通； | | ● | | ● |
| | | c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 | | ● | | ● |
| | 审核和检查 | a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； | | ● | | ● |
| | | b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； | | ● | | ● |
| | | c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。 | | ● | | ● |
| 安全管理人员 | 人员录用 | a）应指定或授权专门的部门或人员负责人员录用； | | ● | | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全管理人员 | 人员录用 | b）应对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核； | | ● | | ● |
| | | c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议； | | ● | | ● |
| | | d）应从内部人员中选拔从事关键岗位的人员。 | | ● | | ● |
| | 人员离岗 | a）应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； | | ● | | ● |
| | | b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。 | | ● | | ● |
| | 安全意识教育和培训 | a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； | | ● | | ● |
| | | b）应针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训； | | ● | | ● |
| | | c）应定期对不同岗位的人员进行技术技能考核。 | | ● | | ● |
| | 外部人员访问管理 | a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； | | ● | | ● |
| | | b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； | | ● | | ● |
| | | c）外部人员离场后应及时清除其所有的访问权限； | | ● | | ● |
| | | d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息； | | ● | | ● |
| | | e）对关键区域或关键系统不允许外部人员访问。 | | ● | | ● |
| 安全建设管理 | 定级和备案 | a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； | | ● | | ● |
| | | b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； | | ● | | ● |
| | | c）应保证定级结果经过相关部门的批准； | | ● | | ● |
| | | d）应将备案材料报主管部门和相应公安机关备案。 | | ● | | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。





| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全建设管理 | 安全方案设计 | a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； | | ● | | ● |
| | | b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件； | | ● | | ● |
| | | c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。 | ● | ● | | ● |
| | 产品采购和使用 | a）应确保信息安全产品采购和使用符合国家的有关规定； | ● | ● | ● | ● |
| | | b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； | | ● | ● | ● |
| | | c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单； | | ● | | ● |
| | | d）应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。 | | ● | | ● |
| | 自行软件开发 | a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； | | ● | | ● |
| | | b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； | | ● | | ● |
| | | c）应制定代码编写安全规范，要求开发人员参照规范编写代码； | | ● | | ● |
| | | d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制； | | ● | | ● |
| | | e）应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； | | ● | | ● |
| | | f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； | | ● | | ● |
| | | g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。 | | ● | | ● |
| | 外包软件开发 | a）应在软件交付前检测其中可能存在的恶意代码； | | ● | | ● |

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全建设管理 | 外包软件开发 | b）应保证开发单位提供软件设计文档和使用指南； | | ● | | ● |
| | | c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。 | | ● | | ● |
| | 工程实施 | a）应指定或授权专门的部门或人员负责工程实施过程的管理； | | ● | | ● |
| | | b）应制定工程实施方案控制安全工程实施过程； | | ● | | ● |
| | | c）应通过第三方工程监理控制项目的实施过程。 | | ● | | ● |
| | 测试验收 | a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； | | ● | | ● |
| | | b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 | ● | ● | | ● |
| | 系统交付 | a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； | ● | ● | ● | ● |
| | | b）应对负责运行维护的技术人员进行相应的技能培训； | ● | ● | ● | ● |
| | | c）应提供建设过程中的文档和指导用户进行运行维护的文档。 | | ● | ● | ● |
| | 等级测评 | a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； | | ● | | ● |
| | | b）应在发生重大变更或级别发生变化时进行等级测评； | | ● | | ● |
| | | c）应确保测评机构的选择符合国家有关规定。 | | ● | | ● |
| | 服务供应商选择 | a）应确保服务供应商的选择符合国家的有关规定； | | ● | | ● |
| | | b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务； | | ● | | ● |
| | | c）应定期监视、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 | ● | | | ● |
| 安全运维管理 | 环境管理 | a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； | ● | | | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。





| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全运维管理 | 环境管理 | b）应建立机房安全管理制度，对有关机房物理访问、物品带进带出机房和机房环境安全等方面的管理作出规定； | ● | | | ● |
| | | c）应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等； | ● | | | ● |
| | | d）应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等。 | ● | | | ● |
| | 资产管理 | a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； | ● | | | ● |
| | | b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； | ● | | | ● |
| | | c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。 | ● | ● | | ● |
| | 介质管理 | a )应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； | ● | ● | | ● |
| | | b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 | ● | | | ● |
| | 设备维护管理 | a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； | ● | | | ● |
| | | b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等； | ● | | | ● |
| | | c）信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密； | ● | | | ● |
| | | d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。 | | ● | | ● |
| | 漏洞和风险管理 | a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补； | | ● | | ● |

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全运维管理 | 漏洞和风险管理 | b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。 | | ● | | ● |
| | 网络和系统安全管理 | a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； | | ● | | ● |
| | | b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； | | ● | | ● |
| | | c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； | | ● | | ● |
| | | d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； | | ● | | ● |
| | | e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； | | ● | | ● |
| | | f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； | | ● | | ● |
| | | g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库； | | ● | | ● |
| | | h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； | | ● | | ● |
| | | i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； | | ● | | ● |
| | | j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。 | | ● | | ● |
| | 恶意代码防范管理 | a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； | | ● | | ● |
| | | b）应定期验证防范恶意代码攻击的技术措施的有效性。 | | ● | | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。





| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全运维管理 | 配置管理 | a）应记录和保存系统的基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等； | | ● | | ● |
| | | b）应将基本配置信息改变纳入系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 | | ● | | ● |
| | 密码管理 | a）应遵循相关密码国家标准和行业标准； | | ● | | ● |
| | | b）应使用国家密码管理主管部门认证核准的密码技术和产品； | | ● | | ● |
| | | c）应采用硬件密码模块实现密码运算和密钥管理。 | | ● | | ● |
| | 变更管理 | a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施； | | ● | | ● |
| | | b）应建立变更的申报和审批控制程序，依据程序控制系统所有的变更，记录变更实施过程； | | ● | | ● |
| | | c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 | | ● | | ● |
| | 备份与恢复管理 | a）应识别需要定期备份的重要业务信息、系统数据及软件系统等； | | ● | | ● |
| | | b）应规定备份信息的备份方式、备份频度、存储介质、保存期等； | | ● | | ● |
| | | c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 | | ● | | ● |
| | 安全事件处置 | a）应及时向安全管理部门报告所发现的安全弱点和可疑事件； | | ● | | ● |
| | | b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； | | ● | | ● |
| | | c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训； | | ● | | ● |

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全运维管理 | 安全事件处置 | d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序； | ● | ● | | ● |
| | | e）应建立联合防护和应急机制，负责处置跨单位安全事件； | | ● | ● | ● |
| | 应急预案管理 | a）应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容； | | ● | | ● |
| | | b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； | | ● | | ● |
| | | c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； | | ● | | ● |
| | | d）应定期对原有的应急预案重新评估，修订完善； | | ● | | ● |
| | | e）应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练。 | | ● | | ● |
| | 外包运维管理 | a）应确保外包运维服务商的选择符合国家的有关规定； | | ● | | ● |
| | | b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； | ● | ● | | ● |
| | | c）应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； | | ● | ● | ● |
| | | d）应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。 | | ● | | ● |

## A.2 网络安全等级保护云扩展要求项安全责任

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全物理环境 | 基础设施位置 | 应保证云计算基础设施位于中国境内。 | | ● | | ● |
| 安全通信网络 | 网络架构 | a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统； | | ● | | ● |
| | | b) 应实现不同云服务客户虚拟网络之间的隔离； | ● | | ● | |
| | | c) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； | ● | | ● | |
| | | d) 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； | ● | | ● | |
| | | e) 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务； | ● | | ● | |
| | | f) 应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问； | ● | | ● | |
| | | g) 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式； | ● | ● | ● | |
| | | h) 应为第四级业务应用系统划分独立的资源池。 | ● | ● | ● | ● |
| 安全区域边界 | 访问控制 | a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； | ● | ● | ● | |
| | | b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 | ● | ● | ● | |
| | 入侵防范 | a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | ● | | ● | |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| 安全区域边界 | 入侵防范 | b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | ● | ● | ● | |
| | | c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | ● | ● | ● | |
| | | d) 应在检测到网络攻击行为、异常流量情况时进行告警。 | ● | ● | ● | |
| | 安全审计 | a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | ● | ● | ● | ● |
| | | b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | ● | ● | ● | ● |
| 安全计算环境 | 身份鉴别 | 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 | ● | ● | ● | ● |
| | 访问控制 | a) 应保证当虚拟机迁移时，访问控制策略随其迁移； | ● | | ● | |
| | | b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。 | ● | | ● | |
| | 入侵防范 | a) 应能检测虚拟机之间的资源隔离失效，并进行告警； | ● | | ● | |
| | | b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； | ● | | ● | |
| | | c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 | ● | ● | ● | |
| | 镜像和快照保护 | a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； | ● | | ● | |
| | | b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； | ● | | ● | |
| | | c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | ● | | ● | |
| | 数据完整性和保密性 | a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定； | ● | ● | ● | ● |
| | | b) 应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； | ● | | ● | |
| | | c) 应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； | ● | | ● | |
| | | d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 | ● | | ● | |
| | 数据备份恢复 | a) 云服务客户应在本地保存其业务数据的备份； | ● | ● | ● | ● |
| | | b) 应提供查询云服务客户数据及备份存储位置的能力； | ● | | ● | |
| | | c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； | ● | | ● | |
| | | d) 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 | ● | | ● | |
| | 剩余信息保护 | a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除； | ● | | ● | |
| | | b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。 | ● | | ● | |
| 安全管理中心 | 集中管控 | a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配； | ● | ● | ● | |
| | | b) 应保证云计算平台管理流量与云服务客户业务流量分离； | ● | | ● | |
| | | c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计； | ● | ● | ● | ● |
| | | d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。 | ● | ● | ● | |
| 安全建设管理 | 云服务商选择 | a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力； | | ● | | ● |
| | | b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标； | | ● | | ● |
| | | c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等； | | ● | | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。

| 等保 2.0 基本要求 | | | 新华三 IaaS 交付模式 | | 新华三 PaaS 交付模式 | |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | 云服务商安全合规能力 | 云客户安全合规能力 | 云服务商安全合规能力 | 云客户安全合规能力 |
| | 云服务商选择 | d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除； | | ● | | ● |
| 安全建设管理 | | e) 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。 | | ● | | ● |
| | 供应链管理 | a) 应确保供应商的选择符合国家有关规定； | ● | ● | ● | ● |
| | | b) 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户； | ● | | ● | |
| | | c) 应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。 | ● | | ● | |
| 安全运维管理 | 云计算环境管理 | 云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。 | ● | ● | ● | ● |

注：“●”表示安全责任归属，安全责任方必须具备的安全能力。





# 附录 B　网络安全等级保护通用要求项安全能力

## B.1　网络安全等级保护云扩展要求项安全责能力

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全通信网络 | 网络架构 | a）应保证网络设备的业务处理能力满足业务高峰期需要； | 1、H3C 云计算环境组网时，根据业务需求可供用户选择高中低档网络设备以 – 满足业务处理能力；<br>2、新华三提供的网络设备安全设备支持 SOP、SCF 横向扩展，业务高峰期设备可按需扩展；<br>3、H3C 态势感知服务系统对设备日志进行分析告警，保证设备业务处理能力出现异常时，实时响应；<br>4、新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对设备性能进行监控，发现异常时进行告警提示。 | 高性能网络设备<br>支持 SOP、SCF 的网络设备<br>态势感知<br>IMC | 1、2、3 | 4 |
| 安全通信网络 | 网络架构 | b）应保证网络各个部分的带宽满足业务高峰期需要； | 1、H3C 态势感知服务系统支持对网络链路进行实时监控告警；<br>2、新华三 LLB 负载均衡设备能够对多出口链路进行合理的流量分担， SLB 负载均衡设备可以将客户对数据中心服务的访问请求合理地分发到数据中心的各台服务器上，以此保证各部分业务带宽的高可用；<br>3、新华三提供 IMC 网管软件，云平台可通过单独部署 IMC 网管软件对网络链路的能力进行监控、告警。 | 态势感知<br>IMC<br>负载均衡（SLB、LLB） | 1、2 | 3 |
| 安全通信网络 | 网络架构 | c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | 1、H3C 云计算环境在组网时划分了安全管理区、安全资源池以及业务区，各安全域间相互隔离；<br>2、不同区域间的网络通过防火墙实现不同网络安全域的划分。 | VxLAN<br>虚拟防火墙<br>VPC | 1、2 | |
| 安全通信网络 | 网络架构 | d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； | 1、H3C 云计算环境部署出口防火墙；<br>2、安全管理区边界部署独立的防火墙，安全资源池部署虚拟防火墙实现不同安全域的隔离，业务区每个客户出口均部署虚拟防火墙，每个客户通过 VRF 进行路由隔离；<br>3、业务区不同的客户分属不同的 VPC，跨 VPC 间通过虚拟防火墙实现南北向流量隔离，同一 VPC 内也部署虚拟防火墙进行安全域隔离。 | 虚拟防火墙<br>出口防火墙 | 1、2、3 | |

安全合规能力

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全通信网络 | 网络架构 | e）应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性； | 1、网络架构从接入层到汇聚层，实现节点冗余和链路 LLB 负载分担，在满足带宽收敛和保证业务性能同时满足整个业务系统的高可用；<br>2、H3C 云计算环境在组网时防火墙通过堆叠的形式，交换机通过 M-LAG 的方式，服务器通过集群的方式，以保证设备可用；<br>3、负载均衡设备提供智能 DNS 服务，保证链路、系统的高可用。 | 负载均衡（SLB、LLB）<br>智能 DNS | 1、2 | 3 |
| 安全通信网络 | 网络架构 | f）应可按照业务服务的重要程度分配带宽，优先保障重要业务。 | 1、新华三云计算环境中可通过链路负载均衡（LLB）、服务器负载均衡（SLB）保障业务带宽；<br>2、新华三云计算环境中的所有路由器、交换机等均可配置 QOS 策略，可根据业务情况进行恰当的 QOS 策略配置，保证重要业务的带宽分配；<br>3、SDN 控制器可自动下发 QOS 策略，保证各部分业务的带宽。 | 负载均衡（SLB、LLB）<br>SDN 控制器 | 1、2、3 | |
| 安全通信网络 | 通信传输 | a）应采用密码技术保证通信过程中数据的完整性； | 1、数据链路采用 IPsec VPN，用户访问使用 SSL VPN，保障通信链路中数据的完整性；<br>2、云平台内部管理通过 HTTPS 的访问方式，保证数据在通信过程中的完整性。 | IPsec VPN<br>SSL VPN | 1、2 | |
| 安全通信网络 | 通信传输 | b）应采用密码技术保证通信过程中数据的保密性； | 1、数据链路采用 IPsec VPN，用户访问使用 SSL VPN，保障通信链路中数据的保密性；<br>2、云平台内部管理通过 HTTPS 的访问方式，保证数据在通信过程中的保密性。 | IPsec VPN<br>SSL VPN | 1、2 | |
| 安全通信网络 | 通信传输 | c）应在通信前基于密码技术对通信的双方进行验证或认证； | 数据链路采用 IPsec VPN，用户访问使用 SSL VPN，保障数据通信前对双方基于密码技术进行验证。 | IPsec VPN<br>SSL VPN | 1 | |
| 安全通信网络 | 通信传输 | d）应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。 | 1、H3C 路由器产品和防火墙产品均内置硬件加密引擎，支持商用密码；同时也支持安装国密卡；数据链路采用 IPsec VPN，用户访问使用 SSL VPN，保障通信链路中数据的保密性；<br>2、新华三云计算平台组网时暂未提供独立的加密机，用户可根据实际业务需求自行部署。 | IPsec VPN<br>SSL VPN | —— | 1 |
| 安全通信网络 | 可信验证 | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。 | 该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信已在测试阶段。 | 可信网络设备 | 1 | |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全区域边界 | 边界防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； | 1、H3C 云计算环境外部的流量访问时需通过出口防火墙，仅允许通过受控的接口进行通信；<br>2、业务区域边界部署虚拟防火墙、安全管理区边界部署独立防火墙、安全资源池部署虚拟防火墙，在防火墙侧设置 ACL，保证跨边界的访问有效性；<br>3、虚拟防火墙对跨 VPC 的访问流量进行检测和控制；<br>4、同一 VPC 内部的流量访问需通过虚拟防火墙；<br>5、VPC 内部基于安全服务链进行自动化编排，实现灵活的访问控制规则，仅允许通过受控的接口进行通信。 | 虚拟防火墙<br>VPC<br>出口防火墙 | 1、2、3、4、5 | |
| 安全区域边界 | 边界防护 | b）应能够对非授权设备私自联到内部网络的行为进行限制或检查； | 1、H3C 云计算环境面向终端和安全设备在接入交换机配置 IP/MAC 地址绑定，并指定端口；对访问内部网络需要安全网关进行身份认证；<br>2、H3C 云计算环境 SDN 控制器能够对非法接入的设备进行自动感知，实时更新拓扑，便于及时发现未授权设备的非法接入；<br>3、H3C 云计算环境底层基础设施硬件设备的所有空闲端口全部关闭；<br>4、H3C 服务器安全监测系统可实时监测非授权的接入；<br>5、H3C 云计算环境态势感知服务的资产管理模块可监控非法用户的接入。 | 态势感知<br>SDN 控制器<br>服务器安全监测 | 1、2、3、4、5 | |
| 安全区域边界 | 边界防护 | c）应能够对内部用户非授权联到外部网络的行为进行限制或检查； | 1、H3C 云计算环境 SDN 控制器能够对非法的设备进行自动感知，实时更新拓扑，便于及时发现未授权设备的非法外联；<br>2、H3C 云计算环境底层基础设施硬件设备的所有空闲端口全部关闭；<br>3、H3C 云计算环境态势感知服务的资产管理模块可监控非法外联；<br>4、互联网出口审计设备 IPS、防火墙、ACG（应用流量审计）可以对非法外联行为进行分析、阻断。 | 态势感知<br>出口防火墙<br>SDN 控制器 | 1、2、3、4、5 | |
| 安全区域边界 | 边界防护 | d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络； | H3C 云计算环境组网不会涉及无线网络接入，无线网络的使用按照客户需求和具体应用场景而定。 | —— | | 1 |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全区域边界 | 边界防护 | e）应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断。 | 1、H3C EAD（终端准入控制）方案，能够对终端用户的接入进行身份认证，安全检查及动态授权。若有非授权设备私自联到内部网络，身份认证不通过，会被直接拒绝；若有内部用户非授权连接外网行为，会无法访问未被授权的资源。<br>2、H3C 态势感知系统的资产管理模块，实时监测全网的设备，若有未授权设备私自外联或内联，态势感知系统会进行监测，并与其他安全设备联动进行阻断。 | 态势感知<br>EAD 系统 | 1、2 | |
| 安全区域边界 | 边界防护 | f）应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。 | 该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信功能已在测试阶段。 | 可信网络设备 | 1 | |
| 安全区域边界 | 访问控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； | H3C 云计算环境在出口防火墙、虚拟防火墙以及业务负载均衡等设备通过五元组进行设置访问控制 ACL 规则进行访问控制，最后存在一条 deny all 的配置。 | 负载均衡（SLB、LLB）<br>虚拟防火墙<br>出口防火墙 | 1 | |
| 安全区域边界 | 访问控制 | b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； | 新华三防火墙产品能够对配置的 ACL 规则进行有效检查，帮助用户进行多余策略的实时检查。 | 负载均衡（SLB、LLB）<br>虚拟防火墙<br>出口防火墙 | 1 | |
| 安全区域边界 | 访问控制 | c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许、拒绝数据包进出； | H3C 云计算环境组网中的所有防火墙基于五元组，即源地址、目的地址、源端口、目的端口和协议，进行访问控制 ACL 规则的设定，来控制进出防火墙的数据包。 | IPsec VPN<br>SSL VPN | 1 | |
| 安全区域边界 | 访问控制 | d）应能根据会话状态信息为进出数据流提供明确的允许、拒绝访问的能力； | 1、新华三下一代防火墙能够对数据会话状态信息进行过滤，提供明确的允许、拒绝访问的能力；<br>2、H3C 云计算环境态势感知服务支持全网网络流量可视，识别威胁、监测，可通过联动其他安全设备的方式进行阻断。 | 态势感知<br>下一代防火墙 | 1、2 | |
| 安全区域边界 | 访问控制 | e）应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。 | 新华三下一代防火墙提供对第七层应用协议和应用内容的访问控制功能，下一代防火墙中包括了 IPS、WAF、AV 杀毒等多个安全模块。（三级）<br>新华三云计算环境中部署安全数据交换系统可实现不同安全域之间的数据隔离、交换。（四级） | 下一代防火墙<br>数据交换系统 | 1（三级）<br>1（四级） | 1 |





| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全区域边界 | 入侵防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； | 1、H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量包进行深度解析，实时地检测出各种攻击和异常行为；<br>2、部署抗 DDoS 设备对进出云平台的所有流量进行检测、清洗；<br>3、H3C 云计算环境出口防火墙开启 IPS 功能，对进出流量进行监测；<br>4、服务器端安装新华三服务器安全监测进行安全加固，防止外部的网络攻击行为。 | 态势感知<br>出口防火墙<br>服务器安全检测<br>抗 DDoS | 1、3、4 | 2 |
| 安全区域边界 | 入侵防范 | b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 1、H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量包进行深度解析，实时地检测出各种攻击和异常行为；<br>2、旁路部署 IDS 硬件设备，对云平台的所有流量进行检测；<br>3、H3C 云计算环境出口防火墙开启 IPS 功能，对进出流量进行监测；<br>4、服务器端安装新华三服务器安全监测进行安全加固，防止内部的网络攻击行为。 | 态势感知<br>出口防火墙<br>服务器安全检测<br>IDS | 1、2、3、4 | |
| 安全区域边界 | 入侵防范 | c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | H3C 云计算环境态势感知服务对全网流量进行监测，完成全流量网络行为画像，并通过与云端情报中心联动感知实现对新型网络攻击的分析。 | 态势感知 | 1 | |
| 安全区域边界 | 入侵防范 | d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。 | H3C 云计算环境态势感知服务对全网流量进行监测，检测到攻击行为时，能够记录的信息包括：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等，可通过邮件、Web 界面的形式进行告警，并且支持细粒度事件分析展示。 | 态势感知 | 1 | |
| 安全区域边界 | 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； | 1、H3C 云计算环境出口防火墙开启防病毒、IPS 等功能，能够对互联网出口的恶意代码进行检测，恶意代码库支持自动更新、手动更新及定期更新；<br>2、虚拟防火墙开启防病毒功能，在业务区提供 WAF ，可实现各节点处的恶意代码检测和清除，恶意代码库支持自动更新、手动更新及定期更新。 | 虚拟防火墙<br>出口防火墙 | 1 | |
| 安全区域边界 | 恶意代码和垃圾邮件防范 | b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | H3C 云计算环境能够为客户提供反垃圾邮件网关、邮件 DLP（数据防泄漏）、沙箱等方式对垃圾邮件进行检测和防护，用户可根据业务需求选择相应的安全技术。 | 反垃圾邮件网关<br>邮件 DLP（数据防泄漏）<br>沙箱 | | 1 |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全区域边界 | 安全审计 | a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 1、H3C 云计算环境态势感知服务能够收集全网的日志和流量，日志能够覆盖到全网的所有用户；<br>2、H3C 云计算环境日志审计服务，能够提供部署日志审计服务器，收集各设备、节点处的日志信息；<br>3、堡垒机能够对租户侧操作行为进行审计。 | 态势感知<br>日志审计<br>堡垒机 | 1、2、3 | |
| 安全区域边界 | 安全审计 | b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； | 1、H3C 云计算环境态势感知服务对收集的全网日志可进行细粒度的分析展示，包括的信息有：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等；<br>2、H3C 堡垒机提供录像式日志回放功能，并且可通过关键信息进行定位回放；<br>3、第三方堡垒机审计日志类型包含事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 | 态势感知<br>日志审计<br>堡垒机 | 1、2、3 | |
| 安全区域边界 | 安全审计 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 | 1、态势感知通过集群的方式部署，客户可根据实际业务需求情况调整存储空间，且提供定期的备份机制，保证审计数据的可用性；<br>2、第三方堡垒机审计日志可存在堡垒机本地，也可保存在云存储上，至少保存 6 个月以上。 | 态势感知<br>日志审计<br>堡垒机 | 1、2 | |
| 安全区域边界 | 安全审计 | d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析（三级）。 | H3C 云计算环境态势感知服务能对远程访问（如 SSLVPN 接入）的用户行为，访问互联网的用户行为（EAD 准入、互联网审计）等单独进行行为审计和分析。 | 态势感知 | 1 | |
| 安全区域边界 | 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。 | 该项能力 H3C 云计算环境正在建设中，目前网络设备侧的安全可信功能已在测试阶段。 | 可信网络设备 | 1 | |





| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； | 1、新华三云计算系列产品本地均可设置用户口令复杂度、最小口令长度以及口令有效期；<br>2、新华三云计算系列产品均允许被堡垒机接管，堡垒机侧可设置强制的口令复杂度策略。 | 安全基线<br>主机安全加固 | 1、2 | |
| 安全计算环境 | 身份鉴别 | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； | 1、新华三云计算系列产品本地均可设置登录失败次数以及限制超时时长；<br>2、新华三云计算系列产品均允许被堡垒机接管，堡垒机侧可设置登录失败次数以及限制超时时长。 | 安全基线<br>主机安全加固 | 1、2 | |
| 安全计算环境 | 身份鉴别 | c）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听； | 1、云平台内部访问通过 HTTPS 的方式进行远程连接，通信过程中信息加密传输；<br>2、新华三云计算系列产品被堡垒机接管后，可设置访问策略，保证信息在传输过程中的完整性和保密性。 | 安全基线<br>主机安全加固<br>HTTPS | 1、2 | |
| 安全计算环境 | 身份鉴别 | d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 1、H3C CloudOS、H3C CAS、H3C SecCloud OMP 等管理平台的鉴别方式有用户名、口令 + 短信验证码、邮件验证码两种身份鉴别方式；<br>2、新华三云计算系列产品均允许被堡垒机接管，且仅允许堡垒机访问，在堡垒机侧通过用户名、口令 +USB Key 的认证方式，实现用户双因素身份鉴别。 | 云平台原生<br>堡垒机 + 第三方认证 | 1 | 2 |
| 安全计算环境 | 访问控制 | a）应对登录的用户分配账户和权限； | 新华三云计算系列产品基于三权分立原则，默认分配系统管理员、安全管理员、审计管理员，如 H3C CloudOS 基于用户角色分配账户，角色分为组织管理员（租户）、普通用户、审计员、云管理员（平台侧）。 | 云平台原生 | 1 | |
| 安全计算环境 | 访问控制 | b）应重命名或删除默认账户，修改默认账户的默认口令； | 新华三云计算系列产品 admin、administrator 等默认账户在交付时，默认禁用，且会对所有用户的默认口令进行更改。 | 云平台原生 | 1 | |
| 安全计算环境 | 访问控制 | c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； | 新华三云计算系列产品可以对账户资源情况进行展示，确定账户无资源使用时，可删除多余账户。 | 云平台原生 | 1 | |
| 安全计算环境 | 访问控制 | d）应授予管理用户所需的最小权限，实现管理用户的权限分离； | 新华三云计算系列产品根据用户所属组织架构角色，为其分配权限，且遵循最小授权原则。 | 云平台原生 | 1 | |
| 安全计算环境 | 访问控制 | e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 新华三云计算系列产品基于用户角色分配权限，限制用户对功能模块的访问。 | 云平台原生 | 1 | |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全计算环境 | 访问控制 | f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 新华三云计算系列产品主体到用户级，客体为功能模块、文件或数据库表。 | 云平台原生 | 1 | |
| 安全计算环境 | 访问控制 | g）应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。 | —— | —— | —— | —— |
| 安全计算环境 | 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； | 1、新华三云计算系列产品自身均有操作日志审计模块，默认开启，且覆盖到系统所有用户；<br>2、新华三云计算系列产品均允许被堡垒机接管，堡垒机通过录屏和记录的方式审计所有用户的行为；<br>3、新华三态势感知、日志审计产品支持全网日志收集，日志审计支持网络设备、安全设备、服务器等云上各类组件的安全审计，态势感知支持安全日志、网络审计日志、数据库审计日志、SSLVPN 日志、DLP 审计日志、运维日志、流量日志等。 | 态势感知<br>日志审计<br>堡垒机<br>安全基线 | 1、2、3 | |
| 安全计算环境 | 安全审计 | b）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； | 1、新华三云计算系列产品审计记录包括登录名称、IP 地址、操作、资源、操作时间、级别、结果等；<br>2、堡垒机侧的审计记录内容包括：时间、IP、用户账户、操作类型、影响内容、结果、操作；<br>3、日志审计的日志类型包括操作日志、审计日志、流量日志、威胁日志、系统日志、安全控制日志、用户接入日志等，态势感知的审计内容包括日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等。 | 态势感知<br>日志审计<br>堡垒机 | 1、2、3 | |
| 安全计算环境 | 安全审计 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； | 1、新华三云计算系列产品审计记录支持导出；<br>2、堡垒机支持审计报表生成，并支持审计记录导出；<br>3、日志审计、态势感知支持审计报表生成，并支持审计记录导出。 | 态势感知<br>日志审计<br>堡垒机 | 1、2、3 | |
| 安全计算环境 | 安全审计 | d）应对审计进程进行保护，防止未经授权的中断。 | 新华三云计算系列产品均可设置审计员，并对审计进程进行保护。 | —— | —— | —— |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全计算环境 | 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； | 物理机、虚拟机侧均最小安装，且经主机安全加固，仅安装必要的组件和应用程序。 | 主机加固<br>安全基线 | 1 | |
| 安全计算环境 | 入侵防范 | b）应关闭不需要的系统服务、默认共享和高危端口； | 云计算管理平台、网络设备、安全设备、物理机、虚拟机侧只开放必要的端口。 | 主机加固<br>安全基线 | 1 | |
| 安全计算环境 | 入侵防范 | c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； | 新华三云计算系列产品可设置终端接入方式，如堡垒机、LDAP 认证或者特定地址范围。 | 堡垒机 | 1 | |
| 安全计算环境 | 入侵防范 | d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； | 新华三产品上线前会进行安全测试，会对数据的有效性输入进行校验。 | 云平台原生 | 1 | |
| 安全计算环境 | 入侵防范 | e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； | H3C 云漏洞扫描系统提供 Web 漏洞扫描、数据库漏洞扫描、系统漏洞扫描，会提供漏扫报告，发现漏洞，提供升级服务。 | 云漏洞扫描系统 | 1 | |
| 安全计算环境 | 入侵防范 | f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 1、主机层面安装亚信安全服务器深度安全防护系统，支持入侵防御；<br>2、网络层面防火墙包含 IPS 模块，在各区域边界节点处部署服务器，能够对入侵行为进行检测，并提供报警机制；<br>3、新华三态势感知系统对全网流量进行监测分析，并能够与 IDS、IPS、防火墙等进行联动，对入侵行为进行检测，并提供报警功能。 | 亚信安全服务器深度安全防护系统<br>下一代防火墙<br>态势感知 | 2、3 | 1 |
| 安全计算环境 | 恶意代码防范 | 应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 | 主机层面安装亚信安全服务器深度安全防护系统，支持防恶意软件、防火墙、入侵防御、完整性监控、日志审查，并支持病毒查杀功能。 | 亚信安全服务器深度安全防护系统 | | 1 |
| 安全计算环境 | 可信验证 | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。 | 该项能力 H3C 云计算安全正在建设中，目前网络设备侧的安全可信已在测试阶段。 | —— | 1 | |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全计算环境 | 数据完整性 | a）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 1、云平台内部访问时通过 HTTPS 访问，数据上传时会进行完整性校验；<br>2、关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证在加载到存储过程中数据的完整性。 | HTTPS<br>ONE Stor | 1、2 | |
| 安全计算环境 | 数据完整性 | b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； | 关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证数据存储过程中的完整性。 | ONE Stor | 1 | |
| 安全计算环境 | 数据完整性 | c）在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。 | 由租户侧根据部署的应用系统功能建设相应的抗抵赖能力。 | —— | | 1 |
| 安全计算环境 | 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 云平台内部访问时通过 HTTPS 访问，可保证数据在传输过程中的保密性； | HTTPS | 1 | |
| 安全计算环境 | 数据保密性 | b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 关键的数据会挂载到存储，存储侧采用分布式存储可有效的保证数据存储过程中的保密性。 | ONE Stor | 1 | |



| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全计算环境 | 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； | H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式。 | 云平台原生 | 1 | |
| 安全计算环境 | 数据备份恢复 | b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； | H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式。 | 云平台原生 | 1 | |
| 安全计算环境 | 数据备份恢复 | c）应提供重要数据处理系统的热冗余，保证系统的高可用性； | 新华三云计算安全服务器侧采用虚拟机、存储侧为分布式存储系统，还有负载均衡等可保证数据处理系统的冗余。 | 负载均衡<br>云平台原生 | 1 | |
| 安全计算环境 | 数据备份恢复 | d）应建立异地灾难备份中心，提供业务应用的实时切换。 | 租户业务应用系统能够支持异地双中心部署，满足实时切换。 | —— | | 1 |
| 安全计算环境 | 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； | 数据的存储空间删除后，底层存储会进行写零回收，可有效的防止剩余信息残留。 | 写零机制 | 1 | |
| 安全计算环境 | 剩余信息保护 | b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 | 数据的存储空间删除后，底层存储会进行写零回收，数据只有在被写零后才能重新分配。 | 写零机制 | 1 | |
| 安全计算环境 | 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； | 由租户侧根据部署的应用系统功能建设相应的个人信息清除机制。 | —— | | 1 |
| 安全计算环境 | 个人信息保护 | b）应禁止未授权访问和非法使用用户个人信息； | 由租户侧根据部署的应用系统功能建设相应的个人信息清除机制。 | —— | | 1 |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全管理中心 | 系统管理 | a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； | 1、设备层默认分配系统管理员、审计管理员、安全管理员，堡垒机侧默认分配系统管理员、安全审计员、运维人员；<br>2、系统管理员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，系统管理员的操作均可被堡垒机审计。 | 堡垒机 | 1、2 | |
| 安全管理中心 | | b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等； | 1、设备层的系统管理员的权限主要包括系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；<br>2、堡垒机侧系统管理员主要分配运维人员、安全审计员的账户和权限。 | 堡垒机 | 1、2 | |
| 安全管理中心 | 审计管理 | a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； | 设备侧的审计管理员、堡垒机侧的审计管理员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，且所有的操作被堡垒机实时审计，系统管理员可查看审计管理员的操作行为。 | 堡垒机 | 1 | |
| 安全计算环境 | | b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 | 审计管理员对设备、系统的审计记录进行分析、统计，审计策略由审计管理员制定，审计记录的存储、管理、查询工作均由审计管理员在堡垒机侧进行操作。 | 堡垒机 | 1 | |
| 安全管理中心 | 安全管理 | a） 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； | 设备侧的安全管理员、堡垒机侧的运维人员仅允许通过堡垒机访问，鉴别信息由堡垒机接管，且所有的操作被堡垒机实时审计。 | 堡垒机 | 1 | |
| 安全管理中心 | | b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 | 安全管理员主要对安全业务功能配置、安全业务状态监控。 | 堡垒机 | 1 | |





| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全管理中心 | 集中管控 | a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； | 1、划分了安全管理区，安全管理区部署了堡垒机、H3C SecCloud OMP 管理平台，能够对所有的设备进行管控；<br>2、第三方安全管理设备可根据用户需求，部署在安全管理区。 | 堡垒机 | 1 | 2 |
| 安全管理中心 | | b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； | 1、建立带外管理网络；<br>2、外部区域访问安全管理区需通过 IPsec VPN 或 SSLVPN 访问网络中的设备，安全管理区内部访问网络中的设备需通过 HTTPS、SSH，在安全管理区边界部署了防火墙，保证信息传输路径的安全性。 | IPsec VPN<br>SSL VPN | 1、2 | |
| 安全管理中心 | | c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； | 1、H3C 云计算环境态势感知服务能够对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；<br>2、H3C CloudOS 管理平台可集中对网络设备、安全设备、服务器的运行情况进行监测；<br>3、H3C SecCloud OMP 管理平台能够对安全资源的运行状况、资源使用情况进行监测；<br>4、H3C 服务器集中监测能够对服务器运行状况、资源使用情况进行监测；<br>5、SDN 控制器运维模块包括物理网络、逻辑网络、拓扑映射、网络健康监控、流量监控。<br>6、新华三 IMC 能够对网络链路、网络设备、安全设备的运行状况和资源使用情况进行集中监测，云服务客户可根据业务需求选择性部署。 | 态势感知<br>服务器集中监测<br>云平台原生<br>IMC | 1、2、3、4、5 | 6 |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全管理中心 | 集中管控 | d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求; | 1、H3C 态势感知系统能够收集全网日志，对日志进行集中分析，并进行细粒度展示，态势感知集群部署，至少保存 6 个月以上，可手动或自动转存至第三方设备；<br>2、日志审计支持收集全网日志，可作为态势感知探针使用，与态势感知进行二次联动，进行细粒度展示。 | 态势感知<br>日志审计 | 1、2 | |
| 安全管理中心 | | e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理; | 1、态势感知、集中式漏扫、H3C SecCloud OMP 管理平台、服务器安全监测能够对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；<br>2、H3C SecCloud OMP 管理平台支持安全策略统一下发。 | 态势感知<br>集中式漏扫<br>云平台原生 | 1 | |
| 安全管理中心 | | f）应能对网络中发生的各类安全事件进行识别、报警和分析; | 态势感知、日志审计对全网的日志流量、日志进行集中监测，支持各类安全事件的分类、识别、分析、报警。 | 态势感知<br>日志审计 | 1 | |
| 安全管理中心 | | g）应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性 。 | 新华三云技术环境中的所有产品均可通过 ntp 协议，将系统范围内所有设备同步至唯一确定的时钟服务器。 | 时钟服务器 | 1 | |

注 ：无编号的默认编号 1。





## B.2 网络安全等级保护云扩展要求项安全责任

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全物理环境 | 基础设施位置 | 应保证云计算基础设施位于中国境内。 | H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，部署在用户内部或租用运营商机房。 | —— | —— | —— |
| 安全通信网络 | 网络架构 | a）应保证云计算平台不承载高于其安全保护等级的业务应用系统; | H3C 云计算环境通过等级保护安全性评估具有承载四级应用系统的安全防护能力。 | —— | —— | —— |
| | | b）应实现不同云服务客户虚拟网络之间的隔离; | 1、H3C 云计算环境专有网络（Virtual Private Cloud）VPC 采用隧道技术，帮助用户构建出一个隔离的网络环境，实现不同云服务客户间的网络资源的隔离；<br>2、同一 VPC 内通过虚拟防火墙进行安全域隔离；<br>3、不同 VPC 间通过 VRF 进行路由隔离，在云端部署虚拟防火墙，划分网络安全域，实现不同 VPC 间的访问控制；<br>4、虚拟防火墙能够帮助用户实现云计算环境中东西向流量的隔离。 | 虚拟防火墙 VPC | 1、2、3、4 | |
| | | c、应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力; | 1、H3C 安全有云在通信传输层面为云服务客户提供 IPsec VPN、SSL VPN 服务，云平台内部所有通讯访问均通过 https 实现，保证了传输过程中的保密性；<br>2 在边界防护层面，部署出口防火墙，各安全域边界处部署防火墙，对常见的 Web 应用攻击进行通过 WAF 拦截旁路阻断；<br>3）H3C 下一代防火墙包含 IPS 模块，提供入侵防范功能，态势感知服务对全网流量进行监测；<br>4）基于虚拟防火墙实现灵活的访问控制规则。 | 虚拟防火墙<br>出口防火墙<br>IPsec VPN<br>SSL VPN | 1、2、3、4 | |
| | | d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略; | H3C 云计算环境所有安全产品（服务）均支持云服务客户根据业务需求，自主定义安全访问路径，设置安全组策略，自主选择使用各种安全组件； | 云平台原生 | 1 | |
| | | e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务; | 1、H3C 云计算环境提供开放的 API 接口<br>2、第三方安全产品（服务）如防火墙、漏扫、安全审计、负载均衡等，接入到云平台后，H3C 云计算环境可通过纳管的方式管理第三方安全产品或服务，如绿盟、山石、F5。 | 云平台原生 | 1、2 | |
| | | f）应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问; | —— | —— | —— | |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| | | g） 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式； | 新华三提供安全数据交换系统，能够实现不同安全域间的数据隔离、交换，云服务客户可根据业务需求选择边界数据交换方式。 | 数据交换系统 | | 1 |
| | | h）应为第四级业务应用系统划分独立的资源池。 | 新华三云计算平台为重要业务系统及四级业务系统划分独立的资源池 | —— | —— | —— |
| 安全区域边界 | 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则 | 1、虚拟网络边界处部署虚拟防火墙，业务区内跨 VPC 的访问需通过虚拟防火墙，可根据业务实际情况在防火墙上配置访问控制规则<br>2、虚拟网络东西向流量需通过安全服务链控制 VPC 内部流量走向，并在防火墙上配置访问控制规则 | 虚拟防火墙<br>VPC | 1、2 | |
| | | b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则； | 1、H3C 云计算环境在不同的安全域边界部署了防火墙，如出口防火墙、虚拟防火墙；<br>2、同一 VPC 内通过虚拟防火墙进行访问控制，并根据需求设置访问控制规则；<br>3、在安全管理区域部署了单独的物理防火墙。安全资源池、业务区部署虚拟防火墙，云平台侧和云服务客户侧可以根据业务实际情况独立设置访问控制规则。 | 虚拟防火墙<br>VPC<br>出口防火墙 | 1、2、3 | |
| | 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 1、H3C 云计算环境态势感知服务在云平台侧的关键节点处部署流量探针，对云平台的全流量深度解析，实时地检测出各种攻击和异常行为，记录的主要内容有：日志产生时间、产生日志设备名称、攻击子类型、攻击名称、源 IP、目的 IP、严重级别、特征命中方向、动作类型等；<br>2、各安全域边界处部署的防火墙能够对跨区域的攻击行为进行检测、记录，记录的内容有：时间、威胁类型、威胁 ID、威胁名称、源安全区域、目的区域、源 IP 地址、目的 IP 地址、应用、协议、内容安全策略等。 | 态势感知<br>虚拟防火墙<br>出口防火墙<br>下一代防火墙 | 1、2 | |
| | | b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； | 1、各安全域虚拟网络边界处部署的防火墙能够对跨区域的攻击行为进行检测、记录，记录的内容有：时间、威胁类型、威胁 ID、威胁名称、源安全区域、目的区域、源 IP 地址、目的 IP 地址、应用、协议、内容安全策略等；<br>2、跨 VPC 的攻击行为可通过虚拟防火墙（IPS 模块）对攻击行为进行检测；<br>3、同一 VPC 内的攻击行为可通过虚拟防火墙（IPS 模块）对攻击行为进行检测。 | 虚拟防火墙<br>VPC<br>出口防火墙<br>下一代防火墙 | 1、2、3 | |





| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| 安全区域边界 | | c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； | 1、虚拟机与宿主机分属不同的网段，默认不通，从虚拟机到宿主机的异常流量会通过态势感知流量探针进行监测，联动防火墙 IPS 进行检测；<br>2、宿主机服务器部署新华三服务器监测系统对虚机与宿主机间的流量进行监测；<br>3、跨 VPC 的虚拟机间的访问流量需通过虚拟防火墙，虚拟防火墙 IPS 模块可对流量进行检测；<br>4、同一 VPC 内不同网段的虚拟机间流量通过虚拟机防火墙 IPS 模块进行流量检测；<br>5、同一 VPC 内同一网段的虚拟机间访问需通过 VSwitch，VSwitch 可以对流量进行重定向，将流量定向至态势感知探针、IPS 等工具，对异常流量进行检测。 | 虚拟防火墙<br>VPC<br>出口防火墙<br>服务器安全检测<br>下一代防火墙 | 1、2、3、4、5 | |
| | | d、应在检测到网络攻击行为、异常流量情况时进行告警。 | 1、态势感知与 IPS、IDS 进行联动，能够对异常的攻击行为进行告警、阻断；<br>2、新华三服务器安全监测系统能够对异常流量进行告警。 | 态势感知<br>服务器安全检测<br>IDS | 1、2 | |
| | 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； | 1、H3C 堡垒机（运维审计系统）能够提供完整的审计回放和权限控制服务，能够记录用户的重要操作；<br>2、H3C CloudOS 收集用户的日志，能够查看重要特权的操作，如虚拟机删除、重启等。 | 堡垒机<br>云平台原生 | 1、2 | |
| | | b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 | H3C 云计算环境能够为用户提供运维审计系统，云服务客户可通过堡垒机审计云服务商的操作。 | 堡垒机 | 1 | |
| 安全计算环境 | 身份鉴别 | 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 | 1、管理终端对服务器通过 https 访问时，服务器端向终端下发证书，实现客户端对服务器端的认证；<br>2、服务器对终端通过用户名密码 + 邮箱或短信实现云平台的双因子认证，CloudOS 实现对终端的验证，CloudOS 可配置 LDAP 实现对终端的认证；<br>3、远程管理时，可设置仅允许通过堡垒机访问云平台管理平台，堡垒机侧支持双因素身份认证。 | 证书认证 | | 3 |
| | 访问控制 | a）应保证当虚拟机迁移时，访问控制策略随其迁移； | 1、H3C CloudOS 安全组会随虚拟机的迁移一起迁移；<br>2、虚拟机迁移过程中，网络属性不会发生改变，系统属性保证安全策略在虚拟机迁移后仍有效。 | 云平台原生（迁移保护） | 1 | |
| | | b）应允许云服务客户设置不同虚拟机之间的访问控制策略。 | 同一 VPC 内的虚拟机、不同 VPC 间的虚拟机访问需通过虚拟防火墙，云服务客户可在防火墙上配置访问控制策略。 | 虚拟防火墙<br>VPC | 1 | |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| | 入侵防范 | a）应能检测虚拟机之间的资源隔离失效，并进行告警； | 1、H3C CAS 云计算管理平台对虚拟机的资源、运行情况进行监控，对虚拟机的资源使用率设置阈值，有异常时会告警，可设置邮件告警、短信告警；<br>2、H3C CAS 虚拟机开启保密模式后，虚拟机资源独占、不共享，保证资源隔离。 | 云平台原生（CAS） | 1、2 | |
| | | b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； | 1、H3C CAS 虚拟资源审计模块对虚拟机的所有操作进行审计，包括虚拟机重启、新建；<br>2、态势感知系统资产管理模块能够对非授权的虚拟机新建进行告警提示；<br>3、H3C CAS 虚拟化拓扑进行实时展示，有异常虚拟机新建时，可通过拓扑进行查看。 | 态势感知<br>云平台原生（CAS） | 1、2、3 | |
| | | c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 | 1、虚拟机上部署主机安全加固（亚信安全服务器深度安全防护系统），对恶意代码进行查杀，支持报警功能；<br>2、虚拟机上部署服务器安全监测可实时监测、隔离恶意代码；<br>3、态势感知能够对虚机间流量进行分析，可发现恶意代码的攻击，并进行告警。 | 态势感知<br>亚信安全服务器深度安全防护系统<br>服务器安全检测 | 1、2、3 | |
| | 镜像和快照保护 | a）应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； | H3C 能够为用户提供主流的操作系统镜像，对镜像进行安全基线加固，安装防恶意代码软件、服务器安全监测软件等 | 云平台原生（虚拟镜像安全） | 1 | |
| | | b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； | 1、H3C CloudOS 对虚拟机镜像、快照进行上传时会进行校验，生成 MD5 值，上传完成后会再次生成 MD5 值，进行校验比对；<br>2、H3C CAS 对虚拟机进行迁移前后会进行完整性校验。 | 云平台原生 | 1、2 | |
| | | c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 | 1、在 H3C CAS 系统管理处参数配置处启用保密模式后能够对虚拟机、镜像进行保密；<br>2、镜像、快照保存在磁盘后会对磁盘进行加密<br>3、H3C CAS 特定版本能够对虚拟机镜像的硬盘进行加密。 | 云平台原生<br>磁盘加密 | 1、2、3 | |
| | 数据完整性和保密 | a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定； | H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，部署在用户内部或租用运营商机房，均位于中国境内。 | —— | 1 | |
| | | b）应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； | H3C 行业云在客户授权云服务商人员后，云服务商才能访问客户资源。 | —— | 1 | |
| | | c）应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； | H3C 提供迁移服务，对 P2V、V2V 的迁移会通过 TCP 协议进行校验，保证迁移的完整性。 | 云平台原生（迁移保护） | 1 | |





| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| | | d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 | H3C CloudOS 用户在创建虚拟机时，能够为用户提供虚拟机密钥对，保证虚拟机访问过程中的安全性。 | 云平台原生 | 1 | |
| | 数据备份恢复 | a）云服务客户应在本地保存其业务数据的备份； | 1、H3C CAS 与 One Stor 深度融合，用户可将数据存储在 One Stor 保证数据高可用；<br>2、H3C CAS 能够为用户提供存储数据下载功能，用户可根据业务需求进行下载，并选用适当的备份方式；<br>3、租户根据业务需求，选择适当的方式在本地保存其业务数据。 | 云平台原生 | 1、2 | 3 |
| | | b）应提供查询云服务客户数据及备份存储位置的能力； | 1、H3C CAS 可查看虚拟机运行状态、存储位置；<br>2、云服务客户在创建虚拟机时，可选择存储磁盘的存储池，在存储池中可查看虚拟机对应的存储卷。 | 云平台原生 | 1、2 | |
| | | c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； | H3C Unistor 支持多副本存储（2-5），副本内容保持一致。 | ONE Stor | 1 | |
| | | d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 | 新华三提供迁移工具 Movesure、迁移服务，保证迁支持热迁移、冷迁移。 | 迁移工具 Movesure | 1 | |
| | 剩余信息保护 | a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除； | 1、虚拟机所有的内存和存储空间被回收时，用户可根据需求进行选择，H3C CAS 提供彻底销毁数据功能，通过写零的方式进行完全清除；<br>2、H3C CAS 提供虚拟回收保存期功能。 | 云平台原生 | 1、2 | |
| | | b）云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。 | 用户删除数据存储卷的时候，各副本会同步删除。 | 云平台原生（剩余信息销毁） | 1 | |
| 安全管理中心 | 集中管控 | a）应能对物理资源和虚拟资源按照策略做统一管理调度与分配； | 1、H3C CloudOS 对物理资源、虚拟资源进行统一调度、分配；<br>2、H3C SecCloud OMP 对安全资源进行统一调度、分配。 | H3C CloudOS<br>H3C SecCloud OMP | 1、2 | |
| | | b）应保证云计算平台管理流量与云服务客户业务流量分离； | 1、建立带外管理网，保证管理流量和业务流量分离；<br>2、安全管理区和业务区边界部署了防火墙，对跨区域的流量进行策略控制。 | 带外管理 | 1、2 | |

| 等保 2.0 基本要求 | | | 安全技术能力 | 对应产品 | 定量 | 变量 |
|---|---|---|---|---|---|---|
| 安全层面 | 控制点 | 要求项 | | | | |
| | | c）应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计； | 1、云平台侧 H3C 态势感知系统能够收集全网日志，对日志进行集中分析，并进行细粒度展示；<br>2、H3C 堡垒机支持云平台侧和云服务客户侧的日志收集。 | 态势感知<br>日志审计<br>堡垒机 | 1、2 | |
| | | d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。 | 1、H3C 态势感知系统支持全网全流量的监测，能够所有的网络设备、安全设备、服务器、虚拟机进行集中监测。<br>2、H3C Cloud 、H3C SecCloud OMP 管理平台为云平台侧和云服务客户侧分别分配账户，可对两侧各自部分的资源进行集中监测。 | 态势感知<br>H3C CloudOS<br>H3C SecCloud OMP | 1、2 | |
| | 云服务商选择 | a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力； | H3C 云计算环境为云服务提供商，云平台能够承载 4 级业务应用系统所需要的安全防护能力。 | —— | —— | —— |
| | 供应链管理 | a）应确保供应商的选择符合国家有关规定； | 1、H3C 云计算环境组网时选用的网络、计算、存储等设备均符合国家相关要求，H3C SecCloud OMP 安全产品准许销售，已获得销售许可证；<br>2、云服务客户根据供应商选择要求，确保供应商的选择符合国家有关规定。 | —— | —— | —— |
| | | b）应将供应链安全事件信息或安全威胁信息及时传达到云服务客户； | H3C 云计算环境态势感知服务推送最新的安全事件信息，以保证第一时间传达给云服务客户。 | —— | —— | —— |
| | | c）应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。 | 1、H3C 云计算环境的变更会通过 H3C SecCloud OMP 进行公告，以保证第一时间传达；<br>2、H3C 云计算环境提供一对一服务，变更的通知会及时送达，提供安全风险的应急响应。 | —— | —— | —— |
| 安全运维管理 | 云计算环境管理 | 云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。 | H3C 云计算环境主要面向国内用户，基础设施机房由用户选址，基本运维地点在中国境内。 | —— | —— | —— |

注 ：无编号的默认编号 1。