中企通信
CHINA ENTERCOM

云时代 SmartCLOUD
服务安全白皮书

中企网络通信技术有限公司

2017 年 7 月

目录

概述 1
1. 合作伙伴 1
1.1 虚拟化技术合作伙伴 1
1.2 基础设施合作伙伴 2
2. 数据中心安全 2
2.1 设施及人员访问安全 2
2.2 环境安全 3
3. 云平台安全 4
3.1 云平台整体架构安全 4
3.2 虚拟主机的安全 4
3.3 云平台数据存储安全 4
3.4 云平台数据传输安全 5
3.5 云平台数据使用安全 5
3.6 云平台的可用性 6
4. 通信与网络安全 6
4.1 云端网络架构设计原则 6
4.2 网络及端口安全 7
5. 云平台运维安全 8
5.1 员工安全培训 8
5.2 员工权限控制 9
5.3 审计跟踪 9
5.4 入侵检测 10
6. 变更管理 10
7. 数据销毁/硬件报废 11
7.1 数据销毁 11
7.2 硬件设备报废 12
8. 数据保护策略 13
8.1 数据备份及快速恢复服务 13
8.2 数据复制及灾难恢复服务 13
9. 持续优化 15
9.1 漏洞报告 15
9.2 漏洞评估 15
9.3 漏洞公布 15
10. 专业资质 16
11. 责任划分 17
11.1 客户义务和责任 17
11.2 中企通信的义务和责任 17

12. 用户行为守则.....18

概述

中企网络通信技术有限公司（以下简称“中企通信”）云时代 SmartCLOUD 服务提供了一个基于 VMware 虚拟化平台，并且具备高性能、高可靠性以及安全保障的 IT 基础设施服务。

使用云时代 SmartCLOUD 服务的客户，可以根据自身的需求，灵活调整 CPU、内存和存储等 IT 资源。云时代服务平台具备完善的容错能力和可靠性，能够避免因为硬件故障等原因导致的业务中断，从而最大限度的保障客户的利益。

本文档对云时代 SmartCLOUD 服务的安全性进行了全面的说明，包含以下 10 个方面内容：

- 合作伙伴介绍
- 数据中心安全
- 云平台安全
- 通信与网络安全
- 云平台运维安全
- 服务变更管理
- 数据销毁与硬件报废
- 数据保护策略
- 持续优化
- 相关专业资质

1. 合作伙伴

1.1 虚拟化技术合作伙伴

VMware（中文名：威睿）

作为全球公认的最成熟、稳定及安全的虚拟化技术领导者，VMware 拥有 400,000 多家客户和 55,000 多家合作伙伴，它的解决方案可帮助各种规模的组织降

低成本、提高业务灵活性并确保选择自由。

作为 VMware 的金牌合作伙伴，中企通信使用 VMware 作为其核心的虚拟化技术。基于 VMware vSphere 套件的丰富功能，客户可根据项目持续时间长短和对 IT 基础设施服务能力的需求变化，灵活的调整 CPU、内存、存储容量等 IT 资源；对于经常需要根据业务的实际需求动态调整 IT 资源的企业，中企通信云时代服务可称得上是最适合的解决方案。

1.2 基础设施合作伙伴

性能与安全一直是客户评估云计算服务的重要标准，为此中企通信与全球多家处于领先地位的厂商合作，包括 DELL（“戴尔”）、Juniper （“瞻博网络”）、EMC (“易安信”)及 Fortinet（“飞塔”）等，在提供性能优异，方便快捷的云计算服务的同时，也最大限度保障了云计算服务平台的可用性和安全性。

2. 数据中心安全

2.1 设施及人员访问安全

云时代服务平台内所有的基础设施均位于 Tier III+ 企业级数据中心的专用安全机柜内，与数据中心内其他设施物理隔离。

对于云时代服务平台基础设施的任何访问（如硬件升级/更换/维护等）均须得到中企通信云计算运营中心经理的批准。

中企通信云计算运营团队将对云时代服务平台内所有的基础设施进行 24x7x365 小时监控并记录详细信息，以便追踪。

放置云时代服务平台的数据中心内的所有设施，包括机架、电源系统、冷却系统、服务器、存储等，均处于严格的 24x7x365 小时访问控制和监控下。

当中企通信的工作人员需要进入数据中心时，必须在登记系统中登记其相关信息。仅当数据中心安全运营经理批准其访问请求后，此员工才可进入数据中心，且其所有行为会被实时监控。

当非中企通信工作人员（客户/数据中心访客等）需要进入数据中心设施，必须由中企通信工作人员在登记系统中登记访问者的相关信息。仅当数据中心安全运营经理批准其访问请求后，该人员才可进入数据中心，且访问全程均须有中企通信工作人员的陪同并实时监控其所有行为。

所有进出数据中心的设施设备均须经过审批并记录详细信息，以便追踪。

中企通信在以下数据中心均可为客户提供 SmartCLOUD 服务：

SmartCLOUD 站点代码	地址（国家及地区）
HK-ALC	香港岛，香港
HK-CTT	新界，香港
CN-GZYUJ	广州，中国
CN-BJ	北京，中国
CN-SHWGQ	上海，中国
CN-SHBAO	上海，中国
TW-TPE	台北，台湾
SG-DRT	新加坡
TW-TCH	台中，台湾
JP	东京，日本
DE-FRA	法兰克福，德国
US-LAX	洛杉矶，美国
US-NYC	纽约，美国
CN-BJKC	北京，中国
ZA-CPT	开普敦，南非

2.2 环境安全

数据中心的交流电电源系统具有冗余，一旦主电源发生中断，备份的不间断电源（UPS）和电子发电机会立即开始工作，以确保连续的电源供应。

温度控制系统将为数据中心中的所有设施保持一个恒定的运行温度，任何异常情况（如过热），都会触发警报，数据中心运营人员会立即采取适当的措施。

数据中心安装了自动火灾检测和灭火系统。所有数据中心机房、机械和电力设施、制冷机房和发电机房中的火灾探测系统均采用烟雾探测感应器。

3. 云平台安全

3.1 云平台整体架构安全

中企通信云时代服务平台在承载客户关键业务的同时，也具备完善的容错能力和高可用性。服务平台内的所有核心设备均采用冗余设计，任何单一硬件的故障均不会对客户的业务系统造成中断，最大限度的保障了客户的利益。

此外，中企通信的云计算运营团队将 24x7x365 不间断对云时代服务平台内的设施进行监控，当有任何硬件故障发生时，云计算运营团队的工程师将第一时间联系厂商进行硬件更换。

3.2 虚拟主机的安全

作为虚拟化基础架构的底层，VMware ESXi 虚拟化管理程序开箱时即受到安全保护。通过使用锁定模式和其他内置的功能，可以进一步保护 ESXi 主机。

中企通信通过如下方式确保及强化云时代服务平台虚拟主机的安全性：

- 限制 ESXi 访问；
- 使用指定用户和最小特权；
- 尽可能减少打开的 ESXi 防火墙端口数；
- 自动化 ESXi 主机管理；
- 使用锁定模式；
- 检查 VIB 软件包完整性；
- 管理 ESXi 证书；
- ESXi 帐户锁定。

3.3 云平台数据存储安全

云时代服务平台中的所有数据均存储在具有 RAID 保护的集中式 SAN（存储区域网络）

中，该 SAN 存储与云时代服务平台的基础设施位于同一机柜。

在云时代服务平台中，每位客户均有专用的 VMware 数据卷（Datastore）和 SAN 存储逻辑单元号(LUN)；系统对每个卷/LUN 定义不同的访问策略，没有该卷/LUN 访问权限的用户不能访问，每个卷/LUN 之间是互相隔离的。

3.4 云平台数据传输安全

每位使用云时代服务的客户均有专用的 vLAN 号码，确保其数据在传输过程中与其他客户完全隔离。

每位使用云时代服务的客户均有专用的网络连接物理端口，在物理上实现与其他客户数据隔离。

中企通信强烈建议客户在云时代服务平台前端部署安全设备，当客户需要访问云时代服务平台上的虚拟机（如 SSH/RDP 连入）时，应首先与平台前端的 UTM 建立 SSL VPN 连接，从而确保所有的操作及数据传输都是在加密的情况下进行。

3.5 云平台数据使用安全

- **登录平台**

当客户需要登录云时代服务管理平台对虚拟机或数据进行管理时，必须首先经过双因子 SSL VPN 验证。双因子 SSL VPN 采用动态密码验证方式，客户必须在接收到动态密码（可通过云时代服务专用密码器或电子邮件接收）后的 60 秒内登录平台，否则密码将作废，客户需重新操作。

- **使用平台**

登录云时代服务管理平台后，客户进行的任何数据传输操作（如上传ISO镜像）均采用 SSL（Security Socket Layer）加密。

3.6 云平台的可用性

云时代服务平台内的所有核心设备均采用冗余设计，任何单一硬件的故障均不会对客户的业务系统造成中断。

云时代服务平台建立在安全稳定的 VMware 虚拟化平台之上。中企通信定期更新 VMware 软件版本，并对关键 VMware 组件（如 vCenter）应用安全补丁，以确保云平台的安全和稳定。

云时代 SmartCLOUD 的服务等级协议（SLA）如下：

- SmartCLOUD 资源池：**99.99%**
- SmartCLOUD 端口：**99.9%**

有关云时代 SmartCLOUD 服务等级协议的详细规定，请参考《云时代 SmartCLOUD 服务等级协议》。

4. 通信与网络安全

4.1 云端网络架构设计原则

- **区域层次防护**

相比传统的IDC，云计算数据中心的网络架构同样需要多层设计原则，通过划分区域及层次进而确认各自负责的安全防御任务。

中企通信根据内外部分流原则，将数据中心网络分为四层：

- 互联网接入层
- 汇聚层
- 业务接入层
- 运维管理层

按照关联性、管理及安全防护等方面的不同需求，再将数据中心网络划分为不同的区域：

- 互联网域
- 接入域

- 服务域
- 管理域
- 计算域等

各安全区域之间经过防火墙隔离，再设置独立的访问控制策略

- **边界安全防护举例**
  - 通过FW（防火墙）/Anti-DDoS（抗分布式拒绝服务攻击）防御外界攻击。
  - 通过IPSec（网络协议安全性）/SSL VPN（安全套接字 虚拟专用网络） 提供安全接入。

- **内网深度防御举例**
  - 通过 vFW（虚拟防火墙）实现多租户安全。
  - 通过 IPS（入侵防御系统）对流量深度防御。

备注：以上的某些安全功能可能需要额外收费，具体情况请咨询中企通信销售人员。

4.2 网络及端口安全

中企通信通过在网络边缘以及网络中的不同节点部署受控设备实施了周边防护措施。

- **部署防火墙**

为虚拟网络增加防火墙保护，方法是在其中的部分或所有虚拟机上安装和配置基于主机的防火墙。为提高效率，可设置专用虚拟机以太网或虚拟网络。有了虚拟网络，可在网络最前面的虚拟机上安装基于主机的防火墙，此防火墙可以充当物理网络适配器和虚拟网络中剩余虚拟机之间的保护性缓存。

由于基于主机的防火墙会降低性能，因此请先根据性能目标对安全需求进行权衡，然后再决定在虚拟网络中的其他虚拟机上安装基于主机的防火墙。

- **网络分段**

将主机中的不同虚拟机区域置于不同网络段上。如果将每个虚拟机区域隔离在自己的网

络段中，可以大大降低虚拟机区域间泄漏数据的风险。

网络分段可防止多种威胁，包括：

- **地址解析协议（ARP）欺骗：**攻击者操作 ARP 表格以重新映射 MAC 和 IP 地址，从而访问进出主机的网络流量。达到劫持目标系统、执行拒绝服务 (DoS) 攻击或以其他方式破坏虚拟网络的目的。
- **中间人攻击（MITM）：**攻击者通过拦截正常的网络通信数据，并对数据进行篡改而通信的双方却毫不知情。
- **嗅探攻击：**此类攻击窃听网络上流经的数据包，从而窃取数据包内的重要私隐信息。

➢ **阻止未授权的访问**

中企通信防护网络安全的首要原则是只允许系统执行必要的连接和网络通讯，所有其他端口、协议，以及连接都会被阻止。具体安全措施举例：

- 在路由器上使用分层式访问控制列表(ACLs)
- 在主机上应用 IPsec 策略
- 在网络中使用防火墙规则和基于主机的防火墙规则对网络通讯、协议，以及端口号进行限制。

边界路由器的安全措施使得我们能够在网络层面上检测入侵和代表弱点的特征。

备注：以上的某些功能可能需要额外收费，具体情况请咨询中企通信销售人员。

5. 云平台运维安全

5.1 员工安全培训

中企通信所有新员工均须参加信息安全培训，并签署协议，保证不泄露中企通信及其客户的任何机密信息。

每位云计算运营团队的新员工必须参加产品培训并通过考试。每位员工根据其工作性质和职务，将参加不同级别的产品培训。

每位云计算运营团队的新员工必须参加工作流程培训，确保其在日常工作中能严格遵守各项安全规定。

每位云计算运营团队的新员工必须定期进行季度绩效考核，保证其在日常工作中始终做到诚实、认真和尊重客户。

5.2 员工权限控制

每位中企通信员工均有一个唯一的登录账号，此账号可访问中企通信内部网络和系统。如员工离职，其登录账号会被立即禁用。

中企通信员工必须保持其登录账号的安全，并定期修改密码。

在管理方面中企通信遵循“最低权限”的原则，每一位云计算工程师只赋予能够完成他日常运维工作所需要的最低权限，从而最大限度的保障客户数据或信息的安全性和私密性。一般来说，中企通信的云计算工程师在管理和运维时只能读取以下有限的客户信息：

- 客户资源池名称，类型，大小；
- 客户数据卷名称，类型，大小；
- 客户网络编号（vLAN ID），预配置的 IP 范围，但无法查看网络传输的任何数据；
- 客户虚拟机的资源配置，但无法查看虚拟机上的任何数据；
- 虚拟机资源的使用率；
- 其他与客户数据无关的必要运维信息

当员工在某些特殊情况下需要访问其权限之外的系统或资源时，必须临时申请。当系统负责人批准申请之后，该员工将被赋予临时访问权限。任务完成后，其访问权限将恢复原初始状态。

5.3 审计跟踪

对于中企通信内部网络和系统（包括云时代服务平台）的重要操作（如用户 ID/时间戳/操作详细信息等）的日志都会被详细记录并安全保存，以便在需要的时候随时进行查看。

重要的系统操作日志都会保存足够长的时间，并且可以查询任何时间段内的日志。

5.4 入侵检测

除了对内部员工进行严格管控，中企通信也将对来自外部的威胁或入侵进行监测与防护。

每一个云时代服务平台的边界处均部署了 FortiGate 高端 UTM，24x7x365 不间断的对平台状态及数据流量进行实时监控与告警，当有任何异常事件发生时（如安全威胁/入侵等），中企通信的 24x7x365 安全运营团队将立即采取有效行动应对，保证云时代服务平台不受威胁。

6. 变更管理

未经客户许可，云运营员工不得访问客户的虚拟机或数据。仅当客户发出服务请求时，云运营员工将严格按照流程来处理变更。工作流程如下：

(1) 当中企通信收到客户的服务变更申请后，将立即在客服系统 Remedy 中建立一个工单。

(2) 中企通信的客服人员将向客户发送一份《云时代需求变更申请表》。

(3) 客户在《云时代需求变更申请表》列明需要变更的服务或配置，并加盖公司印章，发回给中企通信客服人员。

(4) 在收到客户发还的《云时代需求变更申请表》后，中企通信的运维部门将确认变更的可行性并批准该申请。

(5) 中企通信的工程师按照《云时代需求变更申请表》中的指示实施变更。

(6) 验证变更后的系统正常运作，确认变更实施无误。

(7) 中企通信的客服人员通知客户变更已完成。

(8) 客户验证变更的正确性。

(9) 客户向中企通信确认该变更准确无误。

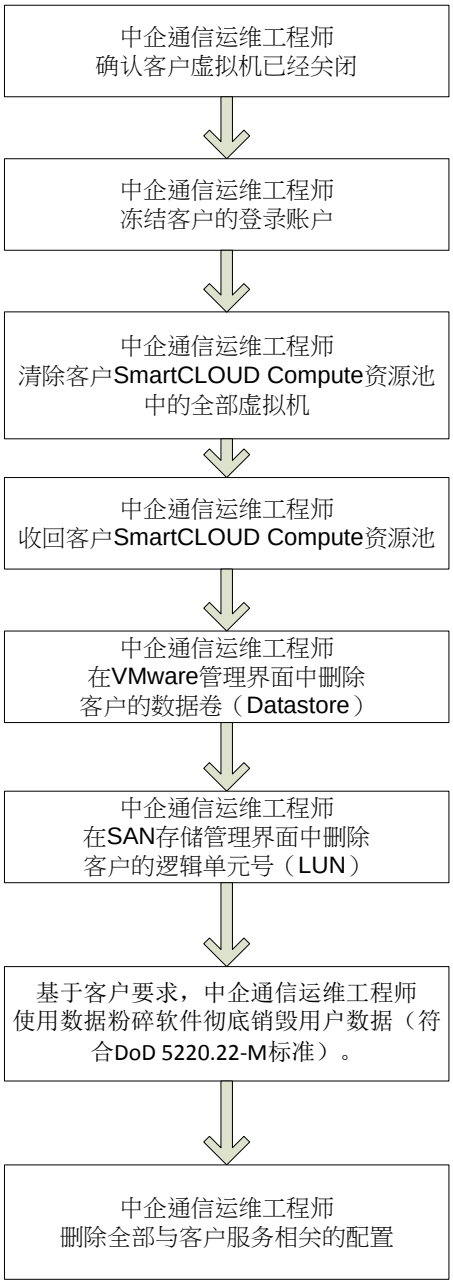
(10) 中企通信的客服人员在 Remedy 中关闭工单。

7. 数据销毁/硬件报废

7.1 数据销毁

7.1.1 客户数据销毁

当客户的《云时代服务合同》终止后，云计算运营团队的员工会彻底删除该客户于云时代服务平台上的所有数据（包括虚拟机/资源池/ datastore / LUN 等）并确认在任何情况下均不可恢复，以保障客户数据的隐私性。数据删除流程如下：



7.1.2 客户资源池回收

1. 中企通信运维工程师确认客户所有的虚拟机都已关闭；
2. 中企通信运维工程师冻结客户所有的 SmartCLOUD 服务登录帐号（包括 SSL VPN / SmartCLOUD Compute Director / SmartCLOUD Compute Reporter）。

7.1.3 虚拟机数据销毁

1. 中企通信运维工程师删除客户所有的虚拟机文件。

7.1.4 存储数据销毁

1. 中企通信运维工程师在 VMware 管理界面中删除客户的数据卷（Datastore）；
2. 中企通信运维工程师在 SAN 存储管理界面中删除客户的逻辑单元号（LUN）；
3. 基于客户特别要求（需额外付费），中企通信运维工程师使用数据粉碎软件彻底销毁客户数据（符合 DoD 5220.22-M 标准）；
4. 中企通信运维工程师删除全部与客户服务相关的配置（包括网络、端口、备份及复制任务等）。

7.2 硬件设备报废

中企通信云时代服务平台所有硬件（包括服务器、 存储、 网络及安全设备等）的默认使用期限均为三个自然年，到达使用期限无论该设备是否仍能使用，均将被替换为同等或更高规格的同类型产品。

报废原则：

- 非存储设备：此类硬件首先保存于运维中心的库房，待指定合资格的服务商统一回收并物理销毁。
- 存储设备：此类硬件会先将所有用于存储的磁盘移除，先经过 7.1 中的步骤彻底销毁数据，在确认任何情况下均不可恢复后，再待指定合资格的服务商统一回收并物理销毁。

8. 数据保护策略

8.1 数据备份及快速恢复服务

中企通信在提供云计算服务的同时，也为客户提供全面的数据保护服务，防止客户因技术故障、人为错误、自然灾害、病毒和特洛伊木马等原因造成的数据丢失。中企通信提供的数据备份服务包括以下范围：

- 为客户运行于云时代专属云服务平台上的虚拟机提供本地备份和异地备份的服务。
- 为客户创建备份任务和修改备份配置。
- 24x7x365 不间断监控备份任务及提供技术支持服务。
- 为客户提供虚拟机还原，文件夹还原或文件级别的还原服务。
- 监控客户备份空间使用量并主动通知客户。

当中企通信收到客户的数据还原请求时，中企通信的运维团队将严格依照以下流程进行操作：

(1) 当中企通信收到客户的服务请求后，将立即在客服系统 Remedy 中建立一个工单。

(2) 中企通信的客服人员将向客户发送一份《云时代需求变更申请表》。

(3) 客户在《云时代需求变更申请表》列明需要进行的操作（如临时备份，文件还原或修改备份任务配置等），加盖公司印章并发回给中企通信客服人员。

(4) 中企通信的工程师按照《云时代需求变更申请表》上的指示进行操作。

(5) 客户验证（确认虚拟机状态，还原文件的正确性等）。

(6) 客户向中企通信确认该服务请求已成功完成。

(7) 中企通信的客服人员在 Remedy 中关闭工单。

8.2 数据复制及灾难恢复服务

中企通信也为客户提供全面的数据复制和灾难恢复服务；当生产站点出现重大灾难时客户的虚拟机可以立即在灾备站点启动，从而最大限度的缩短了客户业务中断的时间。当客户的生产站点恢复后，中企通信可提供灾难还原服务，将客户的虚拟机从灾备站点切换回生产

站点。

中企通信提供的灾难恢复服务包括以下范围：

- 将客户运行于云时代专属云服务平台上的虚拟机定期（如每 2 小时）复制至异地的数据中心。
- 为客户创建复制任务和修改复制任务配置。
- 24x7x365 不间断监控复制任务及提供技术支持服务。
- 在灾难演习时，为客户提供灾难恢复和灾难还原服务。
- 在真实灾难发生时，为客户提供灾难恢复和灾难还原服务。
- 监控客户灾备站点资源使用量并主动通知客户。

当中企通信收到客户的灾难恢复请求时，中企通信的运维团队将严格依照以下流程进行操作：

(1) 客户拨打中企通信 24x7x365 客服热线，提出灾难恢复请求。

(2) 中企通信的客服人员回拨“客户联络人资料”中的联络电话，验证请求的真实性。

(3) 确认客户灾难恢复请求的真实性后，中企通信的客服人员将立即在 Remedy 客服系统中建立工单，并升级至后台运维部门。

(4) 中企通信的工程师将按《灾难恢复流程》中列明的步骤将客户的虚拟机由生产站点切换至灾备站点。

(5) 中企通信的工程师确认灾备站点的虚拟机全部启动成功。

(6) 中企通信的客服人员通知客户灾难恢复完成，客户可以进行验证。

(7) 客户登录灾备站点虚拟机，验证数据和业务系统的状态。

(8) 客户确认灾备站点已成功启动，灾难恢复完成。

(9) 中企通信的客服人员在 Remedy 中关闭工单。

备注：以上的数据备份和数据复制服务需要额外收费，具体情况请咨询中企通信销售人员。

9. 持续优化

中企通信将定期对所有的操作流程进行审核和优化，同时中企通信也十分重视平台安全问题，不管是中企通信员工、客户或合作伙伴，如在使用云时代服务的过程中发现漏洞，请及时通知中企通信，中企通信将对所有报告的漏洞进行评估。

9.1 漏洞报告

如果要报告一个漏洞，或着有任何关于云时代服务安全方面的问题，请发送邮件至help@china-entercom.net。请尽可能提供有助于我们理解漏洞性质和严重程度的相关信息（如概念验证代码、工具输出等）。未经过报告人的允许，中企通信不会将该信息透露予第三方。

中企通信会给每个收到的漏洞报告指定一个追踪编号，并定期通知报告人后续进展。

9.2 漏洞评估

中企通信会对所有收到的漏洞报告进行验证。如果需要更多信息才能验证或重现该问题，中企通信将会联系报告人。

如果该漏洞涉及第三方产品，中企通信将通知第三方供应商。中企通信会负责报告人和第三方之间的协调。未经过报告人的允许，中企通信不会将报告人的身份透露予第三方。

中企通信使用风险评估工具来评估潜在漏洞。中企通信将根据风险评估工具生成的分数评估潜在漏洞的严重性以及决定响应的优先级。

9.3 漏洞公布

在核实漏洞之后,中企通信将向报告人及客户公布漏洞的具体情况。为保障客户的信息安全，中企通信要求报告人在漏洞未得到中企通信核实及解决之前，不得向外界透露与该漏洞有关的任何信息。

10. 专业资质

合规性和安全性一直是客户评估云计算服务供应商的首要标准，为此中企通信不断努力，持续优化改善自身的云计算服务，务求达到业界公认的专业水准。迄今为止中企通信云时代服务已获得国内外权威机构的多项专业资质认证，包括：

- **可信云：**

可信云服务认证是由数据中心联盟组织，中国信息通信研究院(工信部电信研究院)测试评估的面向云计算服务的评估认证。为了能够让我国云计算产业在国际标准上拥有更多的话语权，中国信息通信研究院从 2014 年开始推动可信云服务标准的国际化工作，在进行充分准备的基础上，于 2015 年 11 月至 12 月的 ITU-T SG13 全会上提交可信云服务的定义、需求和场景三大提案。2016 年 6 月 13 日，在公开征求意见期限（last call）后, ITU 发布修订后的 ITU-T Y.3501ed2 版本，可信云成功写入国际标准。

- **ISO9001：**

ISO9001 质量体系认证是指第三方（认证机构）对企业的质量体系进行审核、评定和注册活动，其目的在于通过审核、评定和事后监督来证明企业的质量体系符合 ISO9001 标准，对符合标准要求者授予合格证书并予以注册的全部活动。

- **TL9000：**

TL9000 是一套专为电信行业质量管理体系的要求和测量标准，以 ISO9001：2015 标准 TL9000 认证为基本要求，新增加了电信行业的专业要求和电信产品的测量指标，包括：质量管理体系及衡量指标为标准基础。

- **ISO20000：**

ISO20000 标准着重于通过“IT 服务标准化”来管理 IT 问题，即将 IT 问题归类，识别问题的内在联系，然后依据服务水准协议进行计划、推行和监控，并强调与客户的沟通。该标准同时关注体系的能力，体系变更时所要求的管理水平、财务预算、软件控制和分配。

- **ISO27001：**

信息安全管理体系通过使用风险管理过程来保护信息的保密性，完整性和可用性，给相关方带来信心并使风险得到充分管理。

ISO27001 提供给准备建立、运作、维护、改进信息安全管理体系的组织。ISO27001 可被用于内部、外部，包括认证机构，评估组织的能力来满足组织自身信息安全要求。

11. 责任划分

11.1 客户义务和责任

- 在 SmartCLOUD Director 平台中管理自己的操作系统，应用程序和数据（包括备份数据）；
- 虚拟机内部的操作系统管理（包括操作系统补丁，安全补丁和安全控制等）；
- 虚拟机内部的应用程序；
- 在 SmartCLOUD Director 平台中配置虚拟机的网络参数；
- 虚拟机内部操作系统和应用程序的日志；
- 中企通信强烈建议客户在虚拟机上安装 VMware Tools，以保证客户虚拟机内部的操作系统时间能与底层 VMware 主机（ESXi Host）同步（底层 VMware 主机的 NTP 服务器使用 stdtime.gov.hk）

11.2 中企通信的义务和责任

- 确保为使用 SmartCLOUD 服务的客户提供安全可靠的基础机构，包括任何与服务有关的硬件、软件、网络及基础设施等；
- 为客户提供虚拟机管理界面，包括任何与虚拟机层面相关的日志、事件及用户操作记录；
- 确保客户使用服务时的安全性和隔离性，包括：
    1. 不同客户之间的环境完全隔离；
    2. 客户环境与中企通信管理环境完全隔离；

3. 客户环境与其他未受信任的环境（如互联网）完全隔离。

- 基于客户申请，为客户提供技术支持服务（如信息查询、故障排查及配置更改等）。

12. 用户行为守则

客户不得利用中企通信提供的 SmartCLOUD 服务：

- 危害国家安全；
- 泄露国家秘密；
- 不得侵犯国家的、社会的、集体的利益和公民的合法权益；
- 不得从事违法、犯罪活动，不得侵犯第三方知识产权。

客户不得利用中企通信提供的 SmartCLOUD 服务制作、复制、查阅和传播下列信息：

- 煽动抗拒、破坏宪法和法律、行政法规实施的信息；
- 煽动颠覆国家政权，推翻社会主义制度的信息；
- 煽动分裂国家、破坏国家统一的信息；
- 煽动民族仇恨、民族歧视，破坏民族团结的信息；
- 捏造或者歪曲事实，散布谣言，扰乱社会秩序的信息；
- 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的信息；
- 公然侮辱他人或者捏造事实诽谤他人的信息；
- 损害国家机关信誉的信息；
- 其他违反宪法和法律、行政法规的信息。

客户在使用中企通信提供的SmartCLOUD服务期间不得从事下列危害计算机信息网络安全的活动：

- 未经允许，进入计算机信息网络或者使用计算机信息网络资源的活动；
- 未经允许，对计算机信息网络功能进行删除、修改或者增加的活动；
- 未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的活动；

- 制作、传播计算机病毒等破坏性程序的活动；
- 其他危害计算机信息网络安全的活动。