中企通信
CHINA ENTERCOM

云时代备份、灾备和恢复服务安全白皮书

中企网络通信技术有限公司

2017 年 7 月

目录

概述

中企网络通信技术有限公司（以下简称“中企通信”）云时代备份、灾备和恢复服务（以下简称“SmartCLOUD BRR”）为 SmartCLOUD 云时代主机服务的客户、vONE 客户或使用 VMware vSphere 虚拟化平台的客户提供全面的数据保护，防止客户因技术故障、人为错误、自然灾害、病毒或特洛伊木马造成的数据丢失，同时为客户提供关键业务数据快速恢复服务。

本文档对 SmartCLOUD BRR 服务的安全性进行了全面的说明，包含以下 8 个方面内容：

- 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
- 持续优化
- 相关专业资质

1. 数据中心安全

1.1 设施及人员访问安全

SmartCLOUD BRR 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 SmartCLOUD BRR 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 SmartCLOUD BRR 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 SmartCLOUD BRR 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 BRR 服务：

SmartCLOUD BRR 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。

2. 服务平台安全

2.1 整体架构安全

中企通信 SmartCLOUD BRR 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 SmartCLOUD BRR 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。

2.2 数据存储安全

SmartCLOUD BRR 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 SmartCLOUD BRR 服务平台的基础设施位于同一机柜。

在 SmartCLOUD BRR 服务平台中，每位客户均配有专用的存储空间和逻辑分区；每个逻辑分区之间是互相隔离且定义了不同的访问策略。

2.3 数据传输安全

客户数据从生产站点传输至 SmartCLOUD BRR 平台时，支持以下几种连接方式，每种方式都有对应的安全策略，保证客户数据在传输时的安全：

1. 专线（如 MPLS/点对点等）连接;
   - 内网传输，vLAN 隔离，安全性最高;
   - 适用于 SmartCLOUD C2C Backup ，C2C/V2C Replication 服务;
2. IPSec 加密通道;
   - 适用于 SmartCLOUD V2C Replication 服务;
3. 公网传输;

- 应用层面数据加密，支持 DES (128 bit)和 AES (128 或 256 bit);
- 支持客户自定义密码加密;
- 适用于 SmartCLOUD V2C Backup ， P2C Replication 服务。

2.4 服务平台的可用性

SmartCLOUD BRR 服务平台内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。

SmartCLOUD BRR 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，以确保服务平台的安全和稳定。

SmartCLOUD BRR 服务等级协议（SLA）为 **99.9%。**

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

3. 通信与网络安全

3.1 云端网络架构设计原则

- **区域层次防护**

相比传统的IDC，中企通信云计算服务平台的网络架构同样基于多层设计原则，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。

3.2 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，方法是在服务平台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。

4. 服务平台运维安全

4.1 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。

4.2 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有限的客户信息。

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。

4.3 审计跟踪

对于中企通信内部网络和系统（包括 SmartCLOUD BRR 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。

4.4 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 SmartCLOUD BRR 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 SmartCLOUD BRR 服务平台不受威胁。

5. 变更管理

未经客户许可，中企通信的运维人员不得访问客户的任何数据。仅当客户发出服务请求时，中企通信的运维人员将严格按照以下流程执行：

(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；

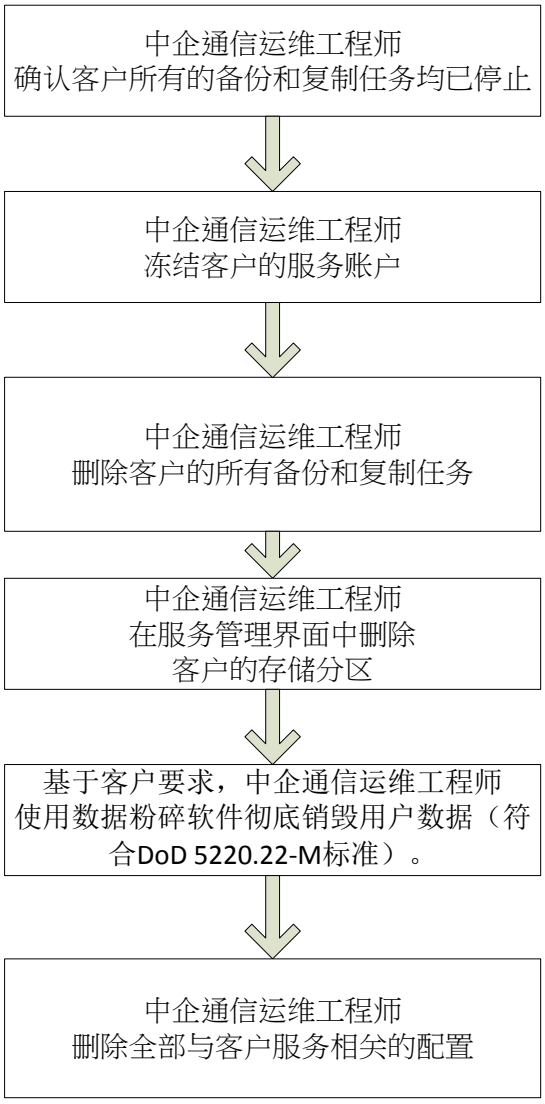
(10) 中企通信的客服人员在 Remedy 中关闭工单。

6. 数据销毁/硬件报废

6.1 数据销毁

6.1.1 客户数据销毁

当客户的《云时代服务合同》终止后，中企通信的工程师会彻底删除该客户于服务平台上的所有数据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：



6.1.2 服务配置清除

1. 中企通信运维工程师确认所有与服务相关的备份和复制任务均已停止；
2. 中企通信运维工程师冻结客户所有的服务登录帐号（如 V2C Backup）；
3. 中企通信运维工程师删除所有与服务相关的备份和复制任务。

6.1.3 存储数据销毁

1. 中企通信运维工程师在服务管理界面中删除客户的存储分区；
2. 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）；
3. 中企通信运维工程师删除全部与客户服务相关的配置。

6.2 硬件设备报废

中企通信 SmartCLOUD BRR 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 6.1 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。

7. 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 SmartCLOUD BRR 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。

7.1 漏洞报告

如果要报告一个漏洞，或着有任何关于 SmartCLOUD BRR 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。

7.2 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。完成初期调查后，中企通信将向报告人发送解决问题及公开披露的计划。

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。

7.3 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。

8. 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。

9. 责任划分

9.1 客户义务和责任

- 向中企通信提供备份或复制任务的具体信息（包括需要备份或复制的数据、备份或复制时间间隔及还原点数量等）；
- 向中企通信提出还原或灾难恢复请求；
- 在中企通信完成还原操作后验证数据状态；
- 在中企通信完成灾难恢复操作后验证灾备站点虚拟机的状态；
- 中企通信强烈建议客户在灾备站点的虚拟机上安装 VMware Tools，以保证客户虚拟机内操作系统的时间能与底层 VMware 主机（ESXi Host）同步（底层 VMware 主机的 NTP 服务器使用 stdtime.gov.hk）。

9.2 中企通信的义务和责任

- 确保 SmartCLOUD BRR 服务的可用性达到承诺的服务等级（SLA）；
- 确保云端备份存储资源或云端灾难恢复资源池的可用性；
- 管理客户备份或复制的数据，确保其安全性和可用性；
- 基于客户申请，修改备份或复制任务配置（包括需要备份或复制的数据、备份或复制时间间隔及还原点数量等）；
- 基于客户申请，为客户提供还原或灾难恢复操作。

10. 用户行为守则

客户不得利用中企通信提供的 SmartCLOUD BRR 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 BRR 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 BRR 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。