H3C HDM 安全技术白皮书

目 录

1 概述

H3C 服务器管理系统 HDM，作为 H3C 全系列服务器设备的重要管理软件，面向终端用户不仅提供基于浏览器的 Web 管理界面，同时也提供大量接口来方便对接用户的网管系统，满足多样的管理需求。

HDM 管理软件在设计时，不仅关注客户功能需求的满足，对外导出服务器硬件对安全的支持情况，同时也充分考虑自身的安全性，以满足用户在多种场景下对管理通道安全性的需求。

对硬件安全特性的支持上，主要是针对各个具体服务器对硬件支持的安全特性上提供对应的用户界面，方便用户查看支持情况、操作日志、使能相关特性等功能。

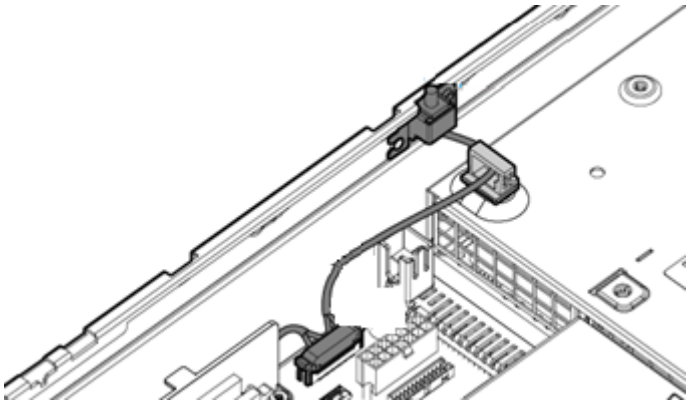
对于 HDM 管理软件，则从接入方式、账号管理、传输链路加密、数据存储、操作审计等多个维度来保障服务器管理操作时的安全。

2 对服务器硬件安全的支持

2.1 机箱入侵检测

如 图 1 所示，当服务器内的开箱检测模块触发了开箱的信号，软件接收到硬件GPIO管脚发送的信号，触发软件中断，进而判断当前发生了开箱信号还是关箱信号。当确认了开关箱信号时，HDM通过传感器将发生的状态通过事件日志的形式体现出来。

图1 开箱检测模块



用户可从Web页面可以看到当前是发生了开箱还是关箱动作。在HDM界面上对应的传感器如 图 2 所示。

图2 传感器信息

设备开箱后，在HDM界面上有对应的事件如 图 3 所示：

图3 事件日志

ID	时间戳	传感器名称	传感器类型	状态	级别	描述
2911	2017-01-15 06:53:24	AreaIntrusion	physical_security	解除	通知	General chassis intrusion
2910	2017-01-15 06:51:04	AreaIntrusion	physical_security	触发	次要	General chassis intrusion

同时，检测到对应的事件后，支持通过 SNMP Trap、邮件方式上报对应的事件。

2.2 可信计算

病毒程序利用操作系统对执行代码不检查一致性的弱点，将病毒代码嵌入到执行代码程序，实现病毒传播；黑客利用被攻击系统的漏洞窃取超级用户权限，植入攻击程序，肆意进行破坏；更为严重的是，对合法的用户没有进行严格的访问控制，从而可以进行越权访问，造成不安全事故。

1999年10月，多家IT巨头联合发起成立可信赖运算平台联盟（Trusted Computing Platform Alliance，TCPA），后改组为可信赖计算组织（Trusted Computing Group，TCG），希望从跨平台和操作环境的硬件和软件两方面，制定可信赖电脑相关标准和规范。

可信平台模块自身必须是安全的，这是可信平台模块有效工作的基础；可信平台模块必须具备构建可信计算平台和远程证明所需的各类功能，这些功能是可信平台模块的核心。

可信计算计算平台在系统中的落地，需要芯片、固件、软件多个维度来支持。通常，在H3C服务器的设计上，支持选配TPM、TCM模块。软件上，当前支持对符合TPM或TCM标准芯片的信息查询。如 图 4 所示，可通过HDM页面查询。

图4 TPM/TCM 状态

受安全政策的影响，不同地方的使用标准不同，如：中国香港使用标准的 TPM 协议。

受兼容性的限制，有些功能模块依赖标准不同，如：Windows 的 BitLocker、虚拟智能卡（Virtual Smart Card）等功能依赖 TPM 才能使用。

2.3 固件安全管理

固件对于系统的正常运行有至关重要的影响，一旦固件受到损坏，系统就会出现异常，甚至无法启动。当前，我们在固件安全方面，做了以下措施：

- 对于关键固件，比如存放 HDM 镜像的 Flash 区域，设计了双镜像方式。当在运行过程中出现 Flash 误操作或者存储块损坏时，可以切换到备份镜像运行。
- 所有对外发布的 HDM、BIOS 固件版本都带有签名机制。固件打包时，通过 sha256 算法摘要，用 RSA2048 加密摘要，在固件升级时，通过签名校验方式来防止篡改，只有签名符合要求的固件才允许升级到设备上。
- 运行时，对镜像所在区域进行写保护，需要通过特殊方式才能进行写操作。同时，每次启动时对镜像文件的完整性进行校验，必要时进行恢复。

3 HDM管理软件安全性

鉴于 HDM 是用来管理服务器的，有大量特权操作存在，比如：对服务器进行上下电、远程访问 Host、对 BIOS 进行修改、固件升级等。故现实使用中，建议把 HDM 的网络连接到独立的内网，而非连接到公网上。若需要连接到公网上，最好通过防火墙对接入的 IP 地址进行严格控制。

在内网上，由于服务器设备接入到网络上，仍然面临多方面的威胁。H3C 服务器的 HDM 管理软件，在设计时，从多个角度来综合考虑，平衡相关功能的性能、易用性和安全性，提供多种访问手段供用户选择。

3.1 安全的管理接口

所有的管理接口都是经过要求通过认证后才能访问相关的管理信息。

3.1.1 标准IPMI 1.5/IPMI 2.0 管理接口

HDM 兼容 IPMI 1.5/IPMI 2.0 规范，通过第三方工具（如：ipmitool)基于 LPC 通道的 KCS 协议或 LAN 通道的 UDP/IP 协议实现对服务器的有效管理。

- 基于 KCS 时，ipmitool 等工具必须运行在服务器本机的操作系统上；
- 基于 LAN 时，ipmitool 等工具可以远程管理服务器，支持基于 RMCP+协议认证；

3.1.2 HTTPS管理接口

HDM 对外提供的 Web 可视化管理接口，是完全基于 HTTPS，可以保证通过 HDM 访问的数据无法被窥视。当前支持的 TLSv1.0，TLSv1.1，TLSv1.2，支持安全算法套件有：RSA_WITH_AES_128_CBC_SHA256、RSA_WITH_AES_256_CBC_SHA256、RSA_WITH_CAMELLIA_256_CBC_SHA、RSA_WITH_AES_128_GCM_SHA256、RSA_WITH_AES_256_GCM_SHA384。

3.1.3 SNMP管理接口

支持 SNMPv3 版本提供了认证和加密安全机制，以及基于用户和视图的访问控制功能，增强了安全性。

3.1.4 Redfish管理接口

对基于 Redfish 设置类型的 API 接口进行访问时，均需在会话认证通过后才可进行，相关数据是基于 SSL 链路来传递。

3.2 链路安全

HDM 除了上述标准的管理接口外，还有一些用于数据传递的链路存在，比如 KVM、虚拟媒体、VNC 等。设计上，这些链路也均支持加密方式来传递对应的报文。

3.2.1 虚拟KVM

虚拟 KVM 是指用户在客户端利用本地的视频、键盘、鼠标对远程的设备进行监视和控制，提供实时操作异地服务器的管理方式。

为了保障用户连接上的服务器信息不在链路上泄露，交互过程的信息不被监听，对 KVM 链接通道传递的数据，支持采用加密方式来通信。

同时，H5 方式下，支持单一端口认证功能，虚拟 KVM 和虚拟媒体相关的功能是通过 Web 服务接口来统一导出，可减少对外开放的 Web 接口，以便减少安全风险。

3.2.2 虚拟媒体

虚拟媒体即通过网络在服务器上以虚拟 USB 光盘驱动器和软盘驱动器的形式提供对本地媒体（光盘驱动器、软盘驱动器或光/软盘的镜像文件，硬盘文件夹）的远程访问方式。虚拟媒体的实现原理是将客户所在的本地主机的媒体设备通过网络虚拟为远端服务器主机的媒体设备。

支持的虚拟媒介有：

- DVD、CD 光驱
- Floppy 软驱
- ISO、IMG 文件

- 虚拟文件夹
- USB key

为了保证对虚拟媒体进行访问时，防止数据在链路上被监听，对数据进行传输时，H5 方式同 HTTPS 的加密方式。基于 OpenJDK 技术的实现，支持采用 AES 128 CBC 算法来加密传输。

3.2.3 VNC

VNC（Virtual Network Computing，虚拟网络 计算机）用于传送服务端的原始图像到客户端，该协议提供一种不用登录HDM即可访问控制服务器的方法，即用本地主机的显示器、输入设备远程控制服务器。

VNC 客户端与 VNC 服务端建立会话时，需要远程计算机的 IP（IPv4/IPv6）和 VNC 密码（认证过程：服务器向客户端发送 16 字节随机码，客户端用 VNC 密码作为 KEY 采用 DES 加密该随机串发给服务端校验）。在访问持续过程中，可根据选择的连接类型来决定是否对链路中的数据进行加密。

部分版本可根据需要选择支持以下两种 VNC 安全连接类型：

- VNC over SSH（数据通过 SSH 通道传输）
- VNC over stunnel（数据通过 stunnel 程序建立的 TLS/SSL 通道传输）

3.3 完善的操作记录和审计记录

对设备的操作相关信息，均记录到操作日志中，包括：审计日志、配置日志、固件更新日志和硬件更新日志。

- 审计日志：记录访问 HDM 的操作信息，包括：通过浏览器登录 HDM、启动远程控制台等信息。
- 配置日志：记录用户的配置操作及操作结果。
- 固件更新日志：记录固件更新的操作信息及操作结果。
- 硬件更新日志：记录硬件更新的操作信息及操作结果。

通过操作日志，可了解到用户登录情况、硬件更换情况、配置变更情况。通过这些信息可以对设备的操作情况进行审计跟踪处理。

3.4 域管理和目录服务

3.4.1 域管理

用户可以将所有被管理服务器加入一个统一的管理域并使用域名来访问被管服务器的 HDM。域管理可以更方便、集中地管理用户账户信息，安全性更高，有利于企业的一些保密资料的管理，大大地提高用户管理效率。域为用户提供了单一的登录过程来访问网络资源，用户只要具有对资源的合法权限，域通过对用户权限的合理划分，确定了对特定资源有合法权限的用户才能使用该资源，从而保障了资源使用的合法性和安全性。

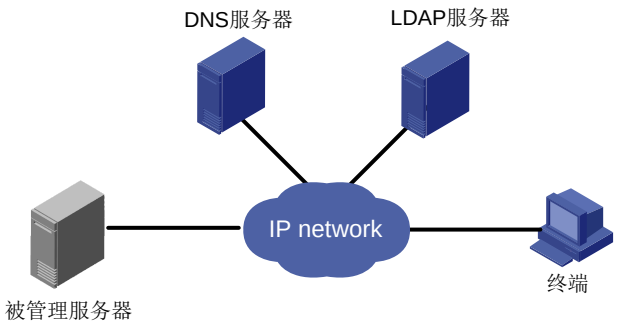
3.4.2 目录服务

LDAP（Lightweight Directory Access Protocol）是一个访问在线目录服务的协议。LDAP 目录中可以存储例如电子邮件地址、邮件路由信息等各种类型的数据，为用户提供更集中、更便捷的查询。

按照如 图 5 所示原理，启用HDM的目录服务，可以将所有HDM的用户管理，权限分配，有效期管理都集中到目录服务器上，避免大量的重复性用户配置任务，提高管理效率。另外将用户集中到目录服务器上，也能大大提高HDM智能管理系统的安全性。

我司服务器 HDM 上的 LDAP 功能可以在角色组中自定义访问 HDM 用户的各种权限，结合域控制器的域用户管理功能，可以配置不同用户具有不同的访问权限，提高了 HDM 使用的安全性。

图5 LDAP 服务器原理图



LDAP 标准优点：

- 可扩展性：可以在所有 HDM 上同时动态支持 LDAP 服务器上新增账户的管理。
- 安全性：用户密码策略都在 LDAP 服务器上实施，数据交互可基于 SSL 来完成。
- 实时性：LDAP 服务器上账户的任何更新都将立即应用到所有的 HDM。
- 高效性：可以将所有 HDM 智能管理系统的用户管理，权限分配，有效期管理都集中到目录服务器上，避免大量的重复性用户配置任务，提高管理效率。

3.5 防火墙

基于安全考虑，HDM 提供防火墙特性以实现基于场景的登录管理。HDM 可以从时间、IP 地址和 IP 协议版本（IPv4/IPv6）、MAC、端口、协议（TCP/UDP）五个维度将服务器管理接口访问控制在最小范围；目前该特性适用于 WEB、SSH、SNMP v1/v2c/v3、IPMI LAN 接口的登录限制。

由用户根据需要设置登录规则的白名单，登录时只要匹配上任意一条登录规则，即可登录，否则拒绝登录；登录规则可应用于所有本地用户和 LDAP 用户组。

3.6 账号安全

账号安全包括：密码复杂度检查、密码有效期、禁用历史密码重复次数、登录失败锁定、密码锁定时长，提示修改初始密码。在“配置->用户配置”的“高级设置”里可配置。如 图 6 所示。

图6 账户安全设置

- 密码复杂度检查：开启该功能后，所有用户的密码设置需符合以下要求，否则密码设置无法通过检查。
  - 密码长度为 8～20 个字符，仅支持字母、数字、空格和特殊字符 `~!@#$%^&*()_+-=[]\{}|;':",./<>?，区分大小写；
  - 至少包含大写字母、小写字母和数字中的两种字符；
  - 至少包含一个空格或特殊字符；
  - 不能与用户名或用户名的倒序相同；
  - 需符合“禁用历史密码”要求。
- 密码有效期：用户密码的使用期限，临近使用期限前，HDM 会提醒用户更换密码。默认管理员不受密码有效期配置影响。
- 禁用历史密码：用户修改密码时，禁止使用设置次数内的历史密码。
- 登录失败锁定：用户登录失败的次数达到设定的次数后，系统会锁定该用户的登录。
- 登录失败锁定时长：用户由于登录失败达到登录失败锁定次数后，被系统锁定的时长。用户被锁定后，在失败锁定时长内不能登录 HDM。

3.7 用户定义

随着客户对安全的重视，不同客户对管理权限的需求各异，不仅需要支持管理员、操作员和普通用户三个角色，还需要定义不同功能的权限。为此，HDM 还增加了面向功能的权限管理功能，可通过 IPMI/Redfish/WEB 禁用用户或用户的部分权限，比如 KVM、VMedia、WEB、IPMI 和 SNMP 这些特性的权限。

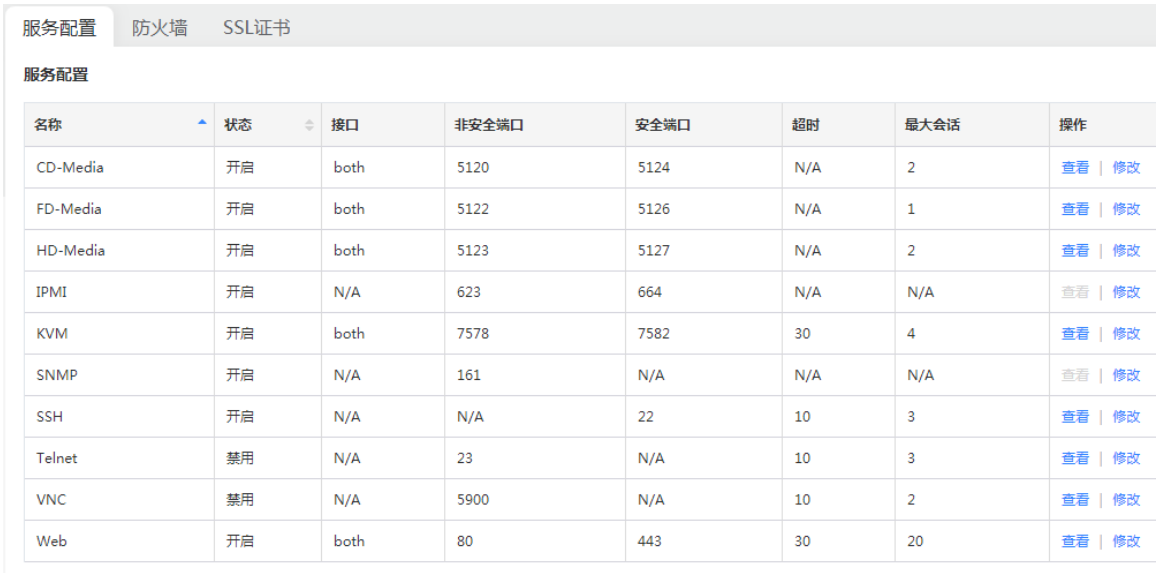
3.8 SSL证书管理

为了提高数据链路的传输安全。当前 HDM 支持 SSL 证书上传功能，用户可以使用在本地生产的 SSL 证书来上传到 HDM 上，替换掉默认集成到 HDM 中的证书和私钥。

3.9 服务管理

为了满足客户的业务和安全需要，HDM提供开关来控制是否提供服务端口。HDM支持修改的服务为：CD-Media、FD-Media、HD-Media、IPMI、KVM、Remote_XDP、SNMP、SSH、Telnet、VNC和Web，如 图 7 所示。

图7 HDM 服务配置



名称	状态	接口	非安全端口	安全端口	超时	最大会话	操作
CD-Media	开启	both	5120	5124	N/A	2	查看 | 修改
FD-Media	开启	both	5122	5126	N/A	1	查看 | 修改
HD-Media	开启	both	5123	5127	N/A	2	查看 | 修改
IPMI	开启	N/A	623	664	N/A	N/A	查看 | 修改
KVM	开启	both	7578	7582	30	4	查看 | 修改
SNMP	开启	N/A	161	N/A	N/A	N/A	查看 | 修改
SSH	开启	N/A	N/A	22	10	3	查看 | 修改
Telnet	禁用	N/A	23	N/A	10	3	查看 | 修改
VNC	禁用	N/A	5900	N/A	10	2	查看 | 修改
Web	开启	both	80	443	30	20	查看 | 修改

3.10 硬件加密

HDM 的 SOC 芯片支持硬件安全加速模块，用来加强 HDM 的安全相关功能。主要应用在认证、数据加解密等安全应用中。当前实现了对 AES、DES、3DES、RC4、MD5、SHA1、SHA224、SHA256、HMAC-MD5、HMAC-SHA1、HMAC-SHA224 和 HMAC-SHA256 算法的硬件支持。

4 总结

H3C 服务器的 HDM 管理软件，不仅对用户展现了当前服务器对安全特性的支持情况。同时也关注自身的安全性，对外提供了多种安全保障手段，可应对来自多方面的安全威胁，可有效保障用户的服务器数据资产的安全。