编号：FGBGJ[2013]1965CPFA-08

2013 年国家信息安全专项
大数据平台安全管理产品测评方案

编制：_____

审核：_____

批准：_____

2014-01-01 发布　　2014-01-15 实施

公安部计算机信息系统安全产品质量监督检验中心

目　　录

（本页以下空白）

1. 测评依据

《国家发展改革委办公厅关于组织实施2013年国家信息安全专项有关事项的通知》（发改办高技[2013]1965号）

MSTL_JGF_04-036 0101—2013 信息安全技术 大数据平台安全管理产品检验规范

GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则（EAL3）

2. 测试环境

2.1. 功能测试环境

2.1.1. 拓扑结构图

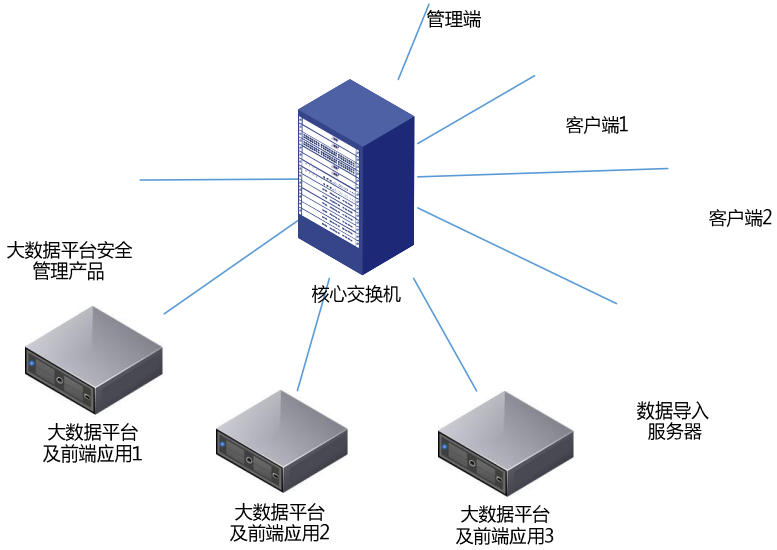

图 2-1 功能测试环境图

2.1.2. 功能测试设备说明

根据上图所述的测试环境结构图，本节对所需的测试设备做一些说明。

表 2-1 测试设备说明

设备名称	说明	备注
万兆核心交换机	为本测试提供骨干网络支持。支持IPv4/6的复杂应用环境部署，提供对高性能流量的线速汇聚和控制。为高性能云计算与大数据应用构建核心高速交换网络。支持336个线速千兆端口和28个线速万兆端口，高密度端口可以支持630个千兆和112个	无

设备名称	说明	备注
	万兆交换能力，支持IPv4/IPv6一致线速转发	
大数据平台及前端应用1~3	在高性能物理实体服务器上虚拟实现3种大数据应用平台的分布式服务器和前端应用（至少虚拟出1台主节点、2台从节点、1台应用服务器。考虑到部署效率，数据采取本地存储）。物理实体服务器为Intel Xeon E5 8~12核CPU/32GB/4~8T SAS/千兆网卡	无
数据导入服务器	用于导入大数据平台中海量数据的服务器设备。配置不低于Intel 2.0GHz 4核/4G/1T SATA/千兆网卡	无
管理端	对被测的大数据平台安全管理产品实施管理控制。配置不低于Intel 2.0GHz 4核/4G/1T SATA/千兆网卡	无
客户端1~2	对大数据平台的应用进行访问、运行状态进行控制。配置不低于Intel 2.0GHz 4核/4G/1T SATA/千兆网卡	无

2.2. 性能测试环境

2.2.1. 拓扑结构图

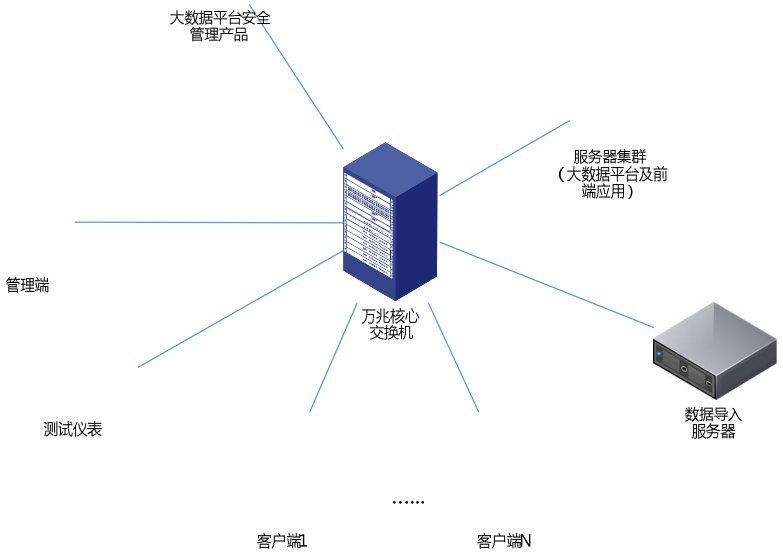

图 2-2 性能测试环境图

2.2.2. 性能测试设备说明

根据上图所述的测试环境结构图，本节对所需的测试设备做一些说明。

表 2-2 测试设备说明

设备名称	说明	备注
万兆核心交换机	为本测试提供骨干网络支持。支持IPv4/6的复杂应用环境部署，提供对高性能流量的线速汇聚和控制。为高性能云计算与大数据应用构建核心高速交换网络。支持336个线速千兆端口和28个线速万兆端口，高密度端口可以支持630个千兆和112个万兆交换能力，支持IPv4/IPv6一致线速转发	无
服务器集群（大数据平台及前端应用）	在高性能物理实体服务器集群上虚拟实现大数据平台的分布式服务器和前端应用（考虑到部署效率，数据采取本地存储）。物理实体服务器为Intel Xeon E5 8~12核CPU/32GB/4~8T SAS/千兆网卡	部署基于Web的应用服务，并能够直接通过URL进行大并发访问
数据导入服务器	用于导入大数据平台中海量数据的服务器设备。物理实体服务器的配置不低于Intel Xeon E5 8~12 核 CPU/32GB/4~8T SAS/千兆网卡	无
管理端	对被测的大数据平台安全管理产品实施管理控制。配置不低于Intel 2.0GHz 4核/4G/1T SATA/千兆网卡	无
测试仪表	测试仪表配置成测试B/S最大并发数模式，模拟生成大量单条B/S并发应用访问事件	网络高性测试仪 BPS ELITE
HP Loadrunner	针对可能存在C/S访问模式以及真实B/S访问模式的模拟需求，进行大规模的并发访问。	无
客户端1~N	由高性能物理实体服务器上虚拟实现。部署并发访问脚本生成工具（自编制或Loadrunner），针对可能存在C/S访问模式以及真实B/S访问模式的模拟需求，进行大规模的并发访问。物理实体服务器配置	无

设备名称	说明	备注
	不低于 Intel Xeon E5 8~12 核 CPU/32GB/4~8T SAS/四千兆网卡	

2.3. 测试设备说明

本节对测试过程中所使用的其他设备做一些说明。

表 2-3 测试设备说明

设备名称	说明	备注
RJ-iTOP 网络隐患扫描系统	对产品的管理平台进行漏洞扫描	无
明鉴 WEB 应用扫描器	对产品的 WEB 管理平台进行 WEB 漏洞扫描	无
Black Duck Protex 6.0.0	对产品进行代码开源比例检测	无
虚拟软件 VMware ESX	为本测试项目提供虚拟化平台支持，部署形成高性能大数据应用环境的虚拟应用测试环境	无

3. 测评前准备

3.1. 测评人员准备

3.1.1. 知识技能

在进行大数据平台安全管理产品测评之前，测评人员必须学习并熟练掌握如下知识、软件及工具：

1) 基于 IPv4/IPv6 协议协议的网络拓扑构建方法；
2) 常见信息安全技术的基本概念和工作原理；
3) 虚拟化、大数据平台和安全管理平台的基本概念和工作原理；
4) 漏洞扫描、补丁管理、去隐私化处理、多维度审计等测试相关技术的基本概念和实现原理；
5) Windows 和 RedHat AS、CentOS 等操作系统及相关服务安装配置方法；
6) 通用数据库如 SQL Server、Oracle 等的使用方法；
7) 第 2 章表 2-1、表 2-2、表 2-3 中设备、测试仪表和软件的使用方法。

3.1.2. 测试环境准备

在检测开始之前，测评人员必须做好如下准备：

1） 根据第 2 章测试设备说明准备检测所需要的硬件设备，并为之安装相应

的操作系统及软件；

2） 根据图 2-1 、图 2-2 检测环境网络拓扑结构图构建测试网络，并为之配置相应的 IP 地址等网络属性以及需要的服务；

3） 以送检产品分发和操作文档为依据，安装送检样品；

4） 确认送检产品能正常运行，准备工作完成。

3.1.3. 标准准备

在检测时，测评人员尚需准备好如下标准，并通读标准，基本掌握标准内容，以便查询。

1） 《国家发展改革委办公厅关于组织实施 2013 年国家信息安全专项有关事项的通知》（发改办高技[2013]1965 号）

2） MSTL_JGF_04-036 0101—2013 信息安全技术 大数据平台安全管理产品检验规范

3） GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则（EAL3）

3.1.4. 测试用例的编写

测评人员应对照每一条测评依据制定出适合送检产品特点的测试用例。测试用例必须包含用例序号、用例作者、设计日期与具体的输入输出信息，以便减少测试的不确定性，并在追溯错误时能将其再现。

在测试用例编写时，有如下原则与方法可以参考：

1） 测评人员需仔细研究标准含义，分析在实际情况中可能出现的每一种情况，然后采用等价类划分的方法做较全面的覆盖测试；

2） 对具有临界值的测试应尽可能采用边界值的方法进行测试；

3） 依据平时测评的经验，可以用错误推测法追加一些测试用例；

4） 建议根据业务流的规律，整理每条业务流所对应的标准功能点，依据业务流来进行检测。

3.2. 送检厂商准备

在测评开始之前，送检厂商必须做好如下准备：

1） 准备全部技术文档及资料（包括部署场景示意图）；

2） 准备送检系统硬件设备及软件安装程序，并在送检之前确认系统版本是否

正确，硬件工作是否正常；

3) 若必要，提供测试所需的，实现产品功能的外围设备；

4) 为检测需要，厂商尚需提供本测评方案第 4 章中“文档要求”所规定的全部文档，并准备文档索引表，标明该部分“文档要求”对应所提供的具体文档名或哪本文档的第几页。

4. 测评方法及结果判定

4.1. 大数据平台安全管理产品检验规范要求

4.1.1. 集中管理功能

4.1.1.1. 对象管理

测评依据：

产品应能够增加、删除受控大数据平台。

文档要求：

厂商应提供文档，说明产品增加、删除受控大数据应用平台的方法。

测评方法：

1) 在受控大数据应用平台进行适当的配置，如配置网络 IP 地址、增加用于产品管理的管理员账号等；

2) 以授权管理员登录产品，添加受控大数据应用平台，尝试通过产品对其进行管理，如配置策略，查看状态，收取日志等；

3) 以授权管理员登录产品，删除已添加的大数据应用平台，尝试通过产品对已删除的大数据应用平台进行管理，如配置策略，查看状态，收取日志等。

预期结果：

1) 步骤 2）管理员能够添加大数据应用平台，添加后能够对其进行管理；

2) 步骤 3）管理员能够删除大数据应用平台，删除后不能对其进行管理。

若同时满足预期结果1)和2)，则判为符合；否则判为不符合。

4.1.1.2. 运行状态监测

测评依据：

产品应能够实时监测各受控大数据平台的相关状态，比如大数据平台各组件是否在线，组件设备的CPU使用率、内存占用率、存储介质的使用情况等。

文档要求：

厂商应提供文档，说明产品对受控大数据应用平台进行监控的方法，并说明所支持的监测内容。

测评方法：

1) 登录产品，查看受控大数据应用平台各组件是否在线，CPU 使用率、内存占用率、存储介质使用情况等信息；
2) 尝试改变受控大数据平台的状态，如断开网络连接，增加建立的连接数等；
3) 通过产品查看该受控大数据应用平台的在线状态变化情况，并与实际情况对比是否一致；
4) 对不同的大数据应用平台，重复步骤 1)-3)，观察产品能否监测大数据应用平台的状态变化。

预期结果：

1) 步骤 1)产品的管理界面上能够查看受控大数据应用平台的在线状态，CPU 使用率、内存占用率、存储介质使用情况等信息；
2) 步骤 2)-3）产品所监测的状态与大数据应用平台的实际情况一致；
3) 步骤 4）产品能够及时监测到不同的大数据应用平台状态的变化。

若同时满足预期结果1)-3)，则判为符合；否则判为不符合。

4.1.1.3. 配置基线检查

测评依据：

产品应能够对大数据平台的配置进行基线检查，检查内容至少包括以下对象中的一种或者多种：

a) 操作系统；
b) 数据库；
c) 大数据应用。

文档要求：

提供文档说明产品配置基线的方法和检查能力。

测评方法：

1) 通过产品收集某一大数据应用平台的配置信息，以此建立基线；
2) 对此大数据应用平台的配置参数进行变更；
3) 检查产品是否能够发现配置变更；
4) 对不同的大数据应用平台，重复步骤1）-3)。

预期结果：

1）步骤 1）能够收集大数据应用平台的配置信息，并建立基线；

2）步骤 3）能够发现大数据应用平台的配置变更；

3）支持对3种以上的大数据应用平台进行配置基线检查。

若同时满足预期结果1)-3)，则判为符合；否则判为不符合。

4.1.1.4. 版本检测

测评依据：

产品应能够获取大数据平台的相关版本信息。

文档要求：

提供文档说明产品对大数据平台进行版本检测的范围和方法。

测评方法：

1）在不同大数据应用平台上分别查看大数据平台软件、操作系统或者数据库的版本信息；

2）通过产品获取不同大数据平台的软件版本、操作系统版本或者数据库版本等信息；

3）比对步骤1）和2）的版本是否一致；

4）对不同的大数据应用平台，重复步骤1）-3）。

预期结果：

1） 步骤3）产品获取的版本信息与大数据平台实际一致；

2） 支持对3种以上大数据应用平台进行版本检测。

若同时满足预期结果 1)和 2)，则判为符合；否则判为不符合。

4.1.1.5. 日志报警信息收集

测评依据：

产品应能够收集各受控大数据平台所产生的报警和日志等信息，对所收集的信息统一格式，形成事件记录，并存储于永久性介质内。

文档要求：

厂商应提供文档，说明产品收集各大数据应用平台所产生的报警和日志等信息的方法，说明事件记录的格式，并说明产品存储日志报警信息的介质类型。

检验方法：

1） 在受控大数据应用平台上进行相关配置，如配置产品为受控大数据应用平台的日志服务器等；

2） 导入预置数据或触发策略以产生各类日志及告警信息；

3） 从产品管理界面查看日志，检查是否接收到各项日志及告警信息；

4) 登录产品后台查看事件记录的存储格式是否和文档描述一致，并且格式统一；

5) 将产品断电后重启，检查断电之前的日志是否丢失。

预期结果：

1) 步骤 1）-3）产品能够接收受控大数据应用平台所产生的各类日志及告警信息；

2) 步骤 4）事件记录的存储格式和文档描述一致，并且格式统一；

3) 步骤 5）产品断电重启后，日志未丢失。

若同时满足预期结果 1)-3)，则判为符合；否则判为不符合。

4.1.1.6. 事件记录查询

测评依据：

应能够对事件记录进行多条件查询，至少能按事件发生的日期和时间、事件主体、事件类型等条件进行组合。

文档要求：

厂商应提供文档，说明对事件记录进行查询的条件范围。

测评方法：

1) 通过产品的管理界面，选择不同条件，查询事件记录；

2) 观察查询结果是否正确。

预期结果：

1) 步骤 1）条件包括事件发生的日期和时间、事件主体、事件类型等范围，支持组合查询；

2) 步骤 2）查询结果正确。

若同时满足预期结果1)和2)，则判为符合；否则判为不符合。

4.1.1.7. 统计报表

测评依据：

产品应能够对事件记录进行统计，按照指定条件生成汇总报表。

文档要求：

厂商应提供文档，说明产品能够对哪些类型的事件记录进行统计，汇总报表

种类有哪些。

测评方法：

1） 选择不同条件对事件记录进行统计。

预期结果：

1） 步骤 1）统计结果正确；可按照指定条件生成汇总报表。

若满足预期结果1)，则判为符合；否则判为不符合。

4.1.1.8. 策略配置管理

测评依据：

产品应能够对大数据平台的策略进行集中管理，至少包括以下范围中的一种：

a）数据采集策略；

b）数据存储策略；

c）去隐私化策略；

d）漏洞扫描规则；

e）用户敏感信息行为处理规则。

文档要求：

厂商应提供文档，说明产品所支持的安全策略，并说明配置方法。

测评方法：

1） 尝试通过产品对受控大数据应用平台的安全策略进行配置，如去隐私化策略等；

2） 下发至大数据应用平台；

3） 验证策略是否生效。

预期结果：

1） 步骤 1）产品能够对受控大数据应用平台配置安全策略；

2） 步骤 2）能够通过产品下发安全策略；

3） 步骤 3）策略能够生效。

若同时满足预期结果 1)-3)，则判为符合；否则判为不符合。

4.1.1.9. 响应机制

测评依据：

系统能够对日志或报警信息提供一定的响应机制，比如email或声音报警等。

文档要求：

厂商应提供文档，说明产品对日志或报警信息提供的响应方式。

测评方法：

1） 针对某些安全事件（如用户敏感行为）或告警事件设置告警规则；

2） 触发所设置的告警规则；

3） 在产品检查是否接收到告警信息。

预期结果：

1） 步骤 3）能够接收告警信息，告警信息准确且内容完整。

若满足预期结果 1)，则判为符合；否则判为不符合。

4.1.1.10. 安全管理

测评依据：

产品应通过安全的方式对大数据平台进行管理，具体包括：

a) 实施管理前必须通过身份鉴别；

b) 对大数据平台进行远程管理时，应采取保密措施保障管理数据传输的安全。

文档要求：

厂商应提供文档，说明产品实施管理前鉴别的方法；说明对大数据平台进行远程管理时，采取何种措施保障管理数据传输的安全。

检验方法：

1） 登录产品，添加受控大数据应用平台；

2） 检查在添加过程中是否需要配置受控大数据应用平台的鉴别信息；

3） 输入错误鉴别信息后，尝试对受控大数据应用平台进行管理；

4） 输入正确鉴别信息后，尝试对受控大数据应用平台进行管理；

5） 截取产品对大数据平台进行管理时的会话数据（产品和大数据平台之间的）；截取会话内容至少包括：策略下发、信息收集等。

预期结果：

1） 步骤 2）产品添加大数据应用平台时，需要配置相应的鉴别信息；

2） 步骤 3）产品配置错误的鉴别信息时，不能管理大数据应用平台；

3) 步骤 4）配置正确的鉴别信息时，能够管理大数据应用平台；

4) 步骤 5）所截取的产品各组件间通信数据包应非明文。

若同时满足预期结果 1)-4)，则判为符合；否则判为不符合。

4.1.2. 自身安全功能

4.1.2.1. 标识与鉴别

4.1.2.1.1. 唯一性标识

测评依据：

产品应为管理员提供唯一标识，并能将标识与其所有可审计事件相关联。

文档要求：

厂商应提供文档，说明标识管理员的方式。

测评方法：

1) 创建一个管理员账号，如 admin；

2) 尝试创建重名账号；

3) 用新创建的管理员账号登录，进行各种操作；

4) 查看审计日志。

预期结果：

1) 步骤 2）不能创建重名账号；

2) 步骤 4）审计日志中包含该管理员的账户信息。

若同时满足预期结果 1)和 2)，则判为符合；否则判为不符合。

4.1.2.1.2. 基本鉴别

测评依据：

产品应在执行任何与安全功能相关的操作之前鉴别用户的身份。

文档要求：

厂商应提供文档，说明产品管理员登录鉴别的方式。

测评方法：

1) 以授权管理员身份尝试登录产品，检测是否必须进行身份鉴别，并且只有输入正确的用户名和口令才能登录待测产品；

2） 尝试以非授权用户身份登录产品。

预期结果：

1） 步骤 1）授权管理员需进行身份鉴别，并且只有输入正确的用户名和口令才能登录产品；

2） 步骤 2）非授权用户不能登录产品。

若同时满足预期结果 1)和 2)，则判为符合；否则判为不符合。

4.1.2.1.3. 鉴别数据保护

测评依据：

产品应保证鉴别数据不被未授权查阅或修改。

文档要求：

厂商应提供文档，说明鉴别数据存储的位置（如数据库名、表名等）。

测评方法：

1） 登录产品，创建一个新的账户；

2） 登录后台，查看新账号的鉴别信息（如口令）是否加密存储；

3） 尝试以非授权人员身份对鉴别数据进行篡改。

预期结果：

1） 步骤2）口令非明文存储；

2） 步骤3）若鉴别数据存储在数据库中，非授权人员无法登录数据库；若鉴别数据以文件形式存储，非授权人员无法修改文件中的内容。

若同时满足预期结果 1)和 2)，则判为符合；否则判为不符合。

4.1.2.1.4. 鉴别失败处理

测评依据：

当对用户鉴别失败的次数达到指定次数后，产品应能够终止用户的访问。

文档要求：

厂商应提供文档，说明产品防止对管理员口令进行暴力猜测的机制。

测评方法：

1） 登录产品，进行防止口令暴力猜测的相关配置，如配置鉴别失败次数阈值等；

2） 以正确的用户名及错误的鉴别信息多次尝试登录，达到预定义的阈值；

3）以正确的用户名及正确的鉴别信息尝试登录；检查产品是否提供锁定账号等措施来防止对管理员口令的暴力猜测。

预期结果：

1）步骤3）以正确的用户名及正确的鉴别信息无法登录。

若满足预期结果 1)，则判为符合；否则判为不符合。

4.1.2.2. 安全角色管理

测评依据：

产品应能够对管理员角色进行区分，能够根据不同的功能模块定义各种不同权限角色。

文档要求：

厂商应提供文档，说明产品所划分的管理员角色及相应的权限。

测评方法：

1） 登录产品建立不同角色的用户；

2） 分别以不同的角色的用户登录管理界面，尝试执行不同操作。

预期结果：

1） 步骤 1）产品至少具有两种角色的管理员身份；

2） 步骤 2）不同角色用户有不同的权限。

若同时满足预期结果 1)和 2)，则判为符合；否则判为不符合。

4.1.2.3. 数据传输安全

测评依据：

若产品组件间通过网络进行通讯，应采取保密措施保障组件间数据传输的安全。

文档要求：

厂商应提供文档，说明产品所有组件之间的管理数据传输的方式。

测评方法：

1） 模拟产品对大数据平台进行管理的过程，分别截取产品各组件间的通信数据。

预期结果：

1） 步骤 1）所截取的产品各组件间通信数据包应非明文。

若满足预期结果1)，则判为符合；否则判为不符合。

4.1.2.4. 审计功能

4.1.2.4.1. 审计日志生成

测评依据：

产品应对与自身安全相关的以下事件生成审计日志：

a) 管理员身份鉴别（包括成功和失败）；

b) 对安全策略进行更改；

c) 对大数据平台的增加/删除；

d) 对管理员进行增加、删除和属性修改；

e) 对事件记录、审计日志的管理操作。

每一条审计日志至少应包括事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式对产品进行管理，还应记录管理主机的地址。

文档要求：

厂商应提供文档，说明产品自身审计范围。

测评方法：

1) 使用正确的用户名和口令进行登录，审查审计记录；

2) 使用错误的用户名或口令分别尝试登录，审查审计记录；

3) 更改产品配置策略，审查审计记录；

4) 对大数据平台的增加、删除，审查审计记录；

5) 对管理员进行增加、删除和属性修改操作，审查审计记录；

6) 对事件记录、审计日志进行管理操作，审查审计记录。

预期结果：

1) 步骤 1）记录管理员登录成功的日志，日志内容正确；

2) 步骤 2）记录管理员登录失败（包括用户名错误或口令错误）的日志，日志内容正确；

3) 步骤 3）记录对安全策略的更改，日志内容正确；

4) 步骤 4）记录对大数据平台的增加/删除，日志内容正确；

5) 步骤 5）记录对事件记录、审计日志的管理操作，日志内容正确；

6) 审计日志内容至少包括事件发生的日期、时间、用户标识、管理主机地址、

事件描述和结果。

若同时满足预期结果1)-6)，则判为符合；否则判为不符合。

4.1.2.4.2. 审计数据管理

测评依据：

产品应提供以下审计数据管理功能：

a) 只允许授权管理员访问审计日志和事件记录；

b) 提供对审计日志的查询功能。

文档要求：

厂商应提供文档，说明产品管理员登录鉴别的方式。

测评方法：

1) 以授权管理员身份登录产品，尝试访问审计日志和事件记录；

2) 对审计日志进行查询；

3) 以普通管理员（无日志访问权限）身份登录产品，尝试访问审计日志和事件记录；

4) 以不存在的管理员账户登录，尝试访问审计日志和事件记录。

预期结果：

1) 步骤 1）授权管理员能够访问审计日志和事件记录；

2) 步骤 2）能够对审计日志进行查询；

3) 步骤 3）普通管理员无法访问审计日志和事件记录；

4) 步骤 4）不存在的管理员账户不能登录产品。

若同时满足预期结果 1)-4)，则判为符合；否则判为不符合。

4.1.2.4.3. 防止审计数据丢失

测评依据：

产品应提供以下措施防止事件记录和审计日志丢失：

a) 当事件记录和审计日志的存储容量达到阈值时，应能够发出报警信息；

b) 能够对事件记录和审计日志进行备份和恢复。

文档要求：

厂商应提供文档，说明产品所采用的防止审计数据丢失的措施，并说明采取的措施的验证方式，如通过后台将磁盘空间以文件写满等。

测评方法：

1) 登录产品，设置防止审计数据丢失的措施：如回滚，剩余或到达一定的空间进行报警等，自动备份、删除较早日志等；
2) 通过数据导入等方式使产品日志磁盘空间达到设置的阈值；
3) 对事件记录和审计日志进行备份；
4) 删除部分事件记录和审计日志；
5) 对事件记录和审计日志进行恢复。

预期结果：

1) 步骤 2）产品能够发出报警信息；
2) 步骤 3）能够备份事件记录和审计日志；
3) 步骤 5）能够恢复步骤 4）删除的数据。

若同时满足预期结果 1)-3)，则判为符合；否则判为不符合。

4.2. 发改办高技[2013]1965 号的要求

4.2.1. 支持 3 种以上大数据应用平台

测评依据：

产品至少要能够支持3种不同的大数据应用平台，能够对其进行远程管理，并且应提供扩展接口。

文档要求：

厂商应提供文档，说明产品所支持大数据应用平台，并说明其远程管理方式以及提供的扩展接口。

测评方法：

1) 对受控大数据应用平台进行配置，如配置网络 IP 地址、增加用于产品管理的管理员账号等；
2) 登录产品，添加受控大数据应用平台；
3) 尝试通过产品对大数据应用平台进行管理，包括配置策略，查看状态，收取日志等；
4) 查看文档是否对扩展接口进行描述；
5) 对不同的大数据应用平台，重复步骤 1）- 3)。

预期结果：

1) 步骤 1）-3）产品能够对大数据应用平台进行远程管理，包括配置策略，查看状态，收取日志等；
2) 步骤 4）文档对扩展接口进行了描述，并且内容完整、合理；
3) 步骤 5）产品至少支持三个不同的大数据应用平台（一种大数据系统支持三种不同领域的业务应用或者一种业务应用采用三种不同结构的大数据系统）进行远程管理。

若同时满足预期结果 1)-3)，则判为符合；否则判为不符合。

4.2.2. 漏洞扫描

测评依据：

应能够对3种及以上的大数据应用平台进行漏洞扫描。

文档要求：

提供文档说明安全管理产品进行漏洞扫描的方式及相关操作步骤。

测评方法：

1) 使用产品对大数据应用平台的底层支撑系统或大数据应用系统等不同的层面分别进行漏洞扫描；
2) 重复步骤 1）对不同的大数据应用平台进行漏洞扫描。

预期结果：

1) 步骤1）产品能够对大数据应用平台的某一个或者几个层面实现漏洞扫描，比如底层支撑系统或大数据应用系统等层面；能够直观地展现扫描结果，且扫描结果正确；
2) 步骤2）能够对至少3种不同的大数据应用平台进行漏洞扫描，比如：电信大数据、银行大数据、警务大数据、地质数据大数据等应用平台；能够直观地展现扫描结果，且扫描结果正确。

若同时满足预期结果1)和2)，则判为符合；否则判为不符合。

4.2.3. 配置基线检查

测评依据：

产品应对3种及以上的大数据应用平台进行配置基线检查。

文档要求：

提供文档说明产品的配置基线检查方法。

测评方法：

参见本测试方案中4.1.1.3检验项目的测评方法。

预期结果：

参见本测试方案中4.1.1.3检验项目的预期结果。

若满足 4.1.1.3 的预期结果，则判为符合；否则判为不符合。

4.2.4. 弱口令检测

测评依据：

应能够对 3 种及以上的大数据应用平台进行弱口令检测。

文档要求：

提供文档说明产品对大数据应用平台进行弱口令检测的方法。

测评方法：

1）配置大数据应用平台的操作系统、数据库、软件管理员的口令为弱口令，如纯数字、纯字母、口令与用户名重复等；

2）通过产品对大数据应用平台进行弱口令检测；

3）重复步骤1）-2）对不同大数据应用平台进行弱口令检测。

预期结果：

1）步骤2)能够检测大数据应用平台上的弱口令，并正确在产品界面中显示；

2）步骤3）支持对3种以上不同大数据应用平台的底层支撑系统或大数据应用系统进行弱口令检测；

3）产品内置弱口令字典库（包括常用数字组合、字母组合）。

若同时满足预期结果1)-3)，则判为符合；否则判为不符合。

4.2.5. 版本检测

测评依据：

产品应能够对3种及以上的大数据应用平台进行版本检测。

文档要求：

提供文档说明产品对大数据平台进行版本检测的范围和方法。

测评方法：

参见本测试方案中4.1.1.4检验项目的测评方法。

预期结果：

参见本测试方案中4.1.1.4检验项目的预期结果。

若满足4.1.1.4的预期结果，则判为符合；否则判为不符合。

4.2.6. 补丁管理

测评依据：

应能够对3种及以上的大数据应用平台进行补丁管理，包括收集大数据应用平台当前补丁安装情况，更新补丁库，对大数据应用平台有选择地进行分发、安

装。

文档要求：

提供文档说明产品对大数据应用平台进行补丁管理的方法。

测评方法：

1）连接互联网，从补丁厂商网站获取最新补丁；

2）通过产品收集大数据应用平台的操作系统、数据库的补丁安装情况；

3）选择一部分补丁，对大数据应用平台进行分发、安装。

预期结果：

1）步骤1）能够对产品的补丁库及时更新；

2）步骤2）能够获取目标大数据应用平台的当前补丁安装情况；

3）步骤3)能够选择补丁进行分发，目标大数据应用平台能够成功修补补丁。

若同时满足预期结果 1)-3)，则判为符合；否则判为不符合。

4.2.7. 去隐私化

测评依据：

应能够对3种及以上的大数据应用平台进行去隐私化处理。

文档要求：

提供文档说明产品实现对大数据的去隐私化操作的原理和方法。

测评方法：

若支持大数据导入过程的去隐私化处理：

1）设置去隐私策略，并下发至大数据应用平台；

2）模拟用户访问业务应用操作，操作内容涉及用户隐私（如用户银行账户、口令、身份证号码、手机号码等信息）触发策略；

3）在大数据应用平台的数据存储文件或者数据库中，检查含有隐私信息的内容是否已经被去除；

若支持分析查询结果的去隐私化处理：

4）导入数据或模拟用户访问业务应用操作，导入的数据或用户操作内容涉及用户隐私（如用户银行账户、口令、身份证号码、手机号码等）信息；

5）设置去隐私策略，并下发至大数据应用平台；

6）通过前端应用或大数据平台上查询步骤4）的相关记录。

预期结果：

1）步骤2）或4）可设置并能有效编辑隐私信息内容关键字或产品内置去隐私化策略；

2）步骤3）针对大数据采集过程的去隐私化，导入大数据应用平台的数据已经被去除了隐私信息；

3）步骤6）针对大数据查询结果的去隐私化，查询结果中含有的隐私信息已经被去除；

4）支持大数据导入过程的去隐私化处理或分析查询结果的去隐私化处理；可对3种以上的大数据应用平台实现去隐私化处理。

若同时满足预期结果 1)-4)，则判为符合；否则判为不符合。

4.2.8. 策略化数据抽取和集成

测评依据：

应能够对 3 种及以上的大数据应用平台进行策略化的数据抽取和集成。

文档要求：

提供文档说明，产品对数据进行抽取和集成的原理和方法。

测评方法：

1）提前准备具备一定特征关系的数据；

2）根据预置数据的特征关系，在安全产品上设置数据抽取和集成策略；

3）模拟数据抽取和集成的过程；检查大数据抽取和集成结果是否满足预置策略要求。

预期结果：

1）步骤2）能够设置大数据抽取和集成策略；

2）步骤3）数据抽取和集成结果满足预置策略要求。

若同时满足预期结果 1)和 2)，则判为符合；否则判为不符合。

4.2.9. 统一的策略管理

测评依据：

应能够对3种及以上的大数据应用平台进行集中策略管理，包括策略增加、修改和删除。

文档要求：

提供文档说明支持的统一策略类型及相关配置步骤。

测评方法：

1）在产品中新增一条策略，如数据去隐私化处理策略；

2）下发新增的策略至产品所支持的一种大数据应用平台；

3）模拟用户访问前端应用，验证新增策略是否生效；

4）对大数据应用平台的安全策略进行修改，如修改敏感信息行为处置策略，对某种敏感信息行为进行报警和阻断；

5）模拟敏感信息行为，验证修改的策略是否生效；

6）对大数据应用平台的安全策略进行删除，如删除数据抽取与集成策略；

7）验证删除的策略是否无效；

8）对不同的大数据应用平台，重复步骤1）-7）。

预期结果：

1）步骤2）大数据应用平台上新增一条数据去隐私化处理策略；
2）步骤3）能够进行数据去隐私化处理；
3）步骤4）大数据应用平台上的敏感信息行为处置策略被修改；
4）步骤5）能够对设置的敏感信息行为进行报警和阻断；
5）步骤6）大数据应用平台上的数据抽取与集成策略被删除；
6）步骤7）无法进行数据抽取与集成；
7）支持对3种以上的大数据应用平台进行统一策略管理，对于内置策略至少能够控制策略有效或无效。

若同时满足预期结果 1)-7)，则判为符合；否则判为不符合。

4.2.10. 统一事件分析

测评依据：

应能够对3种及以上的大数据应用平台进行集中事件收集、存储，并进行统计分析。

文档要求：

提供文档说明支持的统一事件分析的事件类型及相关配置步骤。

测评方法：

1）在受控大数据应用平台上进行相关配置，如配置产品为受控大数据应用平台的日志服务器等；
2）比较产品收集的日志是否与大数据应用平台一致；
3）进行统计；
4）对不同的大数据应用平台，重复步骤1）- 3）。

预期结果：

1）步骤2）产品收集的日志与大数据应用平台一致，事件内容完整，没有遗漏；
2）步骤3）能够生成统计分析报表；
3）支持对3种以上的大数据应用平台进行统一事件存储和分析。

若同时满足预期结果 1)-3)，则判为符合；否则判为不符合。

4.2.11. 全文检索及多维度大数据审计

测评依据：

应能够对3种及以上的大数据应用平台进行全文检索，能够从不同角度进行大数据审计。

文档要求：

提供文档说明全文检索及多维度大数据审计及相关配置步骤。

测评方法：

1）模拟用户访问业务应用，预置多组测试数据；设置安全产品，使其获得相关数据；

2）对全文进行组合条件检索，检索测试数据中的关键字；

3）输入不同检索条件，如设置每个关键词不同的权重、关键词间有不同的命中关系、关键词组之间 “与/或”关系，检索数据；

4）对不同的大数据应用平台，重复步骤1）-3）。

预期结果：

1）步骤2）能够检索出预置的测试数据，查询结果正确；

2）步骤3）能够检索出不同的预置数据，查询结果正确；

3）步骤4）支持对3种及以上的大数据应用平台进行数据查询。

若同时满足预期结果1)-3)，则判为符合；否则判为不符合。

4.2.12. 用户敏感信息行为处理

测评依据：

应能够对3种及以上的大数据应用平台进行用户敏感信息行为处理，发生敏感信息行为必须进行报警、阻断、跟踪和追溯。

文档要求：

提供文档说明产品能够对那些类型的用户访问敏感信息行为进行报警、阻断、跟踪和追溯。

测评方法：

1）配置用户访问敏感信息行为处置策略，对指定的行为进行报警、阻断和记录；

2）模拟用户访问敏感信息行为，触发策略；

3）检查是否能够对用户访问敏感信息行为进行报警、阻断和记录；

4）检查是否能够对用户访问敏感信息行为进行追溯，如关联查询。

预期结果：

1）步骤1）能够设置用户访问敏感信息行为处置策略；

2）步骤2）能够进行报警、阻断和记录；

3）步骤3）能够记录用户访问敏感信息行为，内容包括日期和时间、事件类型、事件描述、处理结果（报警、记录）等信息；

4）步骤4）能够对用户访问敏感信息行为进行追溯。

若同时满足预期结果 1)-4)，则判为符合；否则判为不符合。

4.2.13. 关键安全策略支持结构化与非结构化数据的管理

测评依据：

关键安全策略支持结构化与非结构化数据的管理。

文档要求：

分别针对结构化与非结构化数据，提供文档说明支持的统一策略类型及相关配置步骤。

测评方法：

1) 针对结构化数据，在产品中新增一条策略，如数据去隐私化处理策略；
2) 下发新增的策略至大数据应用平台；
3) 模拟用户访问前端应用，验证新增策略是否生效；
4) 通过产品对大数据应用平台的安全策略进行修改，如修改敏感信息行为处置策略，对某种敏感信息行为进行报警和阻断；
5) 模拟敏感信息行为，验证修改的策略是否生效；
6) 通过产品对大数据应用平台的安全策略进行删除，如删除数据抽取与集成策略；
7) 验证删除的策略是否无效；
8) 针对非结构化数据，重复步骤1）-7)。

预期结果：

1) 步骤2）大数据应用平台上新增一条数据去隐私化处理策略
2) 步骤3）能够进行数据去隐私化处理；
3) 步骤4）大数据应用平台上的敏感信息行为处置策略被修改；
4) 步骤5）能够对设置的敏感信息行为进行报警和阻断；
5) 步骤6）大数据应用平台上的数据抽取与集成策略被删除；
6) 步骤7）无法进行数据抽取与集成；
7) 步骤8）支持非结构化数据的关键策略管理。

若同时满足预期结果 1)-7)，则判为符合；否则判为不符合。

4.3. EAL3 级测评（以下内容仅供参考）

4.3.1. TOE 描述

本次被测产品为 XXX 公司的“XXX VX.X”，以下简称“XXX 大数据管理平台”。XXX VX.X 是一款 XXX，由专用硬件平台及运行于该平台上的软件组成。主要功能包括：XXXX、XXXX 等。XXX VX.X 提供了 x 个 CONSOLE 口，x 个百/千兆电口，可通过 xx 方式对产品进行管理。

本次评估对象（TOE）仅限于在《XXX VX.X 安全目标》中所定义的 TOE 安全功能（TSF），以及构成 TOE 安全功能的接口。其中所有在 TOE 安全功能范围之外

的 XXX、XXX、XXX 以及运行 XXX VX.X 的所有硬件均不属于本次评估范围。

TOE 软硬件配置信息如表所示：

表 4-1 TOE 软硬件配置信息

项目	描述
产品名称	
产品版本	
产品（系统）形态	软件（ ） 硬件（ ） 固件（ ）
生产集成厂商	
软件运行环境	
硬件配置信息	

4.3.2. 测评证据

表 4-2 测评证据

序号	证据
1.	XXX VX.X 安全目标
2.	XXX VX.X 功能规范
3.	XXX VX.X 高层设计
4.	XXX VX.X 对应性分析
5.	XXX VX.X 配置管理
6.	XXX VX.X 交付和运行
7.	XXX VX.X 开发安全
8.	XXX VX.X 管理员指南
9.	XXX VX.X 用户指南
10.	XXX VX.X 测试文档
11.	XXX VX.X 脆弱性分析
12.	用于测试的 TOE

4.3.3. 测评活动

GB/T 18336 EAL3 测评活动包括：

1) 安全目标评估；
2) 开发活动评估；
3) 交付和运行评估；
4) 配置管理评估；
5) 指导性文档评估；
6) 生命周期支持评估；
7) 测试评估；
8) 脆弱性评估。

4.3.4. 测评判据

表 4-3 测评判据

评估内容	预期结果
ASE 评估	满足 EAL3 相关要求
ADV_FSP.1	满足 EAL3 相关要求
ADV_HLD.2	满足 EAL3 相关要求
ADV_RCR.1	满足 EAL3 相关要求
ADO_DEL.1	满足 EAL3 相关要求
ADO_IGS.1	满足 EAL3 相关要求
ACM_CAP.3	满足 EAL3 相关要求
ACM_SCP.1	满足 EAL3 相关要求
AGD_ADM.1	满足 EAL3 相关要求
AGD_USR.1	满足 EAL3 相关要求
ALC_DVS.1	满足 EAL3 相关要求
ATE_COV.2	满足 EAL3 相关要求
ATE_DPT.1	满足 EAL3 相关要求
ATE_FUN.1	满足 EAL3 相关要求
ATE_IND.2	满足 EAL3 相关要求
AVA_MSU.1	满足 EAL3 相关要求
AVA_SOF.1	满足 EAL3 相关要求
AVA_VLA.1	满足 EAL3 相关要求

评估活动需满足上表要求，评估最终裁定结果为通过。

4.3.5. 测评内容

4.3.5.1. 安全目标评估

评估子活动包括：

- ST 引言的评估(ASE_INT.1)
- TOE 描述的评估(ASE_DES.1)
- 安全环境的评估(ASE_ENV.1)
- 安全目的的评估(ASE_OBJ.1)
- IT 安全要求的评估(ASE_REQ.1)
- 明确陈述的 IT 安全要求的评估(ASE_SRE.1)
- TOE 概要规范的评估(ASE_TSS.1)
- PP 声明的评估(ASE_PPC.1)

评估证据：

- 开发者应当提供安全目标文档

评估内容：

- ST 引言中应包含 ST 标识信息，该标识应可用于控制和标识 ST 的版本变化，以及与其对应的 TOE 的标识和描述性信息；
- ST 引言中应包含对 ST 概括性描述；
- ST 引言中应包含与 GB/T 18336 的一致性声明，该声明应陈述 TOE 与 GB/T 18336 的一致性，如有与 GB/T 18336 不一致的情况也须声明；
- TOE 描述部分应对概括陈述 TOE 的类型，并从物理和逻辑两方面概述 TOE 的范围和边界；
- TOE 安全环境部分应以 TOE 的预期使用环境为基础分析 TOE 所要保护的资产，标识并解释 TOE 或其环境所保护的资产可能面临的任何已知或假定的威胁；
- TOE 安全环境部分应列出以认为 TOE 是安全的为前提而做出的所有假设；
- TOE 安全环境部分应列出所有 TOE 及其环境必须遵守的组织安全策略，这些策略是由控制 TOE 使用环境的组织制定的；
- ST 的安全目的一节应包括 TOE 安全目的和环境安全目的两部分，并证明安全目的与假设、威胁、组织安全策略之间的对应关系；
- 确认文档描述了安全功能要求和安全保证要求，并对其内容进行了正确的个性化描述，以及组件之间的依赖关系是正确的；
- 确认文档是否存在自定义的安全组件，并判断其正确性；
- 确认文档描述了 TOE 的安全功能和保证措施，并证明其与安全要求之间的对应关系；
- 对于所有用到了概率和置换机制实现的安全功能，应在 ST 中声明其应达到的最低强度级别；
- 确认 ST 包含了与 PP 的符合性声明，未遵循 PP 的 ST 此项可不考虑；

- ST 的各部分的陈述应是一致的。

4.3.5.2. 开发活动评估

评估子活动包括：

- 功能规范评估(ADV_FSP.1)
- 高层设计评估(ADV_HLD.2)
- 表示对应性评估（ADV_RCR.1）

评估证据：

- 开发者应当提供功能规范文档
- 开发者应当提供高层设计文档
- 开发者应当提供对应性分析文档

评估内容：

- 功能规范应以非形式化的语言描述**所有的**安全功能及其外部接口，上下文之间不得有矛盾的地方；
- 功能规范应说明所有安全功能外部接口的用途与使用方法，必要时还要给出接口操作所可能产生的影响、例外情况和错误信息；
- 高层设计应以非形式化的语言，以子系统的形式描述 TOE 安全功能的结构，以及每个子系统所提供的安全功能，上下文之间不得有矛盾的地方；
- 高层设计需标识出执行 TOE 安全功能所需的所有基础性硬件、固件或软件，并列出由这些硬件、固件或软件实现的支持性保护机制所提供的功能；
- 高层设计应标识出 TOE 安全功能子系统的所有接口，并标识出哪些接口是外部可见的；
- 高层设计应将 TOE 分成与 TSP 相关的子系统和其他子系统来描述；
- 功能规范、高层设计与 ST 文档之间的描述需一致；
- 确认功能规范和高层设计是 TOE 安全功能要求的准确且完备的实例。

4.3.5.3. 交付和运行评估

评估子活动包括：

- 交付评估（ADO_DEL.1）
- 安装、生成和启动评估（ADO_IGS.1）

评估证据：

- 开发者应提供交付文档
- 开发者应提供 TOE 安装、生成和启动相关文档。

评估内容：

- 确认文档描述了将 TOE 交付给最终用户各个环节所采取的安全程序和安全措施；
- 确认文档描述了 TOE 安全安装、生成和启动的所有程序和步骤；
- 结合测试结果确认安装、生成和启动程序最终能够产生安全配置；
- 评估者需进行现场核查。

4.3.5.4. 配置管理评估

评估子活动包括：

- CM 能力评估（ACM_CAP.3）
- CM 范围评估（ACM_SCP.1）

评估证据：

- 开发者应提供用于测试的 TOE；
- 开发者应提供一个 TOE 的参照号；
- 开发者应使用一个配置管理系统；
- 开发者提供的 CM 文档应包括一个配置管理清单和一个配置管理计划。

评估内容：

- 配置管理文档应包括配置项清单和配置管理计划，配置项清单应列出所有组成 TOE 的配置项；
- 配置管理文档中应给出配置项的命名规则，保证配置项清单中标识的配置项的唯一性；
- 确认开发者提交的 TOE 标记了参照号；
- 确认开发者提供的 TOE 参照号，确认 TOE 版本是唯一的，可以被用户识别出。
- 配置管理计划应描述配置管理系统是如何运行的，配置管理系统中应包含所有的配置项，且系统的运行应与配置管理计划中的描述一致；
- 配置管理系统应提供措施使得只能对配置项进行授权改变。
- 评估者需进行现场核查。

4.3.5.5. 指导性文档评估

评估子活动包括：

- 管理员指南评估（AGD_ADM.1）
- 用户指南评估（AGD_USR.1）

评估证据：

- 开发者应提供管理员指南文档；
- 开发者应提供用户指南文档。

评估内容：

- 确认管理员指南文档描述了 TOE 管理员可使用的管理功能和接口；
- 确认管理员指南文档与提交的其他文档保持一致；
- 确认用户指南文档描述了非管理员用户可用的功能和接口；
- 确认用户指南文档描述了用户可访问的安全功能的用法；
- 确认用户指南文档与提交的其他文档保持一致。

4.3.5.6. 生命周期支持评估

评估子活动包括：

- 开发安全评估（ALC_DVS.1）

评估证据：

- 安全目标；
- 开发安全文档；
- 其他交付件，特别是配置管理文件；
- 开发者提供的保证开发安全的执行程序方面的证据。

评估内容：

- 开发安全文档应描述在 TOE 的开发环境中，为保证在 TOE 设计和实现的过程中的机密性和完整性所必需遵守的所有安全制度和规则，所有必需的安全措施；
- 采取的安全措施至少应包括物理上的、过程上的、人员上的和其他安全措施（例如：所有开发机上的逻辑保护）；
- 开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据；
- 评估者需进行现场核查。

4.3.5.7. 测试评估

评估子活动包括：

- 范围评估（ATE_COV.2）
- 深度评估（ATE_DPT.1）
- 功能测试（ATE_FUN.1）
- 独立性测试（ATE_IND.2）

评估证据：

- 开发者应提供用于测试的 TOE；
- 开发者应提供测试文档，包括：对安全功能的测试、测试范围分析、测试深度分析；
- 评估者进行的独立性测试的结果。

评估内容：

- 确认测试文档对安全功能进行了测试；
- 确认测试文档中的测试与功能规范中描述的 TSF 是完全对应的；
- 确认测试文档描述了测试目的、测试步骤、预期结果以及实际结果；
- 检查测试文档中的预期测试结果是否与给出的实际测试结果相一致；
- 确认高层设计中描述的子系统和接口在测试文档中都有相应的测试；
- 检查测试文档中的自测结果是否与独立性测试结果相一致；
- 评估者依据独立设计的测试用例及对开发者测试用例的抽样执行独立性测试，测试要求如表 2-7；（**具体可根据实际产品的安全功能增加或删减有关测试要求）：**

表 4-4 独立性测试要求

序号	安全功能要求	安全功能	备注
1.	对象管理	集中管理	
2.	运行状态监测		
3.	配置基线检查		
4.	版本监测		
5.	日志报警信息收集		
6.	事件记录查询		
7.	统计报表		
8.	策略配置管理		
9.	响应机制		
10.	安全管理		
11.	唯一性标识	标识与鉴别	
12.	基本鉴别		
13.	鉴别数据保护		
14.	鉴别失败处理		

序号	安全功能要求	安全功能	备注
15.	安全角色管理		
16.	数据传输安全		
17.	审计日志生成	审计功能	
18.	审计数据管理		
19.	防止审计数据丢失		
20.	漏洞扫描		
21.	基线检查		
22.	弱口令检测		
23.	版本检测		
24.	补丁管理		
25.	去隐私化		
26.	策略化数据抽取和集成		
27.	统一的策略管理		
28.	统一事件分析		
29.	全文检索及多维度大数据审计		
30.	用户敏感信息行为处理		
31.	关键安全策略支持结构化与非结构化数据的管理		

4.3.5.8. 脆弱性评估

评估子活动包括：

- 误用评估（AVA_MSU.1）
- TOE 安全功能强度评估（AVA_SOF.1）
- 脆弱性分析（AVA_VLA.1）

评估证据：

- 开发者应提供脆弱性文档；
- 开发者应提供指导性文档；
- 评估者进行的穿透性测试的结果。

评估内容：

- 确认文档对 TOE 相关安全机制的安全功能强度进行了分析；
- 确认文档对 TOE 的脆弱性进行了分析：明显脆弱性有有效的处置方

法；说明已标识的脆弱性不能在 TOE 的预期使用环境中被利用，同时通过穿透性测试来进行验证；

- 确认指导性文档描述完备：
  1. 标识了 TOE 所有可能的运行模式（包括失败或操作失败后的运行）及运行后果；
  2. 描述对预期使用环境的所有假设；
  3. 列出对外部安全措施，包括外部程序的、物理的或人员的控制的所有要求。
- 确认依据指导性文档能够安全配置和使用 TOE；
- 确认指导性文档没有误导用户的内容，使用指导性文档能将不安全状态检测出来；
- 评估者执行穿透性测试，包括口令暴力破解、管理平台安全性测试、未声明端口安全性测试、越权操作、规则有效性、IP 碎片攻击、ARP 脆弱性、源路由攻击及异常协议攻击测试等共 X 个测试项（**具体可根据实际产品的安全功能增加或删减有关测试项**）：

表 4-5 脆弱性测试列表

序号	测试项	备注
1.	口令暴力破解	
2.	管理平台安全性测试	
3.	管理平台未声明端口安全性测试	
4.	越权操作	
5.	鉴别信息防重放	
6.	超时机制	
7.	规则有效性	
8.	鉴别数据保护	
9.	数据存储保护	

4.3.5.9. 独立性测试

测试目的：

TOE 安全功能执行的正确性。

预期结果：

1. 开发者应提供一个与开发者的安全功能测试中使用的资源相当的合集；
2. 评估者参考开发者提供的测试文档形成抽样子集；如下表：

表 4-6 独立性测试抽样子集

序号	安全功能	测试用例	备注
1.	对象管理		
2.	运行状态监测		
3.	配置基线检查		
4.	版本监测		
5.	日志报警信息收集		
6.	事件记录查询		
7.	统计报表		
8.	策略配置管理		
9.	响应机制		
10.	安全管理		
11.	唯一性标识		
12.	基本鉴别		
13.	鉴别数据保护		
14.	鉴别失败处理		
15.	安全角色管理		
16.	数据传输安全		
17.	审计日志生成		
18.	审计数据管理		
19.	防止审计数据丢失		
20.	漏洞扫描		
21.	基线检查		
22.	弱口令检测		
23.	版本检测		
24.	补丁管理		
25.	去隐私化		
26.	策略化数据抽取和集成		
27.	统一的策略管理		

序号	安全功能	测试用例	备注
28.	统一事件分析		
29.	全文检索及多维度大数据审计		
30.	用户敏感信息行为处理		
31.	关键安全策略支持结构化与非结构化数据的管理		

4.3.5.10. 穿透性测试

表 4-7 穿透性测试用例

序号	测试项	测试用例	备注
1.	口令暴力破解	口令暴力破解	
2.	管理平台安全性测试	管理平台 telnet 协议安全性测试 管理平台 ssh 协议安全性测试 管理平台 https 协议安全性测试 Web 管理控制台 SQL 注入攻击 Web 管理控制台跨站（XSS）脚本攻击 Web 管理控制台目录遍历攻击 Web 管理控制台其他漏洞检测	有则适用
3.	管理平台未声明端口安全性测试	未声明端口安全性测试	有则适用
4.	越权操作	用户操作权限测试 未授权用户非法访问测试	
5.	鉴别信息防重放	鉴别信息防重放	
6.	超时机制	超时机制	
7.	规则有效性	规则有效性	
8.	鉴别数据保护	鉴别数据保护	
9.	数据存储保护	数据存储保护	

4.3.5.10.1. 口令暴力破解

测试目的：检测 TOE 抵御口令暴力猜测的能力。

结果判定 TOE 能够采取安全措施来防止口令暴力破解攻击。

4.3.5.10.2. 管理平台 telnet 协议安全性测试（有则适用）

测试目的：通过发送 telnet 协议畸形报文验证 TOE 的管理系统能否抵御畸形报文攻击。telnet 管理服务是否存在其他安全漏洞。

结果判定 TOE 的管理系统能够抵御 telnet 协议畸形报文攻击。不存在明显可被利用的其他类型漏洞。

4.3.5.10.3. 管理平台 ssh 协议安全性测试（有则适用）

测试目的：通过发送 ssh 协议畸形报文验证 TOE 的管理系统能否抵御畸形报文攻击。SSH 管理服务是否存在其他安全漏洞。

结果判定 TOE 的管理系统能够抵御 ssh 协议畸形报文攻击。不存在明显可被利用的其他类型漏洞。

4.3.5.10.4. 管理平台 https 协议安全性测试（有则适用）

测试目的：通过发送 https 协议畸形报文验证 TOE 的管理系统能否抵畸形报文御攻击。

结果判定 TOE 的管理系统能够抵御 https 协议畸形报文攻击。

4.3.5.10.5. Web 管理控制台 SQL 注入攻击（有则适用）

测试目的：检查送测 TOE 的 Web 管理控制台是否存在 SQL 注入漏洞，分析其对 TOE 安全性的影响。

结果判定送测 TOE 的 Web 管理控制台应能够阻止 SQL 注入攻击。

4.3.5.10.6. Web 管理控制台跨站（XSS）脚本攻击（有则适用）

测试目的：检查送测 TOE 的 Web 管理控制台是否能够抵御跨站（XSS）脚本攻击，分析其对 TOE 安全性的影响。

结果判定送测 TOE 的 Web 管理控制台应能够阻止跨站脚本攻击。

4.3.5.10.7. Web 管理控制台目录遍历攻击（有则适用）

测试目的：检查送测 TOE 的 Web 管理控制台是否存目录遍历漏洞，分析其对 TOE 安全性的影响。

结果判定 Web 管理控制台应能够阻止目录遍历攻击。

4.3.5.10.8. Web 管理控制台其他漏洞检测（有则适用）

测试目的：检查送测 TOE 的 Web 管理控制台是否存源代码信息泄露、代码上传等漏洞，分析其对 TOE 安全性的影响。

结果判定 Web 管理控制台应不存在明显可被利用的其他类型漏洞。

4.3.5.10.9. 管理平台未声明端口安全性测试（有则适用）

测试目的：验证 TOE 管理平台是否开放了未声明端口及服务

结果判定 TOE 未开放未声明端口及服务，能够抵御对其保护后台管理系统的

扫描。

4.3.5.10.10. 用户操作权限限制测试

测试目的：验证 TOE 的访问控制机制，分析访问控制的安全性。检测 TOE 对合法用户操作权限是否进行了合理控制。

结果判定 TOE 对用户操作权限进行了合理控制。

4.3.5.10.11. 未授权用户非法访问测试

测试目的：检测 TOE 是否能够抵抗用户权限的旁路攻击，防止未登录用户非法访问。

结果判定 TOE 能够抵抗用户权限的旁路攻击，防止未登录用户非法访问。

4.3.5.10.12. 鉴别信息防重放

测试目的：检测 TOE 是否能够抵抗鉴别信息重放攻击。

结果判定 TOE 能够抵抗鉴别信息重放攻击。

4.3.5.10.13. 超时机制

测试目的：检测 TOE 是否进行超时检查和处理。

结果判定 TOE 能够进行超时检查和处理。

4.3.5.10.14. 规则有效性

测试目的：检查 TOE 所设定的安全规则是否能够准确的生效。

结果判定 TOE 安全规则不能被旁路。

4.3.5.10.15. 鉴别数据保护

测试目的：检查 TOE 能否提供对鉴别数据的安全保护措施。

结果判定 TOE 能够防止非授权人员对鉴别数据的破坏。

4.3.5.10.16. 数据存储保护

测试目的：检查 TOE 能否提供对存储数据的安全保护措施。

结果判定 TOE 能够防止非授权人员对存储数据的破坏。

4.3.5.10.17. 数据传输保护

测试目的：检查 TOE 能否提供对传输数据的安全保护措施。

结果判定 TOE 能够防止非授权人员对传输数据的破坏。

4.4. 自主知识产权评估

4.4.1. 企业自主原创环境

4.4.1.1. 企业资质考察

测评依据：

企业应为国内独资企业或国内控股合资企业，应具有规范的质量管理体系，同时，企业应具有足够的资金和员工激励机制保证进行原创代码开发的可持续性。

文档要求：

提供企业法人营业执照、政府或行业协会颁发的企业能力资质证书、企业软硬件研发能力证明文件、企业研发投入和员工激励机制证明文件。

测评方法：

1) 对企业法人营业执照进行审核，核查企业的法人身份、企业类型、经营范围等内容；
2) 对企业提交的相关资质证书、研发投入等文件进行考查，核查企业的运行管理状况、软硬件开发方面的资金投入和研发能力。

预期结果：

企业为国内独资企业或国内控股合资企业，具有规范的质量管理体系，同时，企业具有足够的资金和员工激励机制保证进行原创代码开发的可持续性。

4.4.1.2. 企业管理状况考察

测评依据：

企业应有明确的发展战略和规划，应具备完善的管理制度文件，企业科技人员队伍应相对稳定，其结构和规模应满足企业发展和产品生产的需求，科研部门主管、高层技术人员应具备足够的经验和资历，企业应具备足够的保密措施。

文档要求：

提供企业战略和规划文件、企业管理制度文件、企业人事档案文件、员工保密协议。

测评方法：

1) 与企业各级人员交流，考察企业发展战略及规划在企业内部传达和落实情况；
2) 考察企业的内部职能部门设置、奖惩制度、知识产权保护制度和运营制度，核查企业的自主创新效力；
3) 通过人员访谈和人事档案调阅，考察企业科技人员队伍的结构和规模，科

研管理部门和高层技术人员的经验和资历，科研人员的流动情况、保密制度和保密措施的落实情况。

预期结果：

企业有明确的发展战略和规划，具备完善的管理制度文件，企业科技人员队伍相对稳定，其结构和规模应满足企业发展和产品生产的需求，科研部门主管、高层技术人员具备足够的经验和资历，企业具备足够的保密措施。

4.4.1.3. 产品研发环境和过程

测评依据：

企业应提供产品设计文档、研发流程文档和生产流程文档。产品设计文档应明确说明产品的设计初衷、设计思路等。产品研发流程文档应提供产品的详细说明，产品的结构，以及各个模块的任务分配情况。产品的生产流程文档应与产品的生产一致。

文档要求：

提供产品设计、研发流程和生产流程文档。

测评方法：

1) 与企业产品设计人员交流，查看产品设计文档，考察产品设计思路，确认产品原创的设计依据；
2) 与企业产品研发人员交流，查看产品设计和研发流程文档，确认配置管理系统的使用情况，研发人员与任务分配的一致性情况以及研发代码和文档版本与记录的一致性情况；
3) 与企业生产人员交流，查看产品生产流程文档，确认产品生产的地址、生产的流程和生产的规模与生产流程文档的一致性。

预期结果：

企业提供产品设计文档、研发流程文档和生产流程文档。产品设计文档明确说明产品的设计初衷、设计思路等。产品研发流程文档提供产品的详细说明，产品的结构，以及各个模块的任务分配情况。产品的生产流程文档与产品的生产一致。

4.4.2. 产品关键技术代码开源性分析

测评依据：

将厂家的产品代码同业界已有的产品代码进行比较，检测厂家产品的自主原创情况。

文档要求：

提供对产品源代码的自主知识产权申明，加盖单位公章。

测评方法：

1) 要求厂家以源代码的形式提供产品代码，并提供证明产品代码已经通过代码格式审查工具的检查，格式符合代码相似度检查的要求；
2) 要求厂家在独立干净的机器上进行源代码的编译和生成，并能够对应到已经部署的软硬件设备上的实际执行代码；
3) 使用工具对产品的源代码（关键核心模块）进行对比分析测试，得到相似程度；
4) 相似分析结果。

预期结果：

被测产品关键核心模块源代码与基准数据的相似分析结果符合自主原创测评指南的要求。

企业的关键功能代码的开源代码比例不高于 30%，所使用的开源代码中不应包含 GPL(GNU 通用公共许可证)等强制要求开源的代码类型。

4.5. 性能测试

测评依据：

支持 1000 万以上并发业务访问。

文档要求：

厂家应提供在大并发业务访问背景下可能影响到产品的各主要参数、性能指标相关的技术资料，含有大并发业务访问性能测试相关的自测试计划/方案/报告。

测评方法：

1) 部署完成大数据平台：在大数据服务平台区域中部署3种大数据平台中的一种，建议采用具有B/S架构应用业务接口的大数据应用（部署时考虑到大并发访问的压力，根据不同架构的大数据平台系统，优先保证与大并发访问密切相关的服务器数量）；
2) 部署完成大数据平台产品：根据用户文档，配置部署被测产品对大数据平台的监控配置。打开所有监控功能；
3) 部署完成后，使用客户端对大数据平台进行业务访问，检测被测大数据平台产品的状态，验证功能状态正常后，开始进行性能测试；
4) 使用测试工具模拟生成1000万并发访问的数据量。检测被测大数据平台产品中相关信息的获取情况以及产品状态。

预期结果：

1) 通过步骤3)被测产品能够正确获取由于客户端访问而造成的大数据平台状态的变化，所有被测功能运行正常；

2) 通过步骤4）被测产品未发现失去响应、程序崩溃等非正常情况，且能够正确获取相关信息。

若同时满足预期结果1)和2)，则判为符合；否则判为不符合。

4.6. 支持 IPv4/IPv6 环境

4.6.1. 支持 IPv4/IPv6 网络环境下的产品自身管理

测评依据：

产品组件（如果有多个组件，包括远程管理终端）间的通讯应支持 IPv6 及过渡环境。

文档要求：

提供文档说明产品所包含的组件，以及各组件之间的通讯协议，对 IPv6 的支持情况。

测评方法：

1) 部署模拟IPv4/6双栈环境；

2) 配置产品各个组件地址（IPv4地址或IPv6地址）；

3) 检查产品个组件（包括远程管理）是否能够在各环境下组件间通信正常。

预期结果：

1) 步骤3）产品组件间的通讯正常。

若满足预期结果 1)，则判为符合；否则判为不符合。

4.6.2. 支持 IPv4/IPv6 网络环境下的对大数据应用平台进行管理（有则适用）

测评依据：

对大数据应用平台进行管理时，支持 IPv6 及过渡环境。

文档要求：

提供文档说明产品对 IPv6 的支持情况，配置步骤。

测评方法：

1) 部署模拟大数据应用平台的IPv4/6双栈环境；

2) 检查产品是否能够在各环境下对大数据应用平台正常管理，包括漏洞扫描、补丁管理、策略管理等4.2中规定的项目。

预期结果：

1) 步骤2）在IPv4/6双栈环境下对大数据应用平台正常管理。

若满足预期结果 1)，则判为符合；否则判为不符合。