安华金和产品 FAQ

目录

一. 数据库漏洞扫描（DBScan）

1.1 在 Oracle 数据库上使用漏扫，需要提供哪些参数？

需要提供 Oracle 的 IP 地址、数据库实例名、账户名、密码，账户要有较高权限，比如：sysdba 权限，如果默认端口号没变的话不用提供，默认为 1521，改变的话提供具体端口号；

1.2 在 mysql 数据库上使用漏扫，需要提供哪些参数？

需要提供 mysql 的 IP 地址、用户名、密码，账户要有较高权限，比如：root 账户，如果默认端口号没变的话不用提供，默认为 3306，改变的话提供具体端口号；

1.3 在 DB2 数据库上使用漏扫，需要提供哪些参数？

需要提供 db2 的 IP 地址、数据库名、用户名、密码，账户要有较高权限，比如：db2admin 账户，如果默认端口号没变的话不用提供，默认为 50000，改变的话提供具体端口号；

注意：如不修改，当 dbscan 和 mysql 不是安装在同一个主机上时，进行授权扫描连接时，会出现连接失败的情况。

1.4 扫描账户的用户权限问题？

6 种类型数据库，推荐使用管理员权限的账户进行扫描完全满足要求，比如：Oracle 使用有 sysdba 权限的账户，mysql 使用 root 账户，如果账户权限过低是无法访问某些数据的，建议用户使用我们的只读帐户脚本。

1.5 危险代码是检查什么内容?

用户的数据库包含的存储过程、触发器、函数，可能包含有提权、访问网络、利用数据库漏洞导致服务宕机的 sql 语句，我们认为是危险代码，如果客户不需要检查这类安全问题，可以将危险代码的检测从策略中去掉。

1.6 进行一次授权扫描，时间大致有多长

危险代码、敏感数据发现等部分检测项与用户数据库大小有关，Oracle 检测项最多，目前是两千多项，一般情况下检测时间是十几分钟，在特殊的大型应用环境下时间可能更长，如电信业务系统，可能会在一个小时左右；对于弱口令扫描，建议谨慎使用密码遍历的策略，使用不建议超过 4 位密码遍历探测；建议使用弱口令字典库结合其他典型弱口令探测策略。

1.7 如何保证扫描结果数据的保密性

按国保局要求，漏扫使用三权分立的方式管理登录用户，管理员登录账户的口令不低于 10 位，3 次登录不成功锁定 10 分钟，登陆后 15 分钟（这个时间可设定）不操作软件自动锁定，漏扫不保存用户的登陆账户和密码，扫描出的弱口令用掩码的形式显示。

1.8 漏洞的风险级别是如何确定的

数据库漏洞在国际漏洞库上有 CVE 或 CNNVD 编号的，一般也能在 NVD 网站上查到，国际漏洞网站会对带编号的漏洞项有风险级别打分，同时标明风险级别是高、中、低。如果没有编号的漏洞项，是根据这个漏洞项的危害程度由安华金和数据库攻防实验室进行风险定级。

1.9 漏扫是否访问数据库中的用户数据

DBScan 以数据库安全检测为目标，进行数据库漏洞扫描。主要原理是通过后台一系列的数据库 SQL 语句对系统表、参数、存储过程、函数等内容进行读取操作，从而判定是否存在漏洞。检测不会修改已有对象，不会访问数据库表中的具体数据，总体对系统正常运行的影响风险度很低。

1.10 普通检测方式下对用户数据库的潜在风险

在进行授权和弱口令检测时，扫描过程中对数据库资源有一定开销。

风险：在普通授权方式、弱口令检测方式下，DBScan 检测一台数据库服务器的时间会在 2~3 分钟，期间会占用一定的 CPU、内存开销。

对数据库服务器，CPU 一般会消耗半个 Core,内存会占用 200 多 M。对资源不充足的数据库服务器而言，其业务处理性能会有一定影响。

建议：用户在系统非工作时间，或工作时间的非高峰时段对数据库进行安全检测，规避潜在的性能影响。

1.11 支持哪些数据库类型的扫描

七种国际主流数据库+三种国产数据库：oracle、sql server、mysql、db2、sybase、informix、postgreSQL；DM、kingbase、Gbase

二. 数据库监控与审计（DBAudit）

2.1 DBAudit 该如何选型

答：DBAudit 的选型指标有两个：

SQL 吞吐量：单位是“条 SQL/秒”，即各个型号在一秒内能够审计的最多的 SQL 语句数，DBA-B1000 峰值是 10000 条 SQL/秒；DBA-B5000 是 20000 条 SQL/秒。用户真实环境中的 SQL 吞吐量小于某一型号的标称 SQL 吞吐量，则该用户环境下选用该型号即可。

相对而言，SQL 吞吐量是比较合理、比较科学的选型指标，但在实际的用户环境中，一般情况下用户也不清楚 SQL 吞吐量到底有多大。这时，建议参考第二个选型指标。

数据库实例数：即各个型号推荐审计的数据库实例数，DBA-B1000 推荐不超过 3 个，DBA-B5000 推荐不超过 5 个。

当用户真实环境中的实例数大于 5 时，建议引导用户采购多台设备。

2.2 DBAudit 采用哪种部署模式

DBAudit 安全实例与数据库关联时选择旁路监听的部署模式，采用 IDS 模式。

旁路部署模式下 DBAudit 设备不直接接入网络，而是通过 TAP、SPAN 等技术将网络流量映射到防火墙设备；通过旁路部署模式既不改变网络拓扑，也不在应用链路上增加新的设备点。

2.3 DBAudit 是否会对数据库访问效率产生影响

DBAudit 采用旁路的部署模式，通过镜像端口镜像的数据库访问流量，获得数据库访问协议格式的 SQL 语句、操作用户和返回的流量包等分析线索，所以不会对数据库运行产生影响，也会影响到数据库的访问效率。

端口镜像旁路模式的部署点可以在各个部门出口交换机上，也可以部署在数据库前端交换机上。

2.4 DBAudit 告警处理机制有哪些方式

DBAudit 在处理数据库风险行为告警时，关键在于从合法的 SQL 语句中，有效识别出风险访问行为，DBAudit 提供了丰富的风险行为定义方法和特征库：非法客户端定义、危险访问行为定义、SQL 注入描述、漏洞攻击库、SQL 黑名单。

提供短信、邮件、SNMP、sysLog 等多种告警方式。

2.5 DBAudit 针对审计日志生成报告能力如何

DBAudit 依据数据库访问特点，提供专业化的菜单导航、操作界面和报表。按照数据库用户和会话、应用用户和会话、数据库对象、SQL 语句类别等多种角度对数据库审计记录进行组织和导航；提供会话行为报表、SQL 行为报表、风险分析报表；提供数据库运行状态监控仪表盘，以及灵活可配的“焦点分析”报告，为不同用户和角色提供可定制的持续化报表生成和发送。

2.6 DBAudit 执行数据库审计的粒度和范围

DBAudit 通过数据库的全面审计功能，实现对所有数据库操作语句与操作者、操作时间、操作对象、操作结果的有效关联；提供各种便捷的数据库操作的事后分析途径，使数据库操作行为完备记录与追查，在发现安全事件后提供最为可靠的依据。

TraceLog 审计的内容：SQL 语句、SQL 语句参数、执行结果（成功、失败和详细的失败原因）、被影响的记录、详细的查询结果集、事务状态、会话登录和登出信息等。

审计的范围：对象、操作（上百种操作可选）、SQL 分类类型（基于对 SQL 的分类结果进行筛选）、用户、指定的客户端（IP、MAC）、客户端工具或应用系统等。

2.7 DBAudit 提供了哪些高效的入库策略

DBAudit 通过 SQL 语句规约分类技术实现高效 SQL 解析，通过分级存储和批量入库技术实现审计数据的高效入库。

2.8 DBAudit 如何实现海量数据的存储

DBAudit 采用 SQL 归一化处理和文件压缩存储两个技术实现海量数据的存储。

系统能够存储数据量大小，因硬盘大小而不同，例如 500G 的硬盘，可以存储的数据量能够达到 20 亿。

2.9 DBAudit 是否能监控数据库的运行状态

DBAudit 实时显示数据库的运行状况、数据库访问流量、并发吞吐量、SQL 语句的响应速度，提供当前最为实时的数据库运行状况图表，保障数据库运行的可靠性。

2.10 DBAudit 的产品资质都有哪些？什么时候可以申请齐全

截止到 2015 年 6 月，DBAudit 已经申请到的产品资质有公安部销售许可证（行标二级）、软件著作权和保密局涉密资质。

2.11 DBAudit 是否支持万兆和光纤的型号

答：DBA-E30000 以上支持光纤口，也支持万兆的型号，目前支持 1 个 100/1000M Base-Tx 管理口，4 个 100/1000M Base-Tx 监控口，2 个光纤。

板载 6 电口，扩展槽位上可选配 2 个万兆接口。

三. 数据库保险箱（DBCoffer）

3.1 DBCoffer 支持哪些加密算法

DBCoffer 系统支持的加密算法包括：AES128，AES256，XXX（国密办批准），3DES。

3.2 支持哪些 ORACLE 数据类型的加密

DBCoffer 支持 CHAR、VARCHAR、VARCHAR2、DATE、NUMBER、INTEGER、CLOB、BLOB 类型的加密。

3.3 应用 DBCoffer 对表加密后，对应用系统有哪些影响

应用 DBCoffer 后，由于 CHAR 和 VARCHAR2 类型的密文列长度受到了影响，造成应用系统如果依赖于该密文列的元数据的长度定义来进行编码时，DBCoffer 提供了内置函数用于获取元数据长度，用户可调用该函数获取原长度，该影响只会影响到字符类型的字段，对 NUMBER、DATE 类型的字段没有影响。

3.4 在应用 DBCoffer 进行加密时，是否需要停止 ORACLE 服务

DBCoffer 支持在线和离线两种设置加密列的方式。

在线方式可以不停止 Oracle 服务，不停止应用系统由于在线方式处理速度大概是离线方式的三至五倍，所以推荐用户采取离线方式进行数据初次加密，可利用系统维护、割接、升级等契机，进行数据初次加密。

离线方式需要保证在对表加密时，没有应用对表进行 DML 操作，并且该表上也没有未完成的事务。

3.5 使用 DBCoffer 加密后会引起数据精度的损失吗

DBCoffer 加密后，CHAR 和 VARCHAR2 类型、数值和日期类型不会引起精度损失。

3.6 加密前数据长度的限制有何影响

对于缺省盐来说，支持的字符串最大长度为 4000-16，对于随机盐来说，还要再减去盐的长度，一般来说对于某算法，盐的长度就是该对称算法单块分组长度。

3.7 DBCoffer 支持的最大加密列个数是多少

DBCoffer 理论上对加密列个数没有附加的限制；从性能和资源方面，每个密文字段将占用部分内存和 CPU 的资源。

建议一个 Oracle 实例配置的加密列个数不要超过 128 个。

3.8 DBCoffer 支持的最大数据库连接数

理论上对应用系统与 Oracle 数据库的连接没有附加的限制；从性能和资源方面，每个操作密文数据的数据库连接将占用部分内存和 CPU 的资源。

建议一个 Oracle 实例的最大连接数不要超过 1024 个。

3.9 在应用 DBCoffer 后，对 ORACLE 的并发管理和事务、锁机制有影响吗

DBCoffer 完全遵循 ORACLE 的并发 MVCC 和事务管理机制，对 Oracle 原有的特性没有任何影响，是完全透明的。

3.10 在应用 DBCoffer 后，对 ORACLE 查询计划有影响吗

DBCoffer 对应用是透明的，不影响用户的使用感受。如果应用访问使用了使用 DBCoffer 密文索引的列，Oracle 会通过该密文索引来检索数据。

3.11 如果密钥丢失，如何恢复？有什么机制能够保证密钥的安全

DBCoffer 提供了实施加密所必需的关键管理基础架构。加密的工作原理是将明文数据以及密钥传递到加密程序中。加密程序使用提供的密钥对明文数据进行加密，然后返回加密数据。

密钥是加、解密数据的关键，应该按时、及时的备份。如果密钥由于意外情况丢失，可以通过备份来还原。

四. 数据库防火墙（DBFirewall）

4.1 DBF 支持哪些部署方式

目前支持两种串联模式：

透明网桥模式：在网络上物理串联接入 DBFirewall 设备，所有用户访问的网络流量都串联流经设备；通过透明网桥技术，客户端看到的数据库地址不变。

代理接入模式：网络上并联接入 DBFirewall 设备，客户端逻辑连接防火墙设备地址，防火墙设备转发流量到数据库服务器；通过代理接入模式，网络拓扑结构不变。

一种旁路部署模式：DBFirewall 设备不直接接入网络，而是通过 TAP、SPAN 等技术将网络流量映射到防火墙设备；通过旁路部署模式既不改变网络拓扑，也不在应用链路上增加新的设备点。

4.2 DBF 的部署是否会影响 Oracle 数据库的备份功能？异地备份呢？高级的备份功能呢

串联的情况下是和策略配置情况有关，需要制定相应合适的策略保证串联情况下的异地备份不受影响，但是如果是基于 ogg 的事务日志文件做的备份就没有任何影响。

4.3 DBF 如何防范数据库漏洞攻击的

DBF 虚拟补丁功能通过在数据库外的网络层创建了一个安全层，用户在无需给数据库打补丁的情况下，根据数据库漏洞攻击特征进行有效拦截，实现数据库漏洞防护，DBF 支持 22 类，460 个以上虚拟补丁。

4.4 DBF 如何防范 SQL 注入的

DBF 在 SQL 语法解析的基础上，通过对 SQL 语句进行注入特征描述，采用启发式发现 SQL 注入，完成对 SQL 注入行为的检测和阻断，系统提供缺省 SQL 注入特征库。

DBF 除了通过敏感信息对 SQL 注入进行防范外，还对通过数据库返回错误信息进行 SQL 注入探测的方法进行了防御。DBFirewall 采用对常见错误返回 NODATA 的方式，达到了避免通过数据库产生的错误信息进行 SQL 注入的行为，这个方面来说，DBFirewall 做到了从数据库请求与数据库应答两个方向防止 SQL 注入行为的发生。

4.5 DBF 如何防范批量数据导出行为的

DBF 能够针对不同的数据库用户，对于数据库中表的权限提供具体的操作权限，访问行数和影响行数阀值的控制功能，以及是否允许不带 WHERE 查询，从而达到避免大规模数据泄露和篡改的情况。

4.6 DBF 如何防范运维侧高危操作的

系统维护人员、外包人员、开发人员等，拥有直接访问数据库的权限，有意无意的高危操作对数据造成破坏。DBF 通过限定更新和删除影响行、限定无 Where 的更新和删除操作、限定 drop、truncate 等高危操作避免大规模损失。

4.7 DBF 如何防止对合法应用程序语句误报的

DBF 通过语法抽象描述不同类型的 SQL 语句，规避参数带来的多样化，通过应用学习捕获所有合法 SQL 的语法抽象，建立应用 SQL 白名单库，构建应用程序的行为模型，对合法应用行为放行，将误报率降低为“零”。

4.8 DBF 如何应对不同应用场景快速部署实施

DBF 提供应用场景、维护场景、混合场景多种策略模版帮助用户快速建立安全策略。提供学习期、学习完善期、保护期三种运行周期，以帮助用户在防火墙建设的不同阶段平滑过渡。

4.9 DBF 实时控制支持的控制与审计动作有哪些

DBF 对白名单只允许设置审计类策略和放行，对黑名单可以进行全部的控制策略。当 DBF 检测到用户提出的请求和行为模型出现差异时，将根据用户的配置进行警告或者阻断等操作。

阻断动作包括：中断会话和拦截语句。

审计行为分为：普通审计和告警审计。

告警通知包括：syslog、snmp、邮件和短信。

4.10 DBF 的应用模式有哪些

DBF 可以支持四种应用模式：

数据库审计产品：提供全面数据库审计能力，符合等保三级需求；

数据库入侵防御产品：接入在应用服务器和数据库服务器之间，防止外部黑客入侵；

数据库运维管控产品：内部数据库运维接口，防止运维人员高危操作和泄漏敏感数据；

内外网隔离装置：替代传统防火墙、IDS、IPS 产品，实现唯一内网接入通道安全数据库通讯。

4.11 如果 DBF 死机了是否会影响正常应用和数据库通讯

DBF 以串联方式部署在数据库之前，如果死机了会影响应用和数据库的正常通讯，通过断电 bypass 功能或者以 HA 方式部署两台 DBF 可以解决这个问题。

五. 联系我们

总机：4000 258 365

北京营销中心

地址：北京市海淀区中关村南大街 17 号韦伯时代中心 C 座 15 层 邮编 100089

电话：010－88571665

天津研发中心

地址：天津华苑产业园区海泰信息广场 D 座 5 层 邮编 300382

电话：022－23707020