Sybase 数据库评估指南

网络安全焦点 http://www.xfocus.net 整理

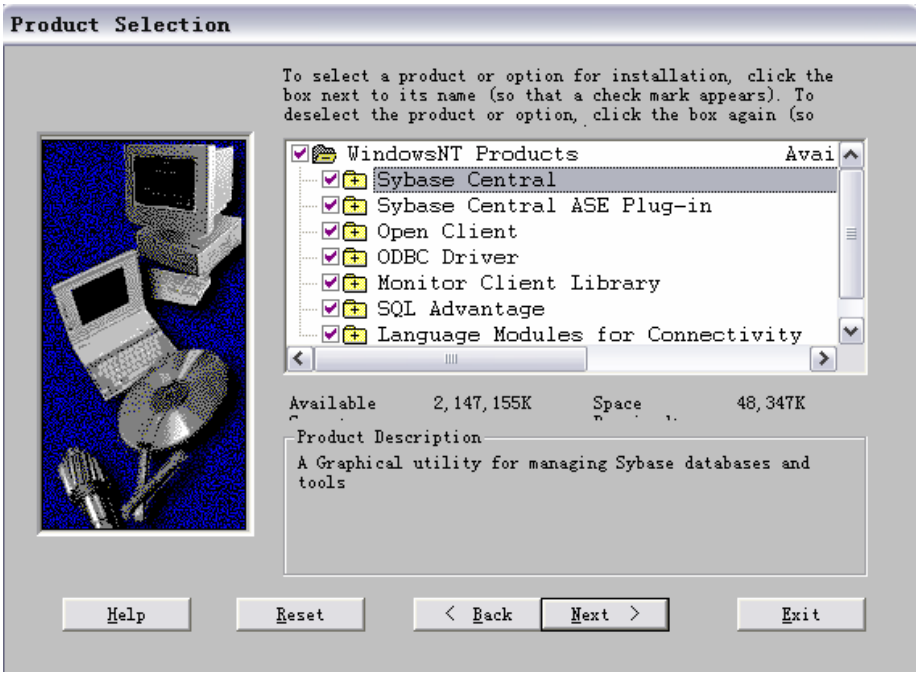
2005-10-17

版本：v1.0

目录

1. 客户端工具

安装 Sybase PC Client，可以按照默认设置进行安装，如下图所示：



1.1. 命令行工具

喜欢命令行的朋友可以采用%sybaseroot%\bin\isql.exe 工具连接数据库进行人工审计：

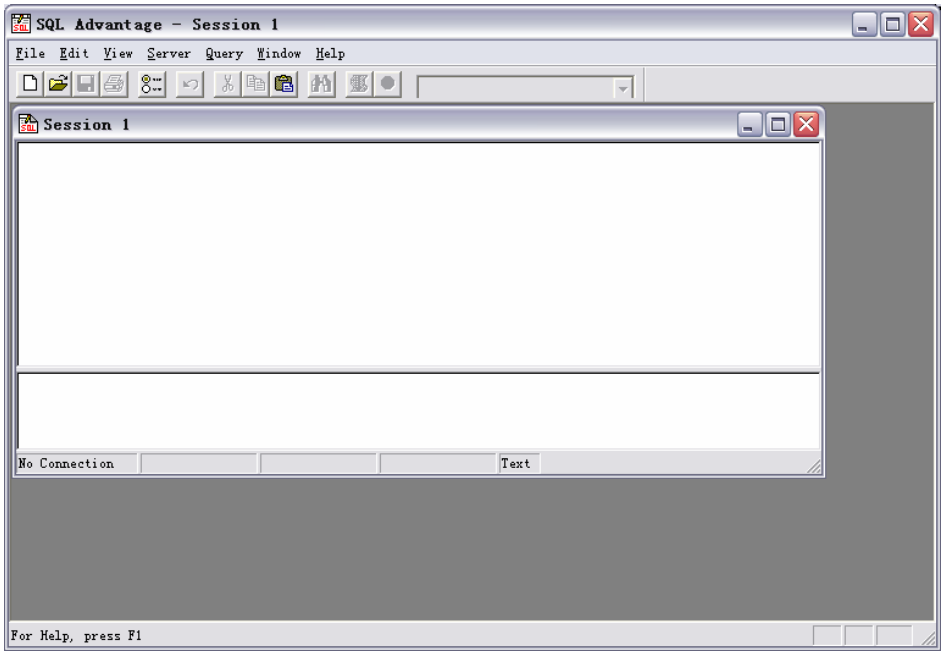
```
C:\sybase\bin>isql --help
Syntax Error in '--help'.
usage: isql [-b] [-e] [-F] [-p] [-n] [-v] [-X] [-Y]
        [-a display_charset] [-A packet_size] [-c cmdend] [-D database]
        [-E editor [-h header [-H hostname [-i inputfile]
        [-I interfaces_file] [-J client_charset] [-K keytab_file]
        [-l login_timeout] [-m errorlevel] [-M labelname labelvalue]
        [-o outputfile] [-P password] [-R remote_server_principal]
        [-s col_separator] [-S server_name] [-t timeout] [-U username]
        [-V [security_options]] [-w column_width] [-z localename]
        [-Z security_mechanism]

C:\sybase\bin>
```

我们后面提到的命令集，可以直接采用如下命令得到结果输出：

```
isql –S ServerName –U UserName –i QueryFile.txt –o Output.txt
```

1.2. 图形化工具

为了方便起见，我们也可以选择菜单中的 SQL Advantage，该工具是命令行工具 isql 的一个图形前端:



通过在 dsedit 进行目标服务器配置后即可进行连接，登陆后，SQL Advantage 上方为查询窗口，下方为结果输出窗口。我们同样可以将命令集合复制到查询窗口，点击执行后保存需要的结果输出。

2. Sybase 安全机制简介

Sybase 本身能够提供很好的安全机制。它的安全架构可以分为五个部分:

1) 自由访问控制机制（Discretionary Access Controls ， DAC）: 在对象级别赋予用户访问权限。
2) 鉴别和认证控制: 保证只有授权用户可以访问数据库对象。
3) 角色分离: 基于系统和用户任务级别的分离。例如 DBA 使用的 sa 角色，安全管理员使用的 sso 角色。
4) 基于网络的安全: Sybase 提供远程认证保护，在网络上使用加密传输数据，保证并进行完整性校验。

5) 审计：Sybase 拥有很好的审计机制，如果配置得到，能够提供很好的审计。

因此如果正确配置，它能够达到较高的安全等级。

3. 检查列表

3.1. 通用安全机制

3.1.1. 操作系统检查

- 检查 sybase 安装目录的权限，确保只有系统管理员才能访问该目录。
- 对 Windows 操作系统而言，采用 regedt32 检查 HKLM\Software\Sybase 中的权限键值。

3.1.2. 服务器信息

- 列举网络上的远程服务器

  exec sp_helpserver

  检查输出内容:

  网络密码加密的部份可能如下:

  "net password encryption" = true

  "net password encryption" = false

  安全机制部份可能如下:

  "rpc security model A" 是不提供安全机制

  "rpc security model B" 是提供不同的安全服务，如互相认证、消息加密、完整性校验等。

- 列举特定服务器的信息

  exec sp_helpdb

3.1.3. 登陆配置

- 检查认证模式是否开启

exec sp_loginconfig "login mode"

0 - 标准认证模式:

这是默认的认证模式，Sybase 使用自己的数据库（master 数据库中的 syslogins 表）来认证用户。Windows NT/2000 的管理员如果没有正确的帐户也不能进行登陆。

1 - 集成认证模式:

在统一认证模式中，Sybase 仅依赖于 Windows 来认证用户。Windows 用户或组都可以获得访问 Sybase 的权限。

2 - 混合认证模式:

在混合模式里，用户首先以 Windows 来认证，如果 Windows 用户不正确，Sybase 将会使用它自己的数据库即标准安全模式中储存的用户名密码对来认证用户。

- 检查默认登陆

exec sp_loginconfig "default account"

在集成认证模式中，确认默认登陆角色不是 sa ，设置为 NULL 或者一个低权限的用户。

3.1.4.补丁

- 查看服务器版本信息

select @@VERSION

到Sybase网站上下载最新的补丁：http://downloads.sybase.com/swd/swx

补丁类型:

1) 紧急漏洞修补补丁 EBF (Expedited Bug Fix or Emergency Bug Fix)
2) 补丁服务包 ESD (Electronic Software Delivery)
3) 服务器中间发布版本 IR (Interim Release)

注：在应用 ESD 之前必须安装前一个版本的 IR。

3.2.数据库配置

3.2.1.通用数据库参数

- 获得当前 Sybase ASE Server 的配置

  exec sp_configure

- 检查输出 'allow updates to system tables'

如果是“on”状态，DBA 可以通过存储过程修改系统表。建议 sso 将其设置为“off”状态。因为已经建立的存储过程可以被执行，建议审计数据库的存储过程列表。

exec sp_configure "allow updates to system tables"

- 检查并保证'allow resource limit'的值设为“1”

  exec sp_configure "allow resource limit"

- 保证系统表'syscomments' 已经被保护

该系统表非常重要，但默认情况下被设置为“1”，确认该值被设置为“0”。

exec sp_configure "select on syscomments.text"

3.2.2.错误日志配置

- . 检查是否设置失败登陆日志，确认该值设置为“1”

  exec sp_configure "log audit logon failure"

- 检查是否设置成功登陆日志，确认该数值设为“1”

  exec sp_configure "log audit logon success"

3.3.用户级安全

3.3.1.组

- 列举某数据库的所有组:

use DBName

exec sp_helpgroup

- 列举某组内的用户:

  use DBName

  exec sp_helpgroup GroupName

3.3.2.角色

- 检查服务器角色和用户定义的角色:

  select name, password, pwdate, status from syssrvroles

- 检查每个角色的详细信息:

  exec sp_displayroles "RoleName", expand_up

- 检查每个用户的详细信息:

  exec sp_displayroles UserName, expand_down

- 检查角色中空口令用户:

  select name from syssrvroles where password = NULL

3.3.3.用户

- 检查某数据库的所有用户:

  exec sp_helpuser

- 检查散列用户口令:

  select name, password from syslogins

- 检查特定用户的详细信息:

  sp_displaylogin UserName

  Default login name: 默认登陆名

  Default database: 默认数据库

  Auto login script: 自动登陆脚本

  Roles assigned : 角色分配

  Whether this account locked: 用户锁定状态

  Last date of password change: 最后口令更改日期

  Password expiration interval: 口令有效时间

Whether password got expired: 口令是否过期

Minimum password length : 最短口令长度

Maximum failed logins: 最大登陆尝试次数

Current failed login attempts: 当前登陆失败尝试次数

- 检查每个数据库的用户权限:

use DBName

exec sp_helprotect

3.3.4.其它用户安全选项

- 使用强 sa 用户口令
- 删除 sa 的'sa_role'和'sso_role'角色，将'sa_role'赋予 DBA 用户，将'sso_role'赋予系统安全管理员
- 删除除 *master* 和 *tempdb* 之外的所有数据库的'guest'用户
- 从组的级别设定对象访问权限

3.3.5.口令安全参数

- 检查口令过期时间，建议设置为14天

exec sp_configure "password expiration interval"

'0' – 密码从不过期

'n' – 天数.

- 检查口令是否至少包含一位数字

exec sp_configure "check password for digit"

'1' – 强制用户口令中至少包含一个数字

- 检查最小密码长度，建议为8位以上

exec sp_configure "minimum password length"

删除无用的系统帐号，并检查下列系统帐号的口令:

用户名	缺省口令	注释

Mon_user	mon_user	服务器监视用户
sybmail	User defined	当安装'Sybase Mail Service'时创建
Dba	SQL	在 Enterprise Portal Express Edition 中创建
entldbdbo	dbopswd	Database Access Control 创建
entldbreader	rdrpswd	Database Access Control 创建
jagadmin	空	Enterprise Portal Application Server 创建
PIAdmin	PIAdmin	Enterprise Portal Application Server 创建
pkiuser	pkipasswd	Enterprise Portal
PortalAdmin	sybase	Enterprise Portal
pso	123qwe	Enterprise Portal

3.4. 数据级安全

3.4.1. 权限

- 检查关键表、过程、触发器的权限，检查赋予public组权限的对象:

  use DBName

  exec sp_helprotect ObjectName

  输出:

  1. 用户权限列表
  2. 所有对象的权限类型
  3. 是否设置WITH GRANT权限

3.4.2. 存储过程

- 列出数据库中所有扩展存储过程:

  use sybsystemprocs

  select name from sysobjects where type='XP'

- 删除扩展存储过程xp_cmdshell，并删除sybsyesp.dll

exec sp_dropextendedproc xp_cmdshell

如果一定需要使用 *xp_cmdshell*，则审核其权限分配:

use sybsystemprocs

exec sp_helprotect "xp_cmdshell"

- 检查其它存储过程

如 sendmail, freemail, readmail, deletemail, startmail, stopmail，删除无用的存储过程，并删除 mail 帐号'sybmail'.

3.5. 审计

Sybase 默认不会安装审计工具，必须在默认安装之外额外安装。Sybase 审计存储过程位于审计工具安装后创建的 *sybsecurity* 库里。

- 检验Sybase是否安装审计工具的方法是检查sybsecurity库是否存在。

  Sybase由此可以产生嵌入的审计机制。Sybase将会把审计配置的细节和审计跟踪表储存在位于sybsecurity库中的sysaudits_01-sysaudits_08表。

- 检查审计功能是够打开

  use master

  exec sp_configure "auditing"

以下部分仅在审计功能被安装且激活的情况下起作用。

- 检查sybsecurity库中审计的表的数量

  Sybase 推荐用至少 2-3 个表用来审计。从而在一个表装满的情况下，另一个表可以即刻被使用以免数据丢失。

  select count(*) from sysobjects where name like "sysaudits%"

- 检查审计表中是否开启了审计，和审计和存储存储过程如何关联

  use sybsecurity

  exec sp_helpthreshold aud_seg1

在每个审计表里面重复这个查询。"sysaudits_01"的字段名为"aud_seg1"，"sysaudits_02"的字段名为"aud_seg2"，依此类推。

- 检查审计表是否存档

推荐把可能记录有恶意行为的行为的审计表存档。确定一个查询特定审计表时的存储过程。当表达到其极限时，这个存储过程将会被执行。推荐存储过程把审计表存档。

- 检查当前审计表参数

```
use master
exec sp_configure "current audit table"
```

输出将会是“n”或“0”的一个整数。推荐值是“0”，此值表示如果当前表写满，Sybase 将会使用下一个审计表。

- 检查当审核表写满时的暂缓审核参数

```
exec sp_configure "suspend audit when device full"
```

保证其值为“1”，这将会使所有的审计表写满的时候暂缓审计。这种情况只会在极端程序没有运行成功时出现。当设置为“0”时，将会截断当前的审计表记录，并且继续使用其作为当前的审计表。

- 检查“audit queue size”的值，并且保证它的值足够大，（约50左右）

```
use master
exec sp_configure "audit queue size"
```

设置这个值的时候需要在安全和性能之间进行平衡。低一点的值将会增加从队列中向审计表中写数据的，将会耗用更多系统资源；频率高一点的值将可能导致安全问题，诸如系统崩溃将会导致队列中的数据丢失。

- 检查以下重要全局设置的安全审核选项

Logins - 所有登陆尝试

Logouts - 所有注销尝试

bcp - 批量复制事件（bulk copy）

create - 所有的创建时间，如创建表，存储过程，视图，触发器等。

delete - 从表或者视图中删除行

disk - 磁盘初始化，再初始化的执行

drop - 数据库，表，存储过程，触发器，试图的删除事件

dump - 数据库，事务的导出

use sybsecurity

exec sp_displayaudit

保证所有的选项都被设置为 “on”.

- 检查错误登陆尝试

use sybsecurity

select * from AuditTable where event =45 and eventmod =2

审计表中的事件细节可以参见:

http://manuals.sybase.com/onlinebooks/group-as/asg1200e/asesag

3.6. 网络层安全

3.6.1. 远端服务器信息

- 检查远端服务器是否允许访问

use master

exec sp_configure "allow remote access"

'1' - 允许远程访问

'0' - 不允许远程访问

如果允许远程访问，检查远程用户的可信性及网络安全。这将允许本地服务器的存储过程在远端服务器通过 RPC 执行。

- 检查信任用户的存在情况

  exec sp_helpremoteserver

Sybase 允许建立不需要密码即可以连接到服务器的信任连接。如果存在这样的信任连接，则需调查那些用户的信任关系。

3.6.2.远程连接机制

- 检查安全机制和其提供的安全服务

  select * from syssecmechs

Syssecmech 表默认并不存在,仅在查询的时候创建,它由以下的列组成:

sec_mech_name　服务器提供的安全机制名

available_service　安全机制提供的安全服务

举例，Windows 网络管理员，其内容将为:

sec_mech_name　= NT LAN MANAGER

available_service = unified login

- 检查libctl.cfg文件

内部包含了网络驱动的信息，安全，目录磁盘和其他初始化信息。

1. 如果 LDAP 密码加密。
2. 安全机制:

"dce"　DCE 安全机制。

"csfkrb5"　CyberSAFE Kerberos 安全机制。

"LIBSMSSP"　Windows NT 或 Windows 95(仅客户端)上的 Windows 网络管理员。

注意: libtcl.cfg 的位置:

UNIX 模式: $SYBASE/config/

桌面模式: SYBASE_home\ini\

- 检查统一登陆需要的参数

  exec sp_configure "unified login required"

如果网络安全被设置为启用，则保证其设置为“1”。设置为“0”，将会允许传统的用户密码方式登陆到 ASE，这样跟信任连接一样会对网络的安全性造成影响。

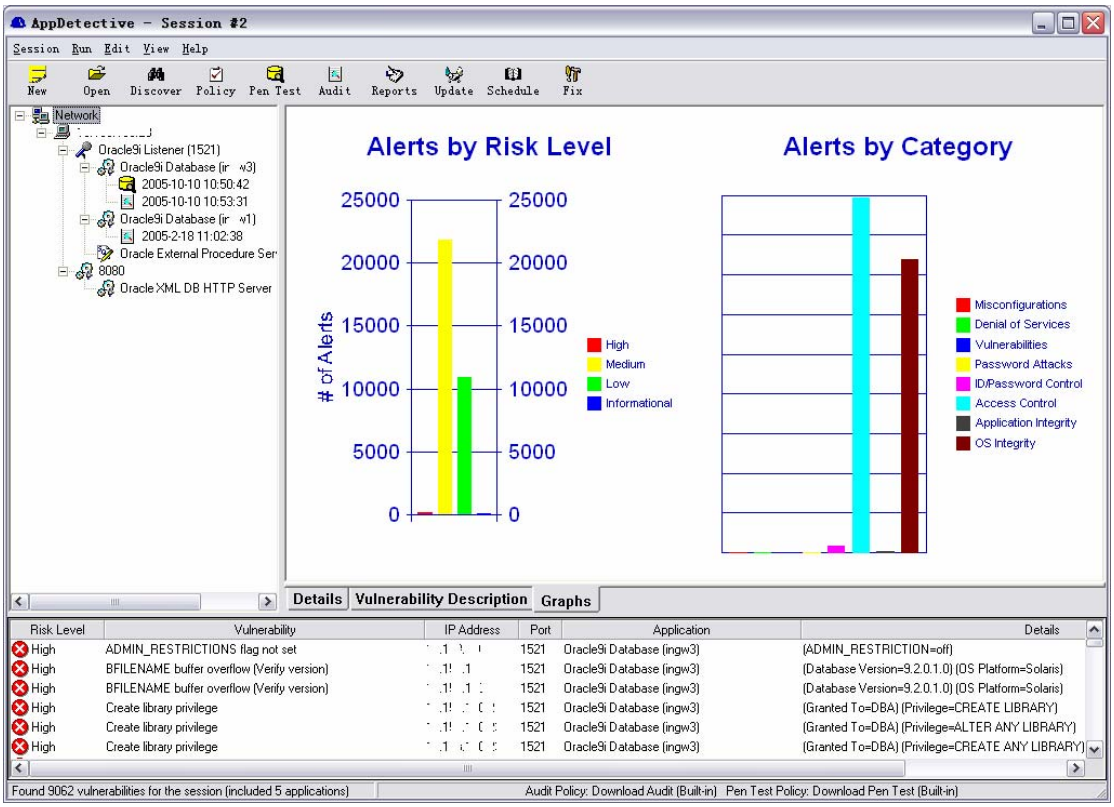
4.其它工具

对运营商的计费系统等动辄上百个 G 的大型数据库，我们推荐采用人工审计的方式进行评估，一方面降低风险，另一方面也能够提高检测的效率（工具检测时载入数据库十分耗时）。

当然，我们也可以采用数据库扫描工具进行 penetration 与 audit，目前国内能见到的数据库审计工具包括以下几种:

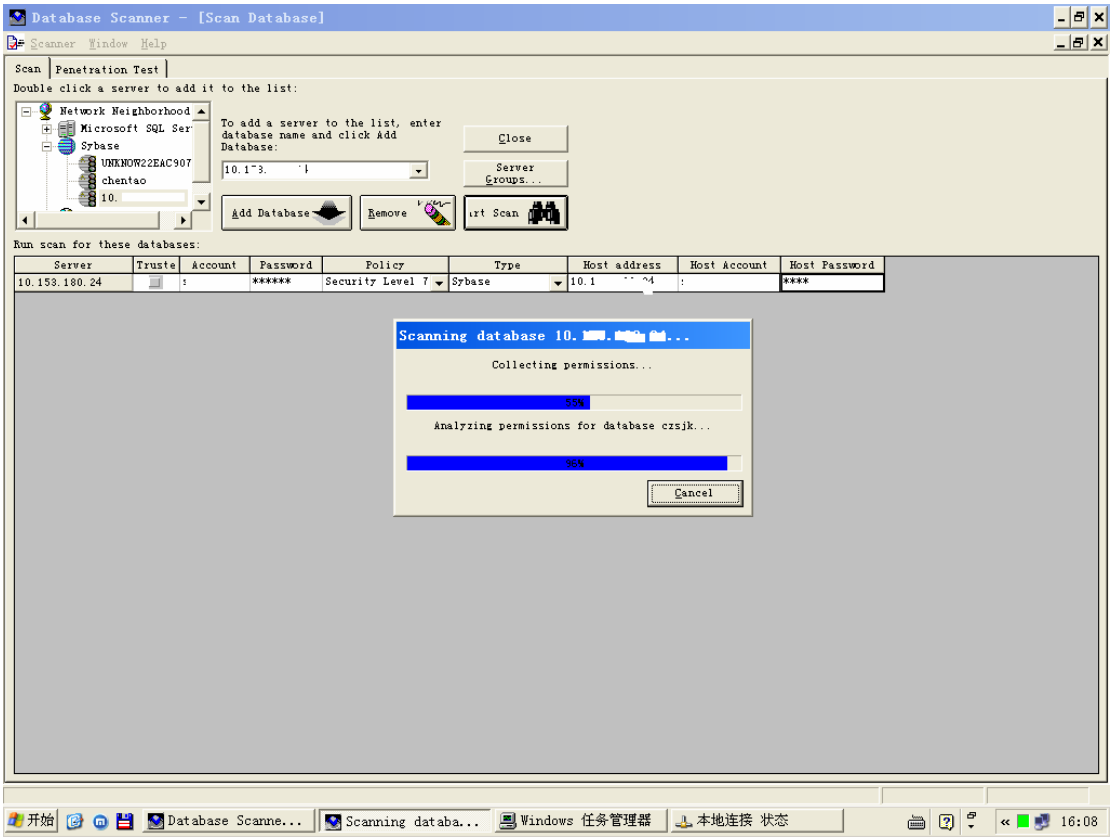
4.1. AppDetetive

这是一款相当出色的数据库及应用软件扫描审计工具，推荐。



4.2. ISS Database Scanner

老牌的数据库扫描工具，不推荐。



4.3. NSGSOFT NGSSQuirreL

这是一系列工具集，在其网站上有试用版本下载，功能相对简单。

5. 参考资料

Nilesh Burghate 《GUIDE TO SYBASE SECURITY》