## AD域功能

员工办公终端管理

配合网络准入

员工电脑软件管理，不能玩游戏

补丁统一安装

密码安全性管理

ADManager Plus，AD域管理工具

## 零信任

员工在入、转、调、离等各个办公周期环节中，员工权限如何能够去跟身份快速匹配。常常发生错配、漏配的问题，最后导致了数据资产的外泄。

多业务系统后，每个系统都会有单独的用户名跟密码。那如何把账号进行统一管理。

## IAM发展阶段

SSO：

1. 实现一点登录，全局进入。无访问控制能力

实现统一账号管理，可以解决离职-增删账号问题

4A（Account、Authentication、Authorization、Audit）

1、关注用户、认证、权限和审计

2、面向内部员工、具备人员生命周期管理

3、具备用户登录时的访问控制

4、关注权限统一管理

5、用户身份变化和访问信息记录后可以事后审计

实现基本安全管理及技术

IAM

1、面向员工、合作伙伴、顾客、设备、应用、特权账号、物理设备等，实现全生命周期管理

2、实现Service All In的单点，将B/S、C/S不同类别的应用，不同浏览器访问的统一纳管

3、实现应用级别的细粒度权限、AP操作、数据权限统一管理

4、访问控制从静态转向动态，具备实时风险发现机制和风险闭环管理能力

1. 实现身份能力的云服务化，增强用户隐私管理

更细粒度的安全管理

伪实现：

建设通用的账号申请流程，在流程中记录 员工-系统-权限 到数据库。离职时统一调取销号。

开源IAM：

<https://eiam.topiam.cn/docs/introduction/overview/>

## 终端安全

### 终端安全加固

通过域控策略统一管理终端的安全策略，几个比较重要的点：

开启屏保以及锁屏时间

域账户密码复杂度，密码更换时间

禁用guest账户

开启主机防火墙

禁止administror账户远程登录（员工自己域账户是本地管理员，可以正常登录，很多公司喜欢用ghost预装电脑，administror账户的密码绝对是个大坑）

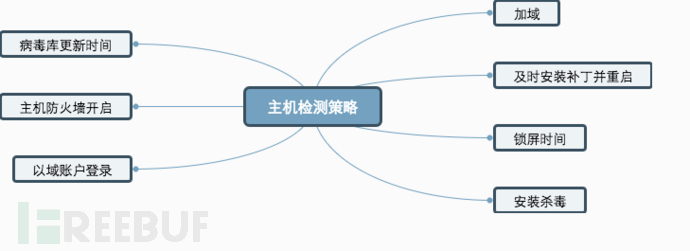
禁止域管理员远程登录（一定要把域控和一般PC放在不同组策略下，不然这个策略害死人）

删除IPC$ C$ D$ admin$（木马经常利用）

开启审计策略，记录登录、账户相关事件

调整事件日志的大小及覆盖策略

关机清理虚拟内存页面文件

[](https://image.3001.net/images/20170207/14864450981709.png)

### 终端防病毒

开源EDR

https://github.com/ComodoSecurity/openedr

## 网络区域划分

划分与隔离，按职能划分并应用不同的安全策略，便于管理。

基本假设是，每个区域都可能被入侵。区域划分就是为了这个时候提供黑客进一步入侵的成本，为后面的入侵检测和应急响应争取时间。

### 内部服务区域

这个区域包含大量运营、人事、研发、财务相关的重要企业数据，安全等级甚至比业务区域还要高，但是往往容易被忽略，成为入侵的重灾区。原则上这个区域只允许来自办公区域的访问。

### 测试开发区域

与内部服务器区域类似，这个区域大量开发中的产品，安全基线最差，最容易被入侵，原则上这个区域只允许来自办公区域的访问。

业务区域、内部服务区域、测试开发区域难免业务上有需要，部分服务需要互通，这个以白名单形式开放。

各个区域针对SSH和远程桌面的访问仅信任堡垒机IP。

### 生产区域

实行最严格的控制策略，优先进行安全建设及防护。

## 权限模型

基于身份的访问控制要设计权限模型才便于管理。

## 重点部门

运维&DBA，系统权限特别大，纵向提权的最佳目标，有种开玩笑的说法，黑掉一个运维的电脑，把所有文本文件翻个遍，找不到一个密码才是见鬼了。应当尽量限制其他人群对他们的访问。

重要业务系统的管理员，这些同学负责对公司核心业务进行运营管理，对重要后台系统具有很高的权限，一旦他们电脑被入侵，后果会很严重。比如游戏公司充值系统的后台、广告公司的客户广告投放管理系统、招聘公司的后台简历管理系统、电商的订单物流管理系统，出点事都是大事。应当尽量限制其他人群对他们的访问，同时严格限制他们的外网访问权限。

高管、HR、财务，这些同学对办公系统的访问需求比较单一，主要网络访问需求在外网，通常不懂技术，安全防护意识也最弱，也最得罪不起。他们的办公电脑集中大量公司重要数据，一旦被入侵就直接产生损失了。这部分同学可以严格限制跟办公网其他区域以及对内部系统的访问。