iMC EAD安全级别的说明

EAD解决方案 何颖 2012-10-26 发表

iMC EAD安全级别的说明

一、 组网：

无

二、 问题描述：

在实际设置EAD安全级别时，需要了解EAD安全级别的含义及对应的处理策略。

三、 过程分析：

每种EAD安全级别含义和处理策略不用，详细分析情况如下文所述。

四、 解决方法：

安全级别管理主要用于：在iNode客户端时行安全检查时，当终端操作系统的各个安全检查项如防病毒软件、可控软件组、补丁管理、资产等不符合安全策略要求时，EAD所采取的应对策略。这个策略会下发给iNode客户端，通常会同时对终端的多个检查项进行健康检查，但由于各个检查项对网络安全和信息安全又不同的重要程度，所以不同的检查项有不同的应对的方式。目前安全级别管理支持下线、隔离、提醒、监控四种安全模式。各种安全模式的具体含义如下：

1、下线模式：终端用户安全检查不合格时，EAD服务器对终端用户进行下线操作。整个过程iNode给出安全检查不合格的提示，同时EAD服务器的安全日志做对应的记录。

2、隔离模式：终端用户身份认证时UAM服务器下发隔离ACL，终端用户受此隔离ACL控制，之后终端进行安全检查，如果安全检查通过EAD服务器下发安全ACL，如果安全检查不通过EAD服务器不下发安全ACL，终端用户始终受隔离ACL控制，网络访问受限。整个过程iNode给出安全检查不合格的提示，同时EAD服务器的安全日志做对应的记录。

3、提醒模式：终端用户身份认证时UAM服务器下发隔离ACL，终端用户受此隔离ACL控制，之后终端进行安全检查。无论安全检查是否通过，EAD服务器均下发安全ACL。整个过程iNode给出安全检查不合格的提示，同时EAD服务器的安全日志做对应的记录。

4、监控模式：终端用户身份认证时UAM服务器下发隔离ACL，终端用户受此隔离ACL控制，之后终端进行安全检查，无论安全检查是否通过EAD服务器均下发安全ACL。整个过程iNode不给出安全检查不合格的提示，同时EAD服务器的安全日志做对应的记录。

举例如下，一个公司里应用了EAD，该公司有普通员工、中层领导、高层领导三类用户。

普通员工使用下线模式与隔离模式。终端安全检查不合格时不能接入网络中（或者访问网络受到隔离ACL限制）。安全检查不合格时iNode会给出提示，EAD服务器记录日志。

中层领导使用提醒模式。终端安全检查不合格时也可以访问网络（因为下发了安全ACL）。整个过程iNode会善意的提醒终端用户进行修复，EAD服务器记录日志。

高层领导使用监控模式。终端安全检查不合格时除了可以正常访问网络（因为下发了安全ACL）外，整个过程iNode不给出提示信息（避免干扰高层领导的工作）。由于EAD服务器记录日志，网络管理员可以通过日志了解到高层领导的安全检查项不合格，并主动进行修复。

安全级别支持配置不安全提示阈值，如下图所示：

图1 增加安全级别

该参数仅在安全级别中所设置的最高级别为隔离和下线时才能够设置（即如果安全级别的所有配置项的安全模式都是提醒或监控时，该参数无法配置）。该参数仅对安全级别为下线或隔离的安全检查项有效。这个参数的作用如下：

1）下线模式：如果安全级别中配置了不安全提示阈值（比如配置为10分钟）,则终端用户安全检查不合格时不立即下线，而是等10分钟之后再执行下线的动作。在此过程中iNode会每隔一段时间提醒一次

2）隔离模式：如果安全级别中配置了不安全提示阈值（比如配置为10分钟）,则终端用户身份认证时先下发安全ACL，如果安全检查不通过等10分钟之后再下发隔离ACL，在此过程中iNode会每隔一段时间提醒一次。

每个安全级别可以配置的安全检查项相当丰富，目前主要有：流量监控、四防软件、可控软件组、补丁管理、注册表、目录共享、资产、操作系统密码等大项，每个大项又分为若干具体小项。

终端用户做安全检查时，如果有多个安全检查项不通过，则以其中最严格的安全级别为准。安全级别的优先级为：下线 > 隔离 > 监控 > 提醒

EAD已经预置了五个安全级别，分别为下线模式，隔离模式，访客模式，VIP模式和监控模式，具体说明如下：

1）访客模式：安全认证后，如果有不合格的项，会先提醒用户有不合格项并请用户修复。5分钟后会自动重新再安全认证一次，如果发现不合格，则下线；如果合格，则不下线。

2）VIP模式：VIP模式就是提醒模式。

3）其他模式：下线模式，隔离模式和监控模式与其对应的安全级别的处理完全相同。

安全级别管理中的每个安全检查项都支持自定义安全级别，如下图所示：

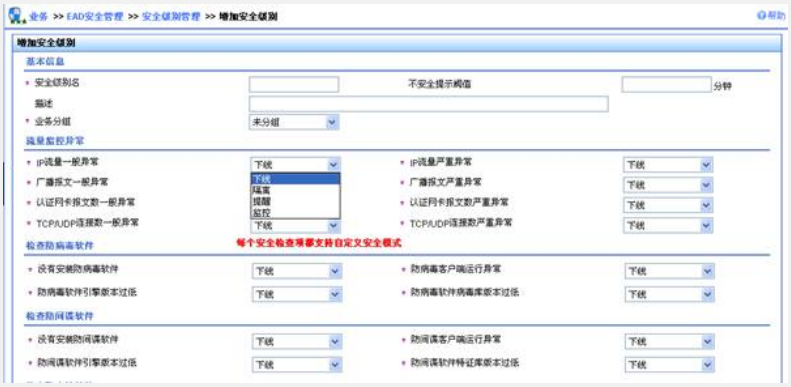

图2 界面说明

安全级别管理中带了一些默认的安全级别，实际中管理也可以根据实际情况自定义安全级别。