iMC-EAD可控软件检查不成功

EAD解决方案 **龚文文** 2019-12-06 发表

组网及说明

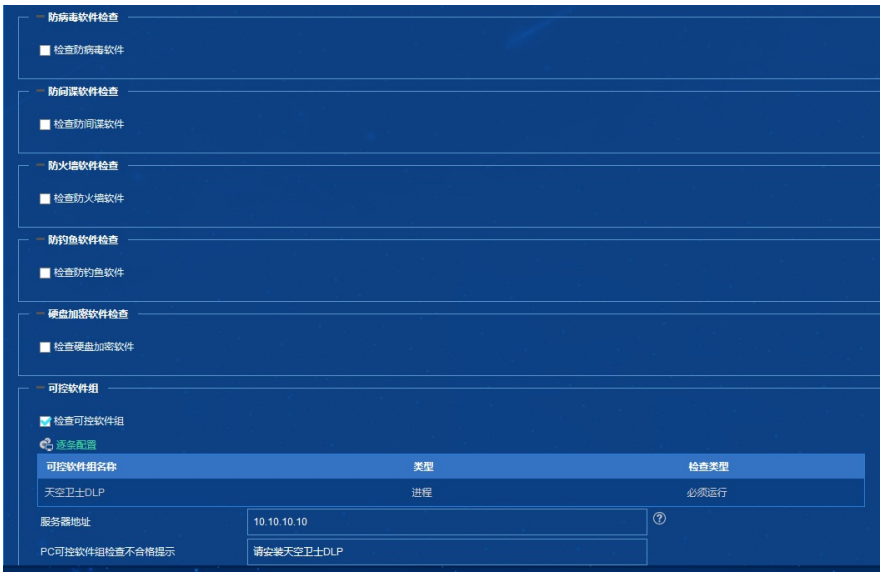
略

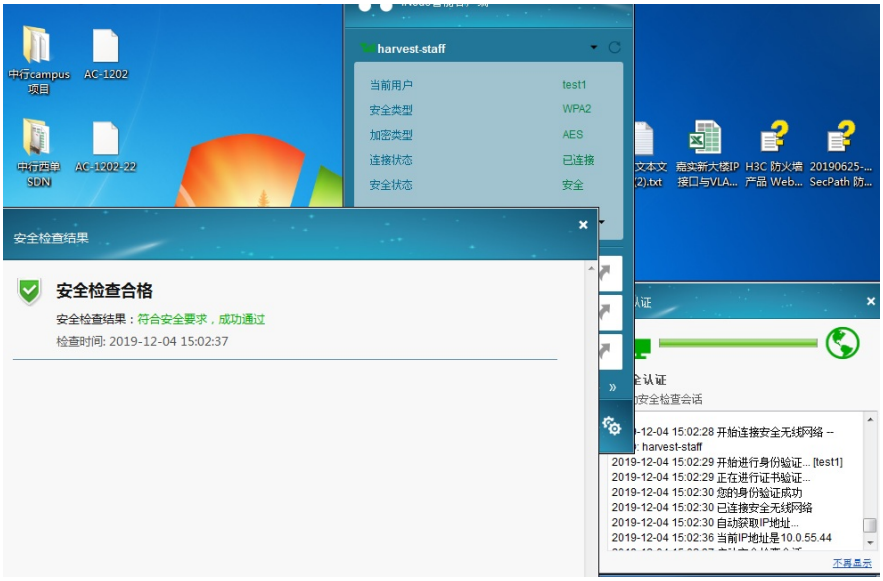
问题描述

本例以某局点检查“天空卫士DLP”进程为例，需要实现的需求是用户接入认证之后对用户进行安全检查：

若客户端未安装“天空卫士DLP”，则安全检查不合格，且提示“请安装天空卫士DLP”。

现场的安全策略里只设置了检查“天空卫士DLP”进程，并新建了test1用户测试，结果发现安全检查并没有检查出客户端未安装“天空卫士DLP”，iNode客户端很快就提示安全检查的结果是安全的。如图所示





可见并没有检查出客户端为未安装“天空卫士DLP”。

但是当和在安全策略里除了设置检查“天空卫士DLP”之外，再设置检查金山毒霸，则能同时检查出金山毒霸和天空卫士DLP未安装，如下图

可见当安全策略同时检查天空卫士DLP和金山毒霸时，iNode能同时检查出两者都未安装。
后续在同一接入服务下新建test2，test3用户，测试时均发生以上现象。

过程分析

查看iNodeSecPkt日志，可以看到当只检查天空卫士DLP时，安全检查会直接通过。

```
[2019-12-04 14:24:31] [DtlCmn] [24e0] SecPkt secPushInner: out-pkt [3]
<data>
    <i n="userName">test1</i>
    <i n="hwAddr">DC:53:60:DE:88:84</i>
    <i n="dictionaryDigest"></i>
    <i n="eventSeqID">S0MgKZCJ</i>
    <i n="supNetScan">true</i>
    <i n="AScheckResult"></i>
    <i n="APcheckResult"></i>
    <i n="FWcheckResult"></i>
    <i n="HDcheckResult"></i>
    <i n="blackSofts"></i>
    <i n="whiteSofts"></i>
    <i n="whiteSoftItems"></i>
    <i n="blackProcess"></i>
    <i n="whiteProcess">天空卫士DLP;</i>
    <i n="whiteProcessItems">天空卫士DLP:EndpointClientAgent.exe;</i>
    <i n="blackServices"></i>
    <i n="whiteServices"></i>
    <i n="whiteServiceItems"></i>
    <i n="NoValidFileGroup"></i>
    <i n="blackFiles"></i>
    <i n="whiteFiles"></i>
    <i n="whiteFileItems"></i>
</data>
[2019-12-04 14:24:31] [DtlCmn] [24e0] SecPkt secPushInner: the state send before is  11
[2019-12-04 14:24:31] [Dbg] [e98] SecPkt secDataProc: The head id is ad879
[2019-12-04 14:24:31] [Dbg] [e98] SecPkt secDataProc: The type is 4
[2019-12-04 14:24:31] [Dbg] [e98] SecPkt secDataProc: The id is 14248
[2019-12-04 14:24:31] [DtlCmn] [e98] SecPkt sndSecMsg: transfer [4] [14248]
<data>
    <i n="isRealtimeMonitor">false</i>
    <i n="realtimeMonitorAll">false</i>
    <i n="patchFailStamp">2NDOXkXvVt8=</i>
    <i n="netScanPolicy"/>
    <i n="netMonItem"/>
    <i n="okMessage"/>
```

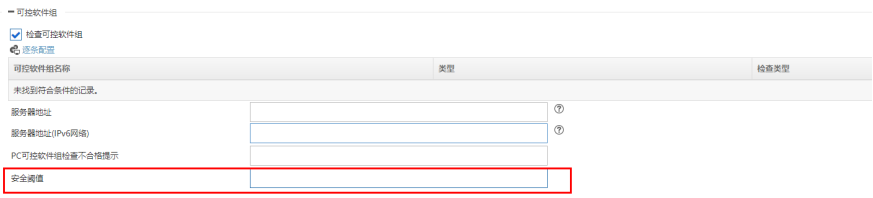
当天空卫士DLP和金山毒霸一起检查时，才会提示安全检查不合格

```
<i n="strategyMode">autoAdapt</i>
<i n="userMessage"/>
<i n="antiIPchange">false</i>
<i n="antiAgent">false</i>
<i n="antiProxy">false</i>
<i n="antiDualNetcard">false</i>
<i n="ipSetMode">unlimit</i>
<i n="macCheck">false</i>
<i n="sameMacCheck">false</i>
<i n="antiMultiOS">false</i>
<i n="antiMultiip">false</i>
<i n="antiVMWareNATservice">false</i>
<i n="antiVMWareUSBservice">false</i>
<i n="iSupVMCheck">false</i>
<i n="iSetWanControl">false</i>
<i n="iSetOnlineUnauthAudit">false</i>
<i n="iSetACL">false</i>
<i n="iSetpingOfflineACL">false</i>
<i n="iSetPingOfflineMon">false</i>
<i n="damProxyIp">168363528</i>
<i n="damProxyPort">9029</i>
<i n="heartBeatInterval">720</i>
<i n="heartBeatOutTimes">3</i>
<i n="AVMode">PluginForbidden</i>
<i n="forcedAVs">Kingsoft</i>
<i n="AVConfigNames">金山毒霸</i>
<i n="forcedAVDelayTimes">Kingsoft|0</i>
<i n="checkList">Virus-Engine-Version;Virus-Def-Version</i>
<i n="whiteProcessGroup">天空卫士DLP;EndpointClientAgent.exe;simple;;;or;0</i>
<i n="ifMonitorPwdforAllUser">false</i>
<i n="ifMonitorPwdOnlydic">false</i>
<i n="checkWeakPwdMoment">afterCheck</i>
<i n="patchLevel">Critical,repair;Important,repair;Moderate,repair;Low,repair</i>
<i n="checkGuestAccount">false</i>
<i n="checkIfDepEnabled">false</i>
<i n="USBStoreAccessControl">0</i>
<i n="iReportLatLongInfo">false</i>
<i n="eventSeqID">2HbmAGUK</i>
<i n="serverVersion">iMCV700R003B05D034SP04</i>
```

```
[2019-12-04 14:29:28] [DtlCmn] [20a8] SecPkt secPushInner: out-pkt [3]
<data>
    <i n="userName">testl</i>
    <i n="hwAddr">DC:53:60:DE:88:84</i>
    <i n="dictionaryDigest"></i>
    <i n="eventSeqID">2HbmAGUK</i>
    <i n="supNetScan">true</i>
    <i n="AScheckResult"></i>
    <i n="APcheckResult"></i>
    <i n="FWcheckResult"></i>
    <i n="HDcheckResult"></i>
    <i n="blackSofts"></i>
    <i n="whiteSofts"></i>
    <i n="whiteSoftItems"></i>
    <i n="blackProcess"></i>
    <i n="whiteProcess">天空卫士DLP;</i>
    <i n="whiteProcessItems">天空卫士DLP;EndpointClientAgent.exe;</i>
    <i n="blackServices"></i>
    <i n="whiteServices"></i>
    <i n="whiteServiceItems"></i>
    <i n="NoValidFileGroup"></i>
    <i n="blackFiles"></i>
    <i n="whiteFiles"></i>
    <i n="whiteFileItems"></i>
</data>
[2019-12-04 14:29:28] [DtlCmn] [20a8] SecPkt secPushInner: the state send before is  11
[2019-12-04 14:29:28] [Dbg] [2024] SecPkt secRcvThrd: [10.9.6.8 : 9019] sent me 316 bytes.
[2019-12-04 14:29:28] [Dbg] [2024] SecPkt secDataProc: The head id is ad879
[2019-12-04 14:29:28] [Dbg] [2024] SecPkt secDataProc: The type is 6
[2019-12-04 14:29:28] [Dbg] [2024] SecPkt secDataProc: The id is 14251
[2019-12-04 14:29:28] [DtlCmn] [2024] SecPkt sndSecMsg: transfer [6] [14251]
<data>
    <i n="action">repair</i>
    <i n="patchFailStamp">2NDOXkXvVt8=</i>
    <i n="netScanPolicy"/>
    <i n="netMonItem"/>
    <i n="avFailMessage">安全检查不合格</i>
    <i n="dissatisfactory">AV-Software|repair</i>
    <i n="whiteProcess">天空卫士DLP|repair</i>
    <i n="softFailMessage">请安装天空卫士DLP</i>
    <i n="softRepairUrl">1.1.1.1</i>
    <i n="softRepairUrlForIPv6"/>
    <i n="virusUpdateUrl">2.2.2.2</i>
    <i n="virusUpdateUrlForIPv6"/>
    <i n="repairPolicy">Virus-Manual-Update</i>
```

但是从日志看并不能看出具体原因。

在用户>安全策略管理>安全策略管理查看对应的安全策略，发现在PC可控软件组下配置的安全阈值为10。



安全阈值：用户安全检查不合格时会累积次数，次数达到安全阈值，触发对应的安全级别的处理，例如下线或者隔离等操作。用户通过安全检查后，不合格累积次数会被清零。如果配置为0，则表示立即执行安全级别配置的模式，即立即隔离或下线。安全阈值只在终端安全认证或重认证检查不合格时才累积次数，实时监控检查违规不会累积。
在设置的阈值次数范围内，如果只是可控软件组检查失败，最终的检查结果是通过的。因此当单独检查天空卫士DLP时，即使检查失败，但最终仍会提示安全检查通过，而当和金山毒霸一起检查时，由于天空卫士DLP和金山毒霸都检查不通过，此时安全阈值就不起作用，最终检查结果会提示不通过。

解决方法

在PC可控软件组下将安全阈值根据需要改小，一般默认为10。本例中将安全阈值改为0后重新检查，此时提示安全检查不通过，请安装天空卫士DLP。