计算机访问限制利弊

目录

简介

本文描述问题遇到与计算机访问限制(3月)，并且提供解决方案给问题。

使用私有拥有的设备增长，重要的是为了系统管理员能提供方式仅限制对网络的某些部分的访问到公司拥有的资产。在本文注意事项描述的问题如何安全地识别这些关注方面和验证他们，不用中断到用户连接。

先决条件

要求

思科建议您有802.1x知识为了充分地了解本文。本文假设与用户802.1x验证的熟悉，并且突出显示问题和优点通常附加对使用3月，和，计算机验证。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

基本上毁损尝试解决常见问题内在大多当前和普遍的可扩展的认证协议(EAP)方法，即该计算机验证和用户认证是独立，无关的进程。

用户认证是跟熟悉多数系统管理员的802.1x认证方法。想法是凭证(用户名/密码)给给每个用户，并

且套凭证代表一个物理人(可以共享在几人之间)。所以，用户能从与那些凭证的任何地方网络登录。

计算机验证技术上是相同的，但是没有典型地提示用户输入凭证(或证书);计算机或计算机独自地执行那。这要求计算机已经有存储的凭证。在您的计算机有<MyPCHostname >设置作为主机名条件下，发送的用户名是**host/<MyPCHostname>**。换句话说，它发送您的主机名跟随的**主机**。

虽然与Microsoft Windows和思科活动目录不直接地涉及，此进程更加容易地被回报，如果计算机加入对活动目录，因为计算机主机名被添加到域数据库，并且凭证在计算机协商(默认情况下和更新了每30天)并且存储。这意味着计算机验证从任一种设备是可能的，但是被回报更加容易地和透明地，如果计算机加入对活动目录和从用户隐藏的凭证逗留。

3月作为解决方案

说是容易的解决方案是为思科结束的访问控制系统(ACS)或的思科身份服务引擎(ISE) 3月，但是有要考虑的优点和缺点，在这实现前。如何在ACS或ISE用户指南此是最佳描述的实现，因此本文是否描述考虑它和一些可能的路障。

专业人员

因为用户和计算机认证完全分开， 3月被发明了。所以， RADIUS服务器不能强制执行用户必须从公司拥有的设备登录的验证。使用3月， RADIUS服务器(ACS或ISE，在思科旁拉)为一给的用户认证强制执行，必须有一有效计算机验证在X先于用户认证同一个终端的小时(典型地8个小时，但是此可配置)。

所以，计算机验证典型地成功，如果计算机凭证由RADIUS服务器知道，如果计算机加入对域，并且RADIUS服务器验证此与对域的一连接。它完全地是至确定的网络管理员一成功的计算机验证是否提供对网络的完全权限，或者仅限制访问;一般，这至少打开连接在客户端和活动目录之间，以便客户端可进行这样操作象用户密码或下载组策略对象(GPOs)的续订。

如果用户认证来自计算机验证未在上一个两个小时内出现的设备，则用户拒绝，即使用户通常有效。

完全权限只授权对用户，如果验证从计算机验证在过去两个小时内出现的终端是有效和完成。

缺点

此部分描述3月使用负面因素。

3月和Microsoft Windows请求方

在3月后的想法是那为了用户认证能成功，不仅必须用户有有效凭证，但是必须从该客户端记录一成功的计算机验证。如果有与该的任何问题，用户不能验证。出现的问题是此功能有时疏忽地能停工一个合法客户端，迫使客户端重新启动为了收复对网络的访问。

(当登录画面出现)时， Microsoft Windows仅执行计算机验证在引导时间;当用户输入用户凭证，用户认证进行。并且，如果用户注销(回归到登录画面)，一新的计算机验证执行。

这是显示的示例情形3月为什么有时引起问题：

用户x在他的笔记本电脑整天工作，通过无线连接连接。当晚，他结束笔记本电脑，并且分支工作。

这放置笔记本电脑到冬眠。次日，他回来到办公室并且打开他的笔记本电脑。现在，他无法建立无线连接。

当Microsoft Windows冬眠时，它在其当前状态采取系统的快照，包括谁的上下文登陆。隔夜，用户笔记本电脑的3月被缓存的条目超时和清除。然而，当笔记本电脑启动时，它不执行一计算机验证。它进入直通用户认证，因为那是什么冬眠记录了。解决此的唯一方法是记录用户，或者重新启动他的计算机。

虽然3月是一个好功能，有可能性导致网络中断。这些中断是很难排除故障，直到您了解方式3月工作;当您实现3月时，教育关于如何的最终用户适当地关闭计算机和注销从每计算机在每天结束时是重要的。

3月和多种RADIUS服务器

它是普通有在网络的几个RADIUS服务器负载平衡和冗余目的。然而，不是所有的RADIUS服务器支持一个共享3月会话缓存。ACS版本5.4和以上和ISE版本2.2和以上支持3月仅缓存同步在节点之间。在这些版本前，因为他们不彼此，对应执行计算机验证一个ACS/ISE服务器和进行用户认证别的是不可能的。

3月和有线的无线交换

3月缓存许多RADIUS服务器依靠MAC地址。它是与膝上型计算机和他们的最后成功的计算机验证时间戳MAC地址的一个表。这样，服务器能知道客户端是否是在为时x小时内验证的计算机。

然而，什么发生，如果启动您的与有线连接的笔记本电脑(并且从您的有线的MAC的一计算机验证)日间然后换成无线？RADIUS服务器没有平均值关联您的无线MAC地址与您的有线的MAC地址和知道您是在过去X小时内验证的计算机。唯一方法是注销和安排Microsoft Windows通过无线执行另一计算机验证。

解决方案

在许多其它特性中，思科AnyConnect有触发计算机和用户认证预先配置的配置文件的优点。然而，当您注销或重新启动时，限制和看到一样在Microsoft Windows请求方遇到，关于只发生计算机的验证。

并且，与AnyConnect版本3.1和以上，执行EAP-FAST与EAP连锁是可能的。这同时基本上是单个验证，您发送两个对凭证、计算机用户名/密码和用户名/密码。ISE，然后，更加容易地检查两个是成功的。没有缓存使用的和没有需要获取上次会话，这提交更加了不起的可靠性。

当PC启动时， AnyConnect发送仅计算机验证，因为用户信息不是可用的。然而，在用户登录，AnyConnect发送同时计算机和用户credentails。 并且，如果变得断开或拔掉/再插上电缆，计算机和用户凭证再发送在单个EAP-FAST验证，与AnyConnect更早版本有所不同，不用EAP连锁。

EAP-TEAP是长期佳解决方案，因为特别是做支持这些认证的类型，但是许多OS本地请求方仍然不支持EAP-TEAP自此天