如何获得 Windows 网络上授权用户的访问信息

www.isdecisions.com

IS Decisions
Secure & Master your Windows® Infrastructure™

如何获得 Windows 网络上授权用户的访问信息

IT 管理员常常要花费大量时间和精力解决**技术性运行中断**、**信息泄漏**和**意外的停机故障**。而很多时候，这些情况并非源于网络外部的攻击，而来自网络内部授权用户的不当操作。

那么，如何强化企业的 Windows 网络使之能够免于这些来自网络内部的威胁？

要想找到一个有效的问题解决方案，这里有三个必须满足的关键要点需要进一步分析.....

1. 保证网络安全而又不失便携性

用户监控与网络执行和预算一样，常常对 IT 管理员构成了巨大的技术和运作上的挑战。如何管理及保证网络安全而又不会对企业网络的关键因素造成影响——例如**数据的便携性**和日益流行的**自带设备**（**BYOD**）办公文化？今天的解决方案需要对所有会话类型实施有效监控，且要控制成本在可接受的范围内。

2. 确保符合相关规范

当下，许多企业都遵守某些标准以确保数据和信息受到保护。如何管理和启用资源，促进企业网络与相关规范的一致性，尤其是在当下日益复杂的商业和技术环境？

例如，对于从事信用卡交易或储存信用卡信息的企业来说，符合**支付卡行业**（**PCI**）**安全标准**正变得越来越重要。遵守 **PCI DSS**（**支付卡行业数据安全标准**）传达的信息就是你的系统是安全可靠的，客户可以信任你们，客户支付卡的任何敏感信息不会泄露出去。

PCI 标准规定：

- 定期对信息系统进行监控
- 对持卡人信用卡数据的所有访问进行跟踪和监控

承诺遵守这一标准进行审计可能会使一些企业疲于网络执行和维护，甚至陷入混乱。因为进行此类审计对网络安全性很较高要求，需要保证将所有持卡人的信用卡数据风险降到最低。

3. 对于 IT 安全事件快速反应

要预防所有的网络安全事件已然不太可能，因此，对于信息技术项目一个重要的部分就是：能否对任何事件做出快速反应。而事件处理的一个关键就是分析与事件相关的数据并快速准确地找到答案，例如：

- “谁登陆过服务器？”
- “是正确的身份认证吗？”
- “会话的源头在哪里？”
- “我需要关于服务器上所有活动的一份报告....！”
- “他本没有权限登录服务器的，怎么回事.....！”
- “使用的是什么协议？”
- “有没有人通过 iPad 获取认证？”
- “文件有被篡改吗？”
- “怎样才能阻止.....？”

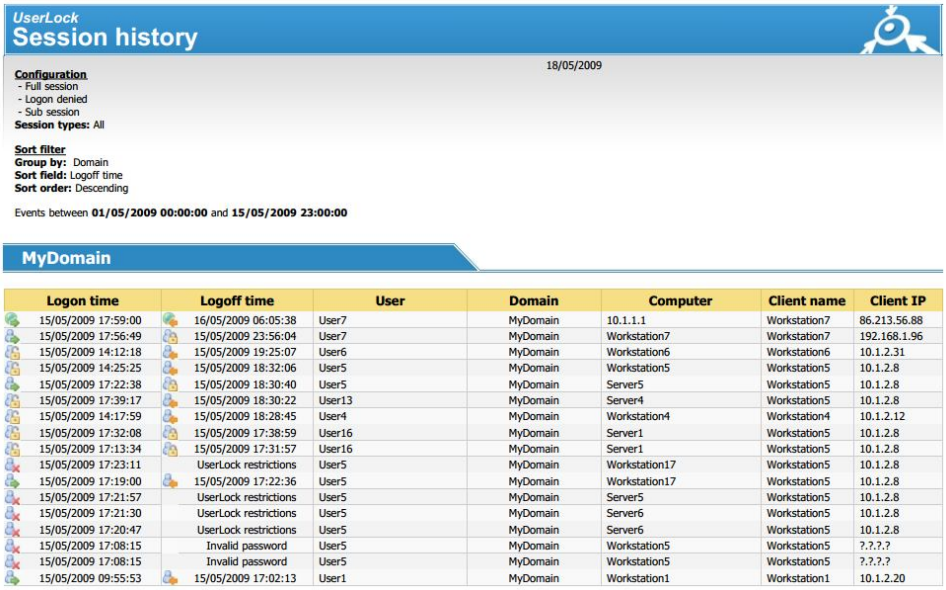
要解决以上问题需要满足的三个条件：**能够保证网络安全而又不失便携性， 能够确保符合相关规范，能对 IT 安全事件快速反应**。

或许作为读者的你也尝试过种种安全系统，一开始也能满足这些需求，但是时间一长，你发现这些最受追捧的安全系统在面对安全事件时也成了顾此失彼的“跛脚鸭”。

全球顶尖软件企业 IS Decisions 为决策者提供高效的软件解决方案，能满足主要的 IT 法规需求（ 如 **PCI 标准**），并为企业的 **Windows 基础架构**提供保护。

报告用户的会话活动——更快的取证

能够对所有用户的**会话活动**获取报告是 IS Decisions 的软件解决方案的一大优势。通过使用 IS Decisions 提供的 **UserLock** 和 **FileAudit** 这两个解决方案，你可以快速准确找到“谁登陆过服务器？”“是正确的身份认证吗？”“会话的源头在哪里？”等问题的答案，且提供强大的**安全监控**，对紧急情况能**快速响应**。



UserLock
Session history

18/05/2009

Configuration
- Full session
- Logon denied
- Sub session

Session types: All

Sort filter
Group by: Domain
Sort field: Logoff time
Sort order: Descending

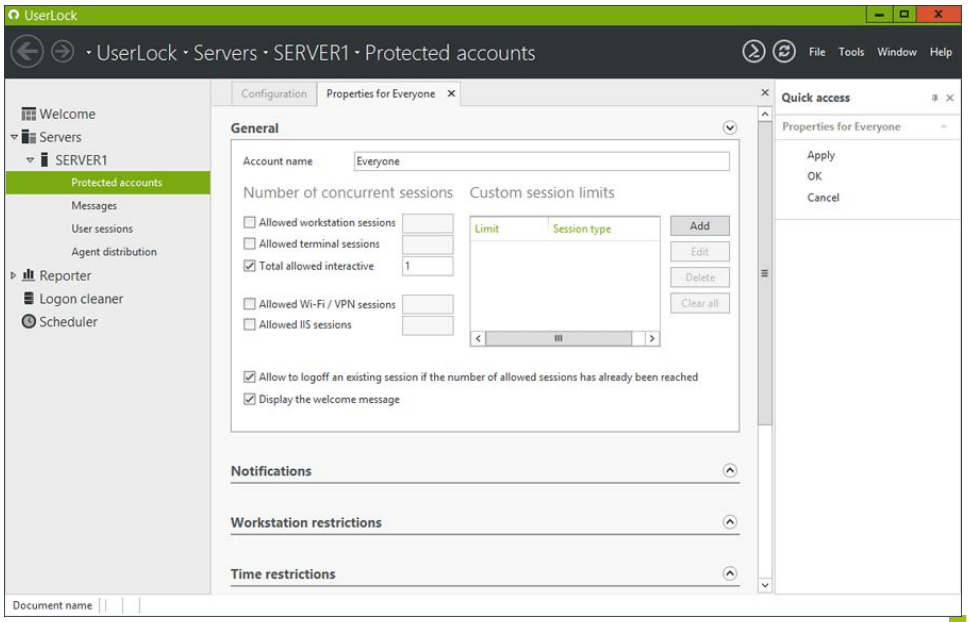
Events between **01/05/2009 00:00:00** and **15/05/2009 23:00:00**

MyDomain

Logon time	Logoff time	User	Domain	Computer	Client name	Client IP
15/05/2009 17:59:00	16/05/2009 06:05:38	User7	MyDomain	10.1.1.1	Workstation7	86.213.56.88
15/05/2009 17:56:49	15/05/2009 23:56:04	User7	MyDomain	Workstation7	Workstation7	192.168.1.96
15/05/2009 14:12:18	15/05/2009 19:25:07	User6	MyDomain	Workstation6	Workstation6	10.1.2.31
15/05/2009 14:25:25	15/05/2009 18:32:06	User5	MyDomain	Workstation5	Workstation5	10.1.2.8
15/05/2009 17:22:38	15/05/2009 18:30:40	User5	MyDomain	Server5	Workstation5	10.1.2.8
15/05/2009 17:39:17	15/05/2009 18:30:22	User13	MyDomain	Server4	Workstation5	10.1.2.8
15/05/2009 14:17:59	15/05/2009 18:28:45	User4	MyDomain	Workstation4	Workstation4	10.1.2.12
15/05/2009 17:32:08	15/05/2009 17:38:59	User16	MyDomain	Server1	Workstation5	10.1.2.8
15/05/2009 17:13:34	15/05/2009 17:31:57	User16	MyDomain	Server1	Workstation5	10.1.2.8
15/05/2009 17:23:11	UserLock restrictions	User5	MyDomain	Workstation17	Workstation5	10.1.2.8
15/05/2009 17:19:00	15/05/2009 17:22:36	User5	MyDomain	Workstation17	Workstation5	10.1.2.8
15/05/2009 17:21:57	UserLock restrictions	User5	MyDomain	Server5	Workstation5	10.1.2.8
15/05/2009 17:21:30	UserLock restrictions	User5	MyDomain	Server6	Workstation5	10.1.2.8
15/05/2009 17:20:47	UserLock restrictions	User5	MyDomain	Server6	Workstation5	10.1.2.8
15/05/2009 17:08:15	Invalid password	User5	MyDomain	Workstation5	Workstation5	?.?.?.?
15/05/2009 17:08:15	Invalid password	User5	MyDomain	Workstation5	Workstation5	?.?.?.?
15/05/2009 09:55:53	15/05/2009 17:02:13	User1	MyDomain	Workstation1	Workstation1	10.1.2.20

执行用户访问策略

使用 **UserLock**，企业可通过执行一个精确且定制化的用户策略即允许或拒绝登录来监控用户访问，且 UserLock 的**禁止并发登录**或多个登录的功能，使 Windows 网络能够避免这一潜在的危险。



对用户访问的监控和限制能够大大提高基础设施的安全性，帮助挫败网络内部的攻击，并避免要回答上述问题的情况。

监测所有网络访问

通过监控所有用户的访问，包括 **Wi-Fi 和 VPN 会话**，企业可以监控通过无线网络的访问，使用 UserLock 来**保障 Windows 网络的自带设备安全**。

获取用户访问信息

Userlock 授权给系统管理员获取所有用户的访问信息，并对不受欢迎的会话及用户访问策略执行严格控制。

IT 管理员可以依靠 UserLock 进行自动监控，如:

- 用户从何处登录
- 什么时间窗口进行登录
- 能否使用 WIFI、VPN 或 IIS
- 允许哪些会话类型
- 可以使用哪些协议