安全访问控制控制系统5.x及以后FAQ

Contents

Introduction

本文提供回答关于多数常见问题(FAQ)与思科安全访问控制系统(ACS) 5.x有关和以后。

认证相关问题

Q. ACS 5.x内部数据库的一些个用户/组能从用户密码策略(系统管理> Users被排除>认证设置) ？

A. 默认情况下，每个内部数据库用户必须符合用户密码策略。目前， ACS 5.x内部数据库的用户/组不可以被排除。

Q. ACS 5.x的一些个GUI管理员能从管理用户密码策略(系统管理>管理员>设置>认证)被排除？

A. 默认情况下，每个GUI管理用户必须符合管理用户密码策略。目前， ACS 5.x的管理用户不可以被排除。

Q. ACS是否5.x为VMWare工具提供技术支持？

A. No.目前， VMWare工具没有用ACS版本5.x支持。参考Cisco Bug ID CSCtg50048 (仅限注册用户)欲知更多信息。

Q. 当LDAP被配置作为身份存储时，什么是ACS的5.x支持的EAP身份验证协议？

A. 当LDAP使用作为身份存储时， ACS 5.2支持仅PEAP-GTC、EAP-FAST-GTC和EAP-TLS协议。它不支持EAP-FAST MSCHAPv2、PEAP EAP-MSCHAPv2和EAP-MD5。欲知更多信息，请参见认证协议和用户数据库兼容性。

Q. WLC的认证与在ACS的使用半径为什么发生了故障，并且ACS为什么没有显示任何失败的尝试？

A. 问题存在与**ACS 5.0和WLC互通性，**在补丁程序4.下载补丁程序8，并且应用在CLI前的补丁程序。请勿使用TFTP为了调整此问题。

Q. 为什么是无法恢复tar.gz备份与备份LOG in命令ACS 5.2的文件？

A. 您不能恢复备份用备份**LOG**命令的日志文件。您能恢复为ACS配置和ADE-OS备份了的仅那些文件。请参见**备份**和备份**日志**in命令Cisco Secure Access Control System 5.1的CLI参考指南欲知更多信息。

Q. 能否限制不成功的密码尝试的数量在ACS 5.2的？

A. No.此功能不是可用的在ACS 5.2，但是在ACS 5.3预计集成。请参见版本注释的功能没支持部分思科安全访问控制系统的5.2欲知更多信息。

Q. 我无法使用选项更改密码在内部用户的下登录ACS的5.0。如何解决此问题？

A. 在下登录ACS 5.0不支持更改密码的选项。此功能的技术支持有ACS 5.1及以后版本。

Q. 在ACS的此警报是什么意思？

```
Cisco Secure ACS - Alarm Notification
Severity: Warning
Alarm Name delete 20000 sessions
Cause/Trigger active sessions are over limit
Alarm Details session is over 250000
```

A. 此错误意味，当ACS视图达到250,000次会话时限制，投掷警报删除20,000次会话。ACS视图数据库存储所有上次认证会话，并且，当到达250,000时，产生一个警报清除高速缓冲存储器和删除20,000次会话。

Q. 我如何解决此错误信息：24407？

A. 当有密码管理的一个问题在SDI Authentication时，此错误信息出现。ACS 5.x，当RADIUS代理和用户必须由RSA服务器，验证使用。对RSA的RADIUS代理将仅工作，不用密码管理。原因是OTP值一定是可退回的由RADIUS服务器为了代理密码值对RSA服务器。当密码管理在隧道组中时被启用， RADIUS请求用MS-CHAPv2属性传送。RSA不支持MS-0CHAPv2;它支持仅PAP。

为了解决此问题，功能失效密码管理。欲知更多信息，请参见Cisco Bug ID CSCsx47423 (仅限注册用户)。

Q. 限制ACS admin管理在ACS 5.1内的仅某些设备是否是可能的？

A. 不，限制ACS admin管理在ACS 5.1内的仅某些设备是不可能的。

Q. ACS是否支持在认证的QoS，以便RADIUS可以在TACACS优先安排？

A. 不， ACS不支持在认证的QoS。ACS不会优先安排在TACACS或TACACS请求的RADIUS认证请求在RADIUS。

Q. 能ACS 5.x代理TACACS和RADIUS认证到其他TACACS或RADIUS服务器？

A. 是，所有ACS 5.x版本能代理RADIUS认证到其他RADIUS服务器。ACS 5.3和以后能代理TACACS认证到其他TACACS服务器。

Q. ACS 5.x能否检查激活目录用户的拨入属性为了准许访问？

A. 是，在ACS 5.3和以后您能允许，拒绝和控制用户的拨入许可的访问。在认证或查询期间从激活目录，权限被检查。它在激活目录投入的字典设置。

Q. ACS是否5.x支持CHAP或MSCHAP TACACS+的认证类型？

A. 是， TACACS+ CHAP和MSCHAP ACS版本5.3和以上支持认证类型。

Q. 能否设置ACS内部用户的密码类型为任何外部数据库？

A. 是，在ACS 5.3和以后您能设置ACS内部用户的密码类型。此功能是可用的在ACS 4.x。

Q. 能通过/失败根据用户在ACS内部身份存储被创建的时间的认证？

A. 是，在ACS 5.3和以后您能使用**几小时的数量，因为用户创建**属性为了创建您的策略。因为用户在当前认证请求的时期的内部身份存储被创建了此属性包含几小时的数量。

Q. 能否使用通配符为了添加在ACS内部数据库的新的主机条目？

A. 是，当您添加新的主机到内部身份存储时， ACS 5.3和以后允许您使用通配符。它也允许您输入通配符(在您输入前三个八位位组)后为了指定从被识别的制造商的所有设备。

Q. 配置在ACS 5.x的IP地址池和能否从ACS分配他们？

A. 不，创建在ACS 5.x的IP地址池是不目前可能的。

Q. 能看到请求进来失败的认证报告AAA客户端的IP地址？

A. 不，发现AAA客户端IP地址从请求进来是不可能的。

Q. 什么是View Log在ACS 5.3的消息恢复？

A. ACS 5.3提供一个新功能恢复丢失的所有日志，当视图发生故障时。ACS在其数据库收集这些丢失的日志并且存储他们。使用此功能，在视图是备份后，您能从ACS数据库检索丢失的日志到视图数据库。为了使用此功能，您必须设置日志消息恢复配置至**开**。欲了解更详细的信息在配置View Log消息恢复，请参见监控&报告查看器系统操作。

Q. 能否通过发出从解决方案引擎CLI的数据库压缩命令压缩ACS 5.x数据库？此功能是可用的在ACS 4.x。

A. 是，在ACS 5.3和以后，数据库**压缩**命令减少ACS数据库大小以选项删除ACS处理table.ACS管理员能发出此命令为了减少数据库大小。这帮助减少花费的数据库大小和时间的备份和为维护是需要的充分的同步。

Q. 能否搜索根据其IP地址的AAA客户端条目？

A. 是，使用其IP地址， ACS 5.3和以后允许您搜索网络设备。您能也使用通配符和范围为了搜索特

定的网络设备。

Q. 能否创造根据用户在ACS内部身份存储被创建的时间的条件？

A. 是，在ACS 5.3和以后您能使用**几小时的数量，因为用户**enable (event)配置策略规则条件的您，根据时间用户在ACS内部身份存储被创建的**创建**属性。例如：IF **group=HelpDesk&NumberofHoursSinceUserCreation>48**然后拒绝。因为用户在当前认证请求的时期的内部身份存储被创建了此属性包含几小时的数量。

Q. 能否登记身份存储用户在服务策略的授权部分验证？

A. 是，在ACS 5.3和以后您能使用**认证身份存储**属性， enable (event)配置策略规则条件的您根据认证身份存储。例如：IF **AuthenticationIdentityStore=LDAP_NY**然后拒绝。此属性包含使用的身份存储的名字，并且用相关身份存储名称更新在成功的验证以后。

Q. ACS什么时候去在身份存储顺序定义的下身份存储？

A. ACS去在身份存储顺序在这些情况下定义的下身份存储：

- 用户没有在第一身份存储找到
- 身份存储不是可用的在顺序

Q. 什么是在ACS 5.3的帐户不合格策略？

A. 帐户不合格策略允许您禁用内部身份存储的用户，当配置的日期是在允许的日期之外时，几天的配置的号码是在允许的日之外，或者连续的不成功的登录尝试的数量超出阈值。DEFAULT值在日期超出从当前日期的30天。DEFAULT值好几天不应该超过从当前日的60天。DEFAULT值失败的尝试的是5。

Q. 能否更改ACS的内部数据库用户的密码在telnet的？

A. 是，您允许更改使用在telnet的一个内部数据库用户的密码TACACS+。您需要选择**Enable (event) TELNET更改密码**在ACS 5.x的**密码更改控制下**。

Q. 当配置更改了时，主要的ACS 5.x实例是否周期地自动地更新备份实例或者应该它只发生？

A. ACS 5.x将立即复制对附属ACS，每当您在主要的ACS做变动。另外，如果然后不做对主要的ACS的任何变动，它将执行强制复制每15分钟。这时，没有控制计时器的选项，以便ACS能在特定时间之后复制信息。

Q. 能查看/导出关于ACS从在不同的NAS客户端的ACS当前登陆并且验证所有用户的5.x的报告？

A. 是，这是可能的。有RADIUS和TACACS+的两个独立的报告。您能找到他们在**监控&报告>报告>目录>会话Directory> RADIUS激活的会话**和**TACACS激活的会话下**。两个报告根据从NAS客户端的记帐信息，因为允许您跟踪，当用户连接和退出时。在一特定日期间，会话历史记录甚而允许您从开始获得信息和终止消息。

Related Information

- 思科安全访问控制系统支持页面
- Technical Support & Documentation - Cisco Systems