Search our Knowledge base, Community, and more...

PI AF Server和安全性：为什么域优于工作组

适用于：

0 0

解决方案未经验证 - 更新于 2019年 6月3日 - 英语

问题

内容来自KB00824

此KB的此内容最初发布为2013年1月技术支持时事通讯技术提示。

在本文中，我们将探讨PI AF Server在工作组中托管时对其的影响。具体而言，我们将了解安全管理的后果，对多层身份验证方案施加的限制，以及在工作组与域中托管时禁止远程管理PI AF Server的限制。

有关与PI Server的类似讨论，请参阅KB 3246OSI8。 (https://osisoft.lightning.force.com/lightning/articles/Knowledge/3246OSI8)

环境

解

额外的安全管理

在Windows域环境中设置PI AF Server可利用Active Directory（AD）对用户凭据的集中管理。在Windows工作组中，此功能不可用。由于PI AF Server是为支持Windows Integrated Security而构建的，因此为了在Windows Workgroup环境中访问PI AF Server，必须将客户端计算机上的本地用户（相同的用户和密码）复制到PI AF Server。使用此配置，PI AF Server的客户端连接（例如PI System Explorer）需要两倍的维护。但是，对于域，所有域用户都在一个Active Directory环境中进行管理，从而减少了用户凭据的维护时间（图1）。

st-widget- {image：afdomain.png}

图1. Workgroup与Domain中的用户名和密码管理。

分散式安全性设置还可能使PI MDB与PI AF同步过程复杂化。考虑到PI模块数据库中的每个模块的安全访问都被复制到相应的PI AF元素，反之亦然，可以快速理解这种复杂程度。因此，要开始成功将PI MDB同步到PI AF Server，必须在PI Server和PI AF Server上复制所涉及的本地用户。

为避免此复杂性，建议将PI Server和PI AF Server放在同一个域或受信任域或受信任林中。有关此内容的更多详细信息，请参阅"配置PI Server安全性"用户手册。

此外，要连接PI AF Server服务和PI AF SQL数据库的独立安装，必须打开与SQL Server的远程连接，并且如果未实现本地用户复制，则允许SQL Server身份验证。这里重要的一点是，PIFD数据库生成的SQL Server登录用户的凭据必须存储在PI AF Server配置文件的连接字符串中。虽然限制对此配置文件的访问可以防止向未授权用户泄露用户和密码，但与使用域用户运行PI AF Server服务相比，这是一种不太安全的方法。有关在同一域，受信任域，不受信任的域中安装PI AF Server服务和PI AF SQL数据库时所需内容的更多详细信息，

多层安全功能的限制

在某些情况下，使用工作组还可能会限制在PI Server中保护数据的功能。特别要考虑一个设置，其中：

- 客户端从托管PI WebParts的Web服务器访问PI AF数据
- 用户的浏览器，SharePoint Server（托管PI WebParts）和PI AF Server都在不同的计算机上。

如果我们在Workgroup环境中实现此体系结构（如图2所示），则不会对最终用户强制执行正确的权限，因为工作组无法使用Kerberos，并且NTLM无法执行双跃点身份验证。

为了澄清在这种情况下会发生什么，浏览器使用的凭据将传递给PI WebParts管理进行身份验证，假设在两台计算机上手动复制本地用户; 但是，这不会传递给PI AF Server。相反，运行MS SharePoint站点的应用程序池用户将传递到PI AF Server进行身份验证。最终，从浏览器进行查询的最终用户将继承SharePoint应用程序池用户的访问权限。

st-widget- {image：dh.png}

图2.尝试通过Workgroup环境中的Sharepoint服务器访问AF数据的Web浏览器客户端。

这可以通过将初始用户从客户端计算机传递到PI AF Server以使用Kerberos双跃点身份验证进行身份验证来避免，这在域环境中是可能的。有关详细信息以及如何设置，请参考KB00599 (https://customers.osisoft.com/s/knowledgearticle?knowledgeArticleUrl=KB00599)。

远程管理的限制

如果使用属于本地Administrators组的本地帐户远程访问计算机，PI AF Server的管理员将被拒绝提升权限。这是Windows中的UAC（用户访问控制）安全功能（Microsoft KB 951016 (http://support.microsoft.com/kb/951016)）的结果。例如，如果仅允许本地管理员组进行此类编辑，则UAC将阻止PI AF数据库上的安全权限编辑（通过与PI System Explorer的远程连接）。但是，UAC不会限制远程登录到PI AF Server的域用户的此类编辑。

域和工作组中的PI Server

有关使用PI Server的域和工作组的类似讨论，请参阅KB 3246OSI8。 (https://osisoft.lightning.force.com/lightning/articles/Knowledge/3246OSI8)

原因