IBM 关于 Lotus Domino HTTP 密码散列安全性的说明和最佳实践

本文档是IBM针对目前倍受关注的互联网信息中心（CN Cert）发布的关于Lotus Domino 目录中存储的HTTP密码散列安全问题的技术说明，在此基础上，介绍了Lotus Domino 8.5及最新版本在HTTP 密码安全性的保护方面的改进，并提出关于如何加强对HTTP密码保护的最佳实践和建议。

Lotus Domino HTTP 密码散列加密的相关说明

Lotus Domino/Notes平台对于用户的HTTP密码存储的实现是把HTTP密码经过散列加密处理以后，把散列值保存在用户的个人文档中。把密码散列值保存在Domino目录中不代表这些密码一定会被破解。Domino目录所保存的HTTP密码都是经过散列加密的处理，这些散列值采用了高强度的、单向的加密算法，是不可逆的。当然如果从暴力破解方面来考虑，暴力破解不仅仅是对Lotus Domino才会造成威胁，任何的应用软件不管它把密码保存在什么地方，这些密码都是有可能受到被暴力破解的威胁。

在十几年前，支持Web访问的第一个Domino版本所保存的HTTP密码的格式采用了安全较低的加密算法。在这种算法对一个固定的密码字符串处理时，每次产生的散列值都是一样的。例如，字符串“password”经过散列加密处理以后所生成的散列值是“355E98E7C7B59BD810ED845AD0FD2FC4”。从Domino 4.6版本以后，Domino采用更加安全的散列加密算法，这种新的算法在做加密的过程中都添加了随机因子，也就是说同一个字符串每次加密处理以后都是不一样的值。旧的散列加密算法容易被暴力破解或者受到字典式的攻击。Domino出于向前兼容的原因目前还支持这种加密方式。同时提供了新的更加安全的密码格式的支持。

Lotus Domino从8.5及后续的版本中默认启用了“使用更加安全的因特网密码”，默认对HTTP密码采用了安全性较高的散列加密，从而确保了HTTP密码的更高的安全性。而对于Domino8.5之前的版本，虽然Lotus Domino提供了新旧两种加密方式的支持，默认还是采用旧的方式，为了确保HTTP密码不受到暴力破解的攻击，对于Domino 8.5之前的版本需要管理员手动设置Domino目录概要文档，启用“使用更加安全的因特网密码”并确认所有的个人文档都使用新的格式。

Lotus Domino 8.5 及以后版本对 HTTP 安全性的改进

Lotus Domino一直致力于对HTTP密码安全方面的保护，以下是Lotus Domino 在Lotus Domino8.5及以后的版本中，Lotus提供了“强制因特网密码锁定”的设置，此功能可以针对用户在特定时间内达到错误的密码尝试次数以后对此用户进行锁定，管理员可以通过设置此功能来更好的防范字典式的密码猜测的攻击。

在Lotus Domino8.5及以后的版本中，Lotus Domino默认启用了“使用更加安全的因特网密码”，从而保证在8.5及以后的版本中储存的用户密码是使用了更加安全的加密方式。

基于以上的考虑，IBM建议客户考虑把服务器升级到8.5系列的最新版来更好地确保HTTP密码具有更高的安全性。

Lotus Domino HTTP 密码安全性的最佳实践

IBM公司非常关注信息安全方面的保护。IBM公司一直致力于给客户提供一套完整的工具来保护我们客户企业数据的安全。基于这方面的考虑，Domino提供了几种可选的配置来防范甚至完全消除暴力破解的风险。我们鼓励每一个客户检查系统的相关配置并根据企业的实际情况来选择最适合自己企业的安全保护配置。

下面是可采用的配置方式及详细的步骤：

1. 严格控制服务器names.nsf的访问权限
   在Domino服务器的names.nsf的存取控制列表对话框上，将 Anonymous 设置为“无访问权限”，将 -default- 设置为“读者”的访问权限
2. 利用“扩展ACL（XACL）”的功能来防止读者读取http散列值（关于如何启用XACL，请参考附件）
3. 启用更加安全的因特网密码加密方式
   打开Domino的names.nsf, 操作菜单 —>编辑目录概要文件 ->“使用更安全的因特网密码”域中选择“是”，保存并关闭
   请注意：
   此设置只针对设置以后所存储的HTTP密码生效，对于原有的个人文档则需要管理员选中个人文档，操作菜单 -> 升级到新的Internet密码格式。
   在Domino8.5及以后的版本默认启用了更加安全的因特网加密方式。如果所有的用户都是在Domino8.5及以后的版本注册的，管理员不需要做任何的操作。否则，建议管理员选中所有的个人文档，选择升级到新的Internet密码格式。

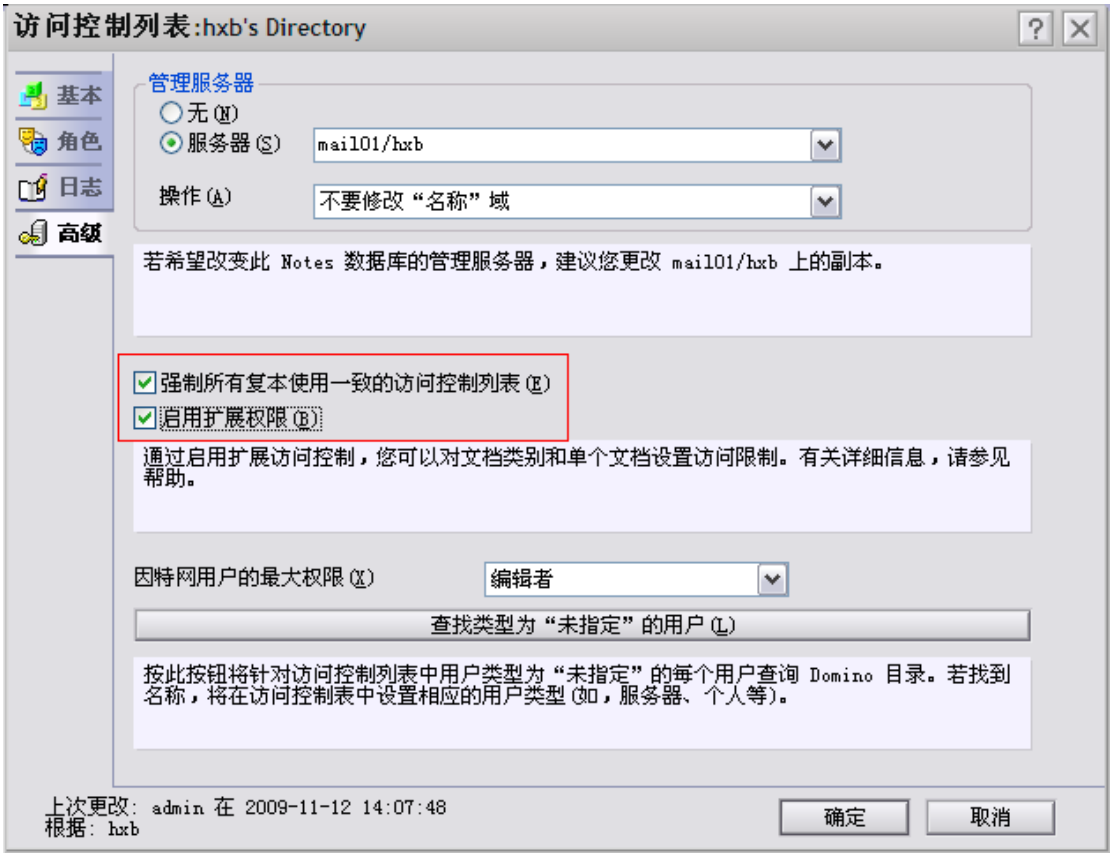
4. 启用“强制因特网密码锁定”来防止Domino受到字典式的攻击（“强制因特网密码锁定”是Domino 8及以后版本的新功能）
   要启用此选项，打开服务器的配置文档，安全性附签
5. 通过公司政策来强制用户使用高强度的密码，要求不低于8位，混合使用大小写字母、数字和符号。
   从Domino管理设置方面，管理员可以通过安全策略来统一部署密码策略
6. 在Domino Designer中打开“Person”表单，选择“Design”，选择“Form Properties”，在第二个选项卡中，禁用“Generate HTML for all fields”选项，隐藏网页源代码中的密码散列字段
7. 对http密码采用新的"@Password3"的功能，"@Password3"会使得黑客猜测密码的速度比"@Password2"要慢成千上万倍。原有的"@Password"的功能仅仅被Domino4.6及之前的版本所使用，建议客户只有在需要支持4.6版本的环境才使用此选项。
8. 对安全性要求更高的公司，可以考虑把HTTP密码删除并使用客户端证书来进行用户验证

附件：利用“扩展 ACL（XACL）”的功能来防止读者读取 http 散列值的操作步骤

1. 启用扩展的 Domino 目录访问

   1.1 使用管理员 ID 打开 Domino 目录数据库 names.nsf, 文件－>应用程序（数据库）－>访问控制

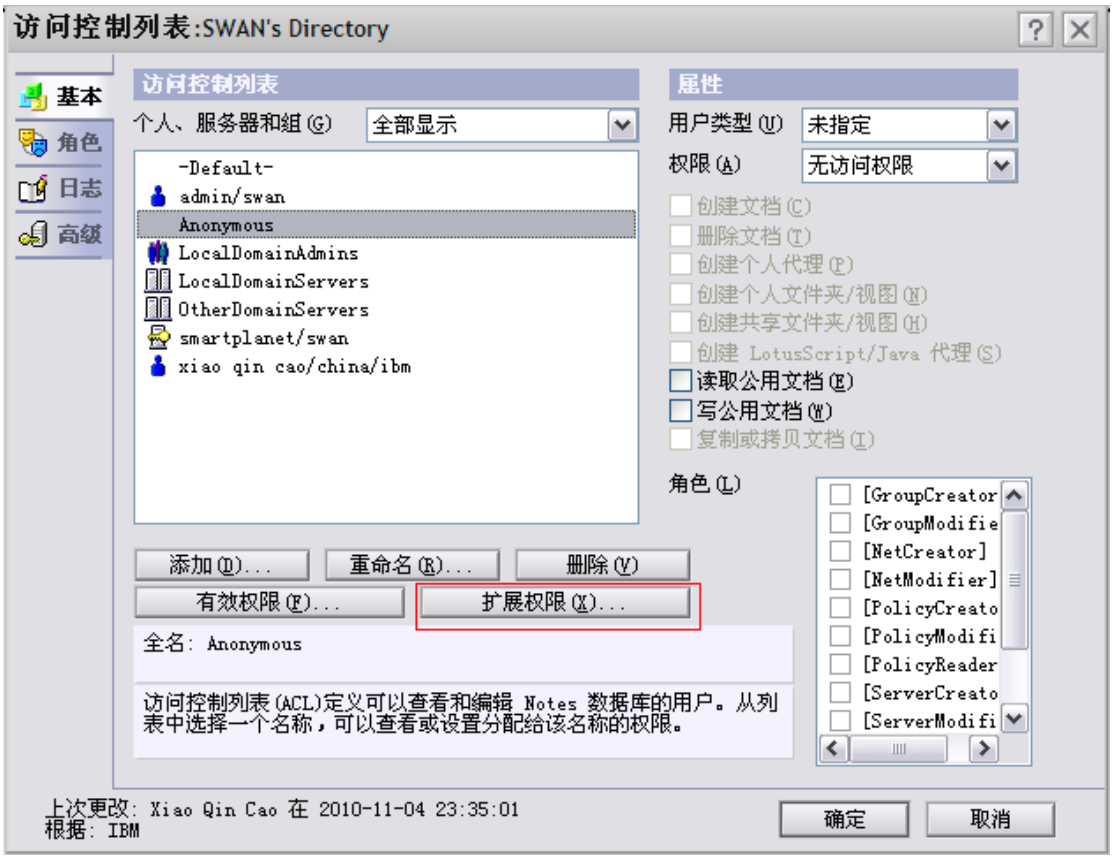
   1.2 点击“高级”，启用“强制所有复本使用一致的访问控制列表（E）”及“启用扩展权限”，点击“启用扩展权限”以后会出现两个对话框，分别选择“是”和“确定”



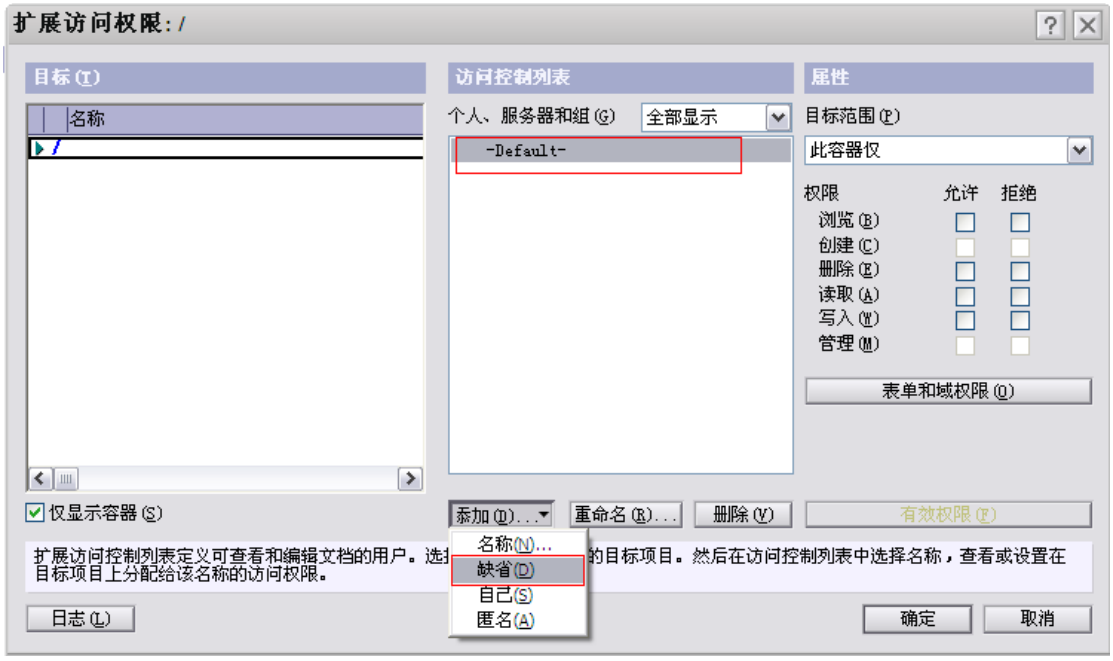
   1.3 点击“确定”来关闭访问控制列表对话框，此时会出现另一个对话框提示“启用扩展访问控制的限制可能需要一定时间”，点击确定

2. 通过扩展权限来进一步限制用户对 HTTP 密码的访问

   2.1 使用管理员 ID 打开 Domino 目录数据库 names.nsf, 文件－>应用程序（数据库）－>访问控制，出现对话框以后点击“扩展权限”，如下图所示

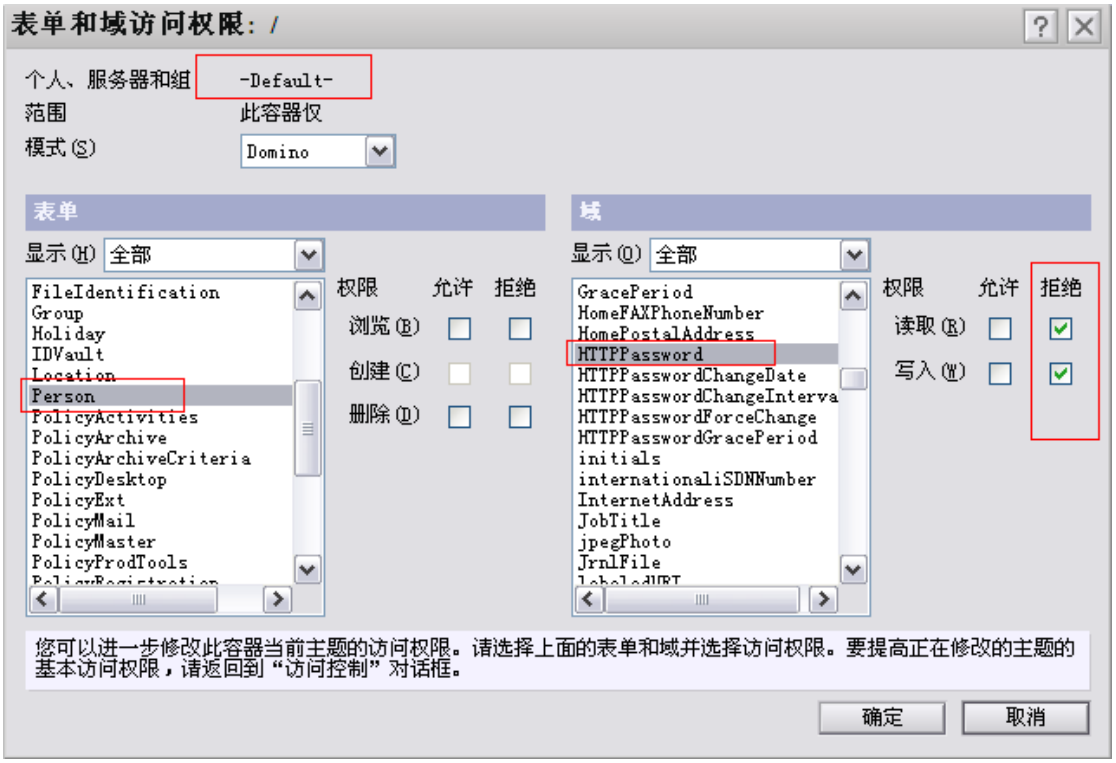


2.2 在扩展访问权限对话框中，点击“添加” “缺省”



2.3 点击“表单和域权限”进入“表单和域访问权限：/”对话框，选择“Person”表单，并选择“HTTPPassword”域，在“读取”和“写入”权限中都设置“拒绝”的权限，如下图所示

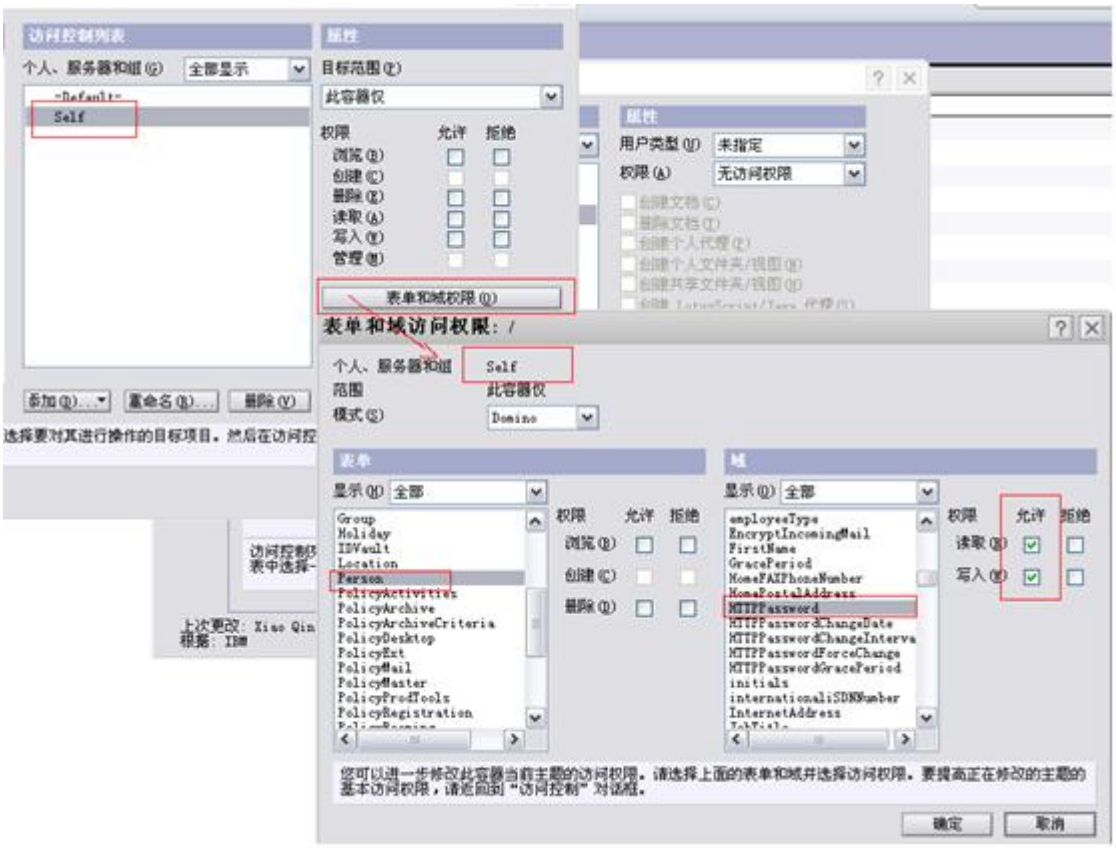
如果是 8..5 以前的版本，同时还需要对“dspHTTPPassword”域设置拒绝读取和写入的权限。



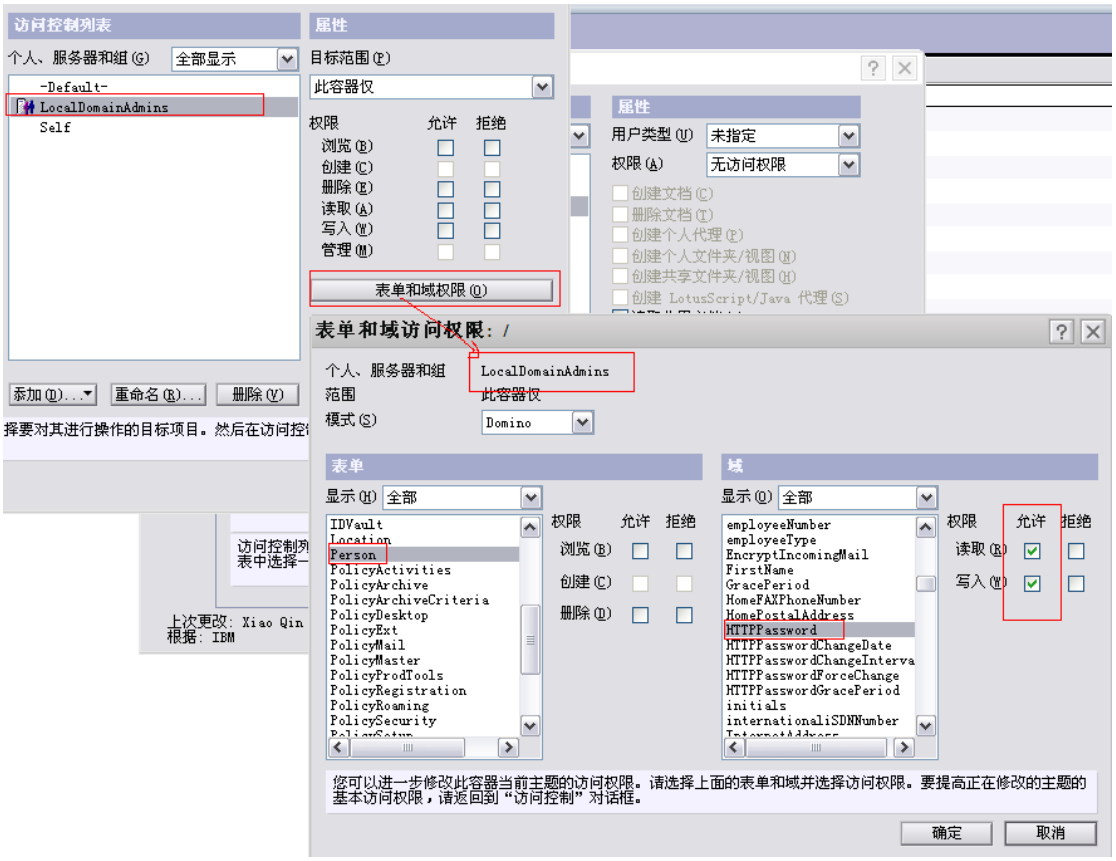
2.4 重复 2.2 – 2.3 的操作，分别对“自己 Self” “LocalDomainAdmins”和“LocalDomainServers”,针对“Person”表单的“HTTPPassword”域及“dspHTTPPassword”设置“允许”的权限，如下列图所示

（Domino8.5 及以后的版本不在存在 dspHTTPPassword 域）

设置“自己 Self”的扩展权限



设置 LocalDomainAdmins 群组的扩展权限，如果客户的管理员群组是别的名称，则此处的名称应该是公司管理员群组的名称



设置 LocalDomainServers 的扩展权限