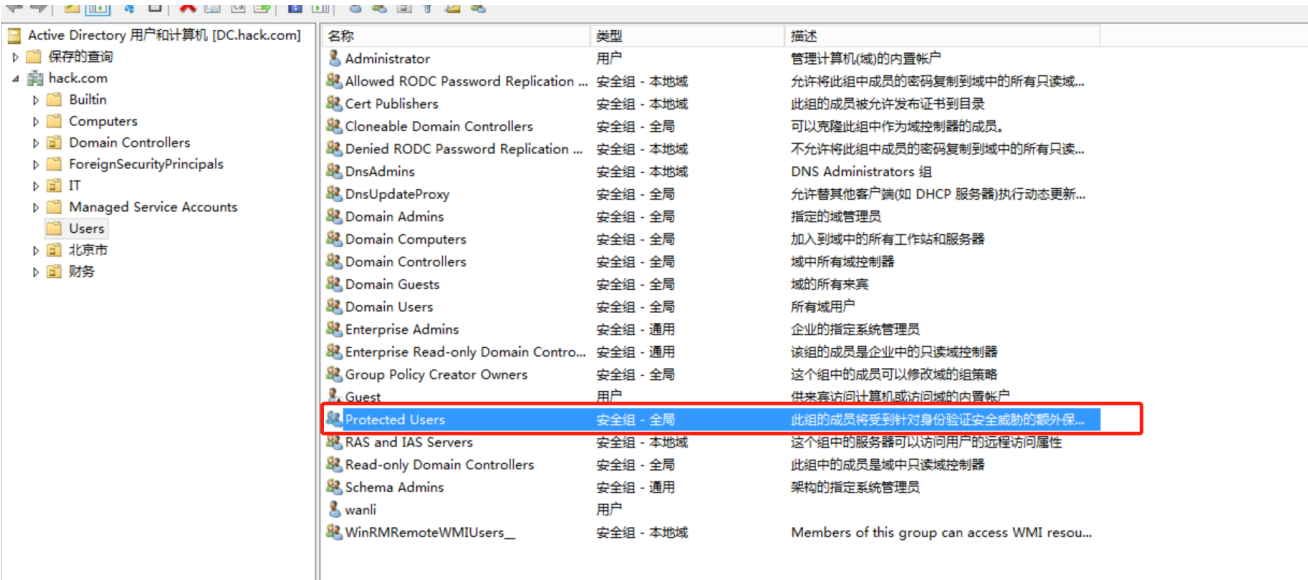


# 密码防范

## 2012R2域控设置

在windows server 2012 R2中，新增了一个Protected Users 安全组，将用户加入到该组，用户的明文密码就不会被获取



The screenshot shows the Active Directory Users and Computers console for the domain DC.hack.com. The left pane shows the tree structure with 'Users' selected. The right pane displays a list of groups with columns for Name, Type, and Description. The 'Protected Users' group is highlighted with a red rectangle.

名称	类型	描述
Administrator	用户	管理计算机(域)的内置帐户
Allowed RODC Password Replication ...	安全组 - 本地域	允许将此组中成员的密码复制到域中的所有只读域...
Cert Publishers	安全组 - 本地域	此组的成员被允许发布证书到目录
Cloneable Domain Controllers	安全组 - 全局	可以克隆此组中作为域控制器的成员。
Denied RODC Password Replication ...	安全组 - 本地域	不允许将此组中成员的密码复制到域中的所有只读...
DnsAdmins	安全组 - 本地域	DNS Administrators 组
DnsUpdateProxy	安全组 - 全局	允许替其他客户端(如 DHCP 服务器)执行动态更新...
Domain Admins	安全组 - 全局	指定的域管理员
Domain Computers	安全组 - 全局	加入到域中的所有工作站和服务器
Domain Controllers	安全组 - 全局	域中所有域控制器
Domain Guests	安全组 - 全局	域的所有来宾
Domain Users	安全组 - 全局	所有域用户
Enterprise Admins	安全组 - 通用	企业的指定系统管理员
Enterprise Read-only Domain Contro...	安全组 - 通用	该组的成员是企业中的只读域控制器
Group Policy Creator Owners	安全组 - 全局	这个组中的成员可以修改域的组策略
Guest	用户	供来宾访问计算机或访问域的内置帐户
Protected Users	安全组 - 全局	此组的成员将受到针对身份验证安全威胁的额外保...
RAS and IAS Servers	安全组 - 本地域	这个组中的服务器可以访问用户的远程访问属性
Read-only Domain Controllers	安全组 - 全局	此组中的成员是域中只读域控制器
Schema Admins	安全组 - 通用	架构的指定系统管理员
wanli	用户	
WinRMRemoteWMIUsers__	安全组 - 本地域	Members of this group can access WMI resou...

## 安装KB2871997

2014年，Microsoft发布了KB2871997补丁，它主要囊括了Windows 8.1和Windows Server 2012 R2中增强的安全保护机制。所以，以往的例如：Windows 7，Windows 8，Windows Server 2008R2和Windows Server 2012也可以更新该补丁后获得上述安全保护机制。该补丁无法阻止“哈希传递”的攻击方式，但其确实有助于是Windows免受一些常见的攻击，例如：明文密码脱取、RDP凭据盗取、盗取本地Administrator账户进行横向移动。

## 修改注册表

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 0 /f 关闭
```