N-Partner

N-REPORTER

用户如何使用 WMI 管理配置 Windows AD Server 日志

V 1.1.2 (简体)

Update: 2016/2/2

前言

本文件描述 N-Reporter 用户如何使用 WMI 管理配置 Windows AD Server 日志。

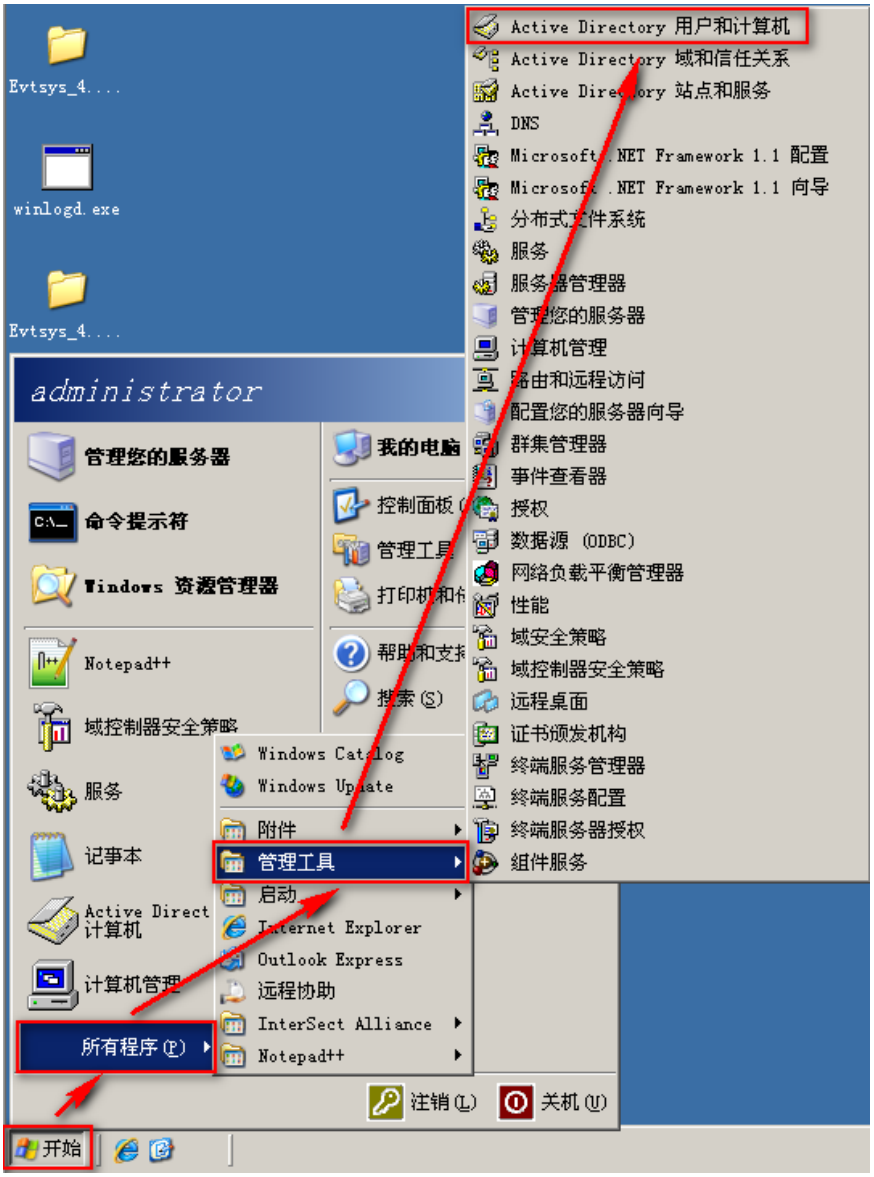
文件章节如下：

1.配置 Windows AD Server

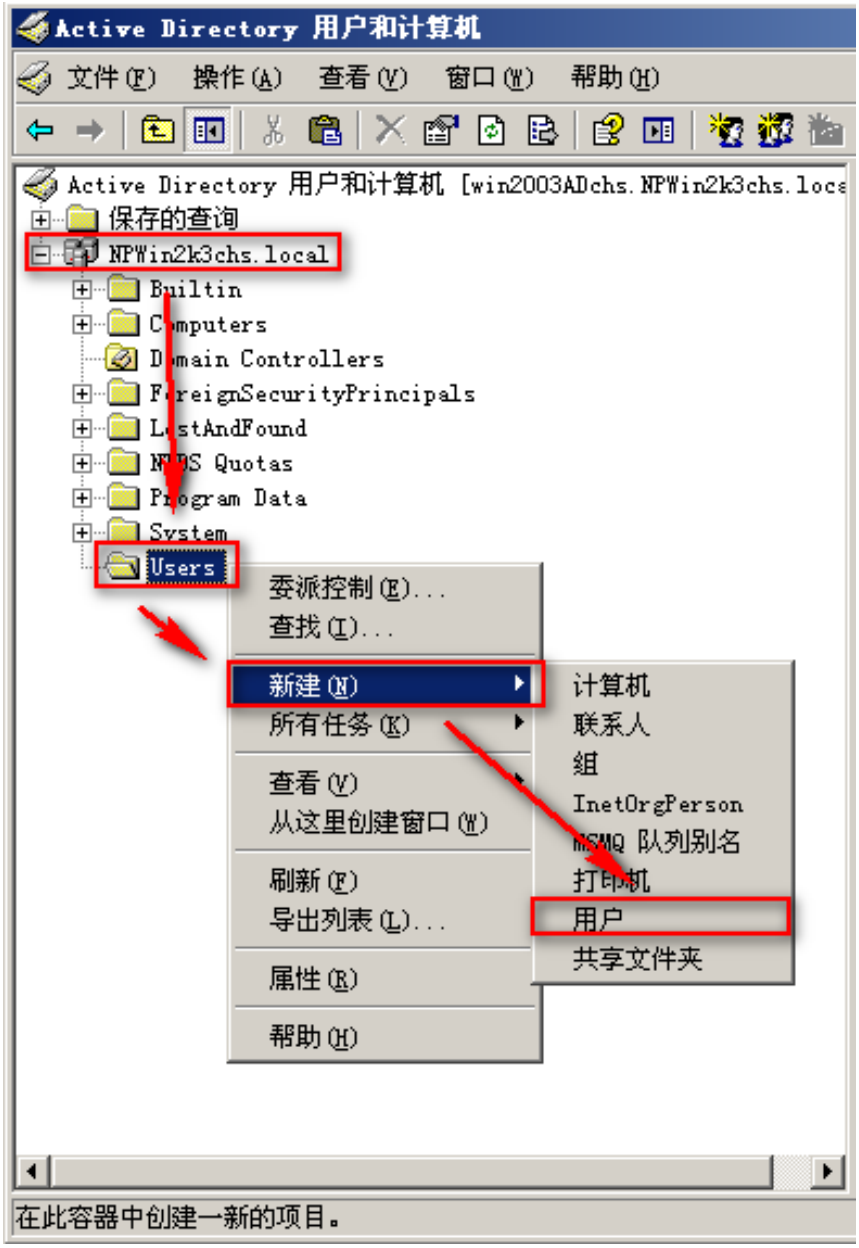
1-1 配置 Windows 2003 AD Server

1-1-1 新增 WMI 远程登录的域用户

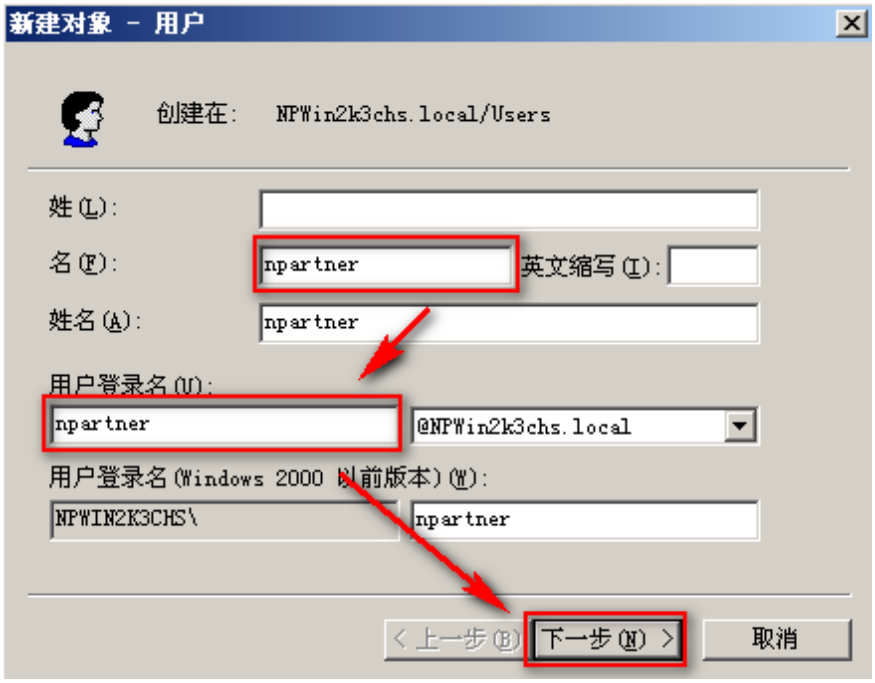
以域管理员账号 administrator 登录Windows AD server，鼠标左点 [开始 / 所有程序 / 管理工具 / Active Directory 用户和计算器]。



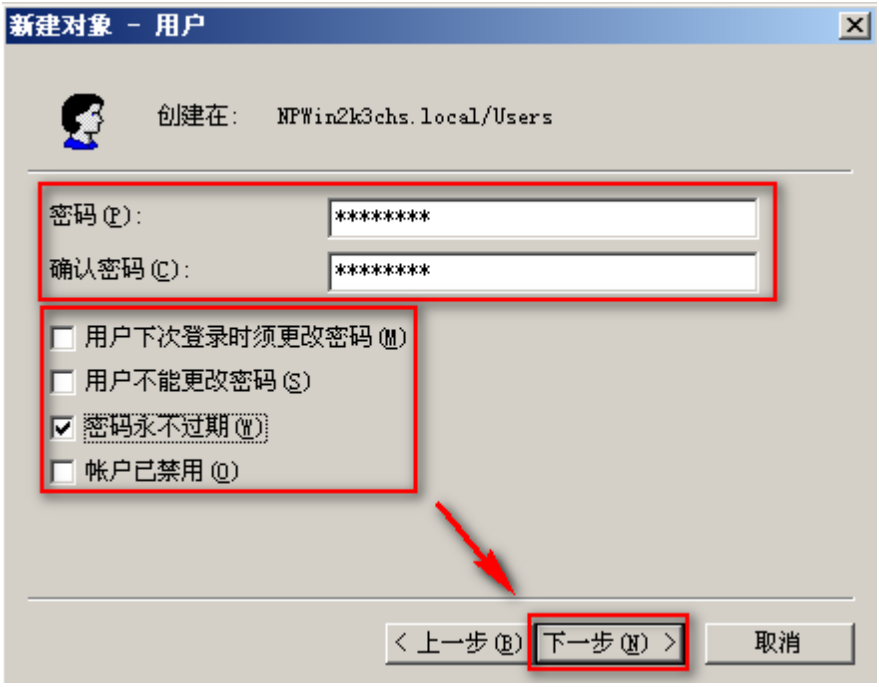
鼠标左点根域(forest root domain)，本例为 NPWin2k3chs.local。右点[Users]，左点[新建 / 用户]。



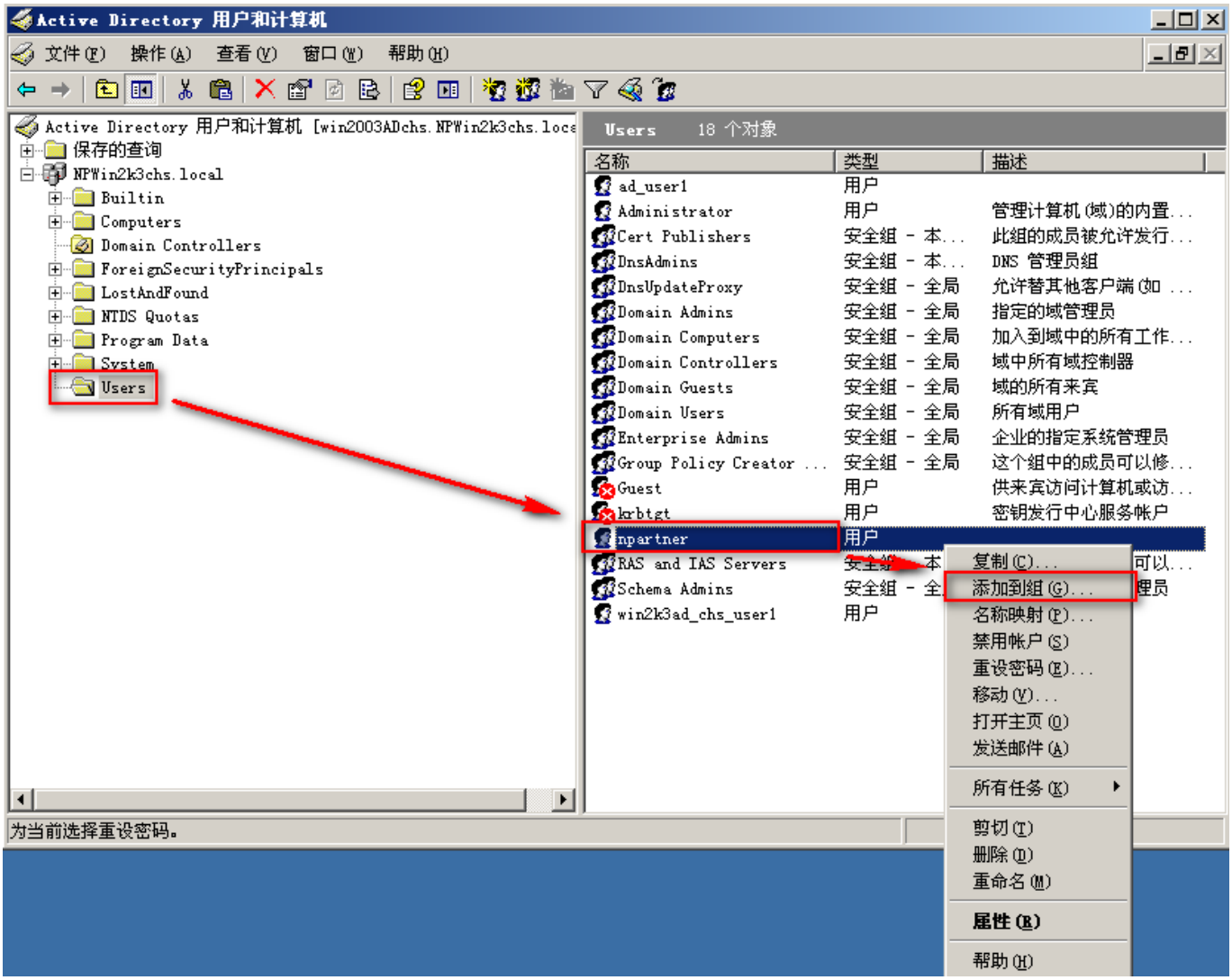
名输入"npartner"，用户登录名输入"npartner"，左点[下一步]。



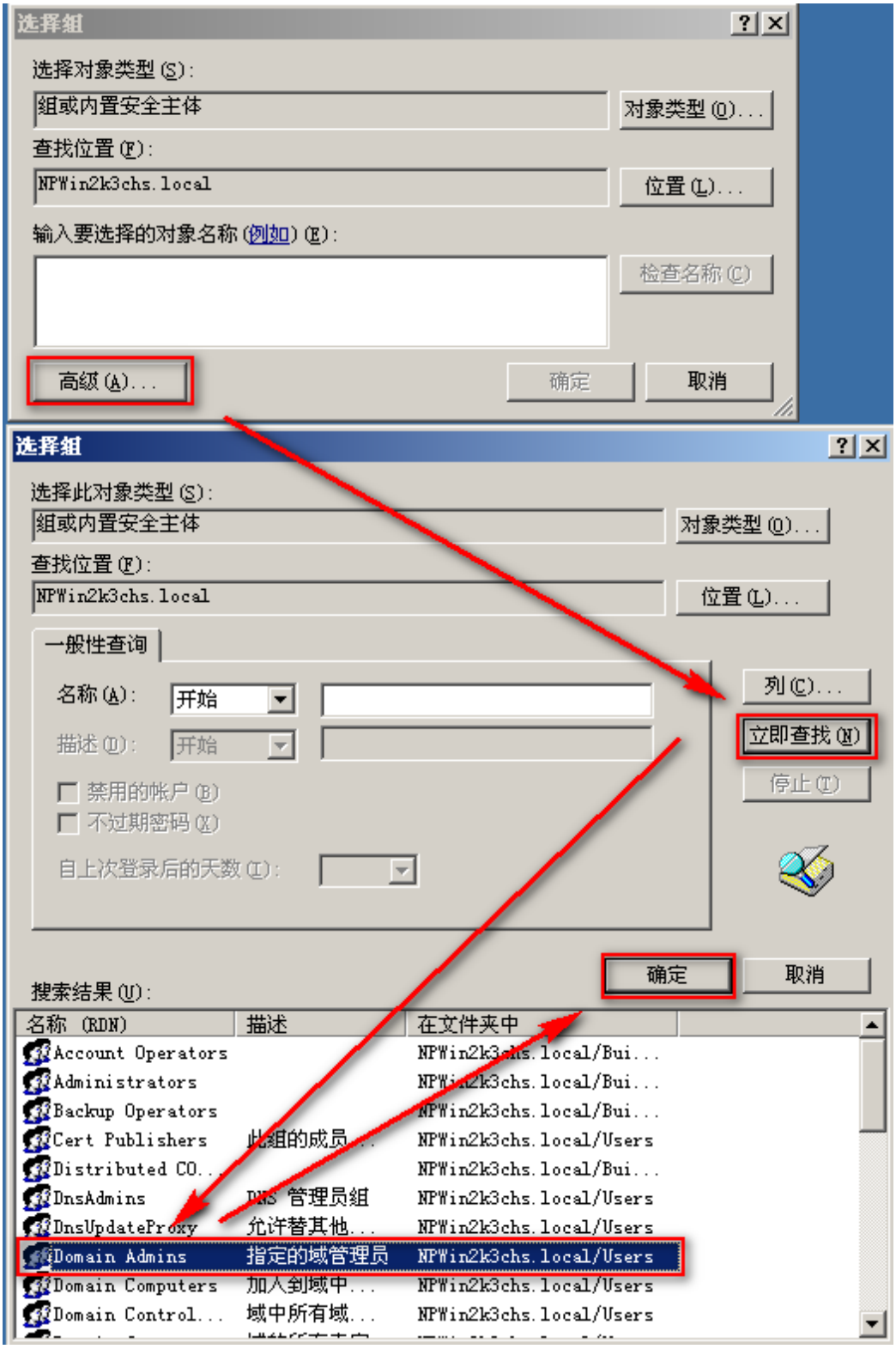
输入密码。只勾选[密码永不过期]。左点[下一步]。左点[完成]。



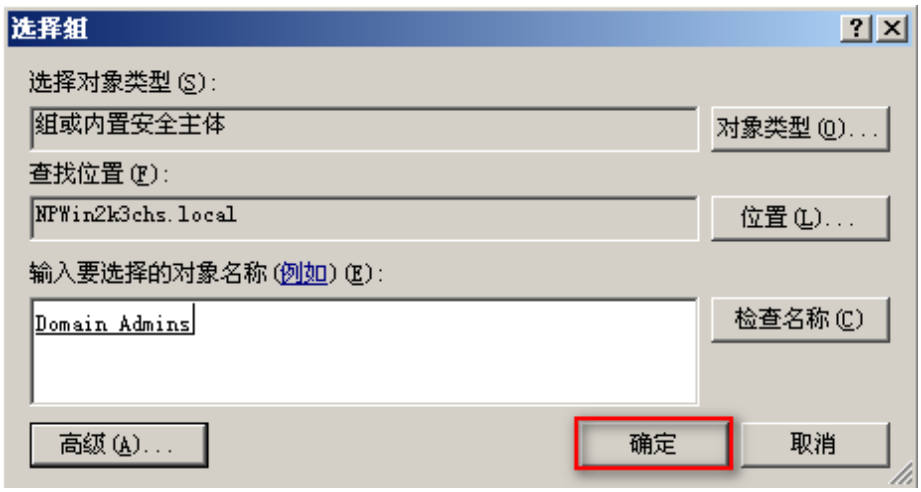
鼠标左点 [Users]。右点 WMI 远程登录用户 npartner，左点[添加到组]。



鼠标左点[高级 / 立即查找 / Domain Admins / 确定]。将 WMI 远程登录用户 npartner 加入到域管理员组中。



左点[确定]。



1-1-2 Windows 2003 AD Server 审核配置

请依照文件「Windows AD audit to syslog」第 2 章「Windows 2003 AD Server 审核配置」，配置默认域控制站(Default Domain Controller)的审核策略(Policy)。

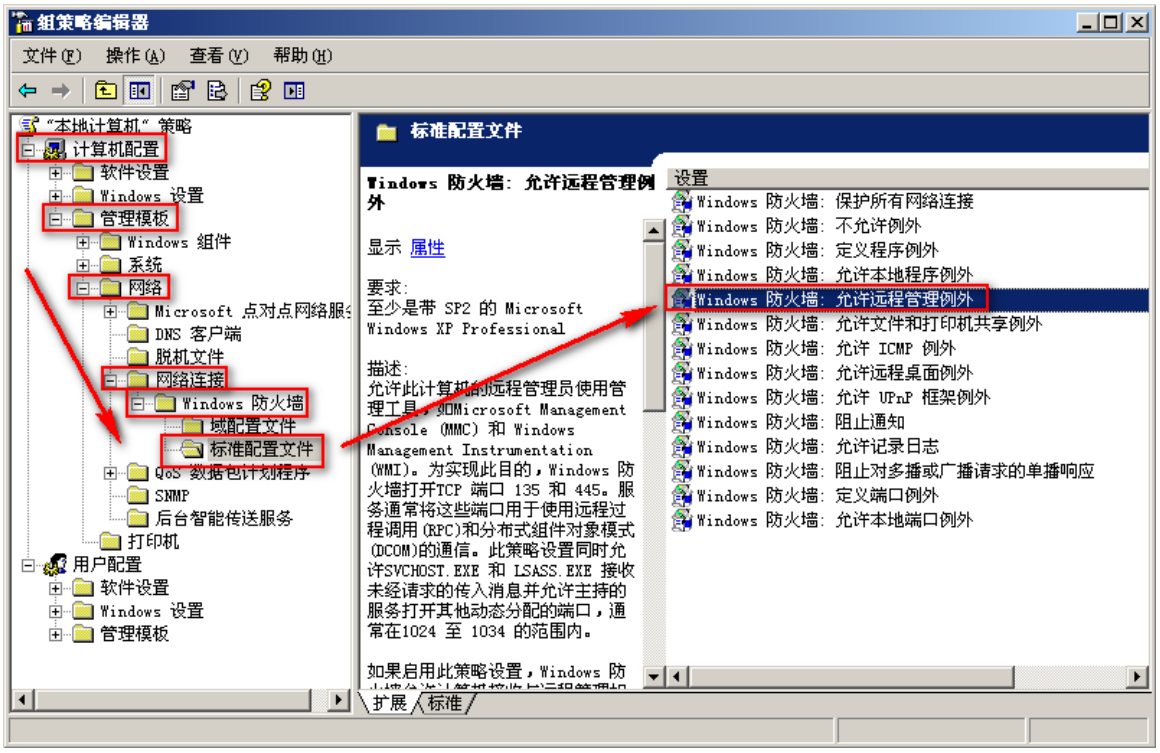
1-1-3 Windows 2003 AD Server 防火墙配置

鼠标左点[开始 / 所有程序 / 附件 / 命令提示符]。

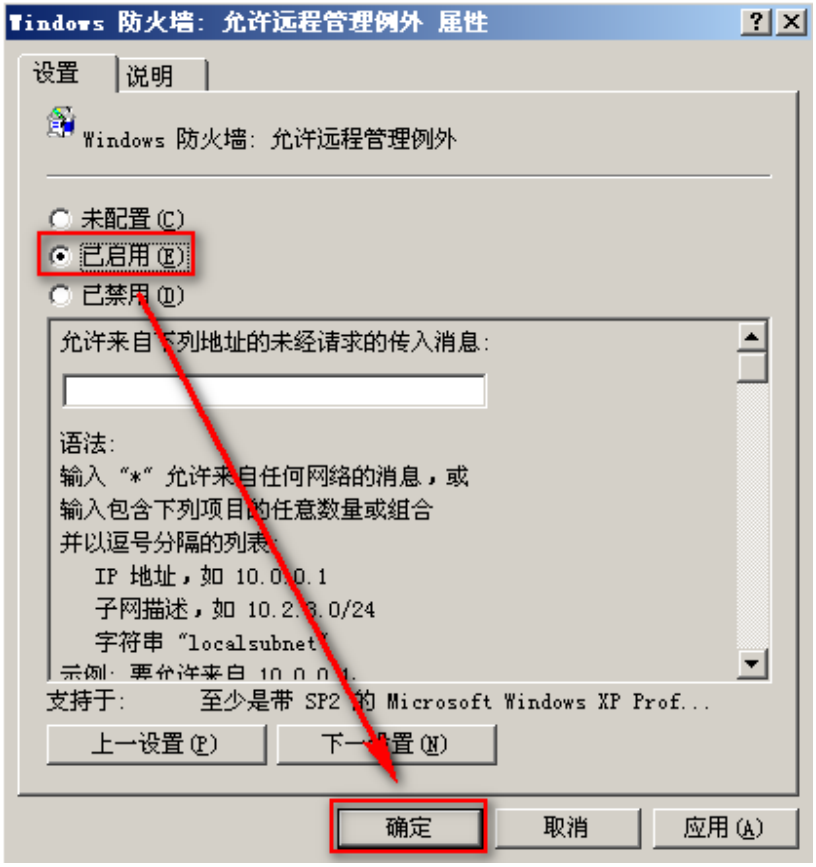
输入『gpedit.msc』，开启[组策略对象编辑器]设定[本机计算器原则(Local Computer Policy)]。

鼠标双击 [计算器配置 / 管理模板 / 网络 / 网络连接 / Windows 防火墙 / 标准配置文件]。

双击[Windows 防火墙: 允许远程管理例外(Windows Firewall: Allow remote administration exception)]。



勾选[已启用]，左点[确定]。

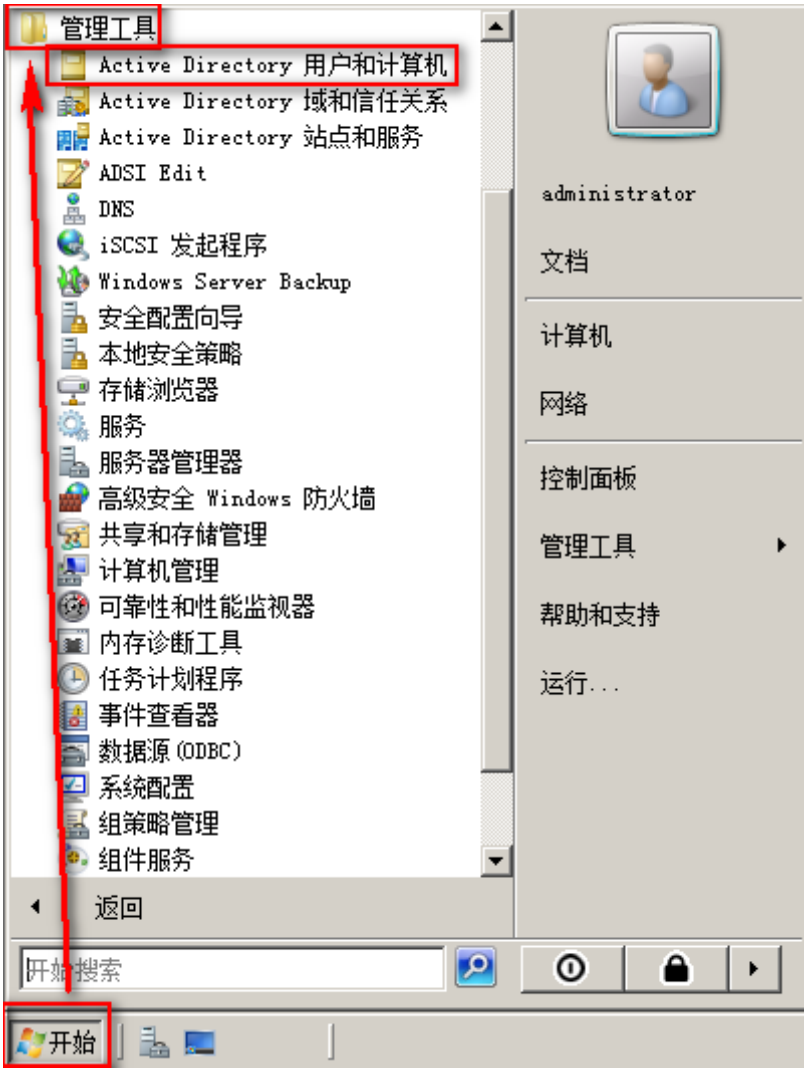


注 1：若用户环境有防火墙设备，请开放 Windows AD Server 的 DCOM port TCP 135。

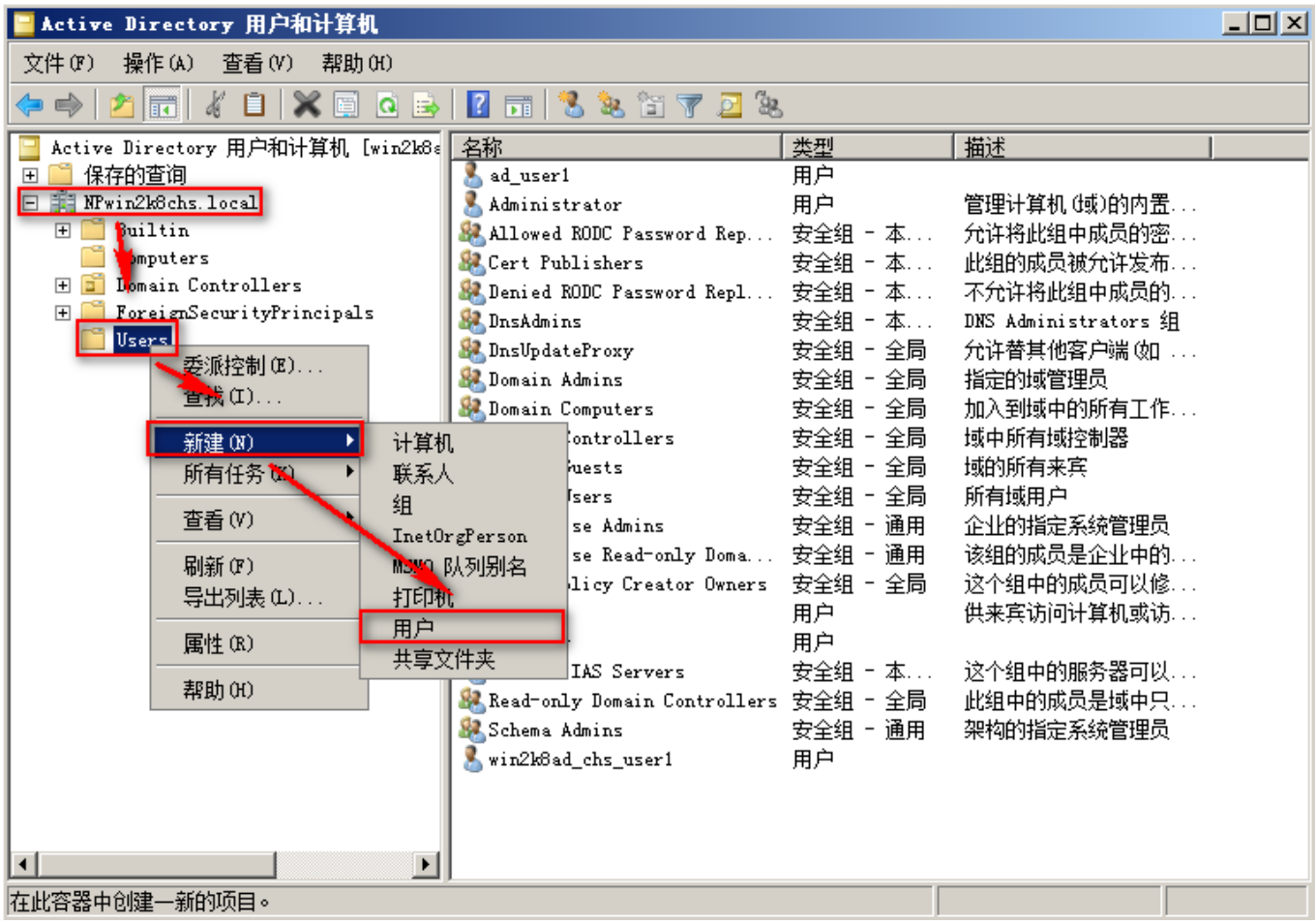
1-2 配置 Windows 2008 AD Server

1-2-1 新增 WMI 远程登录的域用户

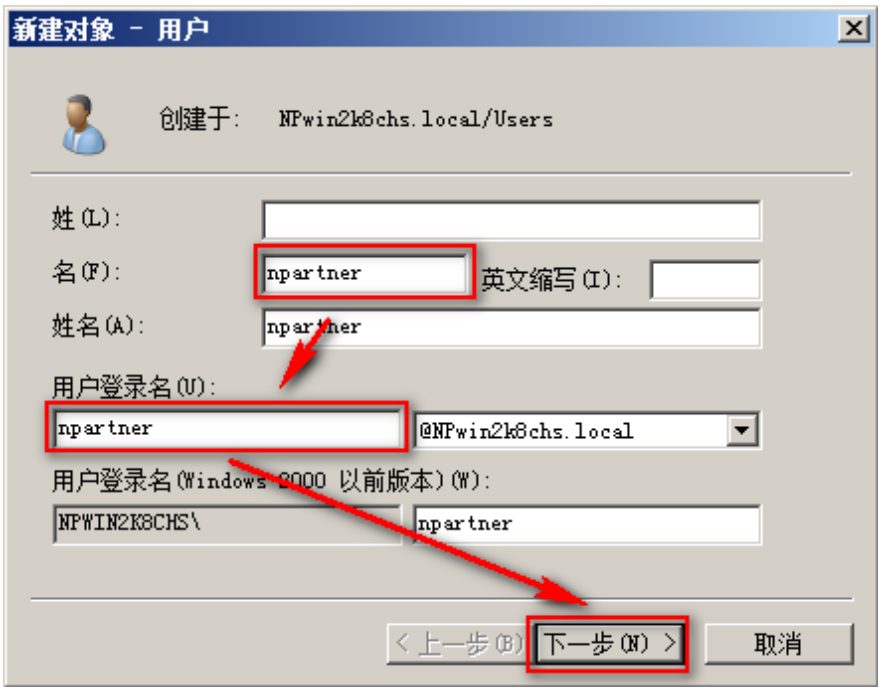
以域管理员账号 administrator 登录Windows AD server，鼠标左点 [开始 / 所有程序 / 管理工具 / Active Directory 用户和计算器]。



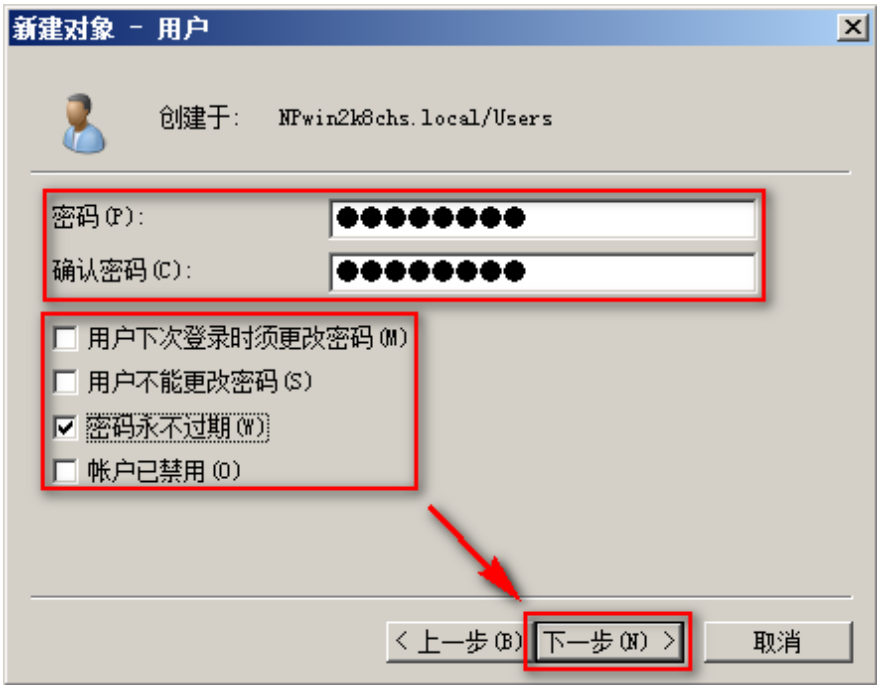
鼠标左点根域(forest root domain)，本例为 NPwin2k8chs.local。右点[Users]，左点[新建 / 用户]。



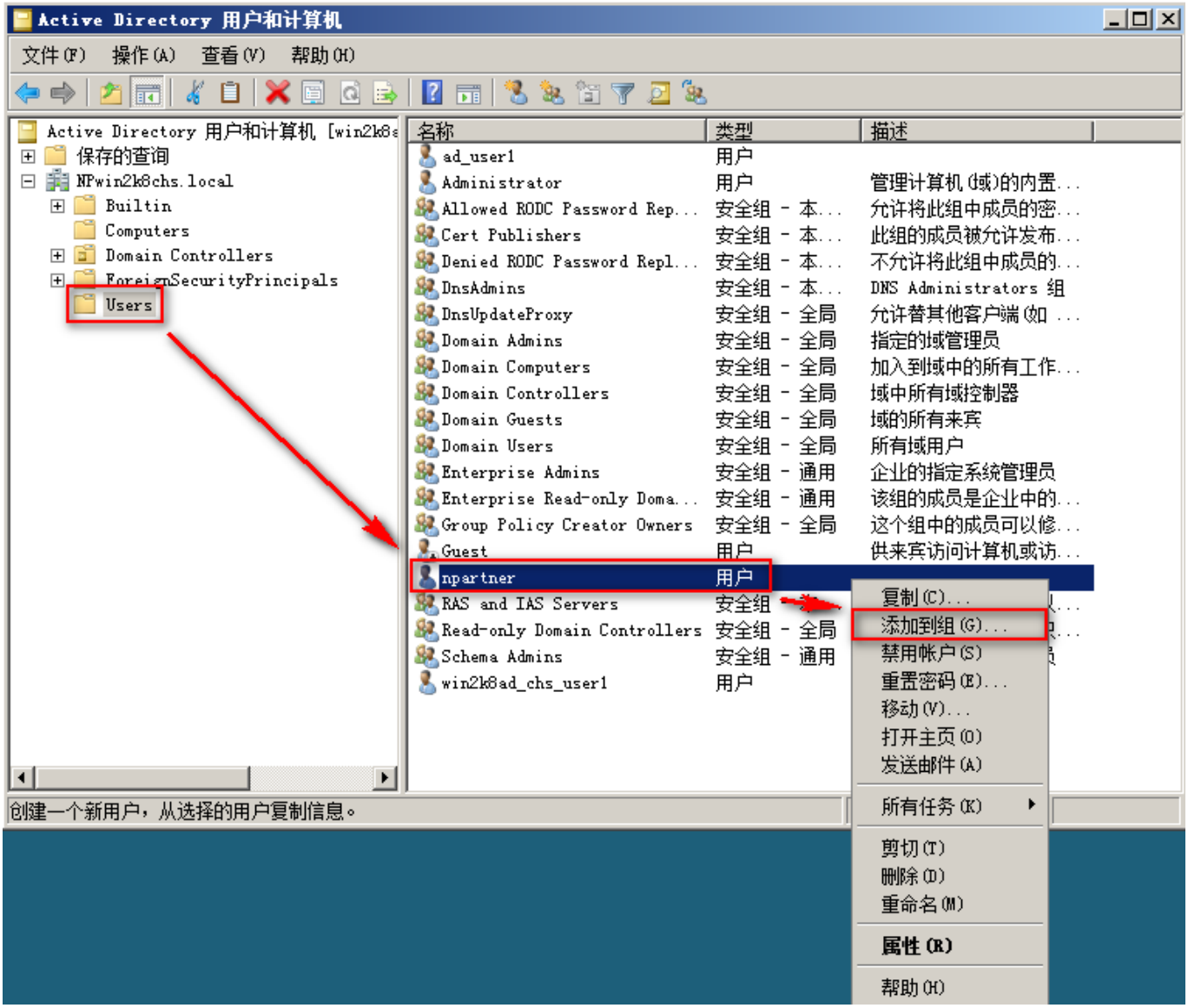
名输入"npartner"，用户登录名输入"npartner"，左点[下一步]。



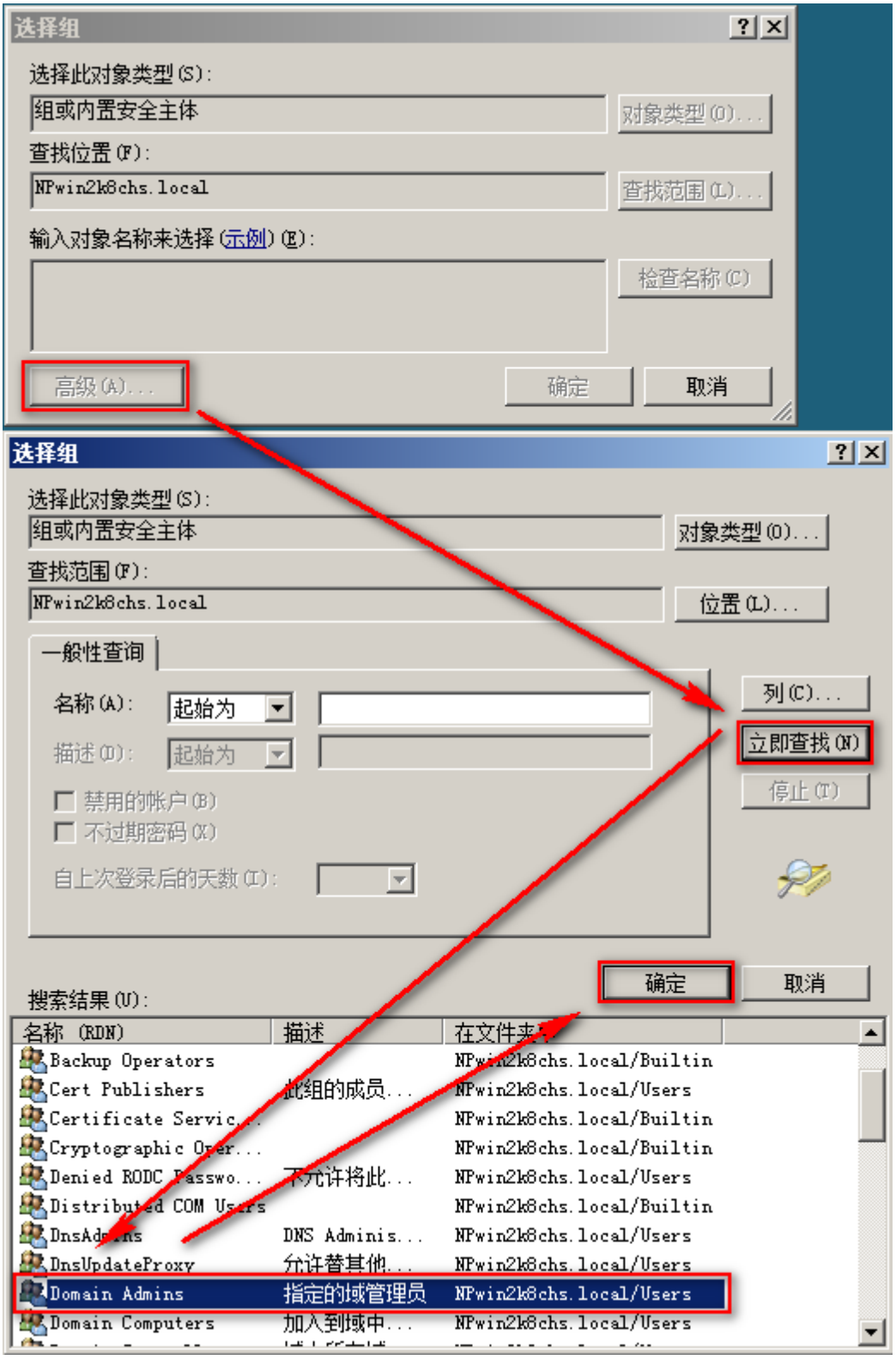
输入密码。只勾选[密码永不过期]。左点[下一步 / 完成]。



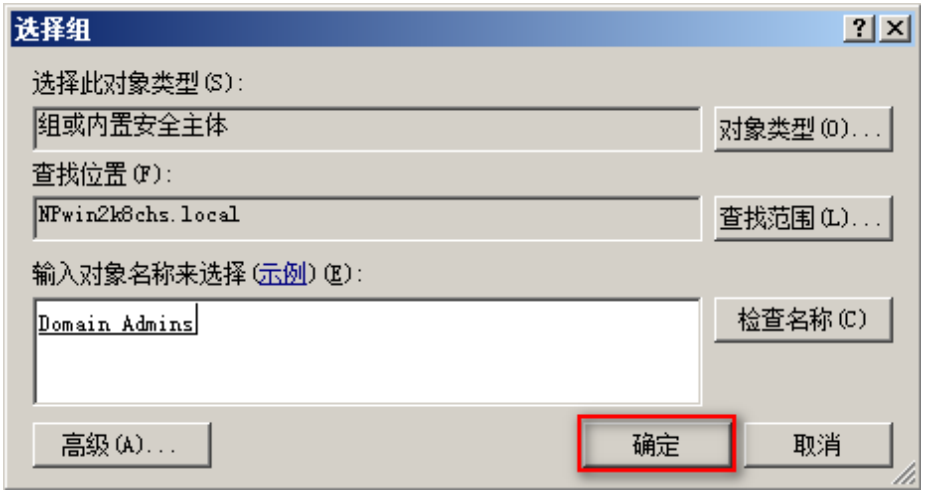
鼠标左点 [Users]。右点 WMI 远程登录用户 npartner，左点[添加到组]。



鼠标左点[高级 / 立即查找 / Domain Admins / 确定]。将 WMI 远程登录用户 npartner 加入到域管理员组中。



左点[确定]。



1-2-2 Windows 2008 AD Server 审核配置

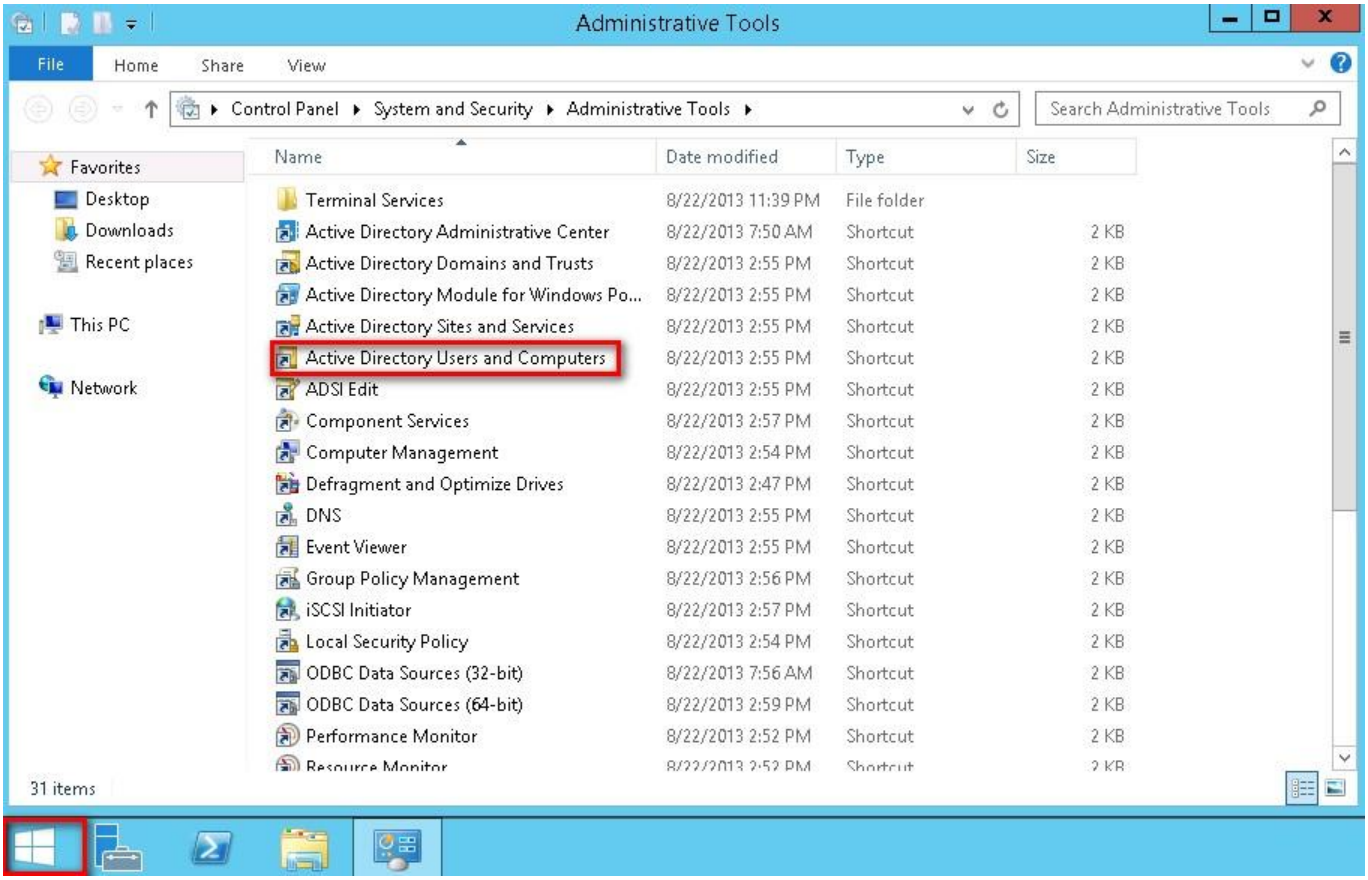
请依照文件「Windows AD audit to syslog」第 3 章「Windows 2008 AD Server 审核配置」，配置默认域控制站(Default Domain Controller)的审核策略(Policy)。

注 2：若用户环境有防火墙设备，请开放此 Windows AD Server 的 DCOM port TCP 135。

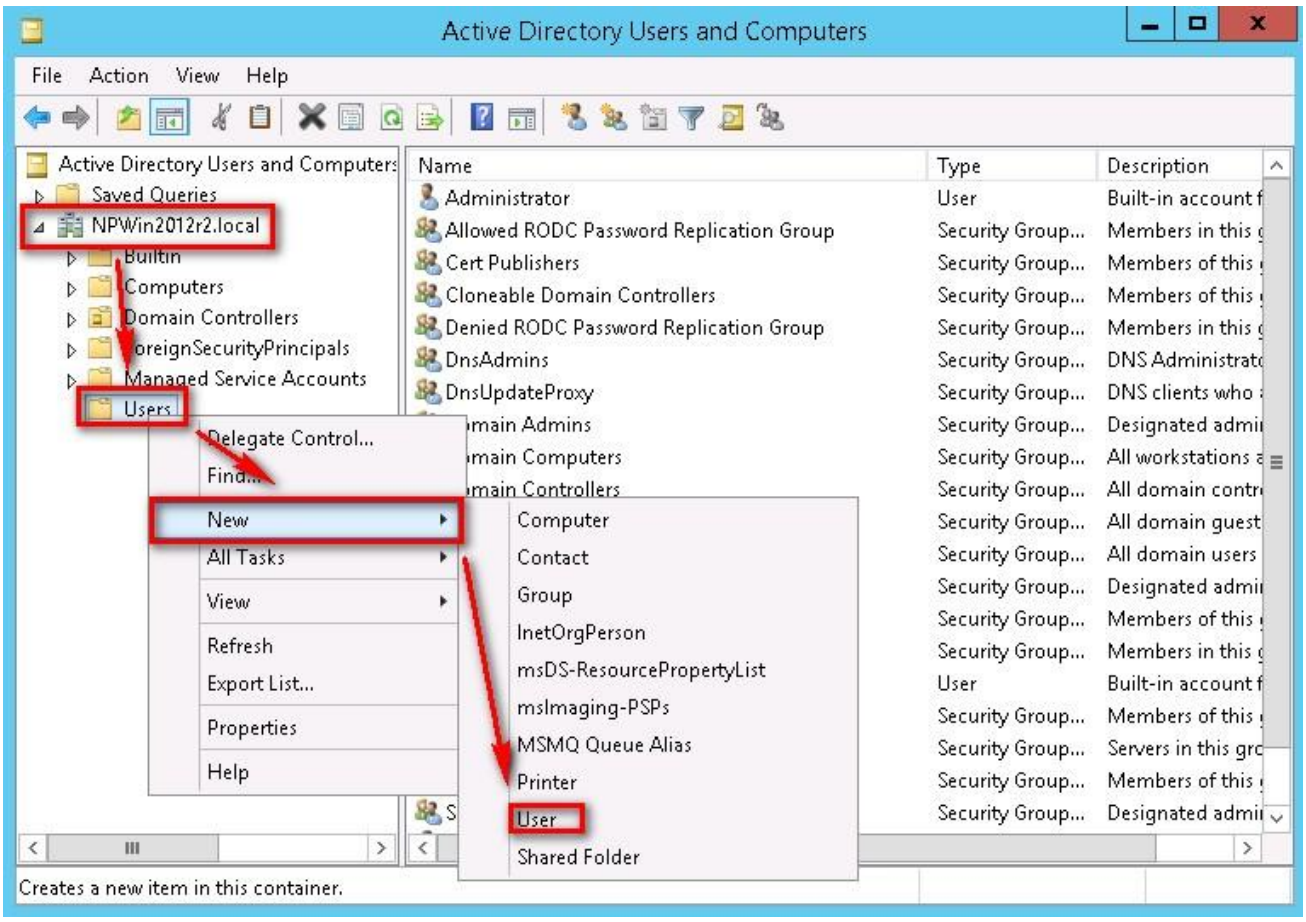
1-3 配置 Windows 2012 AD Server

1-3-1 新增 WMI 远程登录的域用户

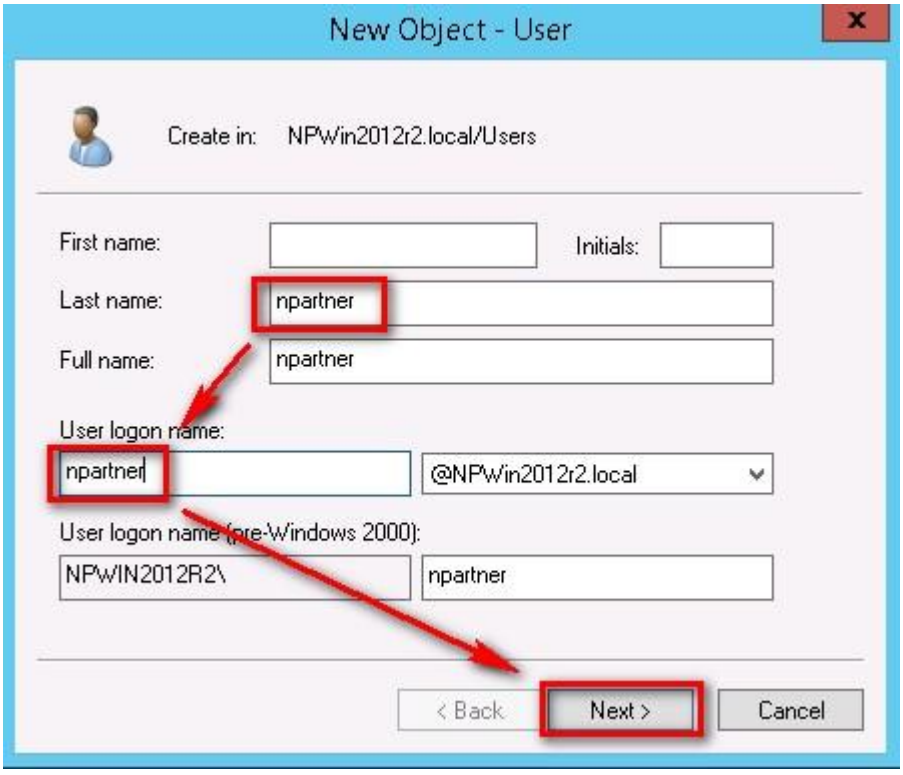
以域管理员账号 administrator 登录Windows AD server，鼠标左点 [Start(开始) / Adminitratives Tools(管理工具) / Active Directory Users and Computers(Active Directory 用户和计算器)]。



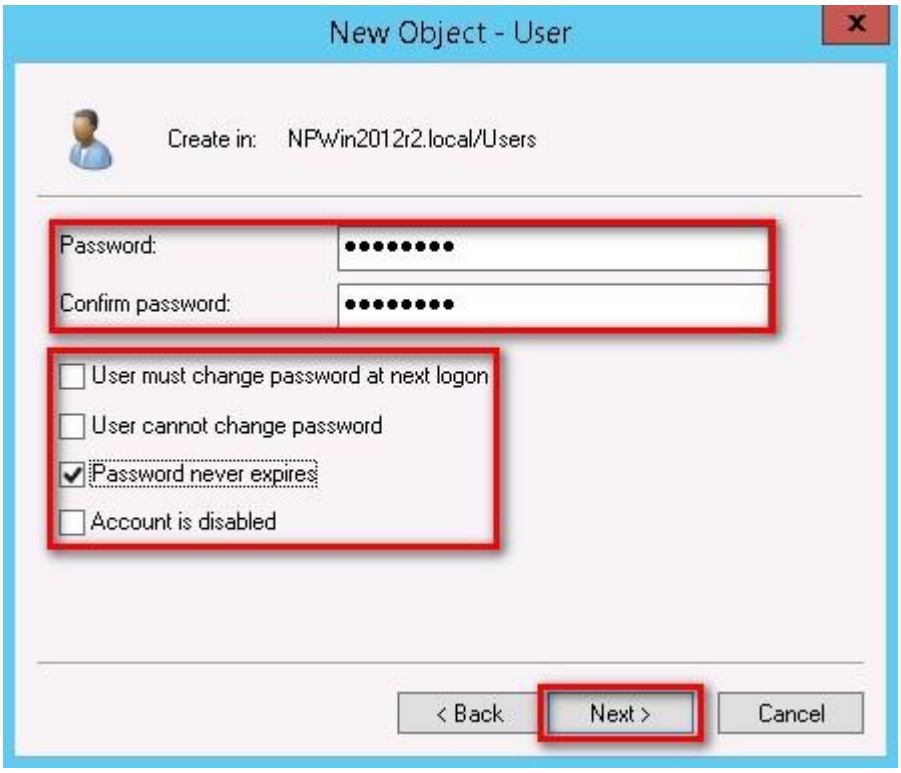
鼠标左点根域(forest root domain)，本例为 NPWin2012r2.local。右点[Users]，左点[New / User]。



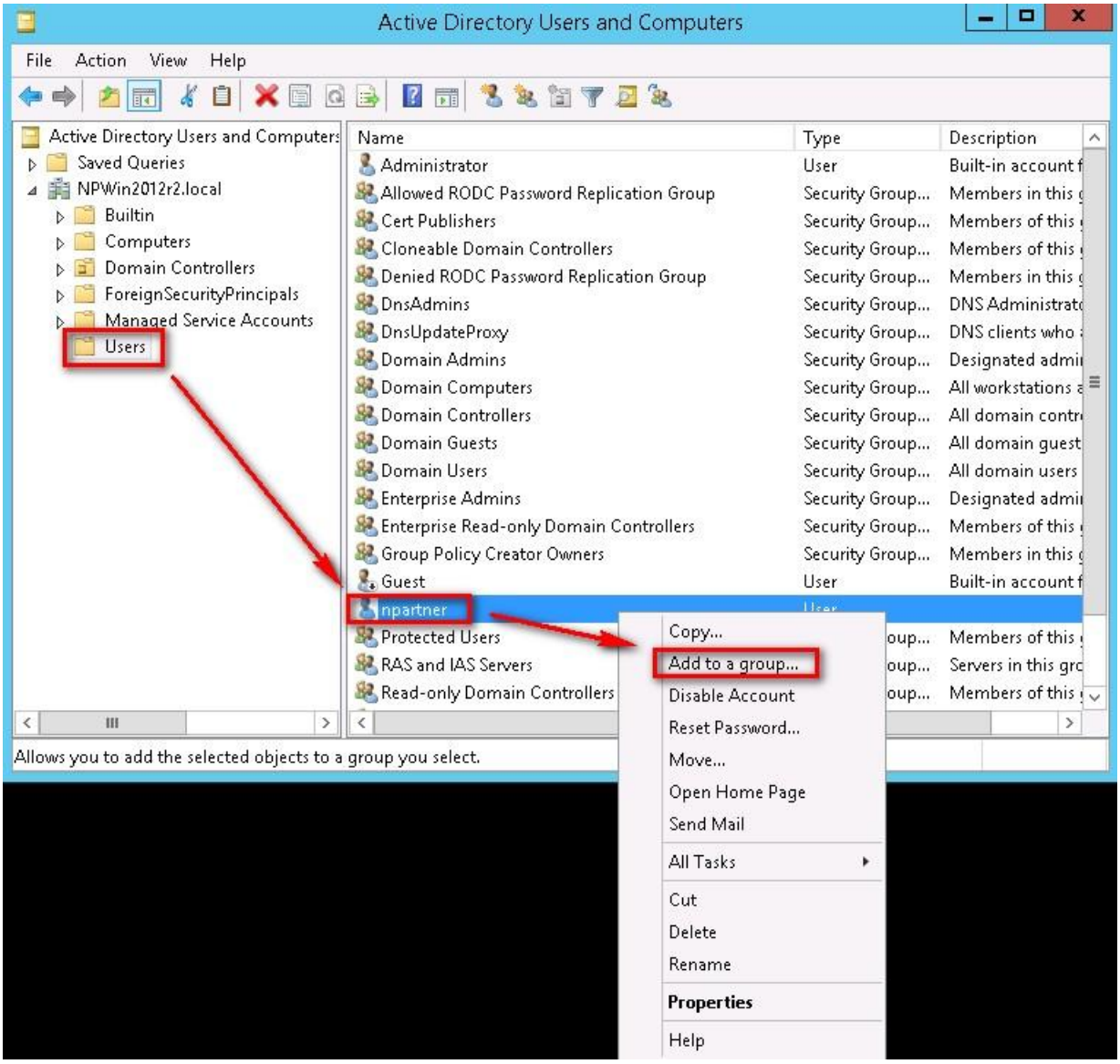
名(Last name)输入"npartner"，用户登录名(User logon name)输入"npartner"，左点[下一步(Next)]。



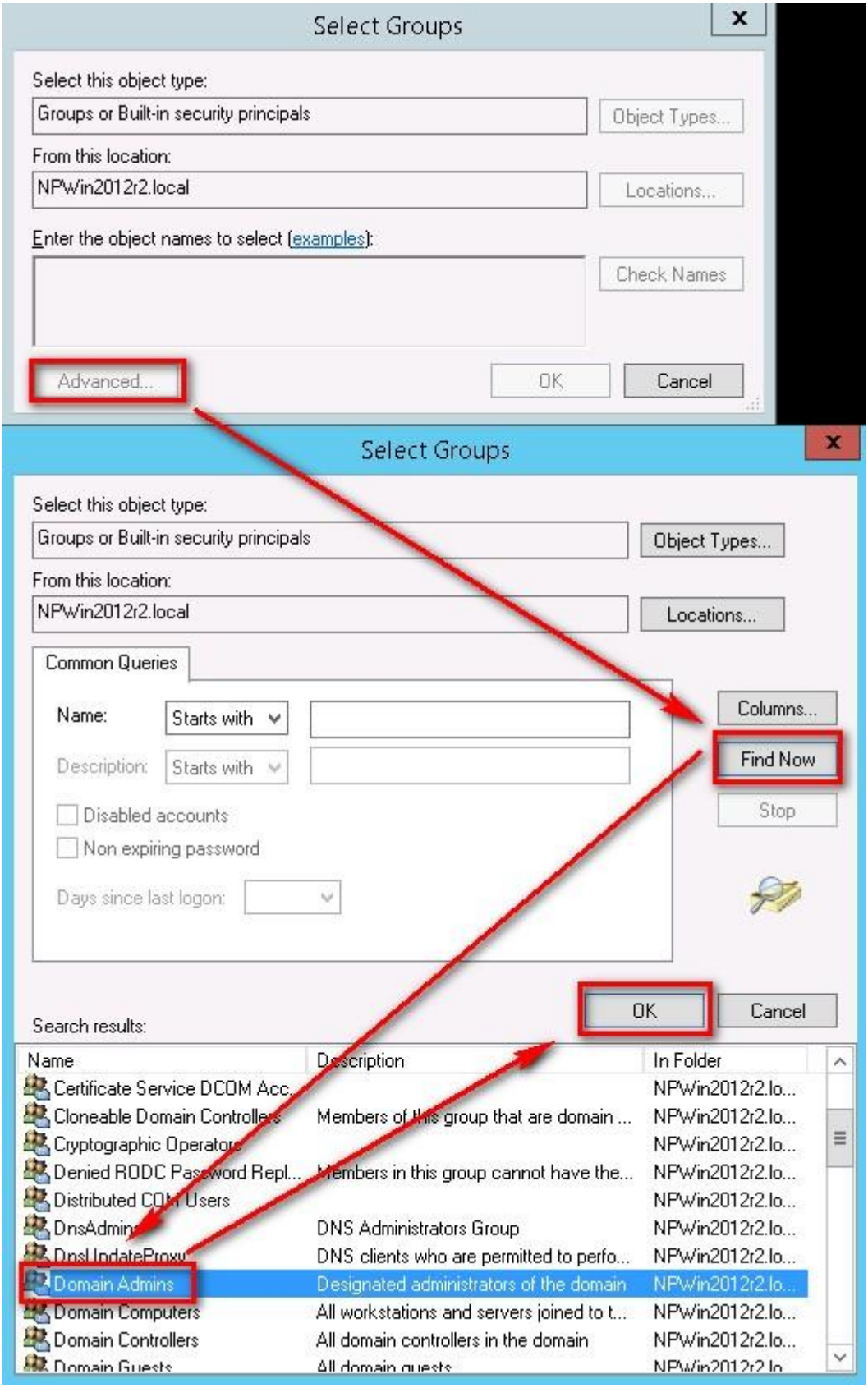
输入密码(password)。只勾选[密码永不过期(Password never expires)]。左点[下一步(Next) / 完成(Finish)]。



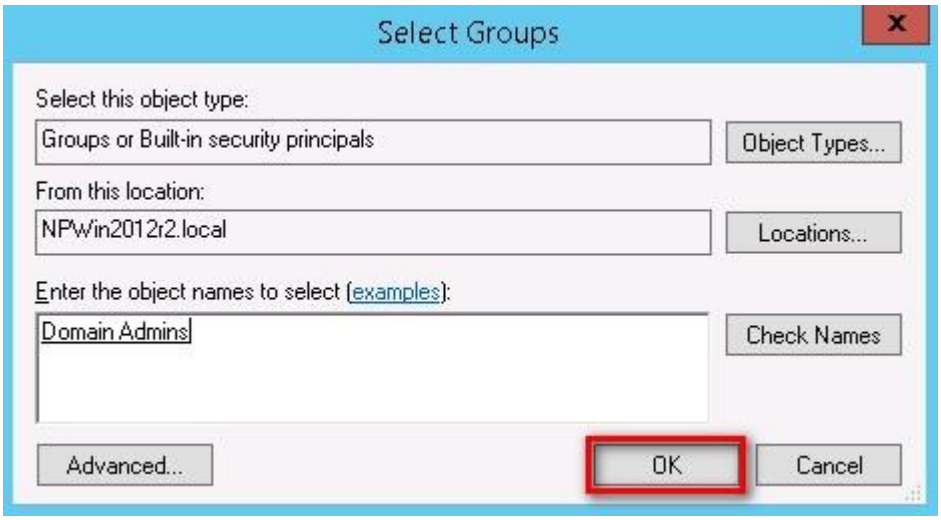
鼠标左点［Users］。右点 WMI 远程登录用户 npartner，左点[添加到组(Add to a group)]。



鼠标左点[高级(Advanced) / 立即查找(Find Now) / Domain Admins / 确定(OK)]。将 WMI 远程登录用户 npartner 加入到域管理员组中。



左点[确定(OK)]。



1-3-2 Windows 2012 AD Server 审核配置

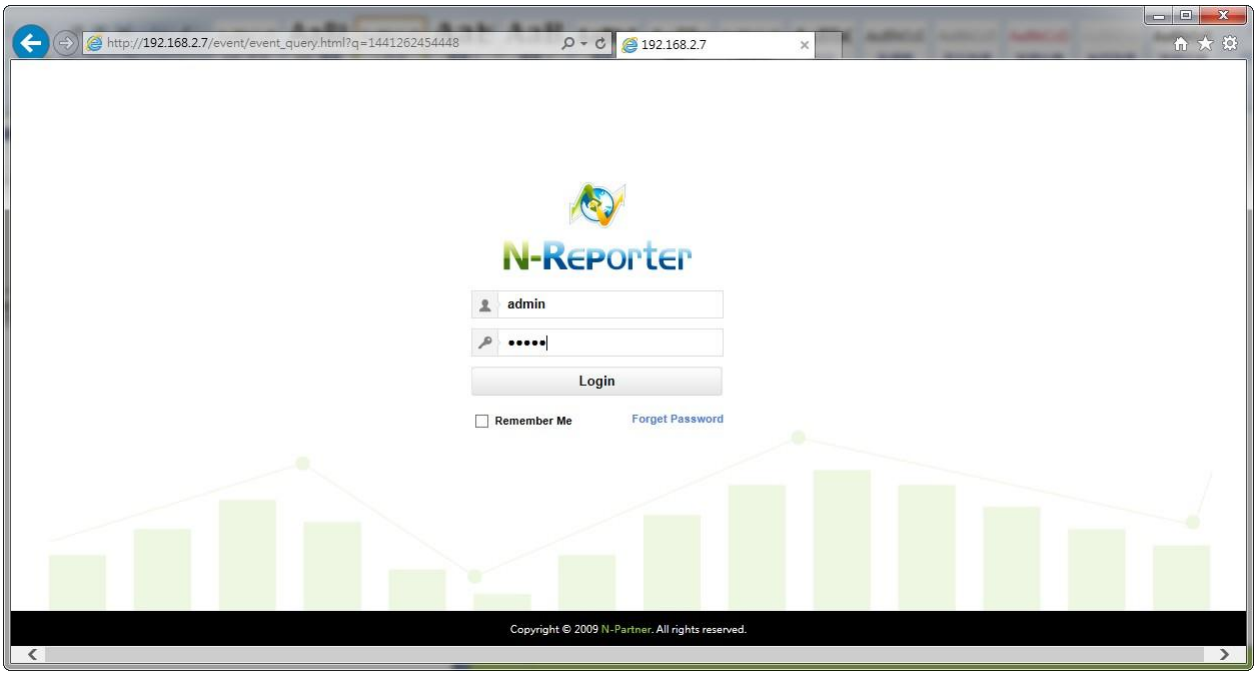
请依照文件「Windows AD audit to syslog」第 4 章「Windows 2012 AD Server 审核配置」，配置默认域控制站(Default Domain Controller)的审核策略(Policy)。

注 3：若用户环境有防火墙设备，请开放此 Windows AD Server 的 DCOM port TCP 135。

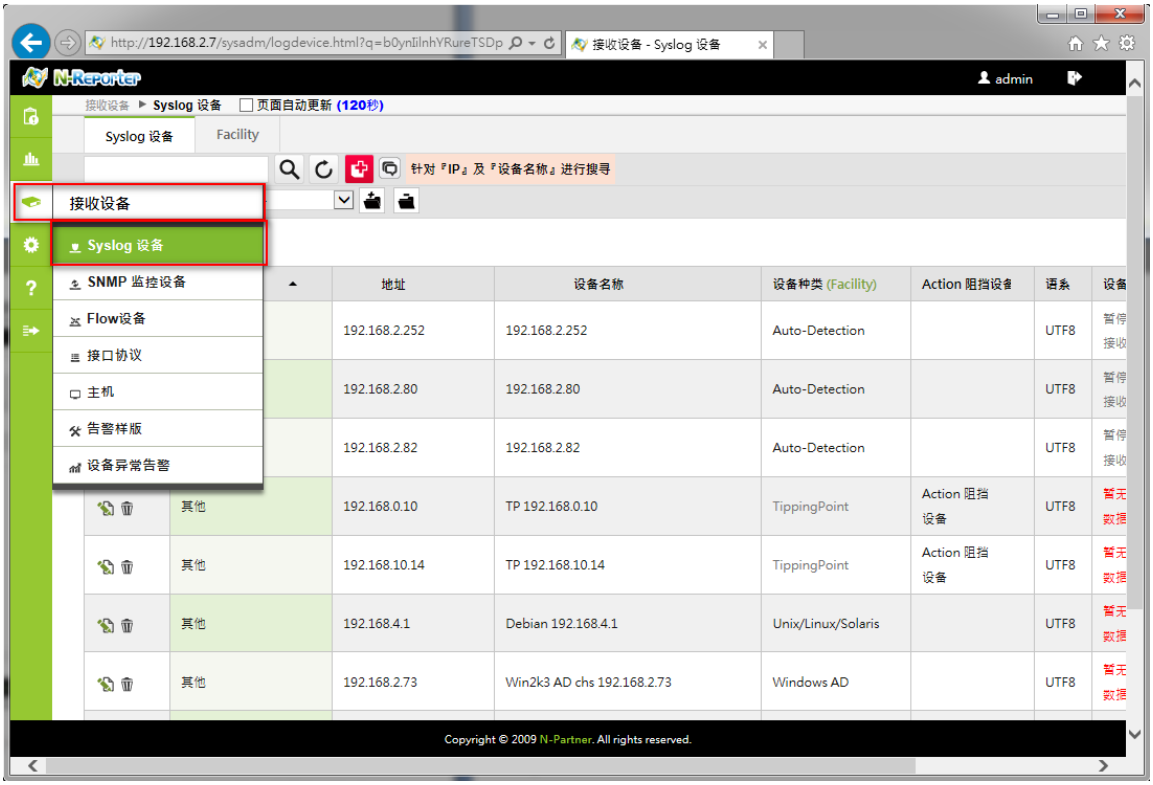
2.新增 Windows AD Server WMI 设备

2-1 新增 Windows AD Server WMI 设备

浏览器 URL 输入 http://$N-Reporter_IP，本例输入"http://192.168.2.7"。输入 N-Reporter 管理员账号/密码，默认 admin/admin，鼠标左点［Login］，登录 N-Reporter Web。

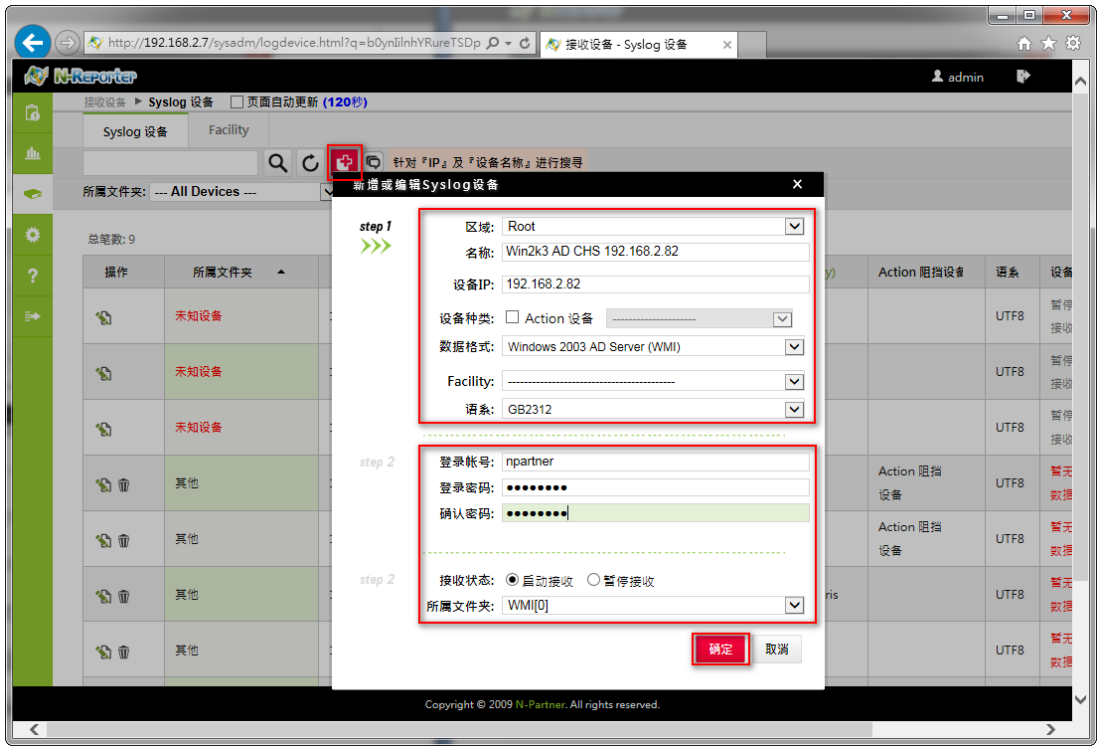


鼠标左点[接收设备 / Syslog 设备]。



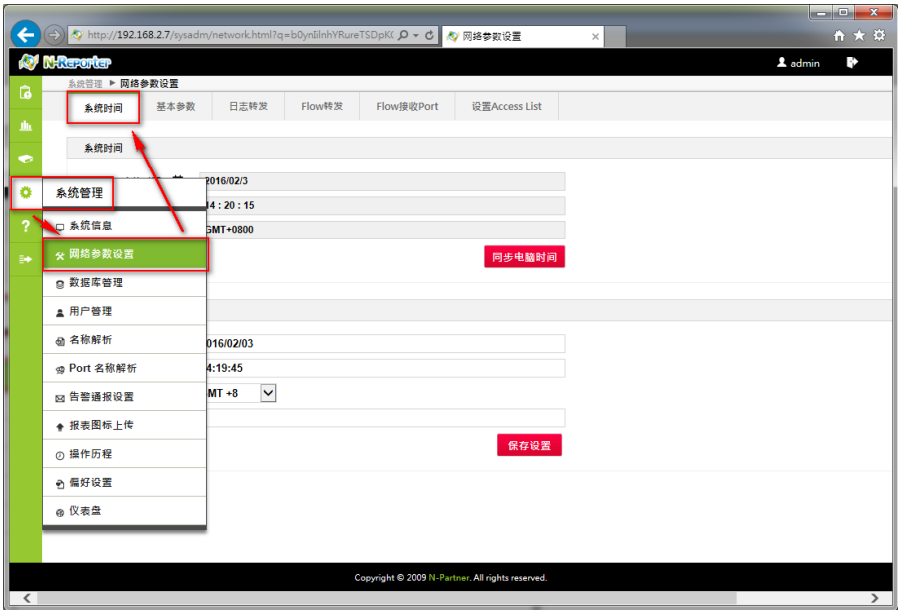
左点[+]，开启[新增或编辑 Syslog 设备]。区域选择此 WMI 设备所在位置，本例为 Root。输入设备名称。输入 WMI 设备 IP。数据格式选[Windows 2003 AD (WMI)]，本例为 Windows 2003 AD Server。语系选[GB2312](注 4)。输入 WMI 设备远程登录账号与密码。设备状态勾选[启动接收]。选择所属活页夹。鼠标左点[确定]。

注 4 ：Windows 2003 繁体版语系选[BIG5]；Windows 2003 简体版语系选[GB2312] ；Windows 2003 英文版语系选[UTF8]。Windows 2008/2012 请选[UTF8] 编码。

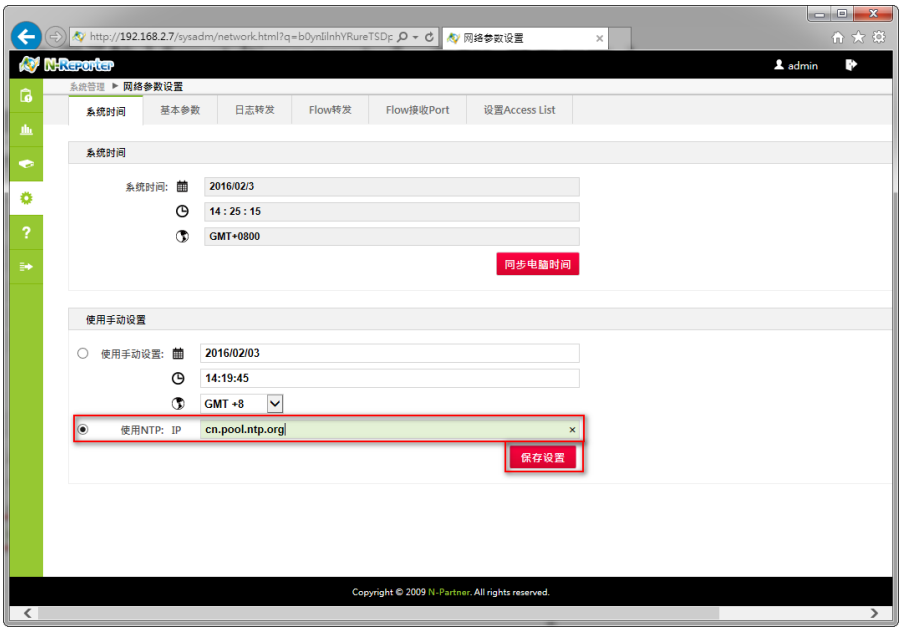


2-2 设定 NTP Server

鼠标左点[系统管理 / 网络参数设置 / 系统时间]。



勾选[使用 NTP]，IP 输入 NTP server IP 或 host name，可输入"cn.pool.ntp.org 或是公司内部的 NTP server IP。本例子输入"cn.pool.ntp.org "。左点[储存设置]。



注 5：如果 WMI 设备与 N-Reporter 时间不一致，将导致 WMI query 数据遗失。新增 WMI 设备后，请再设定 NTP Server，每日定时做时间校正。

連絡資訊

N-Partner 公司連絡方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有關技術問題請洽：

Email: support@npartnertech.com

Skype：support@npartnertech.com

有關業務相關問題請洽：

Email: sales@npartnertech.com

N-Partner