计算机终端安全配置手册（Windows 平台）

**目 录**

1. [审核策略设置 3](#_bookmark0)
   1. [开启密码策略 3](#_bookmark1)
   2. [开启帐户锁定策略 4](#_bookmark2)
   3. [开启审核策略 4](#_bookmark3)
2. [帐户设置 5](#_bookmark4)
   1. [UAC（用户帐户控制）提醒 5](#_bookmark5)
   2. [禁用 Guest 帐户 6](#_bookmark6)
   3. [取消“密码永不过期” 7](#_bookmark7)
   4. [修改密码 8](#_bookmark8)
3. [系统设置 8](#_bookmark9)
   1. [设置计算机名 8](#_bookmark10)
   2. [设置屏幕保护程序 13](#_bookmark11)
   3. [防病毒软件设置 16](#_bookmark12)
   4. [设置时钟同步 19](#_bookmark13)
   5. [系统补丁自动更新 20](#_bookmark14)
   6. [设置防火墙 23](#_bookmark15)
   7. [日志文件设置 24](#_bookmark16)
4. [FAQ 25](#_bookmark17)

[附录 27](#_bookmark18)

1. [常见的服务和功能说明 27](#_bookmark19)
2. [常见端口说明 30](#_bookmark20)

# 审核策略设置

* 1. 开启密码策略

计算机终端启用密码策略，设置帐户密码时会依据密码策略校验密码是否符合要求，以避免设置帐户密码为非强密码对计算机终端造成安全风险。

设置要求：必须设置方法：

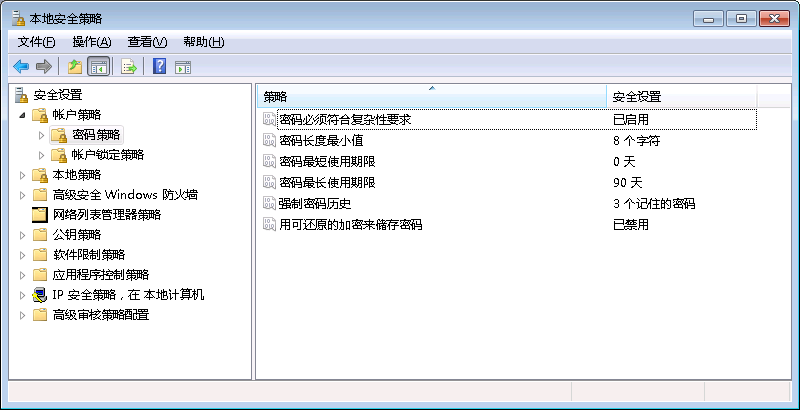
1、打开『控制面板』->『所有控制面板项』->『管理工具』，双击“本地安全策略” ， 或

在『运行』->输入 secpol.msc，并确认。



2、在『安全设置』->『帐户策略』->『密码策略』下，进行密码策略的设置。**密码策略包括：**

* 密码必须符合复杂性要求：已启用
* 密码长度最小值：8 位
* 密码最长留存期：90 天
* 强制密码历史：3 个记住的密码



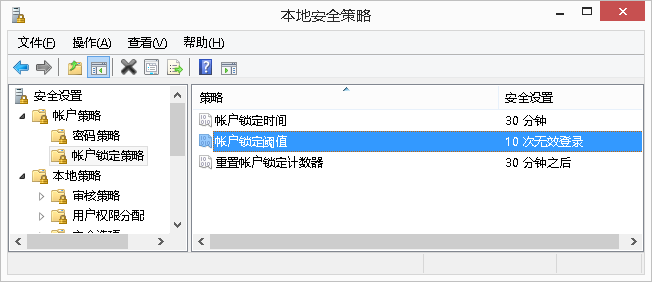
* 1. 开启帐户锁定策略

计算机终端启用帐户锁定策略，可以有效防止攻击者使用暴力破解方式猜测用户密码。设置要求：必须

设置方法：

1、打开『控制面板』->『所有控制面板项』->『管理工具』，双击“本地安全策略”， 或

在 『 运 行 』 -> 输 入 secpol.msc， 并 确 认 。2、在『安全设置』->『帐户策略』->『帐户锁定策略』下，进行帐户锁定策略的设置。先修改“帐户锁定阈值”设置，其它两项会自动提示修改

* 帐户锁定阈值：10 次无效登录
* 帐户锁定时间：30 分钟
* 重置帐户锁定计数器：30 分钟之后
  1. 开启审核策略

审核策略是计算机终端最基本的入侵检测方法，当尝试对系统进行某些方式（如尝试用户密码、改变帐户策略、未经许可的文件访问等）入侵时审核策略会进行系统日志记录。各审核策略含义如下：

1. 审核策略更改：可查看更改本地安全策略的尝试，以及查看某个用户是否更改了用户权限分配、审核策略或信任策略。
2. 审核登录事件：可查看某个用户登录或注销计算机（包括本地和网络登录）的事件。
3. 审核对象访问：可查看用户对 Windows 对象（包括注册表、服务、打印机、文件

/文件夹等）的访问事件。

1. 审核过程跟踪：可查看事件（如程序运行或进程退出）发生的时间，包括由用户执行和系统自动执行的事件。
2. 审核目录服务访问：可查看某个用户访问具有其自身系统访问控制列表的 AD 对象的事件。
3. 审核特权使用：可查看某个用户在其拥有执行权限的计算机上执行任务的时间，即

用户使用分配的特权事件，特权指在本地安全策略中分配给用户的权限。

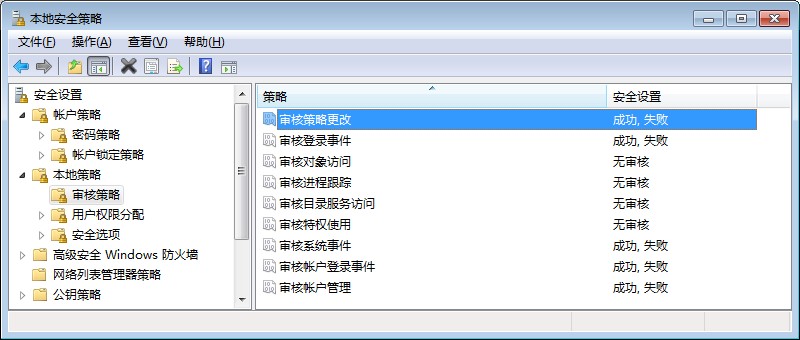
1. 审核系统事件：可查看某个用户关闭或重新启动计算机的时间，或者某个进程或程序尝试执行其没有权限的某项操作的事件。
2. 审核帐户登录事件：可查看在这台计算机用于验证帐户时，用户登录到其它计算机或者从其它计算机注销的事件。
3. 审核帐户管理：可查看某个用户更改帐户名、启用或禁用帐户、创建或删除帐户、更改密码或更改用户组的时间，也包含用户组、DC 中域用户、域用户组等对象的管理、密码设置等事件。

设置要求：必须设置方法：

1、打开『控制面板』->『所有控制面板项』->『管理工具』，双击“本地安全策略”， 或

在『运行』->输入 secpol.msc，并确认。

2、在『安全设置』->『本地策略』->『审核策略』下，进行审核策略的设置。要求开启的审核策略包括：

* 审核策略更改：成功，失败
* 审核登录事件：成功，失败
* 审核系统事件：成功，失败
* 审核帐户登录事件：成功，失败
* 审核帐户管理：成功，失败

# 帐户设置

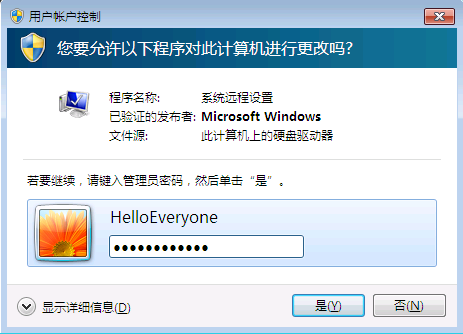
* 1. UAC（用户帐户控制）提醒

UAC（User Account Control）用户帐户控制，是 Windows Vista 以上操作系统中一种特殊的提高授权的运行模式，即平时运行软件在普通用户权限，需要管理员特权操作时，系统会弹出提示（或称为警告），要求用户确认或输入管理员权限密码。

UAC 提醒功能可以对恶意软件的运行制造人为障碍，在使用未经签名的软件时，也会出现相应的授权提示。为确保计算机安全稳定运行，当系统自动弹出“用户帐户控制”， 应谨慎点“是”。

UAC 提醒通知设置建议保留缺省项“仅当应用尝试更改我的计算机时通知我”。例如普通用户模式运行注册表编辑器时会出现提示：

当普通用户运行远程设置管理时，需要输入管理员口令：



* 1. 禁用 Guest 帐户

通过 Guest 帐户身份，非法用户可以操纵并破坏计算机终端，因此任何时候都应禁止开启计算机终端的 Guest 帐户。

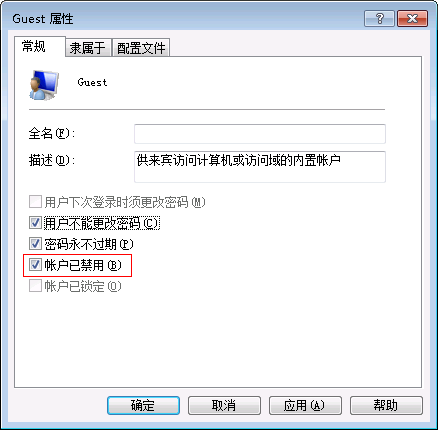
设置要求：必须设置方法：

1、打开『控制面板』->『所有控制面板项』->『管理工具』->『计算机管理』菜单。

2、打开『系统工具』->『本地用户和组』->『用户』，显示系统中所有帐户的信息。

3、在 Guest 帐户上右键单击选择『属性』菜单。

4、弹出的窗口中，复选『帐户已禁用』，点击【确定】按钮。



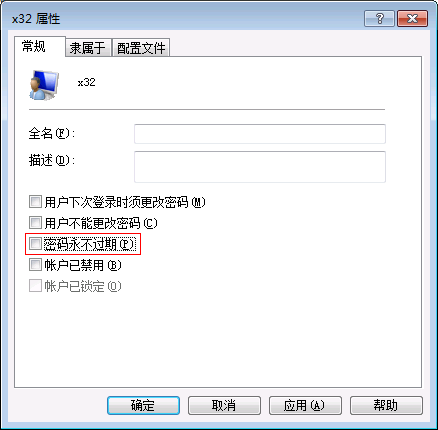
* 1. 取消“密码永不过期”

所有版本的 Windows 操作系统，缺省设置都是用户密码永不过期；当密码使用时间过长，容易造成密码的泄露，因此要求取消帐户“密码永不过期”选项。

设置要求：必须设置方法：

1、打开『控制面板』->『所有控制面板项』->『管理工具』->『计算机管理』

2、打开『系统工具』->『本地用户和组』->『用户』，选择指定用户，右键点击指定用户，选择“属性” 3、去掉“密码永不过期”选项，并确定。



==============================================

# 注意：

当存在多个帐户时，应对所有帐户均取消“密码永不过期”设置。

==============================================

* 1. 修改密码

密码是保护计算机终端安全的一个基本途径，通常的破坏行为或暴力破解都需要猜测帐户的密码。计算机终端密码必须符合公司强密码策略要求。

设置要求：必须 **强密码策略如下：**

* + 1. 不能包含用户的帐户名和显示名
    2. 密码最小长度：8 个字符
    3. 必需包含以下四类字符中的三类字符：

a） 英文大写字母（A 到 Z）

1. 英文小写字母（a 到 z）
2. 10 个基本数字（0 到 9）
3. 非字母字符（如!、\*、@等）
   * 1. 密码有效期：90 天
     2. 密码失效通知期：15 天
     3. 传达失效通知的模式：通过邮件通知
     4. 密码历史记录：3 个

公司最新要求请参见《IT 服务手册》。设置方法：

按下 CTRL+ALT+DELETE 组合键，并单击“更改密码”，输入旧密码后，进行密码修改。

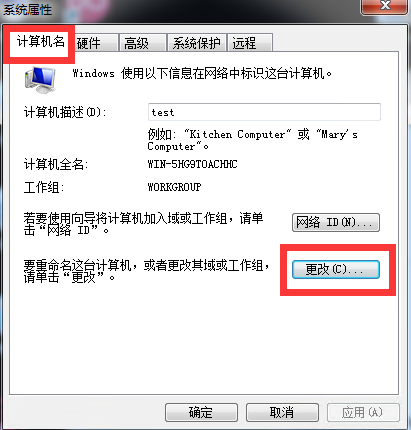
# 系统设置

* 1. 设置计算机名

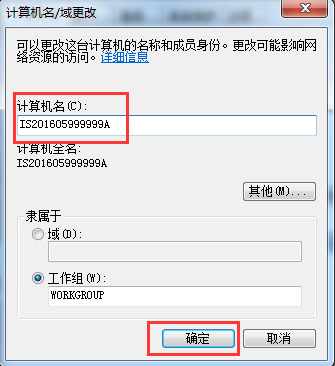
设置规范的计算机终端名称，方便管理员借助计算机名称来识别计算机。

**Windows 7 设 置 方 法 ：** 1、 在 win7 桌面上，右键点击“计算机”，选择“属性”，在弹出的界面中选择“高级系统设置”。

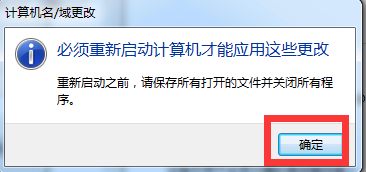


2、 选择“计算机名”，点击“更改”按钮。

3、 输入合法的计算名后，点击“确定”按钮。



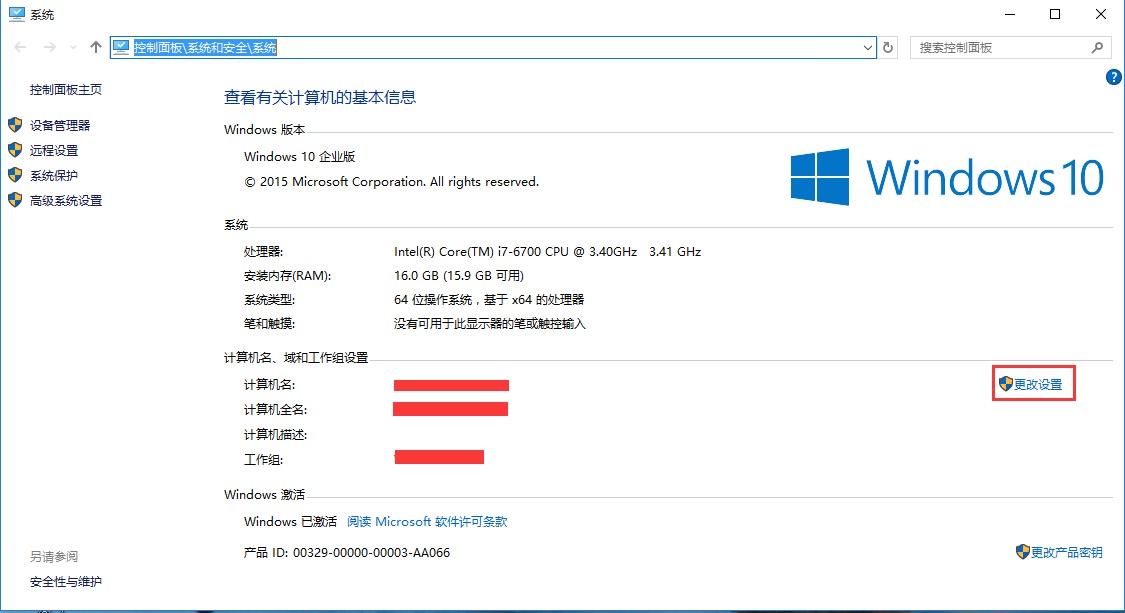
4、 提示需要重启计算机，点击确定。



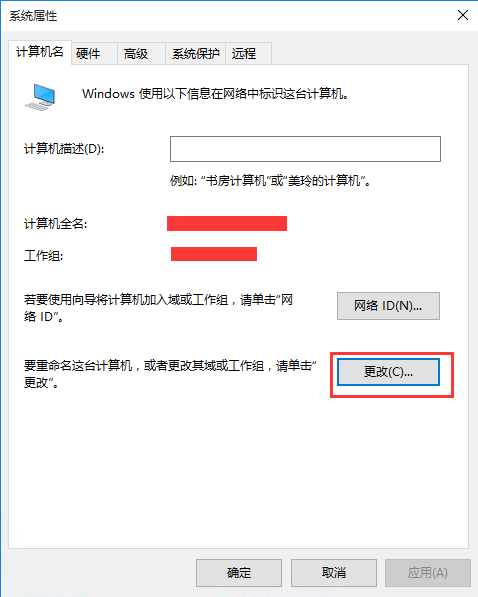
# Windows 10 设置方法：

1、 在 win10 系统桌面上，右键单击此电脑，选择“属性”。

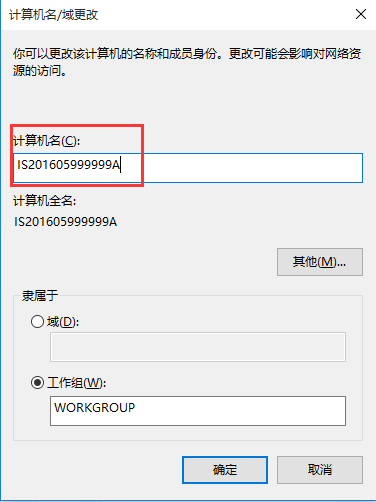


2、点击“更改设置”。

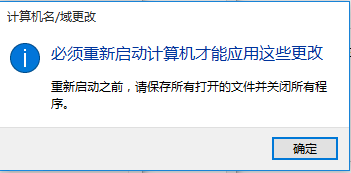
3、点击“更改”。



4、输入符合命名规则的计算机名，点击“确定”按钮。



4、选择“确定”按钮，重启后计算机名称即修改完成。



* 1. 设置屏幕保护程序

设置计算机终端屏幕保护程序，保证员工在离开时的操作系统安全，启用屏幕保护程序的等待时间应小于等于 5 分钟。

设置要求：必须

# Windows 7 设置方法：

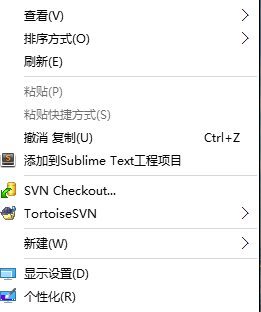
1、打开『控制面板』->『外观和个性化』->『更改屏幕保护程序』，进行设置屏幕保护程序。

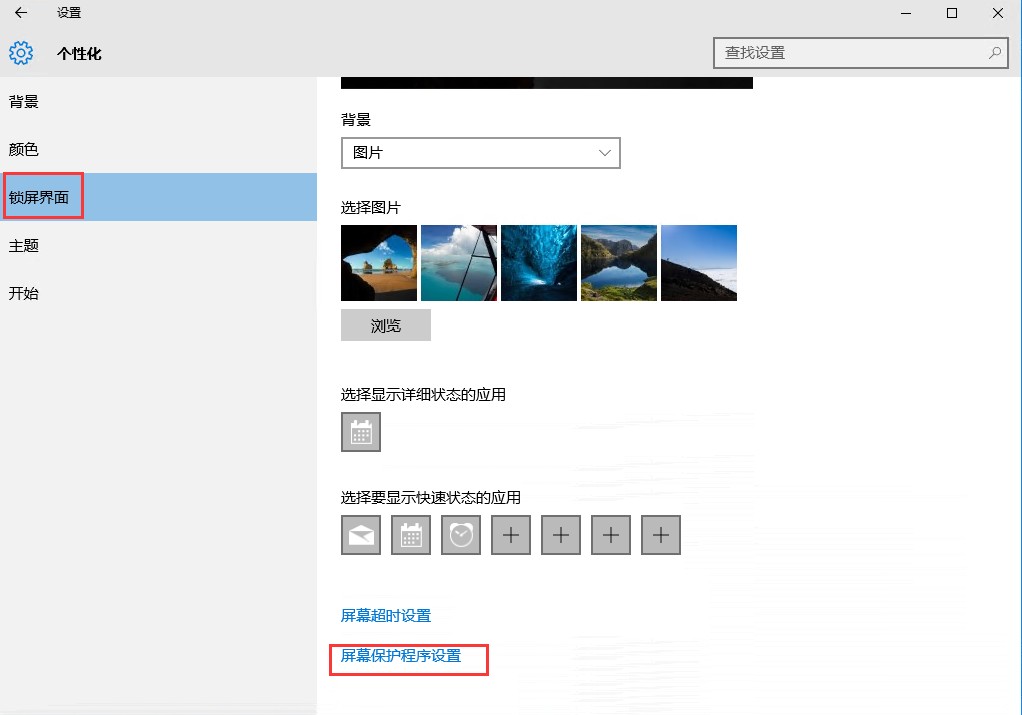


2、在屏幕保护程序下拉列表中选择屏幕保护程序，等待时间设置成小于或等于 5 分钟， 复选『在恢复时使用密码保护』，点击【确定】按钮。

# Windows 10 设置方法：

1、 在电脑桌面空白处单机鼠标右键，选择“个性化”。



2、 选择“锁屏界面”，再选择“屏幕保护程序设置”。

3、在屏幕保护程序下拉列表中选择屏幕保护程序，等待时间设置成小于或等于 5 分钟， 复选『在恢复时使用密码保护』，点击【确定】按钮。



* 1. 防病毒软件设置

公司实施了集中式病毒防护，要求所有计算机终端安装集中式病毒防护软件 Symantec Endpoint Protection（简称 SEP）。

==============================================

# 注意：

1．由于公司对 SEP 采用分组管理模式，安装前请务必同部门信息安全专员确认使用本部门的安装包。 2．计算机终端至少每月执行一次病毒活动扫描，如在活动扫描中发现病毒或安全风险， 须及时进行完整的病毒全面扫描。

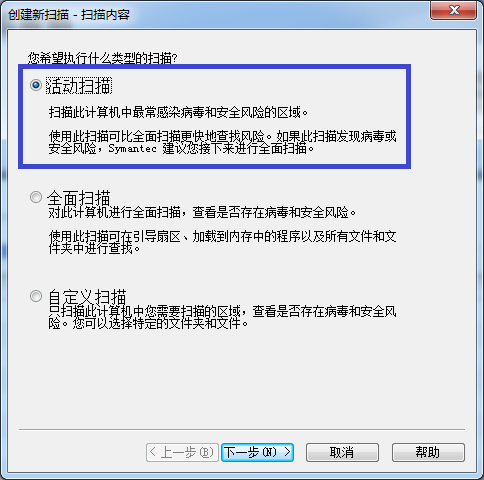
==============================================

设置要求：必须设置方法：

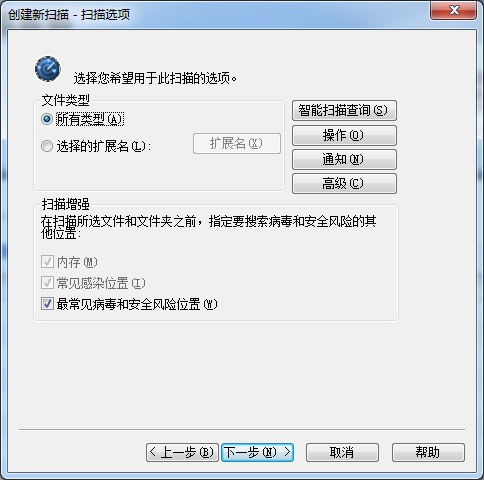
1、双击任务栏右下角的SEP 图?。

2、点击左侧的『扫描威胁』菜单，点击『创建新扫描』菜单。



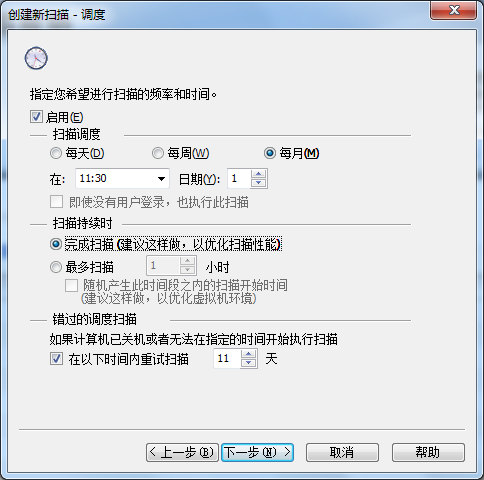
3、单选『活动扫描』选项，点击【下一步】按钮。

4、选择扫描文件的类型『文件类型』为“所有类型”，点击【下一步】按钮。

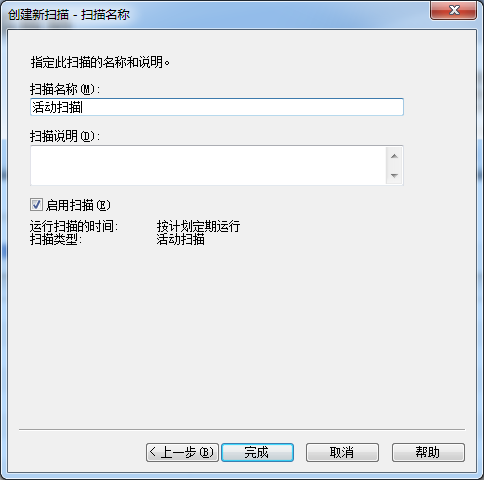


5、单选扫描属性为“在指定时间”，点击【下一步】按钮。

6、设置自动扫描的频率及每次扫描的启动日期和时间，点击【下一步】按钮。



7、设置扫描的名称信息，点击【完成】按钮，完成自动扫描任务的设置。

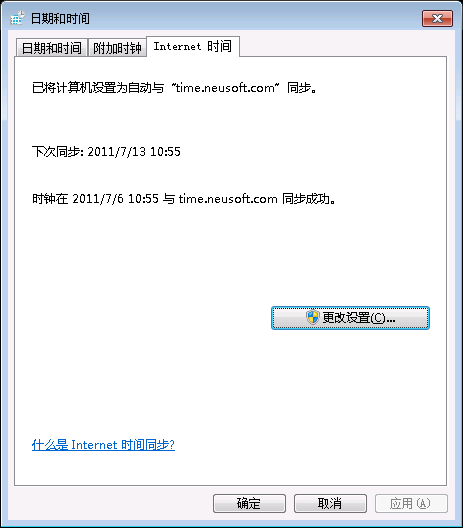


* 1. 设置时钟同步

设置时钟同步可以使公司所有计算机终端的系统时间保持一致，从而准确记录系统操作时间，并实现对事件的回溯。

设置要求：必须设置方法：

1、『控制面板』->『所有控制面板项』->『日期和时间』，选择“Internet 时间”标签。



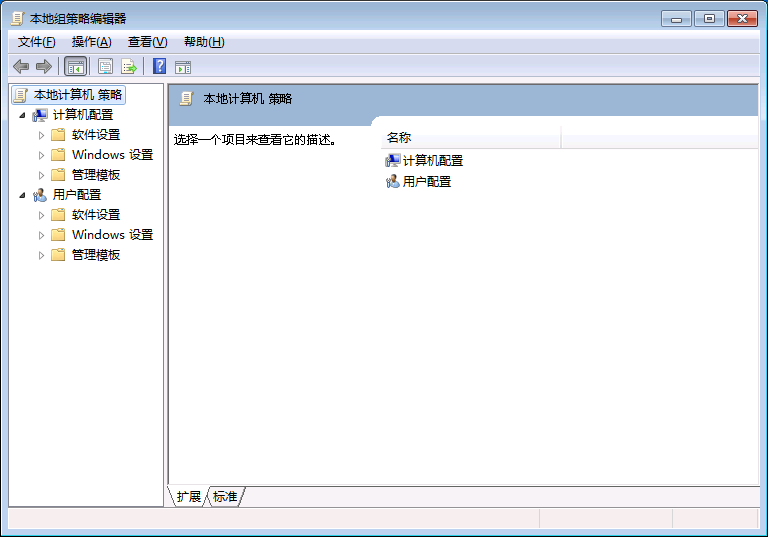
2、单击“更改设置”按钮，在 Internet 时间设置对话框，复选『与 Internet 时间服务器同步』，并在服务器下拉列表中输入“time.neusoft.com”，点击【立即更新】按钮， 更新之后点击【确定】按钮。

* 1. 系统补丁自动更新

公司部署WSUS(Windows Server Update Services)服务器，用于及时下载系统补丁，统一向公司内计算机终端提供下载源。

设置要求：必须设置方法：

1、在『运行』中输入“gpedit.msc”回车，弹出本地组策略编缉器窗口。



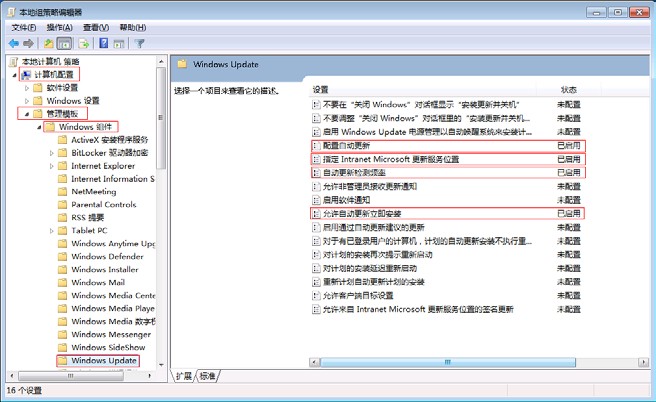
==============================================

# 注意：

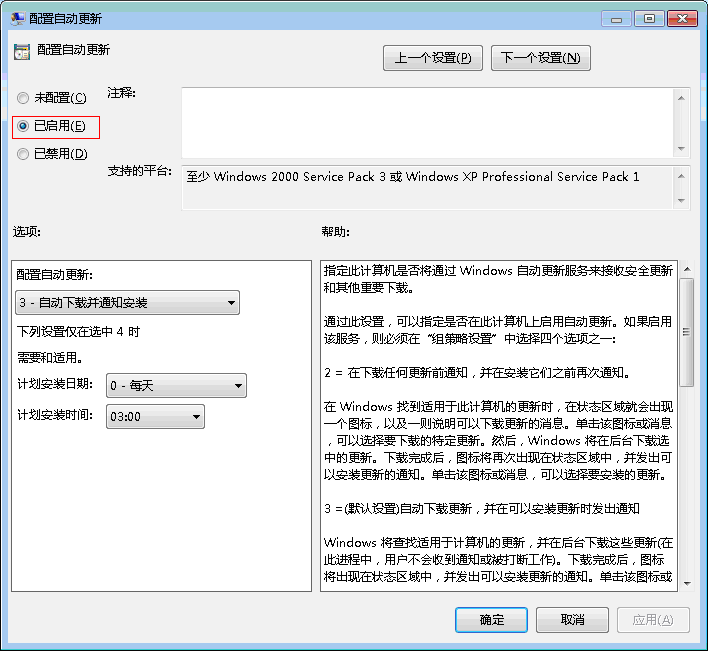
运行“gpedit.msc”时，如果系统提示找不到该程序，说明操作系统版本不支持组策略组件。

==============================================

2 、在本地计算机策略-> 计算机配置-> 管理模板->Windows 组件->Windows

Update 项的右侧，双击“配置自动更新”策略，单选『已启用』，然后点击【确定】按钮。

配置自动更新：

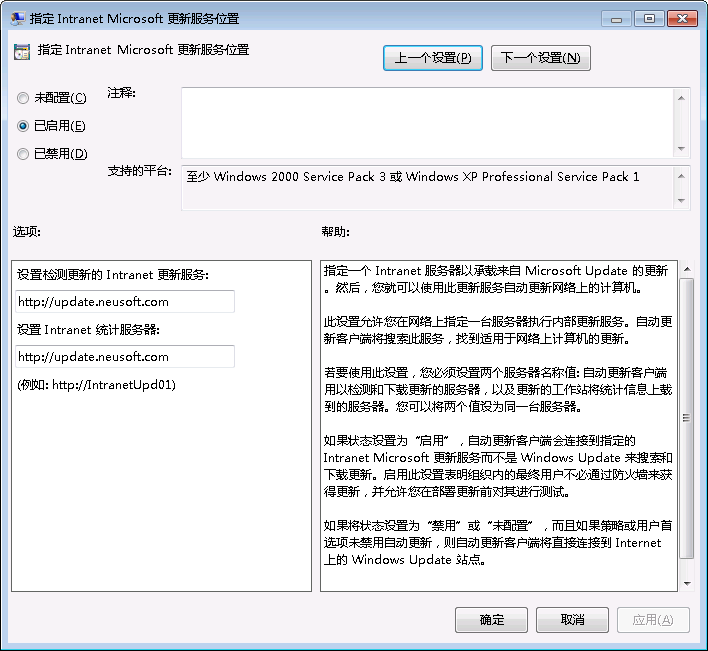


3、双击“指定 Intranet Microsoft 更新服务位置”策略，进入后单选『已启用』，在“设置检测更新设置 Intranet 更新服务”和“设置 Intranet 统计服务器”，输入公司服务器地址（[http://update.neusoft.com](http://update.neusoft.com/)）。

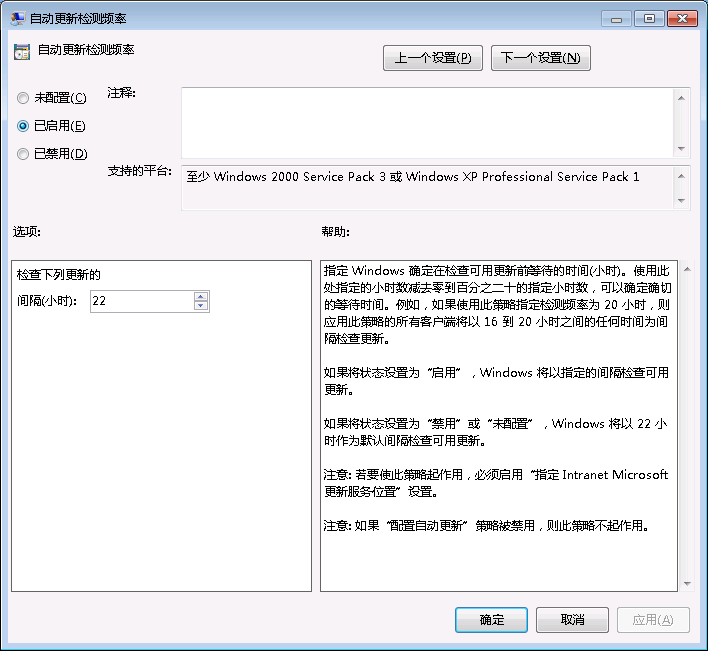
==============================================

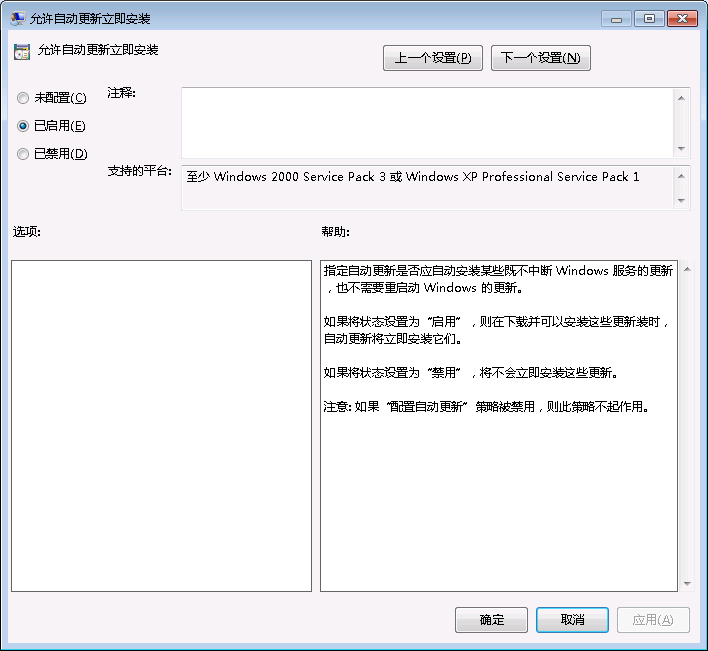
# 注意：

**域名地址应完整输入“http://”。**

==============================================

4、双击“自动更新监测频率”策略，单选『已启用』，点击【确定】按钮。



5、双击“允许自动更新立即安装”策略，单选『已启用』，然后点击【确定】按钮。

6、如果需要计算机立即进行补丁更新，点击『运行』，输入命令“wuauclt /detectnow”。

* 1. 设置防火墙

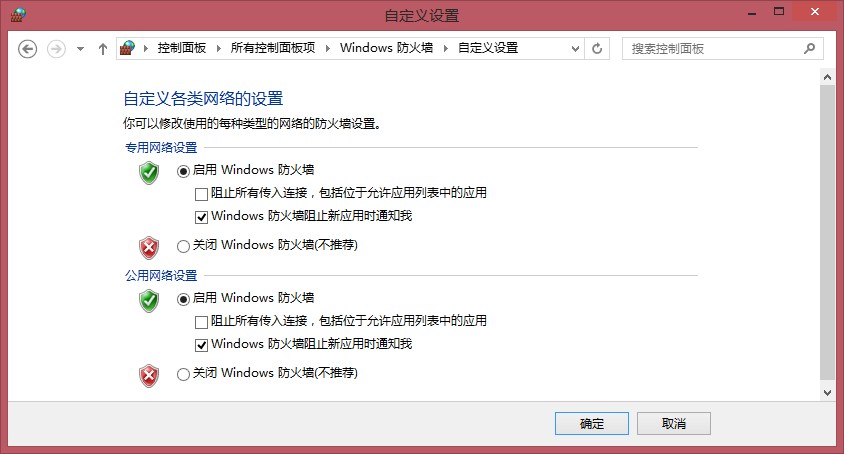
Windows 防火墙是操作系统自我防卫工具，可以有效防止计算机终端被恶意攻击，因此必须将Windows 防火墙设置为开启状态。

设置要求：必须**设置方法：**

1、打开『控制面板』->『所有控制面板』->『Windows 防火墙』，单击“启动和关闭

Windows 防火墙”。



2、在“专用网络设置”和“公用网络设置”中，选定“启用 Windows 防火墙”，并单击“确定”。

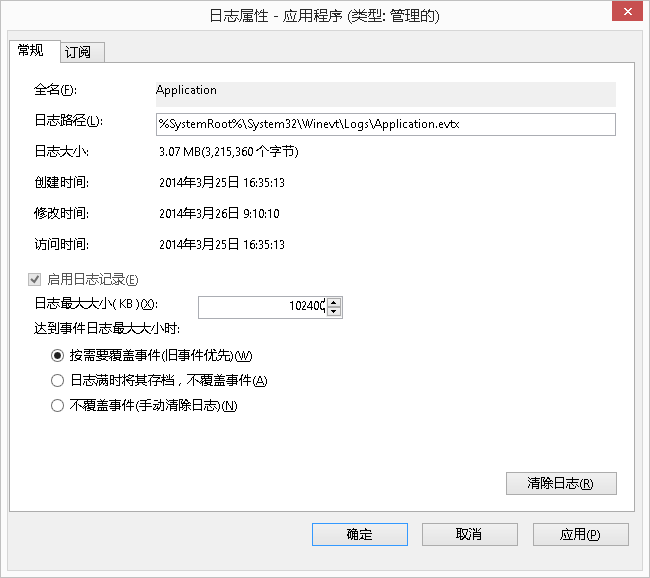
* 1. 日志文件设置

日志文件可以记录计算机终端的应用程序、安全性、系统的日志信息，对日志文件的合理设置可以保证系统记录的日志更合理及对系统出现问题时进行有效追踪。

设置要求：必须设置方法：

1、打开『控制面板』->『所有控制面板项』->『管理工具』，双击“事件查看器”，或在 『 运 行 』 -> 输 入 eventvwr.msc， 并 确 认 。2、双击『Windows 日志』，右键单击“应用程序”，选择『属性』菜单。

3、复选“启用日志记录”，并分配适量的存储空间（计算机终端必须保存 30 天的日志， 按使用的频率设置相应大小，建议不小于 102400Kb）。



==============================================

# 注意：

如需要保存更长时间的日志文件，可以选择“日志满时将其存档，不覆盖事件”选项；事件日志缺省自动存储在“C:\Windows\System32\Winevt\Logs”，当日志过多时，可以手动到相应目录删除存储的过时文件。

==============================================

2、『Windows 日志』下的“安全”和“系统”的日志设置方法同上。

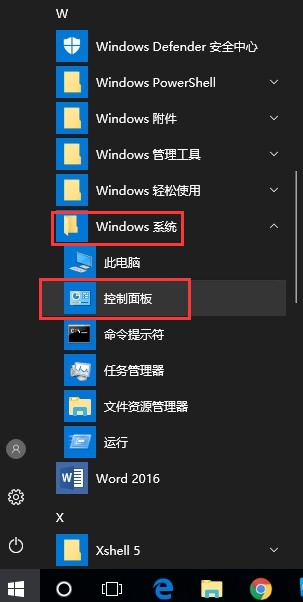
# FAQ

Q1：如何快捷打开控制面板及常用功能？ A1：

Win8：按 ? Win 键+“x”键，在屏幕左下角弹出：程序与功能、计算机管理、控制面板、运行、关机、重启、搜索、桌面等常用功能。



?Win10：按下 Win 键，在弹出屏幕中选择“所有程序”；然后依次选择“Windows 系统”->“控制面板”。

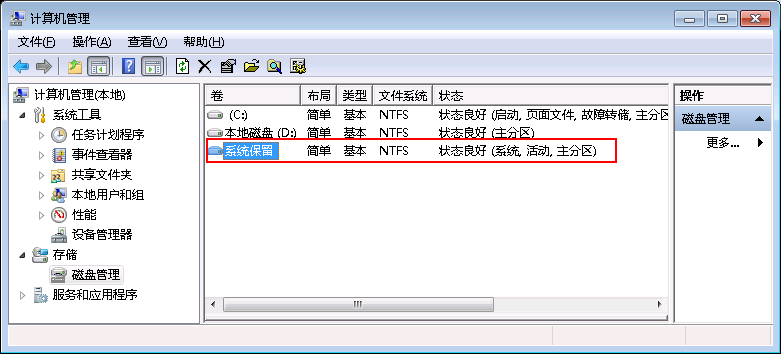


Q2：操作系统安装后，在磁盘分区管理中，为什么有一个系统保留分区？

A2：启动磁盘分区管理（diskmgmt.msc）后，可以看到系统保留分区（System

Reserved），这个分区中保存了用于启动 Windows 7 系统的所有引导文件，以及

WinRE(Windows 恢复环境)使用的必要文件，如果将其删除，或进行其它操作，将导致 Windows 7 无法正常启动及修复。



# 附录

1. 常见的服务和功能说明

|  |  |  |  |
| --- | --- | --- | --- |
| **序**  **号** | **服务名称** | **描述** | **服务路径** |
| 1 | Application Experience | 在应用程序启动时处理应用程序兼容型查询请求。该服务的默认运行方式是自动，不建议更改。 | *\\WINDOWS\system3*  *2\svchost.exe -k netsvcs* |
| 2 | Application Layer Gateway  Service | 为 Internet 连接共享提供第三方协议插件的支持。该服务的默认运行方式是手动，如果你连接  了网络，则该服务会自动启动，不建议更改。 | *\\WINDOWS\System3 2\alg.exe* |
| 3 | Application Management | 为活动目录的智能镜像(IntelliMirror)组策略程序提供软件的安装、卸载和枚举等操作。如果该服务停止，用户将无法安装、删除或枚举任何使用智能镜像方式安装的程序。如果该服务被禁用， 任何依赖该服务的其他服务都将无法运行。该服务默认的运行方式为手动，该功能主要适用于大  型企业环境下的集中管理。 | *\\WINDOWS\system3 2\svchost.exe -k netsvcs* |
| 4 | Background Intelligent Transfer Service | 在后台传输客户端和服务器之间的数据。如果禁用了 BITS，一些功能，如 Windows Update， 就无法正常运行。该服务的默认运行方式是自动， 这个服务的主要用途还是用于进行 Windows  Update 或者自动更新，最好不要更改这个服务。 | *\\WINDOWS\System3 2\svchost.exe -k netsvcs* |
| 5 | Computer Browser | 维护网络上计算机的更新列表，并将列表提供给计算机指定浏览。如果服务停止，列表不会被更新或维护。如果服务被禁用，任何直接依赖于此服务的服务将无法启动。该服务的默认运行方式为自动，不过如果你没有使用局域网或者你根本就不想使用局域网，该功能就可以放心禁用，禁用后任然可以使用\\IP 这样的 UNC 路径访问其  他共享的计算机。 | *\\WINDOWS\system3 2\svchost.exe -k netsvcs* |

|  |  |  |  |
| --- | --- | --- | --- |
| 6 | Cryptographic Services | 提供三种管理服务: 编录数据库服务，它确定  Windows 文件的签字; 受保护的根服务，它从此计算机添加和删除受信根证书机构的证书;和密钥(Key)服务，它帮助注册此计算机获取证书。如果此服务被终止，这些管理服务将无法正常运行。如果此服务被禁用，任何依赖它的服务将无法启动。维护和管理系统的所有证书，密钥以及安全数据库。另外访问一些网站所需要的服务， 比如微软的网站，Windows Update，或者 DRM 的网站，很多时候它会提供和确认 Windows 文  件的签名信息。 | *\\WINDOWS\system3 2\svchost.exe -k netsvcs* |
| 7 | DHCP Client | 通过注册和更改 IP 地址以及 DNS 名称来管理网络配置。如果该服务停止了，这台计算机将无法收到动态 IP 地址以及 DNS 的更新。如果该服务被禁用了，那么任何依赖该服务的其他服务都将无法运行。该服务的默认运行方式是自动， 如果是手动指定的 IP ，完全可以禁用。只有WinHTTP Web Proxy Auto-Discovery  Service 这个服务依赖它。 | *\\Windows\system32\ svchost.exe -k LocalServiceNetworkR estricted* |
| 8 | DNS Client | 为此计算机解析和缓冲域名系统 (DNS) 名称。如果此服务被停止，计算机将不能解析 DNS 名称并定位 Active Directory 域控制器。 | *\\WINDOWS\system3 2\svchost.exe -k NetworkService* |
| 9 | IPsec Policy Agent | Internet 协议安全(IPSec)支持网络级别的对等身份验证、数据原始身份验证、数据完整性、数据机密性(加密)以及重播保护。此服务强制执行通过 IP 安全策略管理单元或命令行工具“netsh ipsec” 创建的 IPSec 策略。停止此服务时，如果策略需要连接使用 IPSec，可能会遇到网络连接问题。同样，此服务停止时，Windows防火墙的远程管理也不再可用。某些公司的网络环境要求必须打开，它提供一个 TCP/IP 网络上客户端和服务器之间端到端的安全连接。其他的  情况建议设置成禁用。 | *\\Windows\system32\ svchost.exe -k NetworkServiceNetwor kRestricted* |
| 10 | Program Compatibility Assistant  Service | 为程序兼容性助手提供支持。 | *\\Windows\system32\ svchost.exe -k LocalSystemNetworkR*  *estricted* |
| 11 | Remote Procedure Call (RPC) | 作为终结点映射程序(endpoint mapper) 和  COM 服务控制管理器使用。如果此服务被停用  或禁用，使用 COM 或远程过程调用(RPC)服务的程序工作将不正常。 | *\\Windows\system32\ svchost.exe -k rpcss* |

|  |  |  |  |
| --- | --- | --- | --- |
| 12 | Remote Registry | 使远程用户能修改此计算机上的注册表设置。如果此服务被终止，只有此计算机上的用户才能修改注册表。如果此服务被禁用，任何依赖它的服  务将无法启动。 | *\\Windows\system32\ svchost.exe -k regsvc* |
| 13 | Server | 支持此计算机通过网络的文件、打印、和命名管道共享。如果服务停止，这些功能不可用。如果服务被禁用，任何直接依赖于此服务的服务将无法启动。保证本机接入网络的文件、打印机和命名管道共享管理，如果不需要在网络上共享什么  东西就可以关掉。 | *\\Windows\system32\ svchost.exe -k netsvcs* |
| 14 | Task Scheduler | 使用户能在此计算机上配置和制定自动任务的日程。如果此服务被终止，这些任务将无法在日程时间里运行。如果此服务被禁用，任何依赖它的  服务将无法启动。 | *\\Windows\system32\ svchost.exe -k netsvcs* |
| 15 | TCP/IP  NetBIOS Helper | 提供 TCP/IP (NetBT) 服务上的 NetBIOS 和网络上客户端的 NetBIOS 名称解析的支持，从而使用户能够共享文件、打印和登录到网络。如果此服务被停用，这些功能可能不可用。如果此服务被禁用，任何依赖它的服务将无法启动。主要是支持 NetBIOS 名称的解析，使得你可以在  计算机之间进行文件和打印机共享、网络登录。 | *\\Windows\system32\ svchost.exe -k LocalServiceNetworkR estricted* |
| 16 | Windows Audio | 管理基于 Windows 的程序的音频。如果此服务被停止，音频设备和效果将不能正常工作。如果此服务被禁用，任何依赖它的服务将无法启动。 | *\\Windows\System32\ svchost.exe -k LocalServiceNetworkR*  *estricted* |
| 17 | Windows Audio Endpoint Builder | 管理 Windows 音频服务的音频设备。如果此服务被停止，音频设备和效果将不能正常工作。如果此服务被禁用，任何依赖它的服务将无法启动。 | *\\Windows\System32\ svchost.exe -k LocalSystemNetworkR*  *estricted* |
| 18 | Windows Backup | 提供 Windows 备份和还原功能。Windows 备份和版本恢复功能，一直都不好使。 | *\\Windows\System32\ svchost.exe -k*  *SDRSVC* |
| 19 | Windows Error Reporting Service | 允许在程序停止运行或停止响应时报告错误，并允许提供现有解决方案。还允许为诊断和修复服务生成日志。如果此服务被停止，则错误报告将无法正确运行，而且可能不显示诊断服务和修复  的结果。 | *\\Windows\System32\ svchost.exe -k WerSvcGroup* |
| 20 | Windows Event Log | 此服务管理事件和事件日志。它支持日志记录事件、查询事件、订阅事件、归档事件日志以及管理事件元数据。它可以用 XML 和纯文本两种格式显示事件。停止该服务可能危及系统的安全性和可靠性。Vista 和其他系统程序经常会用到，  这个不是必须的服务。 | *\\Windows\System32\ svchost.exe -k LocalServiceNetworkR estricted* |

|  |  |  |  |
| --- | --- | --- | --- |
| 21 | Windows Search | 为文件、电子邮件以及其他内容(通过可扩展性  API)提供内容索引和属性缓存。该服务响应文件和电子邮件通知，从而对已修改的内容编制索引。如果该服务已停止或被禁用，资源管理器将无法显示项目的虚拟文件夹视图，在资源管理器中搜索将回退为速度较慢的逐项搜索。新的桌面搜索功能，默认范围太小，扩大了又很耗费资源，可  以试试。 | *\\Windows\system32\ SearchIndexer.exe*  */Embedding* |
| 22 | Windows Time | 维护在网络上的所有客户端和服务器的时间和日期同步。如果此服务被停止，时间和日期的同步将不可用。如果此服务被禁用，任何明确依赖它  的服务都将不能启动。 | *\\Windows\system32\ svchost.exe -k LocalService* |
| 23 | Windows Update | 启用检测、下载和安装 Windows 和其他程序的更新。如果此服务被禁用，这台计算机的用户将无法使用 Windows Update 或其自动更新功能，并且这些程序将无法使用 Windows Update Agent (WUA) API。Windows Update 这个功能取决于你了，它和 Background Intelligent Transfer Service 、 Modules  Installer 服务关联。 | *\\Windows\system32\ svchost.exe -k netsvcs* |
| 24 | WLAN  AutoConfig | 该服务枚举 WLAN 适配器，管理 WLAN 连接和配置文件。很多的时候，还是要自己设置的， 不用无线网络可以关掉。 | *\\Windows\system32\ svchost.exe -k LocalSystemNetworkR*  *estricted* |
| 25 | Workstation | 使用 SMB 协议创建并维护客户端网络与远程服务器之间的连接。如果此服务已停止，这些连接将无法使用。如果此服务已禁用，任何明确依赖它的服务将无法启动。创建和管理到远程服务器的网络连接，一般在网络环境中，特别是局域网中是一个必须的服务，不需访问别人的共享资  源时可以设为手动。 | *\\Windows\System32\ svchost.exe -k LocalService* |

1. 常见端口说明

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **端口** | **服务名** | | **说明** | | |
| 1 | 666 | Doom  Software | Id | 木马 Attack FTP、Satanz Backdoor 开放此端口 | | |
| 2 | 1999 | cisco identification  port | | 木马 BackDoor 开放此端口。 | | |
| 3 | 5000、5001、  5321、50505 |  | | 木马 blazer5 开放 5000 端口。木马 Sockets de Troie 开放  5000、5001、5321、50505 端口。 | | |
| 4 | 2115 |  | | 木马 Bugs 开放此端口。 | | |
| 5 | 2140、3150 |  | | 木马 Deep | Throat | 1.0/3.0 开放此端口。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 6 | 1492 | stone-design  -1 | 木马 FTP99CMP 开放此端口。 |
| 7 | 2000 |  | 木马 GirlFriend 1.3、Millenium 1.0 开放此端口。 |
| 8 | 4590 |  | 木马 ICQTrojan 开放此端口。 |
| 9 | 3129 |  | 木马 Master Paradise 开放此端口。 |
| 10 | 2001 |  | 木马 Millenium 1.0、Trojan Cow 开放此端口。 |
| 11 | 1025、1033 | network  blackjack | 木马 netspy 开放这 2 个端口。 |
| 12 | 2023 | xinuexpansi  on 4 | 木马 Pass Ripper 开放此端口。 |
| 13 | 555 | DSF | 木马 PhAse1.0、Stealth Spy、IniKiller 开放此端口。 |
| 14 | 2801 |  | 木马 Phineas Phucker 开放此端口。 |
| 15 | 3700 |  | 木马 Portal of Doom 开放此端口 |
| 16 | 3333 | dec-notes | 木马 Prosiak 开放此端口 |
| 17 | 3996、4060 |  | 木马 RemoteAnything 开放此端口 |
| 18 | 3210、4321 |  | 木马 SchoolBus 开放此端口 |
| 19 | 1600 | issd | 木马 Shivka-Burka 开放此端口。 |
| 20 | 1981 |  | 木马 ShockRave 开放此端口。 |
| 21 | 1001、1011 |  | 木马 Silencer、WebEx 开放 1001 端口。木马 Doly Trojan  开放 1011 端口。 |
| 22 | 1807 |  | 木马 SpySender 开放此端口。 |
| 23 | 1170 |  | 木马 Streaming Audio Trojan、Psyber Stream Server、  Voice 开放此端 口。 |
| 24 | 1234、1243、  6711、6776 |  | 木马 SubSeven2.0、Ultors Trojan 开放 1234、6776 端口。木马 SubSeven1.0/1.9 开放 1243、6711、6776 端口 。 |
| 25 | 3150 |  | 木马 The Invasor 开放此端口。 |
| 26 | 1245 |  | 木马 Vodoo 开放此端口。 |
| 27 | 2583 |  | 木马 Wincrash 2.0 开放此端口。 |
| 28 | 3024、4092 |  | 木马 WinCrash 开放此端口。 |
| 29 | 4092 |  | 木马 WinCrash 开放此端口。 |
| 30 | 635 | mountd | Linux 的 mountd Bug。这是扫描的一个流行 BUG。大多数对这个端口的扫描是基于UDP 的，但是基 于TCP 的mountd 有所增加（mountd 同时运行于两个端口）。记住 mountd 可运行 于任何端口（到底是哪个端口，需要在端口 111 做  portmap 查询），只是 Linux 默 认端口是 635，就像 NFS  通常运行于 2049 端口。 |
| 31 | 1433 | SQL | Microsoft 的 SQL 服务开放的端口。 |
| 32 | 1720 | NetMeeting | NetMeeting H.233 call Setup。 |
| 33 | 1503 | NetMeeting  T.120 | NetMeeting T.120 |

|  |  |  |  |
| --- | --- | --- | --- |
| 34 | 1731 | NetMeeting Audio Call  Control | NetMeeting 音频调用控制。 |
| 35 | 2049 | NFS | NFS 程序常运行于这个端口。通常需要访问 Portmapper 查  询这个服务运行 于哪个端口。 |
| 36 | 1500 | RPC client  fixed port session queries | RPC 客户固定端口会话查询 |
| 37 | 636 | LDAP | SSL（Secure Sockets layer） |
| 38 | 993 | IMAP | SSL（Secure Sockets layer） |
| 39 | 3389 | 超级终端 | WINDOWS 远程桌面端口。 |
| 40 | 568 | Membership  DPA | 成员资格 DPA。 |
| 41 | 569 | Membership  MSN | 成员资格 MSN。 |
| 42 | 1024 | Reserved | 它是动态端口的开始，许多程序并不在乎用哪个端口连接网络，它们请 求系统为它们分配下一个闲置端口。基于这一点分配从端口 1024 开始。这就是 说第一个向系统发出请求的会分配到 1024 端口。你可以重启机器，打开 Telnet ，再打开一个窗口运行 natstat -a 将会看到 Telnet 被分配 1024  端口。还有 SQL session 也用此端口和 5000 端口 。 |
| 43 | 4000 | QQ 客户端 | 腾讯 QQ 客户端开放此端口。 |
| 44 | 1524 | ingress | 许多攻击脚本将安装一个后门 SHELL 于这个端口，尤其是针对 SUN 系统中 Sendmail 和 RPC 服务漏洞的脚本。如果刚安装了防火墙就看到在这个端口上的连 接企图，很可能是上述原因。可以试试 Telnet 到用户的计算机上的这个端口， 看看它是否会给你一个 SHELL。连接到 600/pcserver 也存在  这个问题。 |
| 45 | 2500 | RPC client using a fixed port session  replication | 应用固定端口会话复制的 RPC 客户 |
| 46 | 3128 | squid | 这是 squid HTTP 代理服务器的默认端口。攻击者扫描这个端口是为了搜寻一个代理服务器 而匿名访问 Internet。也会看到搜索其他代理服务器的端口 8000、8001、 8080 、  8888。扫描这个端口的另一个原因是用户正在进入聊天室。其他用户也会检 验这个端口以确定用户的机器是否支持代  理。 |
| 47 | 1080 | SOCKS | 这一协议以通道方式穿过防火墙，允许防火墙后面的人通过一个 IP 地址 访问 INTERNET。理论上它应该只允许内部的通信向外到达 INTERNET。但是由于 错误的配置，它会允许位于防火墙外部的攻击穿过防火墙。 |

|  |  |  |  |
| --- | --- | --- | --- |
| 48 | 139、445 |  | 网络共享端口。 |