关于服务

[服务控制管理器](https://learn.microsoft.com/zh-cn/windows/win32/services/service-control-manager) (SCM) 维护已安装服务和驱动程序服务的数据库，并提供统一且安全的方法来控制它们。 该数据库包含有关如何启动每个服务或驱动程序服务的信息。 它还使系统管理员能够自定义每个服务的安全要求，从而控制对服务的访问。

以下类型的程序使用 SCM 提供的函数。

展开表

| **类型** | **说明** |
| --- | --- |
| 服务计划 | 为一个或多个服务提供可执行代码的程序。 服务程序使用连接到 SCM 并将状态信息发送到 SCM 的函数。 |
| 服务配置程序 | 查询或修改服务数据库的程序。 服务配置程序使用打开数据库、在数据库中安装或删除服务以及查询或修改已安装服务的配置和安全参数的函数。 服务配置程序同时管理服务和驱动程序服务。 |
| 服务控制程序 | 启动和控制服务和驱动程序服务的程序。 服务控制程序使用将请求发送到执行请求的 SCM 的函数。 |

本概述讨论以下主题：

# [服务控制管理器](https://learn.microsoft.com/zh-cn/windows/win32/services/service-control-manager)

服务控制管理器 (SCM) 在系统启动时启动。 它是一个远程过程调用， (RPC) 服务器，以便服务配置和服务控制程序可以操作远程计算机上的服务。

服务函数为 SCM 执行的以下任务提供接口：

* 维护已安装服务的数据库。
* 在系统启动时或按需启动服务和驱动程序服务。
* 枚举已安装的服务和驱动程序服务。
* 维护正在运行的服务和驱动程序服务的状态信息。
* 将控制请求传输到正在运行的服务。
* 锁定和解锁服务数据库。

以下部分更详细地介绍了 SCM：

* [已安装服务的数据库](https://learn.microsoft.com/zh-cn/windows/win32/services/database-of-installed-services)
* [自动启动服务](https://learn.microsoft.com/zh-cn/windows/win32/services/automatically-starting-services)
* [按需启动服务](https://learn.microsoft.com/zh-cn/windows/win32/services/starting-services-on-demand)
* [服务记录列表](https://learn.microsoft.com/zh-cn/windows/win32/services/service-record-list)
* [SCM 句柄](https://learn.microsoft.com/zh-cn/windows/win32/services/scm-handles)

# [服务计划](https://learn.microsoft.com/zh-cn/windows/win32/services/service-programs)

*服务程序*包含一个或多个服务的可执行代码。 使用 SERVICE\_WIN32\_OWN\_PROCESS 类型创建的服务程序仅包含一个服务的代码。 使用 类型创建的服务程序SERVICE\_WIN32\_SHARE\_PROCESS包含多个服务的代码，使它们能够共享代码。 执行此操作的服务程序的一个示例是托管内部 Windows 服务的泛型服务主机进程Svchost.exe。 请注意，Svchost.exe保留供操作系统使用，不应由非 Windows 服务使用。 相反，开发人员应实现自己的服务托管程序。

可以将服务程序配置为从内置 (本地) 、主域或受信任的域在用户帐户的上下文中执行。 还可以将其配置为在特殊 [服务用户帐户](https://learn.microsoft.com/zh-cn/windows/win32/services/service-user-accounts)中运行。

以下主题介绍服务程序必须包括 [的服务控制管理器](https://learn.microsoft.com/zh-cn/windows/win32/services/service-control-manager) (SCM) 的接口要求：

* [服务入口点](https://learn.microsoft.com/zh-cn/windows/win32/services/service-entry-point)
* [Service ServiceMain 函数](https://learn.microsoft.com/zh-cn/windows/win32/services/service-servicemain-function)
* [服务控制处理程序函数](https://learn.microsoft.com/zh-cn/windows/win32/services/service-control-handler-function)

这些主题不适用于驱动程序服务。 有关驱动程序服务的接口要求，请参阅 Windows 驱动程序工具包 (WDK) 。

服务作为后台进程运行，可能会影响系统性能、响应能力、能源效率和安全性。 有关服务优化指南，请参阅 [开发适用于 Windows 的高效后台进程](https://learn.microsoft.com/zh-cn/windows-hardware/drivers/kernel/implementing-power-management)。 以下主题介绍其他编程注意事项：

* [服务状态转换](https://learn.microsoft.com/zh-cn/windows/win32/services/service-status-transitions)
* [在服务中接收事件](https://learn.microsoft.com/zh-cn/windows/win32/services/receiving-events-in-a-service)
* [多线程服务](https://learn.microsoft.com/zh-cn/windows/win32/services/multithreaded-services)
* [服务和注册表](https://learn.microsoft.com/zh-cn/windows/win32/services/services-and-the-registry)
* [服务和重定向的驱动器](https://learn.microsoft.com/zh-cn/windows/win32/services/services-and-redirected-drives)
* [服务触发器事件](https://learn.microsoft.com/zh-cn/windows/win32/services/service-trigger-events)

请注意，如果服务程序充当 RPC 服务器，则应使用动态终结点和相互身份验证。

# [服务配置程序](https://learn.microsoft.com/zh-cn/windows/win32/services/service-configuration-programs)

程序员和系统管理员使用服务配置程序来修改或查询已安装服务的数据库。 也可以使用注册表函数访问数据库。 但是，应仅使用 SCM 配置函数，这可确保正确安装和配置服务。

SCM 配置函数需要 SCManager 对象的句柄或服务对象的句柄。 若要获取这些句柄，服务配置程序必须：

1. 使用 [**OpenSCManager**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-openscmanagera) 函数获取指定计算机上的 SCM 数据库的句柄。
2. 使用 [**OpenService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-openservicea) 或 [**CreateService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-createservicea) 函数获取服务对象的句柄。

有关详情，请参阅以下主题：

* [服务安装、删除和枚举](https://learn.microsoft.com/zh-cn/windows/win32/services/service-installation-removal-and-enumeration)
* [服务配置](https://learn.microsoft.com/zh-cn/windows/win32/services/service-configuration)
* [使用 SC 配置服务](https://learn.microsoft.com/zh-cn/windows/win32/services/configuring-a-service-using-sc)

# [服务控制程序](https://learn.microsoft.com/zh-cn/windows/win32/services/service-control-programs)

服务控制程序启动并控制服务。 它将执行以下操作：

* 如果启动类型为SERVICE\_DEMAND\_START，则启动服务或驱动程序服务。
* 将控制请求发送到正在运行的服务。
* 查询正在运行的服务的当前状态。

这些操作需要服务对象的打开句柄。 若要获取句柄，服务控制程序必须：

1. 使用 [**OpenSCManager**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-openscmanagera) 函数获取指定计算机上的 SCM 数据库的句柄。
2. 使用 [**OpenService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-openservicea) 或 [**CreateService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-createservicea) 函数获取服务对象的句柄。

有关详情，请参阅以下主题：

* [服务启动](https://learn.microsoft.com/zh-cn/windows/win32/services/service-startup)
* [服务控制请求](https://learn.microsoft.com/zh-cn/windows/win32/services/service-control-requests)
* [使用 SC 控制服务](https://learn.microsoft.com/zh-cn/windows/win32/services/controlling-a-service-using-sc)

# [服务用户帐户](https://learn.microsoft.com/zh-cn/windows/win32/services/service-user-accounts)

每个服务在用户帐户的安全上下文中执行。 帐户的用户名和密码在安装服务时由 [**CreateService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-createservicea) 函数指定。 可以使用 [**ChangeServiceConfig**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-changeserviceconfiga) 函数更改用户名和密码。 可以使用 [**QueryServiceConfig**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryserviceconfiga) 函数获取用户名 (但不能获取与服务对象关联的密码) 。 服务控制管理器 (SCM) 会自动加载用户配置文件。

启动服务时，SCM 会登录到与该服务关联的帐户。 如果登录成功，系统会生成访问令牌并将其附加到新的服务进程。 此令牌标识与安全对象的所有后续交互中的服务进程， (具有) 关联的安全描述符的对象。 例如，如果服务尝试打开管道的句柄，系统会在授予访问权限之前将服务的访问令牌与管道的安全描述符进行比较。

SCM 不维护服务用户帐户的密码。 如果密码已过期，则登录失败，服务无法启动。 将帐户分配到服务的系统管理员可以使用永不过期的密码创建帐户。 管理员还可以使用 [服务配置程序](https://learn.microsoft.com/zh-cn/windows/win32/services/service-configuration-programs) 定期更改密码来管理密码过期的帐户。

如果服务需要在共享其信息之前识别另一个服务，则第二个服务可以使用与第一个服务相同的帐户，也可以在属于第一个服务识别的别名的帐户中运行。 需要跨网络以分布式方式运行的服务应在域范围的帐户中运行。

可以指定以下特殊帐户之一，而不是为服务指定用户帐户：

* [LocalService](https://learn.microsoft.com/zh-cn/windows/win32/services/localservice-account)
* [NetworkService](https://learn.microsoft.com/zh-cn/windows/win32/services/networkservice-account)
* [LocalSystem](https://learn.microsoft.com/zh-cn/windows/win32/services/localsystem-account)

# [交互式服务](https://learn.microsoft.com/zh-cn/windows/win32/services/interactive-services)

通常，服务是控制台应用程序，设计为在没有图形用户界面 (GUI) 的情况下无人参与运行。 但是，某些服务可能需要偶尔与用户交互。 本页讨论从服务与用户交互的最佳方法。

**重要**

从 Windows Vista 起，服务无法直接与用户交互。 因此，不应在新代码中使用标题为“使用交互式服务”一节中提到的技术。

## 从服务间接与用户交互

可以使用以下技术在所有受支持的 Windows 版本上通过服务与用户交互：

* 使用 [**WTSSendMessage**](https://learn.microsoft.com/zh-cn/windows/desktop/api/wtsapi32/nf-wtsapi32-wtssendmessagea) 函数在用户会话中显示一个对话框。
* 创建单独的隐藏 GUI 应用程序，并使用 [**CreateProcessAsUser**](https://learn.microsoft.com/zh-cn/windows/desktop/api/processthreadsapi/nf-processthreadsapi-createprocessasusera) 函数在交互式用户的上下文中运行应用程序。 将 GUI 应用程序设计为通过某种进程间通信方法与服务通信 (IPC) ，例如命名管道。 该服务与 GUI 应用程序通信，以告知它何时显示 GUI。 应用程序将用户交互的结果传达回服务，以便服务可以采取适当的操作。 请注意，除非使用适当的访问控制列表 (ACL) ，否则 IPC 可以通过网络公开服务接口。

如果此服务在多用户系统上运行，请将应用程序添加到以下密钥，使其在每个会话中运行： **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**。 如果应用程序对 IPC 使用命名管道，则服务器可以通过根据会话 ID 为每个管道指定唯一名称来区分多个用户进程。

以下技术也适用于 Windows Server 2003 和 Windows XP：

* 使用 **MB\_SERVICE\_NOTIFICATION** 调用 MessageBox 函数来显示[**消息框**](https://learn.microsoft.com/zh-cn/windows/win32/api/winuser/nf-winuser-messagebox)。 建议用于显示简单状态消息。 除非从单独的线程调用 MessageBox，否则请勿在服务初始化期间或从 [**HandlerEx**](https://learn.microsoft.com/zh-cn/windows/desktop/api/WinSvc/nc-winsvc-lphandler_function_ex) 例程调用 **MessageBox**，以便及时返回到 SCM。

## 使用交互式服务

默认情况下，服务使用非交互式 [窗口工作站](https://learn.microsoft.com/zh-cn/windows/desktop/winstation/window-stations) ，并且无法与用户交互。 但是， 交互式服务 可以显示用户界面并接收用户输入。

**注意**

在提升的安全上下文中运行的服务（如 LocalSystem 帐户）不应在交互式桌面上创建窗口，因为在交互式桌面上运行的任何其他应用程序都可以与此窗口交互。 这会将服务公开给登录用户执行的任何应用程序。 此外，作为 LocalSystem 运行的服务不应通过调用 [**OpenWindowStation**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winuser/nf-winuser-openwindowstationa) 或 [**GetThreadDesktop**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winuser/nf-winuser-getthreaddesktop) 函数来访问交互式桌面。

若要创建交互式服务，请在调用 [**CreateService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-createservicea) 函数时执行以下操作：

1. 为 lpServiceStartName 参数指定 NULL，以便在 [LocalSystem 帐户](https://learn.microsoft.com/zh-cn/windows/win32/services/localsystem-account)的上下文中运行服务。
2. 指定 **SERVICE\_INTERACTIVE\_PROCESS** 标志。

若要确定服务是否作为交互式服务运行，请调用 [**GetProcessWindowStation**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winuser/nf-winuser-getprocesswindowstation) 函数以检索窗口站的句柄，并调用 [**GetUserObjectInformation**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winuser/nf-winuser-getuserobjectinformationa) 函数来测试窗口工作站是否具有 **WSF\_VISIBLE** 属性。

但请注意，以下注册表项包含一个值 **NoInteractiveServices**，该值控制SERVICE\_INTERACTIVE\_PROCESS的效果：

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Windows**

**NoInteractiveServices** 值默认为 1，这意味着无论服务是否具有**SERVICE\_INTERACTIVE\_PROCESS**，都不允许以交互方式运行任何服务。 当 **NoInteractiveServices** 设置为 0 时，允许具有 **SERVICE\_INTERACTIVE\_PROCESS** 的服务以交互方式运行。

**Windows 7、Windows Server 2008 R2、Windows XP 和 Windows Server 2003：NoInteractiveServices** 值默认为 0，这意味着允许具有**SERVICE\_INTERACTIVE\_PROCESS**的服务以交互方式运行。 当 **NoInteractiveServices** 设置为非零值时，无论它是否具有 **SERVICE\_INTERACTIVE\_PROCESS**，之后启动的服务都不允许以交互方式运行。

**重要**

所有服务都在终端服务会话 0 中运行。 因此，如果交互式服务显示用户界面，则它仅对连接到会话 0 的用户可见。 由于无法保证交互式用户连接到会话 0，因此不要将服务配置为在终端服务下或支持快速用户切换的系统上作为交互式服务运行， (使用终端服务) 实现快速用户切换。

# [服务安全性和访问权限](https://learn.microsoft.com/zh-cn/windows/win32/services/service-security-and-access-rights)

使用 Windows 安全模型可以控制对服务控制管理器 (SCM) 和服务对象的访问。 以下部分提供了详细信息：

* [服务控制管理器的访问权限](https://learn.microsoft.com/zh-cn/windows/win32/services/service-security-and-access-rights#access-rights-for-the-service-control-manager)
* [服务的访问权限](https://learn.microsoft.com/zh-cn/windows/win32/services/service-security-and-access-rights#access-rights-for-a-service)

## 服务控制管理器的访问权限

下面是 SCM 的特定访问权限。

展开表

| **访问权限** | **说明** |
| --- | --- |
| **SC\_MANAGER\_ALL\_ACCESS** (0xF003F) | 除此表中的所有访问权限外，还包括 **STANDARD\_RIGHTS\_REQUIRED**。 |
| **SC\_MANAGER\_CREATE\_SERVICE** (0x0002) | 需要调用 [**CreateService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-createservicea) 函数来创建服务对象并将其添加到数据库。 |
| **SC\_MANAGER\_CONNECT** (0x0001) | 连接到服务控制管理器所必需的。 |
| **SC\_MANAGER\_ENUMERATE\_SERVICE** (0x0004) | 需要调用 [**EnumServicesStatus**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-enumservicesstatusa) 或 [**EnumServicesStatusEx**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-enumservicesstatusexa) 函数来列出数据库中的服务。 需要调用 [**NotifyServiceStatusChange**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-notifyservicestatuschangea) 函数，以便在创建或删除任何服务时接收通知。 |
| **SC\_MANAGER\_LOCK** (0x0008) | 需要调用 [**LockServiceDatabase**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-lockservicedatabase) 函数来获取数据库的锁。 |
| **SC\_MANAGER\_MODIFY\_BOOT\_CONFIG** (0x0020) | 调用 [**NotifyBootConfigStatus**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-notifybootconfigstatus) 函数所必需的。 |
| **SC\_MANAGER\_QUERY\_LOCK\_STATUS** (0x0010) | 需要调用 [**QueryServiceLockStatus**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryservicelockstatusa) 函数来检索数据库的锁状态信息。 |

下面是 SCM 的 [一般访问权限](https://learn.microsoft.com/zh-cn/windows/desktop/SecAuthZ/generic-access-rights) 。

展开表

| **访问权限** | **说明** |
| --- | --- |
| **GENERIC\_READ** | **STANDARD\_RIGHTS\_READ** **SC\_MANAGER\_ENUMERATE\_SERVICE** **SC\_MANAGER\_QUERY\_LOCK\_STATUS** |
| **GENERIC\_WRITE** | **STANDARD\_RIGHTS\_WRITE** **SC\_MANAGER\_CREATE\_SERVICE** **SC\_MANAGER\_MODIFY\_BOOT\_CONFIG** |
| **GENERIC\_EXECUTE** | **STANDARD\_RIGHTS\_EXECUTE** **SC\_MANAGER\_CONNECT** **SC\_MANAGER\_LOCK** |
| **GENERIC\_ALL** | **SC\_MANAGER\_ALL\_ACCESS** |

具有正确访问权限的进程可以打开可在 [**OpenService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-openservicea)、 [**EnumServicesStatusEx 和 QueryServiceLockStatus**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-enumservicesstatusexa) 函数中使用的 SCM [**的**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryservicelockstatusa) 句柄。 只有具有管理员权限的进程才能打开可供 CreateService 和 [**LockServiceDatabase**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-lockservicedatabase) 函数使用的 SCM 的句柄。

系统为 SCM 创建安全描述符。 若要获取或设置 SCM 的安全描述符，请使用 [**QueryServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-queryserviceobjectsecurity) 和 [**SetServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-setserviceobjectsecurity) 函数以及 SCManager 对象的句柄。

**Windows Server 2003 和 Windows XP：** 与大多数其他安全对象不同，无法修改 SCM 的安全描述符。 自 Windows Server 2003 Service Pack 1 (SP1) 起，此行为已更改。

授予以下访问权限。

展开表

| **帐户** | **自动删除** |
| --- | --- |
| 经过身份验证的远程用户 | **SC\_MANAGER\_CONNECT** |
| 本地经过身份验证的用户 (包括 LocalService 和 NetworkService) | **SC\_MANAGER\_CONNECT** **SC\_MANAGER\_ENUMERATE\_SERVICE** **SC\_MANAGER\_QUERY\_LOCK\_STATUS** **STANDARD\_RIGHTS\_READ** |
| LocalSystem | **SC\_MANAGER\_CONNECT** **SC\_MANAGER\_ENUMERATE\_SERVICE** **SC\_MANAGER\_MODIFY\_BOOT\_CONFIG** **SC\_MANAGER\_QUERY\_LOCK\_STATUS** **STANDARD\_RIGHTS\_READ** |
| 管理员 | **SC\_MANAGER\_ALL\_ACCESS** |

请注意，通过网络进行身份验证但未以交互方式登录的远程用户可以连接到 SCM，但不能执行需要其他访问权限的操作。 若要执行这些操作，用户必须以交互方式登录，否则服务必须使用其中一个服务帐户。

**Windows Server 2003 和 Windows XP：** 通过身份验证的远程用户被授予 **SC\_MANAGER\_CONNECT**、 **SC\_MANAGER\_ENUMERATE\_SERVICE**、 **SC\_MANAGER\_QUERY\_LOCK\_STATUS**和 **STANDARD\_RIGHTS\_READ** 访问权限。 这些访问权限受到限制，如上表中所述，即 Windows Server 2003 SP1

当进程使用 [**OpenSCManager**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-openscmanagera) 函数打开已安装服务数据库的句柄时，它可以请求访问权限。 在授予请求的访问权限之前，系统会对 SCM 的安全描述符执行安全检查。

## 服务的访问权限

下面是服务的特定访问权限。

展开表

| **访问权限** | **说明** |
| --- | --- |
| **SERVICE\_ALL\_ACCESS** (0xF01FF) | 除此表中的所有访问权限外 **，还包括STANDARD\_RIGHTS\_REQUIRED** 。 |
| **SERVICE\_CHANGE\_CONFIG** (0x0002) | 需要调用 [**ChangeServiceConfig**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-changeserviceconfiga) 或 [**ChangeServiceConfig2**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-changeserviceconfig2a) 函数来更改服务配置。 由于这会授予调用方更改系统运行的可执行文件的权限，因此应仅向管理员授予该文件。 |
| **SERVICE\_ENUMERATE\_DEPENDENTS** (0x0008) | 需要调用 [**EnumDependentServices**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-enumdependentservicesa) 函数来枚举依赖于该服务的所有服务。 |
| **SERVICE\_INTERROGATE** (0x0080) | 需要调用 [**ControlService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-controlservice) 函数，要求服务立即报告其状态。 |
| **SERVICE\_PAUSE\_CONTINUE** (0x0040) | 需要调用 [**ControlService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-controlservice) 函数来暂停或继续服务。 |
| **SERVICE\_QUERY\_CONFIG** (0x0001) | 需要调用 [**QueryServiceConfig**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryserviceconfiga) 和 [**QueryServiceConfig2**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryserviceconfig2a) 函数来查询服务配置。 |
| **SERVICE\_QUERY\_STATUS** (0x0004) | 需要调用 [**QueryServiceStatus**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryservicestatus) 或 [**QueryServiceStatusEx**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryservicestatusex) 函数，以便向服务控制管理器询问服务的状态。 需要调用 [**NotifyServiceStatusChange**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-notifyservicestatuschangea) 函数，以便在服务更改状态时接收通知。 |
| **SERVICE\_START** (0x0010) | 需要调用 [**StartService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-startservicea) 函数来启动服务。 |
| **SERVICE\_STOP** (0x0020) | 需要调用 [**ControlService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-controlservice) 函数来停止服务。 |
| **SERVICE\_USER\_DEFINED\_CONTROL** (0x0100) | 需要调用 [**ControlService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-controlservice) 函数来指定用户定义的控件代码。 |

下面是服务 [的标准访问权限](https://learn.microsoft.com/zh-cn/windows/desktop/SecAuthZ/standard-access-rights) 。

展开表

| **访问权限** | **说明** |
| --- | --- |
| **ACCESS\_SYSTEM\_SECURITY** | 需要调用 [**QueryServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-queryserviceobjectsecurity) 或 [**SetServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-setserviceobjectsecurity) 函数来访问 SACL。 获取此访问权限的正确方法是在调用方当前访问令牌中启用 **SE\_SECURITY\_NAME**[**特权**](https://learn.microsoft.com/zh-cn/windows/desktop/SecAuthZ/privileges) ，打开 **ACCESS\_SYSTEM\_SECURITY** 访问的句柄，然后禁用该权限。 |
| **删除** (0x10000) | 需要调用 [**DeleteService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-deleteservice) 函数来删除服务。 |
| **READ\_CONTROL** (0x20000) | 需要调用 [**QueryServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-queryserviceobjectsecurity) 函数来查询服务对象的安全描述符。 |
| **WRITE\_DAC** (0x40000) | 需要调用 [**SetServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-setserviceobjectsecurity) 函数来修改服务对象的安全描述符的 **Dacl** 成员。 |
| **WRITE\_OWNER** (0x80000) | 需要调用 [**SetServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-setserviceobjectsecurity) 函数来修改服务对象的安全描述符的 **Owner** 和 **Group** 成员。 |

以下是服务的 [通用访问权限](https://learn.microsoft.com/zh-cn/windows/desktop/SecAuthZ/generic-access-rights) 。

展开表

| **访问权限** | **说明** |
| --- | --- |
| **GENERIC\_READ** | **STANDARD\_RIGHTS\_READ** **SERVICE\_QUERY\_CONFIG** **SERVICE\_QUERY\_STATUS** **SERVICE\_INTERROGATE** **SERVICE\_ENUMERATE\_DEPENDENTS** |
| **GENERIC\_WRITE** | **STANDARD\_RIGHTS\_WRITE** **SERVICE\_CHANGE\_CONFIG** |
| **GENERIC\_EXECUTE** | **STANDARD\_RIGHTS\_EXECUTE** **SERVICE\_START** **SERVICE\_STOP** **SERVICE\_PAUSE\_CONTINUE** **SERVICE\_USER\_DEFINED\_CONTROL** |

当 [**CreateService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-createservicea) 函数安装服务时，SCM 会创建服务对象的安全描述符。 服务对象的默认安全描述符授予以下访问权限。

展开表

| **帐户** | **自动删除** |
| --- | --- |
| 经过远程身份验证的用户 | 默认情况下不授予。**Windows Server 2003 SP1：SERVICE\_USER\_DEFINED\_CONTROL** **Windows Server 2003 和 Windows XP：** 经过远程身份验证的用户的访问权限与本地身份验证用户的访问权限相同。 |
| 本地经过身份验证的用户 (包括 LocalService 和 NetworkService) | **READ\_CONTROL** **SERVICE\_ENUMERATE\_DEPENDENTS** **SERVICE\_INTERROGATE** **SERVICE\_QUERY\_CONFIG** **SERVICE\_QUERY\_STATUS** **SERVICE\_USER\_DEFINED\_CONTROL** |
| LocalSystem | **READ\_CONTROL** **SERVICE\_ENUMERATE\_DEPENDENTS** **SERVICE\_INTERROGATE** **SERVICE\_PAUSE\_CONTINUE** **SERVICE\_QUERY\_CONFIG** **SERVICE\_QUERY\_STATUS** **SERVICE\_START** **SERVICE\_STOP** **SERVICE\_USER\_DEFINED\_CONTROL** |
| 管理员 | **DELETE** **READ\_CONTROL** **SERVICE\_ALL\_ACCESS** **WRITE\_DAC** **WRITE\_OWNER** |

若要执行任何操作，用户必须以交互方式登录，否则服务必须使用其中一个服务帐户。

若要获取或设置服务对象的安全描述符，请使用 [**QueryServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-queryserviceobjectsecurity) 和 [**SetServiceObjectSecurity**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/nf-winsvc-setserviceobjectsecurity) 函数。 有关详细信息，请参阅 [修改服务的 DACL](https://learn.microsoft.com/zh-cn/windows/win32/services/modifying-the-dacl-for-a-service)。

当进程使用 [**OpenService**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-openservicea) 函数时，系统会根据服务对象的安全描述符检查请求的访问权限。

向不受信任的用户 (（如 **SERVICE\_CHANGE\_CONFIG** 或 **SERVICE\_STOP**) ）授予某些访问权限可能会使他们干扰服务的执行，并可能允许他们在 LocalSystem 帐户下运行应用程序。

调用 [**EnumServicesStatusEx 函数**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-enumservicesstatusexa) 时，如果调用方对服务没有 **SERVICE\_QUERY\_STATUS** 访问权限，则会从返回给客户端的服务列表中以无提示方式省略该服务。

# [调试服务](https://learn.microsoft.com/zh-cn/windows/win32/services/debugging-a-service)

可以使用以下任一方法调试服务。

* 在服务运行时使用调试器调试服务。 首先， (服务进程的 PID) 获取进程标识符。 获取 PID 后，附加到正在运行的进程。 有关语法信息，请参阅调试器附带的文档。
* 调用 [**DebugBreak**](https://learn.microsoft.com/zh-cn/windows/desktop/api/debugapi/nf-debugapi-debugbreak) 函数以调用调试器进行实时调试。
* 指定启动程序时要使用的调试器。 为此，请在以下注册表位置创建名为 **“映像文件执行选项”** 的项：

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion**

创建与服务同名的子项 (例如MYSERV.EXE) 。 在此子项中，添加**名为 Debugger 的 REG\_SZ** 类型的值。 使用调试器的完整路径作为字符串值。 在“服务”控制面板小程序中，选择服务，单击“**启动**”，检查**“允许服务与桌面交互**”。 该服务必须是交互式服务，否则调试器无法在默认桌面上运行。 请注意，从 Windows Vista 开始，此方法不再受支持，因为所有服务都在专用于服务的会话中运行，不支持显示用户界面。

* 使用 [事件跟踪](https://learn.microsoft.com/zh-cn/windows/desktop/ETW/event-tracing-portal) 来记录信息。

若要调试自动启动服务的初始化代码，必须临时安装该服务并将其作为按需启动服务运行。

有时，出于调试目的，可能需要将服务作为控制台应用程序运行。 在此方案中， [**StartServiceCtrlDispatcher**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-startservicectrldispatchera) 函数将返回 **ERROR\_FAILED\_SERVICE\_CONTROLLER\_CONNECT**。 因此，请确保构建代码，以便返回此错误时不会调用特定于服务的代码。

# [服务触发器事件](https://learn.microsoft.com/zh-cn/windows/win32/services/service-trigger-events)

发生触发器事件时，服务可以注册为启动或停止。 这样就无需服务在系统启动时启动，也无需服务轮询或主动等待事件;服务可以在需要时启动，而不是自动启动，无论是否有工作要做。 预定义触发器事件的示例包括指定设备接口类的设备到达或特定防火墙端口的可用性。 服务还可以注册由 [Windows 事件跟踪](https://learn.microsoft.com/zh-cn/windows/win32/etw/event-tracing-portal) (ETW) 提供程序生成的自定义触发器事件。

**Windows Server 2008、Windows Vista、Windows Server 2003 和 Windows XP：** 在 Windows Server 2008 R2 和 Windows 7 之前，不支持服务触发器事件。

触发器由触发器事件类型、触发器事件子类型、响应触发器事件所要执行的操作以及某些触发器事件类型的 (组成，) 一个或多个特定于触发器的数据项。 子类型和触发器特定的数据项共同指定向服务通知事件的条件。 数据项的格式取决于触发器事件类型;数据项可以是二进制数据、字符串或多字符串。 字符串必须是 Unicode;不支持 ANSI 字符串。

为了注册触发器事件，该服务使用 **SERVICE\_CONFIG\_TRIGGER\_INFO** 调用 [**ChangeServiceConfig2**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-changeserviceconfig2a) 并提供[**SERVICE\_TRIGGER\_INFO**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/ns-winsvc-service_trigger_info)结构。 **SERVICE\_TRIGGER\_INFO** 结构指向[**SERVICE\_TRIGGER**](https://learn.microsoft.com/zh-cn/windows/desktop/api/winsvc/ns-winsvc-service_trigger)结构的数组，每个结构指定一个触发器。

如果系统启动时触发条件为 true，或者当系统运行时触发条件为 true，则执行指定的触发器操作。 例如，如果服务注册为在特定设备可用时启动，则当设备已插入计算机时，将在系统启动时启动该服务;如果用户在系统运行时插入设备，则服务会在设备到达时启动。

如果触发器具有特定于触发器的数据项，则仅当触发器事件附带的数据项与服务使用触发器指定的数据项之一匹配时，才会执行触发器操作。 二进制数据匹配是通过按位比较完成的。 字符串匹配不区分大小写。 如果数据项是多字符串，则多字符串中的所有字符串都必须匹配。

当服务启动以响应触发器事件时，服务在其 [*ServiceMain*](https://learn.microsoft.com/zh-cn/windows/win32/api/winsvc/nc-winsvc-lpservice_main_functiona) 回调函数中接收 *argv*[1] **SERVICE\_TRIGGER\_STARTED\_ARGUMENT**。 *Argv*[0] 始终是服务的短名称。

注册为在响应触发器事件时启动的服务可能会在空闲超时后停止自身，而服务无法执行任何操作。 停止自身的服务必须准备好处理在服务停止自身时到达 **SERVICE\_CONTROL\_TRIGGEREVENT** 控制请求。 每当服务处于运行状态时发生新的触发器事件时，SCM 就会发送 **SERVICE\_CONTROL\_TRIGGEREVENT** 控制请求。 为了避免丢失触发器事件，服务应返回 **ERROR\_SHUTDOWN\_IN\_PROGRESS** 服务从运行过渡到停止时到达的任何 **SERVICE\_CONTROL\_TRIGGEREVENT** 控制请求。 这会指示 SCM 将触发事件排队，并等待服务进入停止状态。 然后，SCM 执行与排队触发器事件关联的操作，例如启动服务。

当服务准备好再次处理触发器事件时，它会在调用 [**SetServiceStatus**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-setservicestatus) 时在其控件接受的掩码中设置**SERVICE\_ACCEPT\_TRIGGEREVENT**。 这通常在服务使用 **SERVICE\_RUNNING** 调用 **SetServiceStatus** 时完成。 然后，SCM 会为每个排队的触发器事件发出 **SERVICE\_CONTROL\_TRIGGEREVENT** 请求，直到队列为空。

无法停止运行有依赖服务的服务以响应触发器事件。

在内存不足的情况下，无法保证触发-启动和触发器-停止请求。

使用 [**QueryServiceConfig2**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Winsvc/nf-winsvc-queryserviceconfig2a) 函数检索服务的触发器事件配置。

SC 工具 (sc.exe) 可用于在命令提示符下配置或查询服务的触发器事件。 使用 **triggerinfo** 选项将服务配置为启动或停止以响应触发器事件。 使用 **qtriggerinfo** 选项查询服务的触发器配置。

以下示例查询 W32time 服务的触发器配置，该服务配置为在计算机加入域时启动，并在计算机离开域时停止。

syntax复制

C:\>sc qtriggerinfo w32time

[SC] QueryServiceConfig2 SUCCESS

SERVICE\_NAME: w32time

START SERVICE

DOMAIN JOINED STATUS : 1ce20aba-9851-4421-9430-1ddeb766e809 [DOMAIN JOINED]

STOP SERVICE

DOMAIN JOINED STATUS : ddaf516e-58c2-4866-9574-c3b615d42ea1 [NOT DOMAIN JOINED]

以下示例查询平板电脑输入服务的触发器配置，该服务配置为在 **具有 GUID** {4d1e55b2-f16f-11cf-88cb-0011111000030} 且任何指定的 HID 设备 ID 到达时启动。

C:\>sc qtriggerinfo tabletinputservice

[SC] QueryServiceConfig2 SUCCESS

SERVICE\_NAME: tabletinputservice

START SERVICE

DEVICE INTERFACE ARRIVAL : 4d1e55b2-f16f-11cf-88cb-001111000030 [INTERFACE CLASS GUID]

DATA : HID\_DEVICE\_UP:000D\_U:0001

DATA : HID\_DEVICE\_UP:000D\_U:0002

DATA : HID\_DEVICE\_UP:000D\_U:0003

DATA : HID\_DEVICE\_UP:000D\_U:0004