BOOL LookupPrivilegeValue(LPCTSTR lpSystemName,LPCTSTR lpName,PLUID lpLuid);

第一个参数表示所要查看的系统，本地系统直接用NULL

第二个参数指向一个以零结尾的字符串，指定特权的名称，如在WinNT h头文件定义。

第三个参数用来接收所返回的制定特权名称的信息。

[函数调用](http://baike.haosou.com/doc/2151920-2276849.html" \t "_blank)成功后，信息存入第三个类型为LUID的[结构体](http://baike.haosou.com/doc/6031580-6244581.html" \t "_blank)中，并且函数返回非0。

函数定义在winbase.h中，链接使用advapi32.lib库。

例： struct quanxiannameclass{

LPCTSTR lpName1 = SE\_ASSIGNPRIMARYTOKEN\_NAME;

LPCTSTR lpName2 = SE\_AUDIT\_NAME;

LPCTSTR lpName3 = SE\_BACKUP\_NAME;

LPCTSTR lpName4 = SE\_CREATE\_GLOBAL\_NAME;

LPCTSTR lpName5 = SE\_DEBUG\_NAME;

} quanxianname;

struct quanxianluidclass{

PLUID lpLuid1;

PLUID lpLuid2;

PLUID lpLuid3;

PLUID lpLuid4;

PLUID lpLuid5;

} quanxianluid;

LookupPrivilegeValue(NULL, quanxianname.lpName1, quanxianluid.lpLuid1);

LookupPrivilegeValue(NULL, quanxianname.lpName1, quanxianluid.lpLuid2);

LookupPrivilegeValue(NULL, quanxianname.lpName1, quanxianluid.lpLuid3);

LookupPrivilegeValue(NULL, quanxianname.lpName1, quanxianluid.lpLuid4);

LookupPrivilegeValue(NULL, quanxianname.lpName1, quanxianluid.lpLuid5);

lpName 值

|  |  |
| --- | --- |
| SE\_ASSIGNPRIMARYTOKEN\_NAME TEXT("SeAssignPrimaryTokenPrivilege") | 必需分配主要的进程令牌  用户权限: 替换一个进程级令牌. |
| SE\_AUDIT\_NAME TEXT("SeAuditPrivilege") | 生成所需的审计日志记录.  获得安全服务器权限  用户权限: 生成安全记录 |
| SE\_BACKUP\_NAME TEXT("SeBackupPrivilege") | Required to perform backup operations. This privilege causes the system to grant all read access control to any file, regardless of the *access control list* (ACL) specified for the file. Any access request other than read is still evaluated with the ACL. This privilege is required by the **RegSaveKey** and**RegSaveKeyEx**functions. The following access rights are granted if this privilege is held:   * READ\_CONTROL * ACCESS\_SYSTEM\_SECURITY * FILE\_GENERIC\_READ * FILE\_TRAVERSE   User Right: Back up files and directories. |
| SE\_CHANGE\_NOTIFY\_NAME TEXT("SeChangeNotifyPrivilege") | Required to receive notifications of changes to files or directories. This privilege also causes the system to skip all traversal access checks. It is enabled by default for all users.  User Right: Bypass traverse checking. |
| SE\_CREATE\_GLOBAL\_NAME TEXT("SeCreateGlobalPrivilege") | Required to create named file mapping objects in the global namespace during Terminal Services sessions. This privilege is enabled by default for administrators, services, and the local system account.  User Right: Create global objects.  **Windows XP/2000/NT:**This privilege is not supported. Note that this value is supported starting with Windows Server 2003, Windows XP SP2, and Windows 2000 SP4. |
| SE\_CREATE\_PAGEFILE\_NAME TEXT("SeCreatePagefilePrivilege") | Required to create a paging file.  User Right: Create a pagefile. |
| SE\_CREATE\_PERMANENT\_NAME TEXT("SeCreatePermanentPrivilege") | Required to create a permanent object.  User Right: Create permanent shared objects. |
| SE\_CREATE\_SYMBOLIC\_LINK\_NAME TEXT("SeCreateSymbolicLinkPrivilege") | Required to create a symbolic link.  User Right: Create symbolic links. |
| SE\_CREATE\_TOKEN\_NAME TEXT("SeCreateTokenPrivilege") | Required to create a primary token.  User Right: Create a token object. |
| SE\_DEBUG\_NAME TEXT("SeDebugPrivilege") | 可以去调试和修改其他账户拥有的进程内存(包括SYSTEM)  用户权限：调试程序 |
| SE\_ENABLE\_DELEGATION\_NAME TEXT("SeEnableDelegationPrivilege") | Required to mark user and computer accounts as trusted for delegation.  User Right: Enable computer and user accounts to be trusted for delegation. |
| SE\_IMPERSONATE\_NAME TEXT("SeImpersonatePrivilege") | Required to impersonate.  User Right: Impersonate a client after authentication.  **Windows XP/2000/NT:**This privilege is not supported. Note that this value is supported starting with Windows Server 2003, Windows XP SP2, and Windows 2000 SP4. |
| SE\_INC\_BASE\_PRIORITY\_NAME TEXT("SeIncreaseBasePriorityPrivilege") | Required to increase the base priority of a process.  User Right: Increase scheduling priority. |
| SE\_INCREASE\_QUOTA\_NAME TEXT("SeIncreaseQuotaPrivilege") | Required to increase the quota assigned to a process.  User Right: Adjust memory quotas for a process. |
| SE\_INC\_WORKING\_SET\_NAME TEXT("SeIncreaseWorkingSetPrivilege") | Required to allocate more memory for applications that run in the context of users.  User Right: Increase a process working set. |
| SE\_LOAD\_DRIVER\_NAME TEXT("SeLoadDriverPrivilege") | Required to load or unload a device driver.  User Right: Load and unload device drivers. |
| SE\_LOCK\_MEMORY\_NAME TEXT("SeLockMemoryPrivilege") | Required to lock physical pages in memory.  User Right: Lock pages in memory. |
| SE\_MACHINE\_ACCOUNT\_NAME TEXT("SeMachineAccountPrivilege") | Required to create a computer account.  User Right: Add workstations to domain. |
| SE\_MANAGE\_VOLUME\_NAME TEXT("SeManageVolumePrivilege") | Required to enable volume management privileges.  User Right: Manage the files on a volume. |
| SE\_PROF\_SINGLE\_PROCESS\_NAME TEXT("SeProfileSingleProcessPrivilege") | Required to gather profiling information for a single process.  User Right: Profile single process. |
| SE\_RELABEL\_NAME TEXT("SeRelabelPrivilege") | Required to modify the mandatory integrity level of an object.  User Right: Modify an object label. |
| SE\_REMOTE\_SHUTDOWN\_NAME TEXT("SeRemoteShutdownPrivilege") | Required to shut down a system using a network request.  User Right: Force shutdown from a remote system. |
| SE\_RESTORE\_NAME TEXT("SeRestorePrivilege") | Required to perform restore operations. This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file. Any access request other than write is still evaluated with the ACL. Additionally, this privilege enables you to set any valid user or group SID as the owner of a file. This privilege is required by the**RegLoadKey** function. The following access rights are granted if this privilege is held:   * WRITE\_DAC * WRITE\_OWNER * ACCESS\_SYSTEM\_SECURITY * FILE\_GENERIC\_WRITE * FILE\_ADD\_FILE * FILE\_ADD\_SUBDIRECTORY * DELETE   User Right: Restore files and directories. |
| SE\_SECURITY\_NAME TEXT("SeSecurityPrivilege") | Required to perform a number of security-related functions, such as controlling and viewing audit messages. This privilege identifies its holder as a security operator.  User Right: Manage auditing and security log. |
| SE\_SHUTDOWN\_NAME TEXT("SeShutdownPrivilege") | Required to shut down a local system.  User Right: Shut down the system. |
| SE\_SYNC\_AGENT\_NAME TEXT("SeSyncAgentPrivilege") | Required for a domain controller to use the *LDAP*directory synchronization services. This privilege enables the holder to read all objects and properties in the directory, regardless of the protection on the objects and properties. By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers.  User Right: Synchronize directory service data. |
| SE\_SYSTEM\_ENVIRONMENT\_NAME TEXT("SeSystemEnvironmentPrivilege") | Required to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.  User Right: Modify firmware environment values. |
| SE\_SYSTEM\_PROFILE\_NAME TEXT("SeSystemProfilePrivilege") | Required to gather profiling information for the entire system.  User Right: Profile system performance. |
| SE\_SYSTEMTIME\_NAME TEXT("SeSystemtimePrivilege") | 请求修改系统时间  用户权限: 更改系统时间. |
| SE\_TAKE\_OWNERSHIP\_NAME TEXT("SeTakeOwnershipPrivilege") | Required to take ownership of an object without being granted discretionary access. This privilege allows the owner value to be set only to those values that the holder may legitimately assign as the owner of an object.  User Right: Take ownership of files or other objects. |
| SE\_TCB\_NAME TEXT("SeTcbPrivilege") | This privilege identifies its holder as part of the trusted computer base. Some trusted protected subsystems are granted this privilege.  User Right: Act as part of the operating system. |
| SE\_TIME\_ZONE\_NAME TEXT("SeTimeZonePrivilege") | Required to adjust the time zone associated with the computer's internal clock.  User Right: Change the time zone. |
| SE\_TRUSTED\_CREDMAN\_ACCESS\_NAME TEXT("SeTrustedCredManAccessPrivilege") | Required to access Credential Manager as a trusted caller.  User Right: Access Credential Manager as a trusted caller. |
| SE\_UNDOCK\_NAME TEXT("SeUndockPrivilege") | Required to undock a laptop.  User Right: Remove computer from docking station. |
| SE\_UNSOLICITED\_INPUT\_NAME TEXT("SeUnsolicitedInputPrivilege") | Required to read unsolicited input from a *terminal* device.  User Right: Not applicable. |