Недокументированные функции NTDLL :: К главной странице сайта

Справочник по недокументированным функциям NT Native API (ntdll.dll). Список системных функций ядра.

Список систематизирован по рубрикам.

APC

- KiUserApcDispatcher
- NtAlertThread (ZwAlertThread)
- NtQueueApcThread (ZwQueueApcThread)
- NtTestAlert (ZwTestAlert)

Атомы

- ATOM_BASIC_INFORMATION
- ATOM_INFORMATION_CLASS
- ATOM_TABLE_INFORMATION
- NtAddAtom (ZwAddAtom)
- NtDeleteAtom (ZwDeleteAtom)
- NtFindAtom (ZwFindAtom)
- NtQueryInformationAtom (ZwQueryInformationAtom)

Сжатие

- RtlCompressBuffer
- RtlDecompressBuffer
- RtlGetCompressionWorkSpaceSize

Отладка

- DbgPrint

Обработка ошибок

- NtDisplayString (ZwDisplayString)
- NtRaiseException (ZwRaiseException)
- NtRaiseHardError (ZwRaiseHardError)
- NtSetDefaultHardErrorPort (ZwSetDefaultHardErrorPort)
- HARDERROR_MSG
- HARDERROR_RESPONSE
- HARDERROR_RESPONSE_OPTION

Исполняемые образы

Окружение

- NtQuerySystemEnvironmentValue (ZwQuerySystemEnvironmentValue)

- NtSetSystemEnvironmentValue (ZwSetSystemEnvironmentValue)
- RtlCreateEnvironment
- RtlDestroyEnvironment
- RtlExpandEnvironmentStrings_U
- RtlQueryEnvironmentVariable_U
- RtlSetCurrentEnvironment
- RtlSetEnvironmentVariable

Образы

- LdrGetDllHandle
- LdrGetProcedureAddress
- LdrLoadDll
- LdrQueryProcessModuleInformation
- LdrShutdownProcess
- LdrShutdownThread
- LdrUnloadDll
- NtLoadDriver (ZwLoadDriver)
- NtUnloadDriver (ZwUnloadDriver)
- RtlImageNtHeader
- RtlImageRvaToVa

Контроль аппаратуры

- NtShutdownSystem (ZwShutdownSystem)
- SHUTDOWN_ACTION

Локаль

- NtQueryDefaultLocale (ZwQueryDefaultLocale)
- NtSetDefaultLocale (ZwSetDefaultLocale)

Управление памятью

Память кучи

- RtlAllocateHeap
- RtlCompactHeap
- RtlCreateHeap
- RtlDestroyHeap
- RtlEnumProcessHeaps
- RtlFreeHeap
- RtlGetProcessHeaps
- RtlLockHeap
- RtlProtectHeap
- RtlReAllocateHeap
- RtlSizeHeap
- RtlUnlockHeap
- RtlValidateHeap
- RtlValidateProcessHeaps
- RtlWalkHeap
- RTL_HEAP_DEFINITION

Виртуальная память

- NtAllocateVirtualMemory (ZwAllocateVirtualMemory)
- NtFlushVirtualMemory (ZwFlushVirtualMemory)
- NtFreeVirtualMemory (ZwFreeVirtualMemory)
- NtLockVirtualMemory (ZwLockVirtualMemory)
- NtProtectVirtualMemory (ZwProtectVirtualMemory)
- NtQueryVirtualMemory (ZwQueryVirtualMemory)
- NtReadVirtualMemory (ZwReadVirtualMemory)
- NtUnlockVirtualMemory (ZwUnlockVirtualMemory)
- NtWriteVirtualMemory (ZwWriteVirtualMemory)
- MEMORY_INFORMATION_CLASS

Объекты ядра

Независимые от типа

- NtClose (ZwClose)
- NtDuplicateObject (ZwDuplicateObject)
- NtMakeTemporaryObject (ZwMakeTemporaryObject)
- NtQueryObject (ZwQueryObject)
- NtSetInformationObject (ZwSetInformationObject)
- NtSignalAndWaitForSingleObject (ZwSignalAndWaitForSingleObject)
- NtWaitForMultipleObjects (ZwWaitForMultipleObjects)
- NtWaitForSingleObject (ZwWaitForSingleObject)
- OBJECT_BASIC_INFORMATION
- OBJECT_INFORMATION_CLASS
- OBJECT_NAME_INFORMATION
- OBJECT_WAIT_TYPE

Директория

- NtCreateDirectoryObject (ZwCreateDirectoryObject)
- NtOpenDirectoryObject (ZwOpenDirectoryObject)
- NtQueryDirectoryObject (ZwQueryDirectoryObject)
- OBJDIR_INFORMATION

Событие

- EVENT_BASIC_INFORMATION
- EVENT_INFORMATION_CLASS
- EVENT_TYPE
- NtClearEvent (ZwClearEvent)
- NtCreateEvent (ZwCreateEvent)
- NtOpenEvent (ZwOpenEvent)
- NtPulseEvent (ZwPulseEvent)
- NtQueryEvent (ZwQueryEvent)
- NtResetEvent (ZwResetEvent)
- NtSetEvent (ZwSetEvent)

Пара событий

- NtCreateEventPair (ZwCreateEventPair)
- NtOpenEventPair (ZwOpenEventPair)
- NtSetHighEventPair (ZwSetHighEventPair)
- NtSetHighWaitLowEventPair (ZwSetHighWaitLowEventPair)
- NtSetLowEventPair (ZwSetLowEventPair)
- NtSetLowWaitHighEventPair (ZwSetLowWaitHighEventPair)
- NtWaitHighEventPair (ZwWaitHighEventPair)
- NtWaitLowEventPair (ZwWaitLowEventPair)
- NtSetHighWaitLowThread (ZwSetHighWaitLowThread)
- NtSetLowWaitHighThread (ZwSetLowWaitHighThread)

Файл

- NtCancelIoFile (ZwCancelIoFile)
- NtCreateFile (ZwCreateFile)
- NtCreateMailslotFile (ZwCreateMailslotFile)
- NtCreateNamedPipeFile (ZwCreateNamedPipeFile)
- NtCreatePagingFile (ZwCreatePagingFile)
- NtDeleteFile (ZwDeleteFile)
- NtDeviceIoControlFile (ZwDeviceIoControlFile)
- NtFlushBuffersFile (ZwFlushBuffersFile)
- FILE_BASIC_INFORMATION
- FILE_FULL_EA_INFORMATION
- FILE_GET_EA_INFORMATION
- FILE_INFORMATION_CLASS
- FILE_NETWORK_OPEN_INFORMATION
- NtFsControlFile (ZwFsControlFile)

- NtLockFile (ZwLockFile)
- NtNotifyChangeDirectoryFile (ZwNotifyChangeDirectoryFile)
- NtOpenFile (ZwOpenFile)
- NtQueryAttributesFile (ZwQueryAttributesFile)
- NtQueryDirectoryFile (ZwQueryDirectoryFile)
- NtQueryEaFile (ZwQueryEaFile)
- NtQueryFullAttributesFile (ZwQueryFullAttributesFile)
- NtQueryInformationFile (ZwQueryInformationFile)
- NtQueryOleDirectoryFile (ZwQueryOleDirectoryFile)
- NtQueryVolumeInformationFile (ZwQueryVolumeInformationFile)
- NtReadFile (ZwReadFile)
- NtReadFileScatter (ZwReadFileScatter)
- NtSetEaFile (ZwSetEaFile)
- NtSetInformationFile (ZwSetInformationFile)
- NtSetVolumeInformationFile (ZwSetVolumeInformationFile)
- NtUnlockFile (ZwUnlockFile)
- NtWriteFile (ZwWriteFile)
- NtWriteFileGather (ZwWriteFileGather)
- FILE_FS_ATTRIBUTE_INFORMATION
- FILE_FS_CONTROL_INFORMATION
- FILE_FS_DEVICE_INFORMATION
- FILE_FS_LABEL_INFORMATION
- FILE_FS_SIZE_INFORMATION
- FILE_FS_VOLUME_INFORMATION
- FILE_INTERNAL_INFORMATION
- FILE_NETWORK_OPEN_INFORMATION
- FILE_NOTIFY_INFORMATION
- FS_INFORMATION_CLASS

Завершение ввода-вывода

- NtCreateIoCompletion (ZwCreateIoCompletion)
- NtOpenIoCompletion (ZwOpenIoCompletion)
- NtQueryIoCompletion (ZwQueryIoCompletion)
- NtRemoveIoCompletion (ZwRemoveIoCompletion)
- NtSetIoCompletion (ZwSetIoCompletion)
- IO_COMPLETION_BASIC_INFORMATION
- IO_COMPLETION_INFORMATION_CLASS

Ключ

- NtCompressKey (ZwCompressKey)
- NtCompactKeys (ZwCompactKeys)
- NtCreateKey (ZwCreateKey)
- NtDeleteKey (ZwDeleteKey)
- NtDeleteValueKey (ZwDeleteValueKey)
- NtEnumerateKey (ZwEnumerateKey)
- NtEnumerateValueKey (ZwEnumerateValueKey)
- NtFlushKey (ZwFlushKey)
- NtLoadKey (ZwLoadKey)
- NtNotifyChangeKey (ZwNotifyChangeKey)
- NtOpenKey (ZwOpenKey)
- NtQueryKey (ZwQueryKey)
- NtQueryMultipleValueKey (ZwQueryMultipleValueKey)
- NtQueryValueKey (ZwQueryValueKey)
- NtReplaceKey (ZwReplaceKey)
- NtRestoreKey (ZwRestoreKey)
- NtSaveKey (ZwSaveKey)
- NtSetInformationKey (ZwSetInformationKey)
- NtSetValueKey (ZwSetValueKey)
- NtUnloadKey (ZwUnloadKey)
- RtlFormatCurrentUserKeyPath

Мутант

- MUTANT_BASIC_INFORMATION
- NtCreateMutant (ZwCreateMutant)
- NtOpenMutant (ZwOpenMutant)
- NtQueryMutant (ZwQueryMutant)

- NtReleaseMutant (ZwReleaseMutant)

Порт

- LPC_SECTION_MEMORY
- LPC_SECTION_OWNER_MEMORY
- LPC_TERMINATION_MESSAGE
- LPC_MESSAGE
- PORT_INFORMATION_CLASS
- NtAcceptConnectPort (ZwAcceptConnectPort)
- NtCompleteConnectPort (ZwCompleteConnectPort)
- NtConnectPort (ZwConnectPort)
- NtCreatePort (ZwCreatePort)
- NtImpersonateClientOfPort (ZwImpersonateClientOfPort)
- NtListenPort (ZwListenPort)
- NtQueryInformationPort (ZwQueryInformationPort)
- NtReadRequestData (ZwReadRequestData)
- NtRegisterThreadTerminatePort (ZwRegisterThreadTerminatePort)
- NtReplyPort (ZwReplyPort)
- NtReplyWaitReceivePort (ZwReplyWaitReceivePort)
- NtReplyWaitReplyPort (ZwReplyWaitReplyPort)
- NtRequestPort (ZwRequestPort)
- NtRequestWaitReplyPort (ZwRequestWaitReplyPort)
- NtWriteRequestData (ZwWriteRequestData)

Процесс

- NtCreateProcess (ZwCreateProcess)
- NtFlushInstructionCache (ZwFlushInstructionCache)
- NtOpenProcess (ZwOpenProcess)
- NtQueryInformationProcess (ZwQueryInformationProcess)
- NtSetInformationProcess (ZwSetInformationProcess)
- NtTerminateProcess (ZwTerminateProcess)
- RtlCreateUserProcess
- PEB
- PEB_FREE_BLOCK
- PEB_LDR_DATA
- RTL_DRIVE_LETTER_CURDIR
- RTL_USER_PROCESS_INFORMATION
- RTL_USER_PROCESS_PARAMETERS
- LDR_MODULE
- PROCESS_INFORMATION_CLASS

Профиль

- KPROFILE_SOURCE
- NtCreateProfile (ZwCreateProfile)
- NtQueryIntervalProfile (ZwQueryIntervalProfile)
- NtSetIntervalProfile (ZwSetIntervalProfile)
- NtStartProfile (ZwStartProfile)
- NtStopProfile (ZwStopProfile)

Секция

- NtCreateSection (ZwCreateSection)
- NtExtendSection (ZwExtendSection)
- NtMapViewOfSection (ZwMapViewOfSection)
- NtOpenSection (ZwOpenSection)
- NtQuerySection (ZwQuerySection)
- NtUnmapViewOfSection (ZwUnmapViewOfSection)
- SECTION_BASIC_INFORMATION
- SECTION_IMAGE_INFORMATION
- SECTION_INFORMATION_CLASS
- SECTION_INHERIT

Семафор

- NtCreateSemaphore (ZwCreateSemaphore)
- NtOpenSemaphore (ZwOpenSemaphore)
- NtQuerySemaphore (ZwQuerySemaphore)
- NtReleaseSemaphore (ZwReleaseSemaphore)
- SEMAPHORE_BASIC_INFORMATION
- SEMAPHORE_INFORMATION_CLASS

Символьная ссылка

- NtCreateSymbolicLinkObject (ZwCreateSymbolicLinkObject)
- NtOpenSymbolicLinkObject (ZwOpenSymbolicLinkObject)
- NtQuerySymbolicLinkObject (ZwQuerySymbolicLinkObject)

Поток

- INITIAL_TEB
- NtAlertResumeThread (ZwAlertResumeThread)
- NtCreateThread (ZwCreateThread)
- NtGetContextThread (ZwGetContextThread)
- NtImpersonateThread (ZwImpersonateThread)
- NtOpenThread (ZwOpenThread)
- NtQueryInformationThread (ZwQueryInformationThread)
- NtResumeThread (ZwResumeThread)
- NtSetContextThread (ZwSetContextThread)
- NtSetInformationThread (ZwSetInformationThread)
- NtSuspendThread (ZwSuspendThread)
- NtTerminateThread (ZwTerminateThread)
- NtContinue (ZwContinue)
- NtDelayExecution (ZwDelayExecution)
- NtYieldExecution (ZwYieldExecution)
- RtlCreateUserThread
- TEB
- THREAD_BASIC_INFORMATION
- THREAD_INFORMATION_CLASS
- THREAD_TIMES_INFORMATION

Таймер

- NtCancelTimer (ZwCancelTimer)
- NtCreateTimer (ZwCreateTimer)
- NtOpenTimer (ZwOpenTimer)
- NtQueryTimer (ZwQueryTimer)
- NtSetTimer (ZwSetTimer)
- TIMER_BASIC_INFORMATION
- TIMER_INFORMATION_CLASS

Токен

- NtAdjustGroupsToken (ZwAdjustGroupsToken)
- NtAdjustPrivilegesToken (ZwAdjustPrivilegesToken)
- NtCreateToken (ZwCreateToken)
- NtDuplicateToken (ZwDuplicateToken)
- NtOpenProcessToken (ZwOpenProcessToken)
- NtOpenThreadToken (ZwOpenThreadToken)
- NtQueryInformationToken (ZwQueryInformationToken)
- NtSetInformationToken (ZwSetInformationToken)

Безопасность

Аудит

- NtAccessCheckAndAuditAlarm (ZwAccessCheckAndAuditAlarm)
- NtCloseObjectAuditAlarm (ZwCloseObjectAuditAlarm)
- NtDeleteObjectAuditAlarm (ZwDeleteObjectAuditAlarm)
- NtOpenObjectAuditAlarm (ZwOpenObjectAuditAlarm)
- NtPrivilegedServiceAuditAlarm (ZwPrivilegedServiceAuditAlarm)

- NtPrivilegeObjectAuditAlarm (ZwPrivilegeObjectAuditAlarm)

Функции безопасности

- NtAllocateLocallyUniqueId (ZwAllocateLocallyUniqueId)
- NtAllocateUuids (ZwAllocateUuids)
- NtPrivilegeCheck (ZwPrivilegeCheck)
- NtQuerySecurityObject (ZwQuerySecurityObject)
- NtSetSecurityObject (ZwSetSecurityObject)

Системная информация

- NtQuerySystemInformation (ZwQuerySystemInformation)
- NtSetSystemInformation (ZwSetSystemInformation)
- SYSTEM_MODULE
- SYSTEM_MODULE_INFORMATION
- SYSTEM_PAGEFILE_INFORMATION
- SYSTEM_REGISTRY_QUOTA_INFORMATION
- SYSTEM_INFORMATION_CLASS

Время

- NtGetTickCount (ZwGetTickCount)
- NtQueryPerformanceCounter (ZwQueryPerformanceCounter)
- NtQuerySystemTime (ZwQuerySystemTime)
- NtQueryTimerResolution (ZwQueryTimerResolution)
- NtSetSystemTime (ZwSetSystemTime)
- NtSetTimerResolution (ZwSetTimerResolution)
- RtlTimeFieldsToTime
- RtlTimeToTimeFields
- TIME_FIELDS