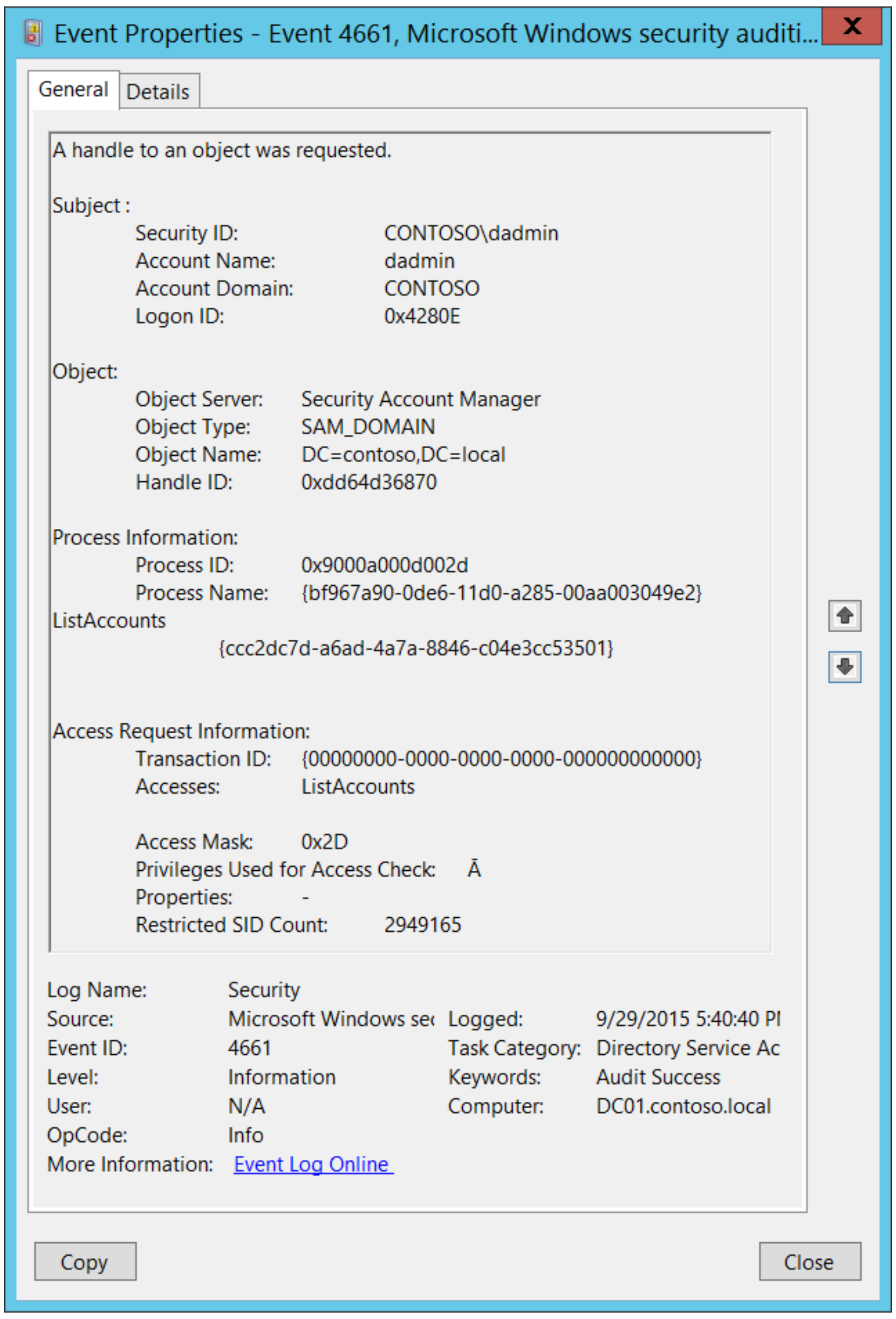
4661(S, F): A handle to an object was requested.

Article • 09/07/2021 • 1 contributor



Event Properties - Event 4661, Microsoft Windows security auditi...
General
Details

```
A handle to an object was requested.

Subject :
          Security ID:                CONTOSO\dadmin
          Account Name:               dadmin
          Account Domain:             CONTOSO
          Logon ID:                   0x4280E

Object:
          Object Server:    Security Account Manager
          Object Type:      SAM_DOMAIN
          Object Name:      DC=contoso,DC=local
          Handle ID:        0xdd64d36870

Process Information:
          Process ID:       0x9000a000d002d
          Process Name:     {bf967a90-0de6-11d0-a285-00aa003049e2}
ListAccounts
                    {ccc2dc7d-a6ad-4a7a-8846-c04e3cc53501}


Access Request Information:
          Transaction ID:   {00000000-0000-0000-0000-000000000000}
          Accesses:         ListAccounts

          Access Mask:      0x2D
          Privileges Used for Access Check:    Ā
          Properties:       -
          Restricted SID Count:       2949165

Log Name:          Security
Source:            Microsoft Windows se(   Logged:          9/29/2015 5:40:40 PI
Event ID:          4661                    Task Category:   Directory Service Ac
Level:             Information             Keywords:        Audit Success
User:              N/A                     Computer:        DC01.contoso.local
OpCode:            Info
More Information:  Event Log Online
```

Subcategories: Audit Directory Service Access and Audit SAM

Event Description:

This event indicates that a handle was requested for either an Active Directory object or a Security Account Manager (SAM) object.

If access was declined, then Failure event is generated.

This event generates only if Success auditing is enabled for the Audit Handle Manipulation subcategory.

> **Note** For recommendations, see Security Monitoring Recommendations for this event.

Event XML:

Copy

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-
 <EventID>4661</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>14080</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-30T00:11:56.547696700Z" />
 <EventRecordID>1048009</EventRecordID>
 <Correlation />
 <Execution ProcessID="520" ThreadID="528" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data
 <Data Name="SubjectUserName">dadmin</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0x4280e</Data>
 <Data Name="ObjectServer">Security Account Manager</Data>
 <Data Name="ObjectType">SAM\_DOMAIN</Data>
 <Data Name="ObjectName">DC=contoso,DC=local</Data>
 <Data Name="HandleId">0xdd64d36870</Data>
 <Data Name="TransactionId">{00000000-0000-0000-0000-000000000000}</Data>
 <Data Name="AccessList">%%5400</Data>
 <Data Name="AccessMask">0x2d</Data>
 <Data Name="PrivilegeList">Ā</Data>
 <Data Name="Properties">-</Data>
 <Data Name="RestrictedSidCount">2949165</Data>
 <Data Name="ProcessId">0x9000a000d002d</Data>
 <Data Name="ProcessName">{bf967a90-0de6-11d0-a285-00aa003049e2} %%5400 {ccc2dc7
 </EventData>
 </Event>
```

Required Server Roles: For an Active Directory object, the domain controller role is required. For a SAM object, there is no required role.

Minimum OS Version: Windows Server 2008, Windows Vista.

Event Versions: 0.

Field Descriptions:

Subject:

- **Security ID** [Type = SID]**:** SID of account that requested a handle to an object. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will see the source data in the event.

> **Note** A **security identifier (SID)** is a unique value of variable length used to identify a trustee (security principal). Each account has a unique SID that is issued by an authority, such as an Active Directory domain controller, and stored in a security database. Each time a user logs on, the system retrieves the SID for that user from the database and places it in the access token for that user. The system uses the SID in the access token to identify the user in all subsequent interactions with Windows security. When a SID has been used as the unique identifier for a user or group, it cannot ever be used again to identify another user or group. For more information about SIDs, see Security identifiers.

- **Account Name** [Type = UnicodeString]**:** the name of the account that requested a handle to an object.
- **Account Domain** [Type = UnicodeString]**:** subject's domain or computer name. Formats vary, and include the following:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase full domain name: contoso.local
  - Uppercase full domain name: CONTOSO.LOCAL
  - For some well-known security principals, such as LOCAL SERVICE or ANONYMOUS LOGON, the value of this field is "NT AUTHORITY".
  - For local user accounts, this field will contain the name of the computer or device that this account belongs to, for example: "Win81".
- **Logon ID** [Type = HexInt64]**:** hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID, for example, "4624: An account was successfully logged on."

Object:

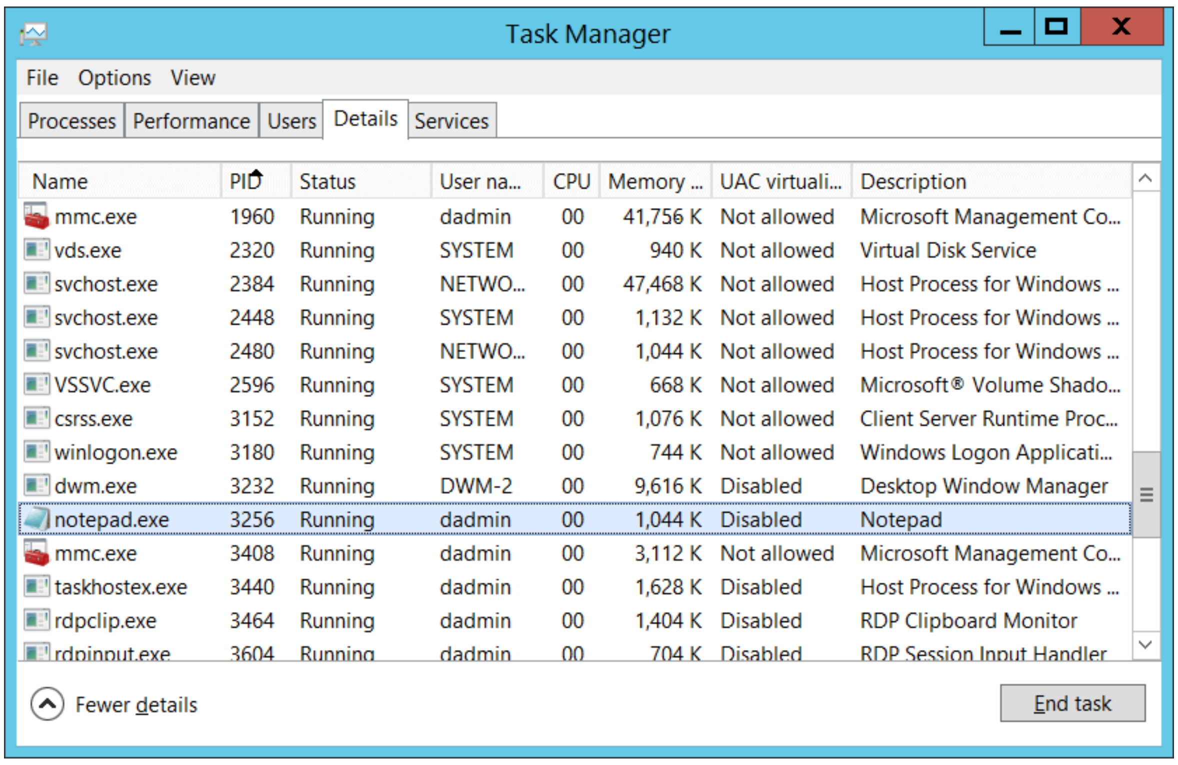
- **Object Server** [Type = UnicodeString]: has "**Security Account Manager**" value for this event.
- **Object Type** [Type = UnicodeString]: the type or class of the object that was accessed. The following list contains possible values for this field:
  - SAM_ALIAS - a local group.
  - SAM_GROUP - a group that is not a local group.
  - SAM_USER - a user account.
  - SAM_DOMAIN - a domain. For Active Directory events, this is the typical value.
  - SAM_SERVER - a computer account.
- **Object Name** [Type = UnicodeString]: the name of an object for which access was requested. Depends on **Object Type.** This event can have the following format:
  - SAM_ALIAS – SID of the group.
  - SAM_GROUP - SID of the group.
  - SAM_USER - SID of the account.
  - SAM_DOMAIN – distinguished name of the accessed object.
  - SAM_SERVER - distinguished name of the accessed object.

> **Note** The LDAP API references an LDAP object by its **distinguished name (DN)**. A DN is a sequence of relative distinguished names (RDN) connected by commas.
>
> An RDN is an attribute with an associated value in the form attribute=value; . These are examples of RDNs attributes:
>
> • DC - domainComponent
>
> • CN - commonName
>
> • OU - organizationalUnitName
>
> • O - organizationName

- **Handle ID** [Type = Pointer]: hexadecimal value of a handle to **Object Name**. This field can help you correlate this event with other events that might contain the same Handle ID, for example, "4662: An operation was performed on an object." This parameter might not be captured in the event, and in that case appears as "0x0".

Process Information:

- **Process ID** [Type = Pointer]: hexadecimal Process ID of the process that requested the handle. Process ID (PID) is a number used by the operating system to uniquely identify an active process. To see the PID for a specific process you can, for example, use Task Manager (Details tab, PID column):



Name	PID	Status	User na...	CPU	Memory ...	UAC virtuali...	Description
mmc.exe	1960	Running	dadmin	00	41,756 K	Not allowed	Microsoft Management Co...
vds.exe	2320	Running	SYSTEM	00	940 K	Not allowed	Virtual Disk Service
svchost.exe	2384	Running	NETWO...	00	47,468 K	Not allowed	Host Process for Windows ...
svchost.exe	2448	Running	SYSTEM	00	1,132 K	Not allowed	Host Process for Windows ...
svchost.exe	2480	Running	NETWO...	00	1,044 K	Not allowed	Host Process for Windows ...
VSSVC.exe	2596	Running	SYSTEM	00	668 K	Not allowed	Microsoft® Volume Shado...
csrss.exe	3152	Running	SYSTEM	00	1,076 K	Not allowed	Client Server Runtime Proc...
winlogon.exe	3180	Running	SYSTEM	00	744 K	Not allowed	Windows Logon Applicati...
dwm.exe	3232	Running	DWM-2	00	9,616 K	Disabled	Desktop Window Manager
notepad.exe	3256	Running	dadmin	00	1,044 K	Disabled	Notepad
mmc.exe	3408	Running	dadmin	00	3,112 K	Not allowed	Microsoft Management Co...
taskhostex.exe	3440	Running	dadmin	00	1,628 K	Disabled	Host Process for Windows ...
rdpclip.exe	3464	Running	dadmin	00	1,404 K	Disabled	RDP Clipboard Monitor
rdpinput.exe	3604	Running	dadmin	00	704 K	Disabled	RDP Session Input Handler

If you convert the hexadecimal value to decimal, you can compare it to the values in Task Manager.

- **Process Name** [Type = UnicodeString]: full path and the name of the executable for the process.

Access Request Information:

- **Transaction ID** [Type = GUID]: unique GUID of the transaction. This field can help you correlate this event with other events that might contain the same **Transaction ID**, such as "4660(S): An object was deleted."

  This parameter might not be captured in the event, and in that case appears as "{00000000-0000-0000-0000-000000000000}".

> **Note** **GUID** is an acronym for 'Globally Unique Identifier'. It is a 128-bit integer number used to identify resources, activities or instances.

- **Accesses** [Type = UnicodeString]: the list of access rights which were requested by **Subject\Security ID**. These access rights depend on **Object Type**. For more information about file access rights, see Table of file access codes. For information about SAM object access right use https://technet.microsoft.com/ or other informational resources.
- **Access Mask** [Type = HexInt32]: hexadecimal mask for the operation that was requested or performed. For more information about file access rights, see Table of file access codes. For information about SAM object access right use https://technet.microsoft.com/ or other informational resources.
- **Privileges Used for Access Check** [Type = UnicodeString]: the list of user privileges which were used during the operation, for example, SeBackupPrivilege. This parameter might not be captured in the event, and in that case appears as "-". See full list of user privileges in the table below:

Expand table

Privilege Name	User Right Group Policy Name	Description
SeAssignPrimaryTokenPrivilege	Replace a process-level token	Required to assign the *primary token* of a process. With this privilege, the user can initiate a process to replace the default token associated with a started subprocess.
SeAuditPrivilege	Generate security audits	With this privilege, the user can add entries to the security log.

SeBackupPrivilege	Back up files and directories	- Required to perform backup operations. With this privilege, the user can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system. 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. The following access rights are granted if this privilege is held: READ_CONTROL ACCESS_SYSTEM_SECURITY FILE_GENERIC_READ FILE_TRAVERSE
SeChangeNotifyPrivilege	Bypass traverse checking	Required to receive notifications of changes to files or directories. This privilege also causes the system to skip all traversal access checks. With this privilege, the user can traverse directory trees even though the user may not have permissions on the traversed directory. This privilege does not allow the user to list the contents of a directory, only to traverse directories.
SeCreateGlobalPrivilege	Create global objects	Required to create named file mapping objects in the global namespace during Terminal Services sessions.
SeCreatePagefilePrivilege	Create a pagefile	With this privilege, the user can create and change the size of a pagefile.
SeCreatePermanentPrivilege	Create permanent shared objects	Required to create a permanent object. This privilege is useful to kernel-mode components that extend the object namespace. Components that are running in kernel mode already have this privilege inherently; it is not necessary to assign them the privilege.
SeCreateSymbolicLinkPrivilege	Create symbolic links	Required to create a symbolic link.
SeCreateTokenPrivilege	Create a token object	Allows a process to create a token which it can then use to get access to any local resources when the process uses NtCreateToken() or other token-creation APIs. When a process requires this privilege, we recommend using the LocalSystem account (which already includes the privilege), rather than creating a separate user account and assigning this privilege to it.
SeDebugPrivilege	Debug programs	Required to debug and adjust the memory of a process owned by another account. With this privilege, the user can attach a debugger to any process or to the kernel. Developers who are debugging their own applications do not need this user right. Developers who are debugging new system components need this user right. This user right provides complete access to sensitive and critical operating system components.
SeEnableDelegationPrivilege	Enable computer and user accounts to be trusted for delegation	Required to mark user and computer accounts as trusted for delegation. With this privilege, the user can set the **Trusted for Deleg**ation setting on a user or computer object. The user or object that is granted this privilege must have write access to the account control flags on the user or computer object. A server

		process running on a computer (or under a user context) that is trusted for delegation can access resources on another computer using the delegated credentials of a client, as long as the account of the client does not have the **Account cannot be delegated** account control flag set.
SeImpersonatePrivilege	Impersonate a client after authentication	With this privilege, the user can impersonate other accounts.
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Required to increase the base priority of a process. With this privilege, the user can use a process with Write property access to another process to increase the execution priority assigned to the other process. A user with this privilege can change the scheduling priority of a process through the Task Manager user interface.
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Required to increase the quota assigned to a process. With this privilege, the user can change the maximum memory that can be consumed by a process.
SeIncreaseWorkingSetPrivilege	Increase a process working set	Required to allocate more memory for applications that run in the context of users.
SeLoadDriverPrivilege	Load and unload device drivers	Required to load or unload a device driver. With this privilege, the user can dynamically load and unload device drivers or other code in to kernel mode. This user right does not apply to Plug and Play device drivers.
SeLockMemoryPrivilege	Lock pages in memory	Required to lock physical pages in memory. With this privilege, the user can use a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. Exercising this privilege could significantly affect system performance by decreasing the amount of available random access memory (RAM).
SeMachineAccountPrivilege	Add workstations to domain	With this privilege, the user can create a computer account. This privilege is valid only on domain controllers.
SeManageVolumePrivilege	Perform volume maintenance tasks	Required to run maintenance tasks on a volume, such as remote defragmentation.
SeProfileSingleProcessPrivilege	Profile single process	Required to gather profiling information for a single process. With this privilege, the user can use performance monitoring tools to monitor the performance of non-system processes.
SeRelabelPrivilege	Modify an object label	Required to modify the mandatory integrity level of an object.
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Required to shut down a system using a network request.
SeRestorePrivilege	Restore files and directories	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. 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 With this privilege, the user can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories and determines which users can set any valid security principal as the owner of an object.
SeSecurityPrivilege	Manage auditing and security log	Required to perform a number of security-related functions, such as controlling and viewing audit events in security event log. With this privilege, the user can specify object access auditing options for individual resources, such as files, Active Directory objects, and registry keys. A user with this privilege can also view and clear the security log.
SeShutdownPrivilege	Shut down the system	Required to shut down a local system.
SeSyncAgentPrivilege	Synchronize directory service data	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. With this privilege, the user can synchronize all directory service data. This is also known as Active Directory synchronization.
SeSystemEnvironmentPrivilege	Modify firmware environment values	Required to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.
SeSystemProfilePrivilege	Profile system performance	Required to gather profiling information for the entire system. With this privilege, the user can use performance monitoring tools to monitor the performance of system processes.
SeSystemtimePrivilege	Change the system time	Required to modify the system time. With this privilege, the user can change the time and date on the internal clock of the computer. Users that are assigned this user right can affect the appearance of event logs. If the system time is changed, events that are logged will reflect this new time, not the actual time that the events occurred.
SeTakeOwnershipPrivilege	Take ownership of files or other objects	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. With this privilege, the user can take ownership of any securable object in the system, including Active Directory objects, files and folders, printers, registry keys, processes, and threads.
SeTcbPrivilege	Act as part of the operating system	This privilege identifies its holder as part of the trusted computer base. This user right allows a process to impersonate any user without authentication. The process

		can therefore gain access to the same local resources as that user.
SeTimeZonePrivilege	Change the time zone	Required to adjust the time zone associated with the computer's internal clock.
SeTrustedCredManAccessPrivilege	Access Credential Manager as a trusted caller	Required to access Credential Manager as a trusted caller.
SeUndockPrivilege	Remove computer from docking station	Required to undock a laptop. With this privilege, the user can undock a portable computer from its docking station without logging on.
SeUnsolicitedInputPrivilege	Not applicable	Required to read unsolicited input from a *terminal* device.

- **Properties** [Type = UnicodeString]: depends on **Object Type**. This field can be empty or contain the list of the object properties that were accessed. See more detailed information in "4661: A handle to an object was requested" from Audit SAM subcategory.

- **Restricted SID Count** [Type = UInt32]: Number of restricted SIDs in the token. Applicable to only specific **Object Types**.

Security Monitoring Recommendations

For 4661(S, F): A handle to an object was requested.

> **Important** For this event, also see Appendix A: Security monitoring recommendations for many audit events.

- You can get almost the same information from "4662: An operation was performed on an object." There are no additional recommendations for this event in this document.