NTFS Security Descriptor

The security descriptor resides in the $SDS data stream. The table below describes the layout of the $SDS data stream.

$SDS Data Stream Entry Layout, showing parts of the Security Descriptor

$SDS Entry Field	Description
Hash	Hash of security descriptor
Security ID	Security ID assigned to this entry
Offset	Entry offset in the #SDS data stream
Size	Entry size
Header	Security Descriptor: Revision number and a set of control flags that describe characteristics of the security descriptor.
Owner_SID	Security Descriptor: Owner SID. The owner of an object can modify permissions and give other users the right to take ownership.
Group_SID	Security Descriptor: SID for the owner's primary group. Used only by the POSIX subsystem.
DACL	Security Descriptor: Discretionary Access Control List. Contains ACEs and controls access to the object. Content controlled by the owner.
SACL	Security Descriptor: System Access Control List Contains ACEs and controls the logging of attempts to access the object. Content controlled by security administrators for the local system.

To assign the appropriate security descriptor for a file or folder, NTFS does the following:

- Calculates a simple hash for that security descriptor and uses it as an index into the $SDH index. The $SDH index is sorted by security descriptor hash and is stored in a B+ tree format.
  - Maps the hash to the security descriptor's storage location within the $SDS data attribute.
- If a match is not found for the map, NTFS assigns a new unique Security ID to the security descriptor and adds

the new ID to the $SDS data attribute. When an entry references this security descriptor in the $SDS data attribute, NTFS adds appropriate entries to the $SDH and $SII indexes.

- Writes the Security ID corresponding to the security descriptor in the $SDS attribute to the $STANDARD_INFORMATION attribute of the file or folder.

When NTFS searches $SDH, it looks for a match for both the hash and the security descriptor.

When an application attempts to open a file or a folder, the following happens:

- NTFS reads the internal Security ID for the file or folder from the MFT entry's $STANDARD_INFORMATION attribute.
- In the $Secure file, NTFS opens the $SII index and looks up the appropriate security descriptor that for that file or folder.
- If NTFS finds the security descriptor, it locates the Security ID entry in the SDS attribute.
- In the SDS attribute, the offset allows NTFS to read the security descriptor and complete the security check.

NTFS does not delete entries in the $Secure file, even if no file or directory on a volume references the entry. The fact that NTFS only adds these entries does not significantly decrease disk space because most volumes, even those used for long periods, have relatively few unique security descriptors.

Two Security Indexes

Entries in the $SDH index map the security descriptor hashes to the security descriptor's storage location within the $SDS data attribute.

$Secure:$SDH index entry layout

$SDS Entry Field	Description
DataOffest	The value of an offset variable indicates the location of a based variable within an area variable relative to the start of the area.
DataLength	Size of data string.
ReservedForZero	Padding with zeroes.
IndexEntryLength	Size of index entry.
IndexKeyLength	Size of index key.
Flags	Arguments that that specify a type of security information.
Pad	Padding to help with alignment of fields.
KeyHash	Key: Hash of the security description
KeySecurityId	Key: The SecurityID assigned to the descriptor
Hash	Data: Hash of the security descriptor

SecurityID	Data: The Security ID assigned to the descriptor
Offset_in_SDS	Data: Offset of the security descriptor in $SDS data stream
Size_in_SDS	Data: Size of the descriptor in $SDS data stream
Reserved_II	Data: Padding - always Unicode "II"

The $SII index entries map NTFS5 security IDs to the security descriptor's location in the $SDS data attribute.

$Secure:$SII index entry layout

$SDS Entry Field	Description
DataOffest	Offset to data.
DataLength	Size of data.
ReservedForZero	Padding with zeroes.
IndexEntryLength	Size of Index Key.
Flags	Arguments that that specify a type of security information.
Pad	Padding to help with alignment of fields.
KeySecurityId	Key: The Security ID assigned to the descriptor
Hash	Data: Hash of the security descriptor
SecurityID	Data: The Security ID assigned to the descriptor
Offset_in_SDS	Data: Offset of the security descriptor in $SDS data stream
Size_in_SDS	Data: Size of the descriptor in $SDS data stream

Previous | NTFS Permissions | Next