Condivisione e sicurezza di file e cartelle

L'uso delle risorse del sistema e della rete Windows è controllato con meccanismi di autenticazione e autorizzazione interdipendenti. Dopo l'autenticazione dell'utente, Windows utilizza le tecnologie di autorizzazione e controllo dell'accesso per implementare la seconda fase di protezione delle risorse, che consiste nel determinare se un utente autenticato abbia o meno le autorizzazioni necessarie per poter accedere a una risorsa.

Le risorse condivise sono a disposizione di utenti e gruppi che non coincidono con il proprietario e pertanto devono essere protette da eventuali usi non autorizzati. Nel modello di controllo dell'accesso in Windows, agli utenti e ai gruppi (definiti anche **entità di sicurezza** o ***security principals***) vengono assegnati **SID** (***S**ecurity **ID***) univoci, oltre a diritti e autorizzazioni in base ai quali il sistema operativo determina quali operazioni possono essere eseguite da ciascun utente e gruppo. Ogni risorsa ha un proprietario, il quale concede le autorizzazioni alle entità di sicurezza. Durante la fase di controllo dell'accesso, queste autorizzazioni vengono esaminate per determinare quali entità di sicurezza possono accedere alla risorsa e in che modo.

Le entità di sicurezza eseguono azioni sugli oggetti, tra cui lettura, scrittura, modifica o controllo completo. Gli oggetti possono essere file, cartelle, stampanti, chiavi del Registro di sistema o Servizi di dominio *Active Directory*. Le risorse condivise usano gli elenchi di controllo dell'accesso (**ACL**) per assegnare le autorizzazioni, consentendo ai gestori delle risorse di imporre il controllo dell'accesso nei due modi seguenti:

- Negare l'accesso a utenti e gruppi non autorizzati
- Fissare limiti precisi per l'accesso consentito a utenti e gruppi autorizzati

In genere i proprietari degli oggetti concedono autorizzazioni a gruppi di sicurezza anziché a singoli utenti. Gli utenti e i computer che vengono aggiunti ai gruppi esistenti acquisiscono le autorizzazioni del gruppo al quale appartengono. Viene definito contenitore un oggetto, ad esempio una cartella, che può contenere altri oggetti, ad esempio sottocartelle e file. In una gerarchia di oggetti, la relazione tra contenitore e contenuto viene descritta definendo il primo padre e il secondo figlio, in quanto erede delle impostazioni di controllo dell'accesso del padre. I proprietari degli oggetti spesso tendono a definire le autorizzazioni per gli oggetti contenitore invece che per gli oggetti figlio, in modo da semplificare la gestione del controllo dell'accesso.

Applicazioni pratiche

Gli amministratori che utilizzano Windows possono perfezionare l'applicazione e la gestione del controllo dell'accesso a oggetti e soggetti per assicurare la protezione seguente:

- Proteggere un numero e una varietà maggiore di risorse di rete da eventuali abusi.
- Consentire agli utenti di accedere alle risorse in maniera coerente con i criteri dell'organizzazione e con i requisiti delle mansioni che esercitano.
- Consentire agli utenti di accedere alle risorse da una serie di dispositivi dislocati in varie posizioni.
- Rivedere periodicamente la capacità degli utenti di accedere alle risorse, alla luce dei cambiamenti nei criteri dell'organizzazione o nelle mansioni degli utenti, tenendo inoltre conto di un numero di

scenari di utilizzo in costante aumento (ad esempio, accesso da posizioni remote o da dispositivi sempre più vari, come i tablet e i cellulari).
- Identificare e risolvere i problemi relativi all'accesso quando gli utenti autorizzati non ottengono l'accesso alle risorse di cui hanno bisogno per svolgere le proprie mansioni.

Access Control List

Un ACL è una lista ordinata di ACEs (***A**ccess **C**ontrol **E**ntries***) che stabiliscono i diritti d'accesso (*right permission*) da applicare ad un oggetto e alle sue proprietà. Ogni ACE specifica univocamente un'identità (utente o gruppo) ed indica quali diritti di accesso ha su quell'oggetto, ovvero se sono consentiti (***allowed***), negati (***denied***) o se riguardano il suo monitoraggio (***audit***).

Ogni oggetto può contenere due tipi di ACLs:

- un DACL che identifica l'utente o il gruppo a cui è consentito o negato l'accesso
- un SACL che controlla come l'accesso è monitorato (*audited*)

Come Windows usa gli ACLs

Quando un utente fa il *logon* alla rete (viene autenticato) ottiene dal sistema un ***token*** (gettone) d'accesso con le informazioni relative alla sicurezza. Il *token* identifica univocamente l'utente, i gruppi a cui appartiene e i suoi privilegi. Inoltre contiene il logon **SID** (***S**ecurity **ID**entifier*) che permette di identificare la sessione corrente di *logon*. Ogni sottoprocesso (***thread***) eseguito dall'utente dopo l'accesso usa una copia di questo *token*.

Quando un *thread* prova ad accedere a un oggetto protetto, la *Local Security Authority* (**LSASS**) può autorizzarne o negarne l'accesso. Per farlo LSASS verifica gli *Access Control Entries* (**ACE**s) relativi a quell'oggetto contenuti nella *Discretionary Access Contro List* (**DACL**). Ogni ACE specifica infatti i diritti d'accesso (***access right***) che sono autorizzati o negati per quella sessione di *logon*. Se il proprietario non ha creato nessun ACE nella DACL relativa a quell'oggetto il sistema garantirà l'accesso a tutti.

Se invece LSASS trova degli ACEs confronterà il SID di ogni ACE con il SID contenuto nel token di accesso del *thread*.

Gli **ACE** possono essere **espliciti**, ovvero direttamente assegnati ad un oggetto oppure **ereditati**. In quest'ultimo caso l'oggetto figlio eredita gli ACEs di tutti i parenti che lo precedono (se non diversamente specificato).

Access Control Entries (ACEs)

Per definizione una ACL (***A**ccess Control List*) è un elenco ordinato di voci ACE. Ogni ACE contiene quanto segue:

- un flag che indica il tipo di ACE
- un insieme di flag per il controllo dell'ereditarietà e dell'auditing
- una maschera di accesso i cui bit specificano i vari diritti di accesso
- un SID che identifica l'utente o il gruppo il cui accesso è controllato o monitorato dall'ACE

Il sistema esamina ogni ACE in sequenza finché non accade uno dei seguenti eventi:

- un ***access-denied*** ACE nega esplicitamente il diritto d'accesso ad uno degli oggetti elencati nel *token* d'accesso del *thread*
- uno o più ***access-allowed*** ACEs concedono i diritti d'accesso richiesti per gli oggetti elencati nel *token* di quel *thread*
- tutti gli ACEs dell'oggetto sono stati verificati, ma esiste ancora almeno un diritto d'accesso che non è stato esplicitamente consentito. In quel caso l'accesso è implicitamente negato.

Poiché il sistema smette di verificare gli ACEs quando una richiesta d'accesso è negata o autorizzata l'ordine in cui gli ACEs sono elencati nella DACL è importante. Tutti i S.O. Windows processano gli ACEs secondo un **ordine canonico**:

1. tutti gli ACEs espliciti sono verificati prima degli ACEs ereditati
2. all'interno del gruppo degli ACEs espliciti, gli *access-denied* ACEs sono posti prima degli *access-allowed* ACEs
3. nel gruppo degli ACEs ereditati, gli ACEs ereditati dall'oggetto padre vengono elaborati prima di quelli ereditati dal processo nonno e così via salendo nell'albero genealogico. Anche in questo caso gli *access-denied* ACEs hanno la priorità sugli *access-allowed* ACEs

L'ordine canonico assicura che avvenga quanto segue:

- un *access-denied* ACE esplicito viene applicato indipendentemente da qualsiasi *access-allowed* ACE esplicito. Ciò consente al proprietario dell'oggetto di autorizzare l'accesso ad un gruppo di utenti e negare l'accesso a un sottoinsieme di quel gruppo
- Tutte le ACE esplicite vengono elaborati prima di qualsiasi ACE ereditata. Questo comportamento è coerente con il concetto di controllo di accesso discrezionale: l'accesso a un oggetto figlio (ad esempio un file) è a discrezione del proprietario di quell'oggetto, non del proprietario dell'oggetto genitore (ad esempio una cartella). In questo caso gli effetti delle autorizzazioni ereditate vengono modificate da quelle esplicite sull'oggetto.

Esempio: negare l'accesso esplicito a un gruppo

In questo esempio, si desidera negare l'accesso alla cartella *Cost* al gruppo *Marketing*, un sottogruppo del gruppo predefinito *Everyone*.

Se gli ACEs della cartella *Cost* sono in ordine canonico, l'ACE che nega l'accesso a *Marketing* verrà prima della ACE che autorizza l'accesso a chiunque (gruppo *Everyone*).

Durante il controllo di accesso, LSASS verifica gli ACEs nell'ordine in cui compaiono nella DACL dell'oggetto. Poiché l'ACE che vieta l'accesso alla cartella *Cost* viene prima di quella che autorizza chiunque (*Everyone*), ai membri del gruppo Marketing sarà negato l'accesso mentre tutti gli altri utenti potranno accedere alla cartella *Cost*.

Esempio: autorizzazioni esplicite prima di quelle ereditate

Partendo dall'esempio precedente, supponiamo che all'interno della cartella *Cost* sia necessario creare una cartella *Balance* a cui deve poter accedere solo il direttore della divisione Marketing, *Bob*. Poiché *Bob* appartiene al gruppo *Marketing* l'accesso alla cartella *Cost* non è autorizzato né è autorizzato l'accesso alla sottocartella *Balance* che ne eredita implicitamente gli ACEs.

Per consentirne l'accesso occorre che il proprietario della cartella *Balance* conceda esplicitamente i diritti di accesso all'utente *Bob*. In questo modo poiché LSASS processa gli ACEs della cartella secondo l'ordine canonico, il diritto esplicito che autorizza *Bob* ad accedere alla cartella *Balance* viene esaminato prima di quello ereditato che vieta l'accesso ai componenti del gruppo *Marketing*. In questo modo *Bob* sarà autorizzato ad accedere direttamente alla cartella *Balance* (e solo a quel contenuto).

Riepilogo sulla precedenza dei permessi

1. in generale le autorizzazioni negate hanno la precedenza su quelle consentite
2. le autorizzazione applicate esplicitamente su un oggetto hanno la priorità su quelle ereditate
3. le autorizzazioni ereditate da un parente prossimo (ad esempio dal padre) hanno la priorità su quelle ereditate da un parente meno prossimo (ad esempio di quelle del nonno)
4. le autorizzazioni di differenti gruppi di utenti che sono allo stesso livello (nel senso di tutte esplicite o tutte ereditate, e tutte permesse o tutte negate) sono cumulative. Ad esempio se un utente appartiene a due gruppi che hanno entrambi autorizzazioni esplicite su una cartella, un gruppo con *access-allow* ***Read*** e l'altro con *access-allow* ***Write***, l'utente potrà leggere e scrivere il contenuto di quella cartella.

Combinazioni di permessi di condivisione (*Sharing*) e permessi NTFS (*Security*)

Nel *File System* FAT32 le uniche autorizzazioni che consentono di proteggere file e cartelle sono quelle applicate alle cartelle condivise (ovvero accessibili anche via rete). Non è possibile proteggere localmente file e cartelle.

Il *File System* NTFS permette invece di utilizzare sia le autorizzazioni di condivisione (come in FAT32) sia quelle di sicurezza (che distingueremo chiamandole NTFS), applicate a qualunque cartella e file.

Le autorizzazioni di condivisione sono inferiori come numero a quelle di sicurezza NTFS e consentono solo un controllo grossolano dell'accesso. Inoltre le autorizzazioni NTFS consentono di proteggere cartelle e file anche se l'accesso avviene localmente.

Quando in un *File System* NTFS si utilizzano insieme entrambe le autorizzazioni di condivisione e di sicurezza NTFS possono verificarsi dei conflitti. In quei casi **prevale l'autorizzazione più restrittiva**. Ad esempio, se un utente ha l'accesso completo a un file specifico contenuto in una cartella non condivisa, quell'utente non potrà accedere al file dalla rete. L'accesso sarà possibile solo se l'utente in questione effettua il login direttamente sul computer che contiene il file. **Le autorizzazioni di condivisione non influenzano l'accesso locale**.

Una strategia per fornire l'accesso alle risorse in un volume NTFS è quello di condividere le cartelle con le autorizzazioni complete per il gruppo *Everyone* e quindi controllarne l'accesso tramite l'assegnazione di specifiche autorizzazioni di sicurezza NTFS.

Quando si utilizza autorizzazioni delle cartelle condivise in un volume NTFS, si applicano le seguenti regole:

- è possibile applicare permessi NTFS diversi a ciascun file e sottocartella contenuti in una cartella condivisa
- oltre ai permessi di condivisione di una cartella, per poter accedere al suo contenuto gli utenti devono possedere gli appropriati permessi di sicurezza NTFS sui file e sulle sottocartelle che contiene
- quando si combinano permessi di condivisione di una cartella e permessi di sicurezza NTFS prevalgono i permessi più restrittivi. Ad esempio se una cartella ha come permesso di condivisione *Read/Write* e come permesso di sicurezza *Read* per il gruppo *Everyone*, in quella cartella gli utenti non potranno memorizzare alcun file (né dalla rete né localmente).

Pianificazione dei permessi di una cartella

Il primo passo è decidere come sarà condivisa la cartella. Per farlo si consiglia di creare una lista che elenchi quali dati vi saranno memorizzati e quali utenti vi accederanno. Ad esempio, i dati potrebbero essere quelli riguardanti i dipendenti oppure clienti. I gruppi di utenti che devono accedervi possono essere manager, amministratori, addetti alle vendite, rappresentanti del servizio clienti, e così via.

Si consigli di creare una tabella con quattro colonne:

- nella prima elencare ogni cartella di dati comprensiva di nome e percorso
- nella seconda scrivere il nome delle corrispondenti condivisioni
- nella terza colonna elencare i nomi dei gruppi di utenti con le autorizzazioni di condivisione
- nell'ultima colonna scrivere i permessi di sicurezza NTFS assegnati alle cartelle condivise

Permessi base NTFS per file e cartelle

Nella scheda ***Sicurezza*** delle *Proprietà* di ogni file e cartella tutti permessi sono appositamente raggruppati in **permessi base** per rendere più semplice l'assegnazione di permessi agli utenti. La tabella seguente elenca nell'intestazione tali permessi:

Permissions	Basic Full Control	Basic Modify	Basic Read & Execute	Basic List Folder Contents	Basic Read	Basic Write
Travers Folder/Execute File	✘	✘	✘	✘		
List Folder/ Read Data	✘	✘	✘	✘	✘	
Read Attributes	✘	✘	✘	✘	✘	
Read Extended Attributes	✘	✘	✘	✘	✘	
Create Files/Write Data	✘	✘				✘
Create Folders/Append Data	✘	✘				✘
Write Attributes	✘	✘				✘

Write Extended Attributes	✘	✘				✘
Delete Subfolders and Files	✘					
Delete	✘	✘				
Read Permissions	✘	✘	✘	✘	✘	✘
Change Permissions	✘					
Take Ownership	✘					

Permessi avanzati NTFS per file e cartelle

Questi permessi si chiamano così perché si trovano nella sezione *Avanzate* della scheda *Sicurezza* di file e cartelle:

- **Visita cartella / Esecuzione file**
  - *Visita cartella*: consente o nega la navigazione per raggiungere file e sottocartelle poste al di sotto di quella a cui viene applicato questo permesso. Questa autorizzazione non implica automaticamente l'esecuzione di file di programma.
  - *Esecuzione file*: consente o nega l'esecuzione di file di programma.

- **Visualiz. contenuto cartella / Lettura dati**
  - *Visualiz. contenuto cartella*: consente o nega la visualizzazione di nomi di file e sottocartelle all'interno della cartella.
  - *Lettura dati*: Consente o nega la visualizzazione dei dati in file.

- **Leggi Attributi**
  - Consente o nega la visione degli attributi di file o cartelle, per esempio, *Sola lettura* o *Nascosto*.

- **Leggi attributi estesi**
  - Consente o nega la visualizzazione degli attributi estesi di un file o di una cartella. Gli attributi estesi sono definiti dai programmi e possono variare in base al programma.

- **Creazione file / Scrittura dati**
  - *Creazione file*: consente o nega la creazione di file all'interno della cartella.
  - *Scrittura dati*: Consente o nega la possibilità di apportare modifiche a un file e sovrascriverne il contenuto esistente.

- **Creazione cartelle / Aggiunta dati**
  - *Creare cartelle*: Consente o nega la creazione di sottocartelle all'interno della cartella.
  - *Aggiunta dati*: Consente o nega l'aggiunta di dati alla fine del file, ma non cambiare, eliminare o sovrascrivere i dati esistenti.

- **Scrivi attributi**
  - Consente o nega cambiare gli attributi di un file o una cartella, per esempio, *Sola lettura* o *Nascosto*. Questo permesso non implica la creazione o l'eliminazione di file o cartelle, include solo il permesso di modificare gli attributi di un file o di una cartella esistente.

- **Scrivi attributi estesi**
  - Consente o nega la modifica degli attributi estesi di un file o di una cartella. Gli attributi estesi sono definiti dai programmi e possono variare in base al programma. Questa autorizzazione non implica la creazione o l'eliminazione di file o cartelle, include solo il permesso di modificare gli attributi estesi di un file o di una cartella esistente.

- **Eliminazione sottocartelle e file**
  - Autorizza o nega l'eliminazione di sottocartelle e file, anche se l'autorizzazione di eliminazione non è stata concessa sulla sottocartella o sul file.

- **Elimina**
  - Consente o nega l'eliminazione del file o della cartella. Se non si dispone dell'autorizzazione di eliminazione di un file o di una cartella, è possibile eliminarlo comunque se è stata autorizzato il permesso *Eliminazione sottocartelle e file* sulla cartella principale.

- **Autorizzazioni di lettura**
  - Consente o nega i permessi di lettura di un file o di una cartella.

- **Cambia autorizzazioni**
  - Consente o nega il cambio dei permessi relativi al file o alla cartella.

- **Diventa proprietario**
  - Consente o vieta di diventare proprietario del file o della cartella. Il proprietario di un file o di una cartella può sempre cambiare i permessi su di esso, indipendentemente dalle autorizzazioni esistenti che proteggono il file o la cartella.

Permessi effettivi

Quando un file o una cartella possiede diversi ACEs a volte diventa complicato capire i permessi effettivi di un utente o di un gruppo su quell'oggetto. Per questo motivo nella sezione *Avanzate* della scheda *Sicurezza* del file o della cartella è presente la sottoscheda *Permessi effettivi* mediante la quale è possibile visualizzare le autorizzazioni risultanti. Tale risultato non tiene conto dei permessi di condivisione che tuttavia vengono applicati solo in caso di accesso mediante rete.

Copia e spostamento di file NTFS protetti

Quando un file protetto da autorizzazioni di sicurezza NTFS viene **copiato** in una cartella presente sullo stesso volume oppure copiato o **spostato** su un volume differente, esso eredita i permessi della cartella di destinazione.

Se il file protetto viene **spostato** in una cartella diversa, ma nello stesso volume, il file conserva la sua impostazione di autorizzazione di accesso, come se si trattasse di un permesso esplicito. In questo caso, infatti, non vengono trasferiti i dati, ma cambia solo il valore del loro puntatore. Per questo l'ACL del file non cambia.

Bibliografia

NTFS permissions (http://www.ntfs.com/ntfs-permissions.htm)
Panoramica sul controllo dell'accesso e autorizzazione (https://technet.microsoft.com/it-it/library/jj134043(v=ws.11).aspx)