Sistemi Operativi Windows - Architettura di Sistema.

Capitolo 1 - Sezione 1: Processi e thread

Capitolo 1 - Sezione 2: L'autenticazione nel quadro architetturale

Capitolo 2 - Utente e Dominio

Capitolo 2 - Utente e Dominio

2.1 Il Dominio e l'identità utente: Introduzione

Il metodo più diffuso oggi per accertare l'identità di una persona è quello della password o del cosiddetto *segreto condiviso*. Ne esistono altri che si basano sull'esistenza di elementi univoci connessi alla persona fisica: lo scanning della retina umana, l'analisi del DNA e le impronte digitali utilizzano questi criteri. Il metodo del segreto condiviso ha il vantaggio di non richiedere l'uso di sistemi di identificazione "bio-orientati" e il pregio di essere applicabile oltre che alle persone fisiche **anche ai servizi**, ai processi e alle macchine (che non hanno né retina, né impronte digitali). Questa caratteristica è importante poiché, oltre agli utenti, di un dominio informatico fanno parte anche le macchine (i Serve i Laptop ad esempio) e i servizi, quindi è necessario poter autenticare nel dominio sia gli uni che gli altri[1].

Quando l'amministratore di sistema crea un utente, "virtualmente" gli associa un *nome-utente* (*username*) e una *password*. Il sistema memorizza in un database (il security Database SAM) le coppie <*nome-utente, password*>. Il *nome-utente* rappresenta un campo chiave vale a dire un elemento univoco: Windows si rifiuterà di creare un nuovo *nome-utente*, se ne esiste uno identico. Il database si chiama SAM dal nome del servizio che vi accede in lettura/scrittura: *Security Account Manager* e usa questi se si tratta di accedere all'utenza locale (il vostro laptop di casa).

In caso di accesso a domini aziendali sarà invece parte dell'Active Directory. Non esamineremo l'Active Directory (non in questo corso), per ora ci limiteremo a dire che il SAM è un "modesto" security database che può contenere fino ad un massimo di 40 Mbyte di dati, mentre l'Active Directory è un grande *directory service* flessibile, praticamente privo di limiti di dimensioni, che ha tra le sue mansioni quella di conservare al proprio interno le coppie nome-utente e password dell'utenza di dominio: ha quindi ***anche*** funzione di security database, ma non solo.

[1] *I PC/Laptop fanno autenticazione allo start up.*

Possiamo quindi dire in prima approssimazione che:

- *il dominio è definito (precisato) proprio dall'elenco di persone o oggetti che sono iscritte (contenute) nel security database.*
- *Ogni utente reale o virtuale del dominio deve essere autenticato, la sua autenticazione richiede unicità di identificazione e la sua verifica avviene quasi sempre tramite il "segreto condiviso" (password).*

Piccolo glossario informale

Privacy

È il diritto che l'utente ha, creando oggetti nel sistema (per lo più file e cartelle ma anche servizi), di impedire ad altri utenti di accedervi in modo improprio o malizioso, ovvero senza avere ottenuto un esplicito consenso.

Accesso discrezionale

Alcune parti del sistema sono accessibili per alcuni utenti ed altre non lo sono. Richiede un'operazione di controllo dell'identità e induce una segmentazione del sistema dal punto di vista della sicurezza.

Autenticazione

Controllo dell'identità di un utente fisico o virtuale.

Identità univoca

Garantisce all'utente la propria individualità nel sistema.

2.5 Logon e autenticazione

L'autenticazione, dal punto di vista dell'utente, corrisponde all'operazione di **fornire** *nome-utente* e *password* (coppie di autenticazione) al momento dell'accesso al sistema (logon). Questa operazione è la “autenticazione" . Dal punto di vista del sistema operativo, invece, l'autenticazione corrisponde all'operazione di **controllare** e **verificare** *l'esistenza* della coppia <nome-utente, password> all'interno del security database. Le autenticazioni si possono effettuare su macchine singole (in "locale") o nei domini (domini aziendali) propriamente detti.

Fig. 2.1 Schermata di autenticazione (logon)

Analizziamo quindi il meccanismo di autenticazione “stand alone”, cioè quello che non fa uso dell’Active Directory.

2.6 Autenticazione: Token e Ticket Grant Ticket

Abbiamo visto nel paragrafo relativo alla architettura interna del sistema (par. 1.39) che in Windows esistono i moduli di subsystem. I processi utente, in user mode, dipendono da un subsystem e abbiamo visto il perché: i subsystem forniscono ai processi utente le interfacce per accedere al kernel.

La fig. 2.2 schematizza il processo di logon ricollegandosi al design architetturale illustrato. Tra i vari subsystem notiamo *il security subsystem (LSASS.EXE).* Non si tratta di un subsystem come il Win32 o WLS subsystem descritti nel capitolo architetturale, il security subsystem è un ambiente di esecuzione, un servizio, che serve ad implementare parte del modello di sicurezza del sistema operativo, in particolare l' autenticazione.

In fig. 2.2 è evidenziata la connessione tra il security subsystem (lsass.exe) ed il logon process (winlogon.exe – Logon UI). Quest'ultimo è il processo che mostra a video il pannello in cui l' utente può inserire username e password. Una volta che le

credenziali di un utente vengono inserite, il logon process le inoltra al *security subsystem* affinché né determinila validità. Quest'ultimo, nel caso in cui l'utente voglia utilizzare una macchina stand-alone, verifica l'esistenza delle credenziali inserite dall'utente cercandole all'interno del security database SAM presente sullo stesso computer. Se la coppia esiste, il security subsystem considera *valida l'autenticazione*. Se non esiste, l'autenticazione viene *ricusata* e l'utente (fisico o virtuale) può riprovare fino ad un numero molto limitato di tentativi, numero che è stabilito da un parametro che è sotto il controllo dell'amministratore[2].

[2] *è specificabile tramite le local security policy.*

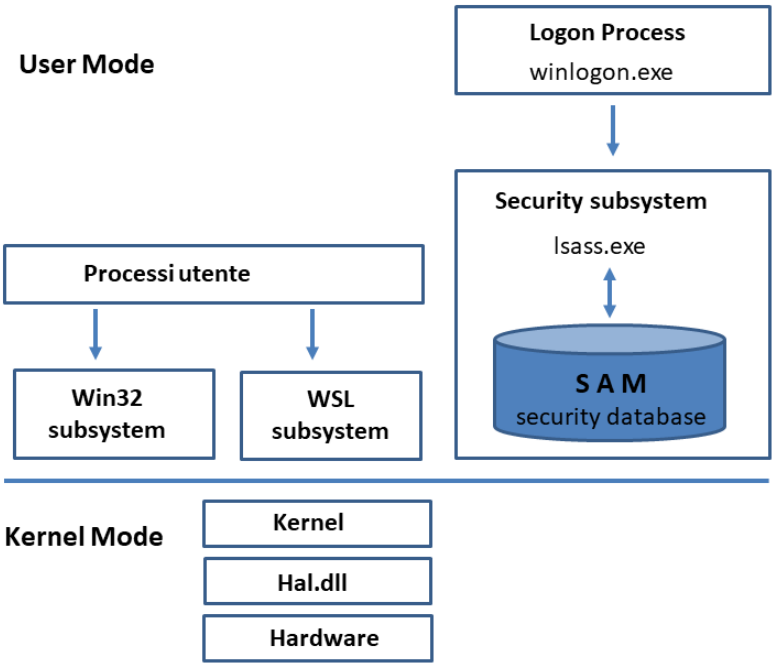

Fig. 2.2 Architettura: logon subsystem

Quando la coppia di autenticazione esiste e viene verificata il security subsystem genera un “biglietto di ingresso”, una sorta di “carta d'identità” contenente varie informazioni descrittive dell'utente che viene consegnata all'utente stesso. Questo “biglietto” prende il nome di Token nel modello di autenticazione NT e Ticket-Granting Ticket (TGT) nel modello di autenticazione usato in Windows da XP in avanti.

Kerberos e NTLM

Corre l'obbligo di citare Kerberos. Nel disegnare l'architettura del sistema Windows, Microsoft ha preferito abbandonare il modello di autenticazione precedente (NTLM), a favore di uno più diffuso ma non proprietario: Kerberos (Kerberos V5).

Microsoft tende ad essere RFC-compliant per quanto riguarda servizi, algoritmi, metodi e protocolli che devono essere usati in ambiente Intenet o comunque che richiedano il massimo della compatibilità

possibile con altri sistemi. Kerberos è un servizio e uno standard di autenticazione non proprietario, "open" e completamente documentato: nel suo ambito è uno dei più diffusi.

Kerberos fa uso di un "token", detto TGT (Ticket-Granting Ticken), che come dicevamo rappresenta la “carta di identità elettronica" dell'utente. La differenza principale tra NTLM e Kerberos consiste nel fatto che il protocollo Kerberos V5 prevede che quando un utente accede ad un servizio vada verificata sia l'identità dell'utente che accede al servizio sia quella del servizio che viene utilizzato. Questa doppia verifica è detta "mutua autenticazione" e fa di Kerberos un modello di autenticazione più "sicuro” specie in ambienti aperti e distribuiti.

Le caratteristiche di Kerberos e la sua grande diffusione hanno spinto Microsoft a preferirlo al modello NTLM: NTLM comunque esiste ancora nei sistemi Windows come modello di autenticazione *down level*, per garantire compatibilità con le vecchie versioni .

2.7 Contenuto del token, tra cui il SID

Questo biglietto di ingresso, il TGT, contiene al proprio interno tutte le informazioni utili al sistema per capire *l'identità* e i *diritti* dell'utente sul sistema: in pratica contiene l'elenco degli *user right dell'utente*, i *gruppi* a cui appartiene[3] e il suo SID (Security IDentifier).

Queste strutture identificano materialmente quello che viene indicato verbalmente col termine di "contesto di sicurezza". Ogni processo "gira" nel contesto di sicurezza di un utente, fosse anche solo un utente virtuale, come è l SYSTEM (usato di norma per i servizi). Una volta autenticato, l'utente, quando agirà sul sistema, lo farà utilizzando questo "biglietto" o "carta d'identità" (il TGT). L'Object Manager e il Security Reference Monitor (due componenti dell'Executive) fanno uso di questa carta d'identità per stabilire se l'utente possa o meno usare le risorse del sistema. Il token entra in gioco anche per l'accesso discrezionale agli oggetti del sistema, ai file o alle cartelle del file system (NTFS).

Il vantaggio del token? Una volta emesso e assegnato all'utente non occorre fare ulteriori accessi al

[3] di cui non abbiamo parlato, sono analoghe al modello UNIX più granulari e implementate con ACL—Access Control List

security database (SAM) per identificare la stessa persona. Fare continuo accesso al security database rallenterebbe il funzionamento del sistema stesso in modo inaccettabile.

> ***Nota:*** *In fig. 2.4 è raffigurato un esempio di SID . Il Token (TGT) oltre al SID definisce i security group dell'utente. Quando l'utente "John Doe" cerca di accedere ad es alla directory RDOCS, il Security Reference Monitor recupera le ACL (Access Contol List) di questa directory, le confronta con le informazioni contenuti nel token (TGT) di John Doe e se questo utente appartienead es al gruppo "Reserved docs" associato alla cartella RDOCS - da noi, o dall'amministratore - eredita i diritti del gruppo (ad esempio Read and eXecute), grazie ai quali può accedere alla directory con quei diritti.*

2.8 Cosa è il SID

Tra gli elementi presenti nel "token", ci sono gli user right, l'appartenenza ai gruppi e il SID (Security IDentifier). Il SID identifica univocamente l'utente all'interno del sistema.

Il SID è un numero, formato da campi che hanno scopi e significati differenti, di norma viene rappresentato nei registry e in letteratura e dai tool in formato decimale (cfr. fig. 2.5). Grosso modo possiamo dire che il SID è suddivisibile concettualmente in due parti. La prima parte, le prime 23 cifre circa identificano il SAM specifico di una macchina. In particolare di queste 23 cifre, il primo campo è composto da 5 cifre fisse (S-1-5-21): queste cifre sono uguali in tutti i sistemi operativi Windows (a parità di versione di sistema) e identificano il formato del SAM in uso.

Le altre 18 cifre circa (gli altri 3 campi) del SID identificano un numero univoco per Dominio: se la macchina non rappresenta un dominio è univoco per macchina e viene generato randomicamente una volta sola quando viene installato il sistema operativo (cfr Fig. 2.4).

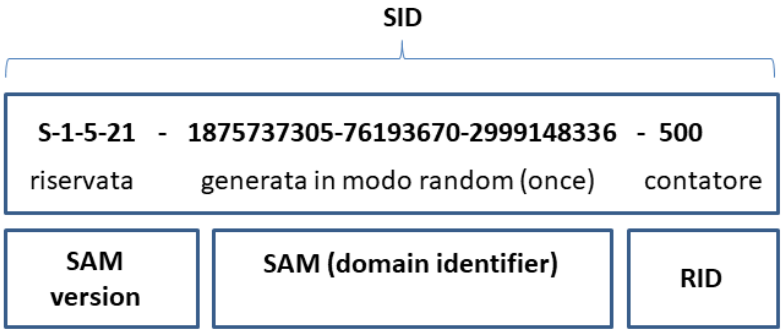

Fig. 2.4 Rappresentazione schematica del SID

Una volta generato, questo numero viene associato al dominio della macchina (singola) o, se volete, al SAM della macchina ed è considerato presumibilmente un numero "unique", ovvero unico sul pianeta terra (e anche sotto terra o nel sistema solare). Si tratta di una presunzione di unicità dato che il numero non è rilasciato da un ente centralizzato (come avviene per le targhe delle automobili o per gli IP address di Internet), è generato random. La presunzione di unicità è basata sul fatto che la probabilità che vengano creati a caso due numeri uguali di questa lunghezza è all'incirca una contro 1018 (circa 18 sono le cifre decimali della parte del SID che identificano il SAM): è abbastanza ragionevole ritenere unici questi numeri.

La seconda parte del numero (l'ultima più a destra) prende il nome di Relative Identifier o RID. Il RID identifica univocamente l'utente, ed è un contatore. I RID che vanno da 500 a 5xx sono riservati al sistema operativo stesso, l'account amministrativo generato dal sistema operativo è sempre associato al RID 500 (1F4 in esadecimale). I RID che vanno dal numero 1000 in avanti sono invece associati agli utenti e ai gruppi generati dopo l'installazione del sistema, tipicamente dall'amministratore. Gli utenti sono di norma creati facendo uso di un tool fornito dal sistema operativo: lo User Manager (in NT) il Computer Management (in Windows) o lo snap-in "AD Users and Computer" (nei domini). Il primo utente che verrà creato nel sistema avrà sempre il RID 1000.

Quando viene creato un nuovo utente, o un nuovo gruppo, il RID viene incrementato di una unità e viene associato all'utente o al gruppo appena creati: in questo modo ogni utente, ogni oggetto che fa parte del SAM avrà un proprio RID

Il SID è dunque composto da circa 23 cifre, 18 circa divise in quattro "campi" e uniche in senso globale più il RID che identifica il singolo utente del sistema e che è unico per quel sistema o dominio. Questo fa sì che il SID identifichi universalmente l'utente dato che l'unicità del numero è data globalmente dalla prima parte e localmente dalla seconda.

È possibile visualizzare il SID dell'utente attualmente "loggato" sulla macchina, semplicemente lanciando il regedit e visualizzando il contenuto della key HKEY_USERS (cfr. fig. 2.5). Nell'esempio in fig. 2.5 (immagine presa da internet) è visibile il SID di un utente di un laptop (quello con RID 1002) secondo il formato descritto in fig. 2.4.

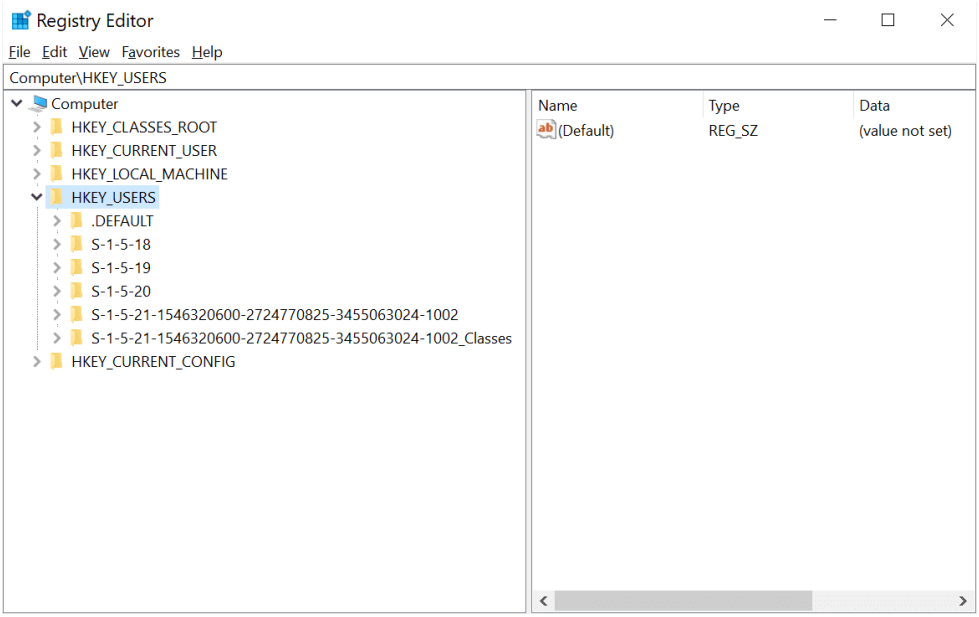

Fig. 2.5 Il SID dell'utente nell'hive del registro Computer|HKEY_USER (immagine presa da internet)

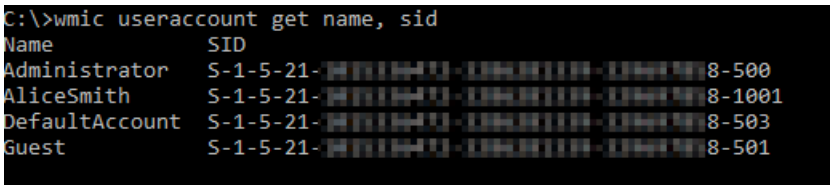

Fig. 2.6 RID di tre utenti built-in (500 l'amministratore, 501 ,503) e del primo utente creato dall'amministratore (1001) (immagine presa da internet).

2.9 SAM su macchina standalone: autenticazione locale

Ogni Windows ha un proprio security database. Quindi, dato che esiste un security database per ogni macchina, ogni PC è, a tutti gli effetti, un dominio a sé stante: un sistema autonomo, sicuro e separato dagli altri. La sicurezza è un requisito, la separatezza è una conseguenza logica. La sicurezza è **necessaria** ed è richiesta in ogni ambiente multiutente per garantire privacy e protezione dei dati, ma la presenza di un SAM per ogni macchina genera il problema della **gestione multipla di un'utenza in un dominio**, quando l'utenza appartiene a macchine diverse aventi SID differenti (cfr. fig. 2.10).

Con questo "vincolo", se volessi permettere a 100 utenti di accedere a 100 Laptop Windows - ovvero se volessi permettere a ciascun utente di loggarsi su una qualsiasi macchina indifferentemente con la stessa configurazione e gli stessi diritti (come avviene in un laboratorio studenti universitario) - dovrei creare necessariamente su **ogni macchina** (su tutti e 100 i laptop) **tutti** e 100 gli account degli utenti: il che significa effettuare 100*100 = 10.000 operazioni di management dell'utenza (troppe).

Inoltre, anche se decidessimo di effettuare questa operazione onerosa di replicare *ogni* utente su tutte e 100 le macchine con lo stesso username e password, dato che una volta autenticati è il SID e non lo username ciò che permette di identificare l'utente nel sistema, a tutti gli effetti è come se avessimo creato 10.000 utenti (100 per ognuno dei 100 PC) quindi dovremo gestire non 100 SID, ma 10.000 SID.

Se voglio permettere a questi utenti (10.000) di usare una risorsa comune, ad esempio la posta o i permessi di un firewall aziendale, come dovrei procedere? Dovrei creare 10.000 differenti regole una per ciascun utente virtuale o dovrei crearne 100 **ognuna** con i diritti di accesso ai 100 SID che fanno

riferimento alla stessa persona fisica ? Ovviamente non è logico né pratico procedere né in un modo né nell'altro. In caso di multiutenza che accede a risorse comuni, come capita nelle soluzioni aziendali e "enterprise", e nei laboratori studenti universitari, serve sicuramente un metodo più razionale .Serve una visione *centralizzata e univoca* dell'utenza e delle risorse, e un punto di autenticazione valido per tutti (SSO, Single Sign On), per garantire una visione e un corretto uso condiviso delle risorse comuni (come ad es. i firewall, le stampanti, i DHCP, etc.)

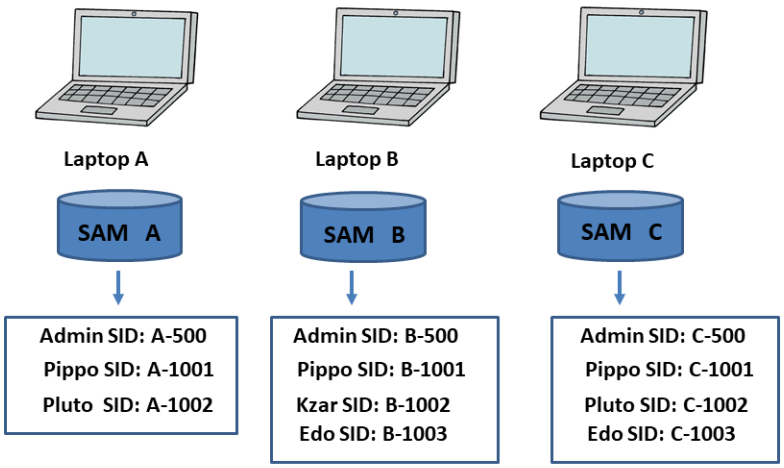

Fig. 2.10 Tre macchine Windows "standalone" con i propri SAM. Le lettere A e B e C indicano in modo sintetico la parte del SID di Dominio univoca per macchina .

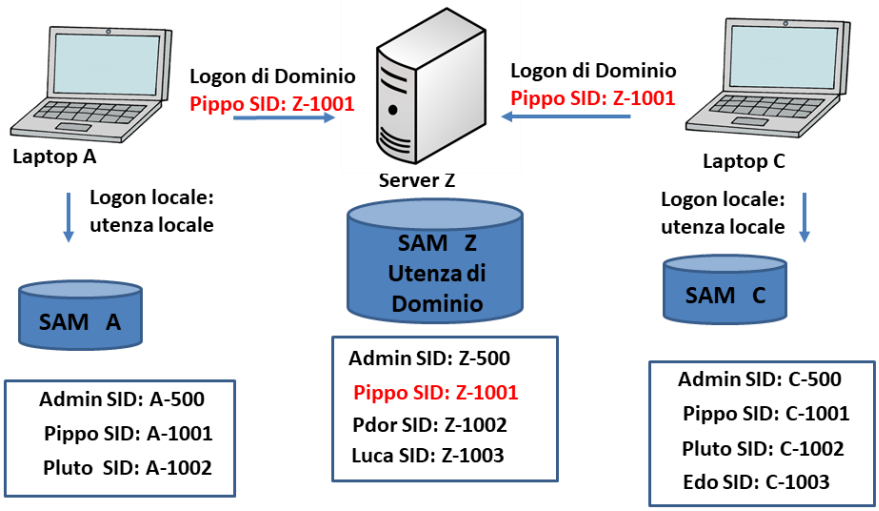

Fig. 2.11 Il Server Zeta è un Domain Controller (log on server), fa da SSO e contiene l'utenza di Dominio.

Il modo più logico di evitare la "moltiplicazione dei SID", è di rendere dominante il security database di **una particolare macchina** rispetto alle altre, forzando l'uso del security database di questa macchina per le operazioni di autenticazione. Questo permetterà di centralizzare tutta l'utenza su una sola macchina e di eliminare il problema della moltiplicazione dei SID. Questa macchina viene chiamata genericamente "logon server" o Domain Controller. Parleremo più appropriatamente di SSO (Single Sign On) parlando di Dominio, e di Domain Controller e di Active Directory on premises. In altre realizzazioni si usa Azure Active Directory (AD on the cloud) una soluzione più evoluta e moderna che comunque si fonda sempre sul concetto di fornire un punto di autenticazione univoco per l'utenza e le macchine, e un database univoco.

2.10 Single Sign On e Domain Controller

In pratica quello che abbiamo descritto è il concetto di Dominio come è implementato dai sistemi operativi Windows: se è necessario che più utenti e più macchine accedano ad un insieme di servizi comuni identificati univocamente e sempre allo stesso modo vale a dire avendo sempre la stessa identità (lo stesso SID), dobbiamo centralizzare gli account su un security database di una specifica

macchina e utilizzare questo database per effettuare l'autenticazione di dominio: il termine usato per indicare il modello di autenticazione centralizzato è Single Sign On (SSO) , in italiano “unico punto diautenticazione”. La macchina che svolge funzione di autenticazione che fa da SSO per un gruppo di utenti e macchine (il logon server) è detta Domain Controller (DC) in ambiente Windows, ed era detto Primary (o Backup) Domain Controller (PDC, BDC) in ambiente NT4/NT3.51.

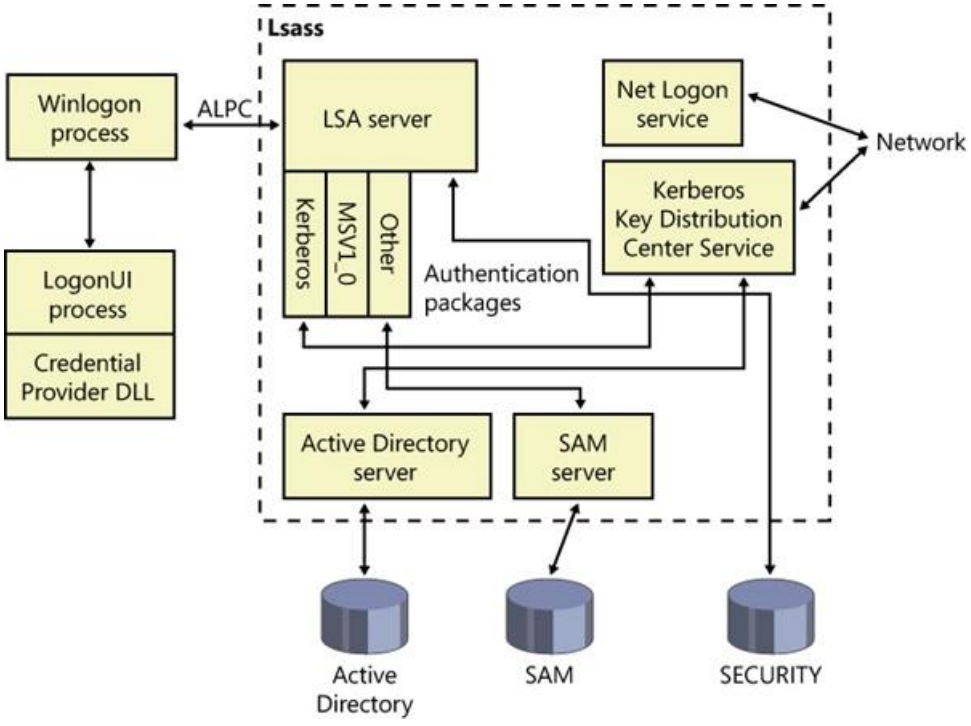

Fig. 2.11b Rappresentazione schematica delle componenti coinvolte durante il logon (immagine presa da internet)

2.12 Riassumendo: il Dominio

Ora possiamo dare una definizione più specifica di dominio Windows. Un dominio è:

- in senso stretto, un gruppo di utenti e di risorse iscritti (contenuti) in un security database;
- in senso operativo, un gruppo di utenti e di risorse (in particolare i computer), iscritti (contenuti) in un security database centralizzato, su una macchina detta logon server (genericamente) o Domain Controller (in ambiente Microsoft);

- un boundary fisico di autenticazione (definito “geograficamente” dalle macchine e risorse che appartengono al dominio);

- un sistema che fornisce servizi informatici, in modo discrezionale, a chi abbia il diritto di accedervi.

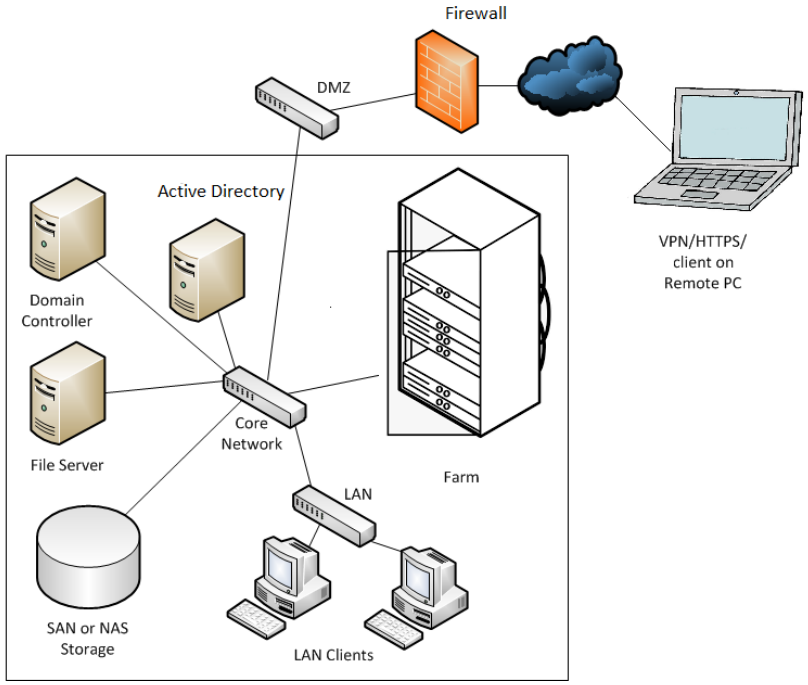

Fig 2.12 Rappresentazione schematica di un dominio e delle sue risorse (anche utenti esterni sono parte del dominio a patto che siano parte del SAM del Domain Controller o della Active Directory del Dominio)

Ovviamente prima di poter accedere a un dominio occorre *appartenervi*: come già detto possono appartenere a un dominio non solo gli utenti, ma anche i laptop, i servizi, e così via. L’operazione con cui si aggiunge un utente o una macchina a un dominio viene formalmente detta *join*. E’ un operazione sensibile dal punto di vista della sicurezza, richiede quindi diritti amministrativi, o diritti di join sulla AD, in sostanza una delega a poter aggiungere un utente o un laptop a un dominio o alla AD (come avviene per i laptop di una organizzazione).

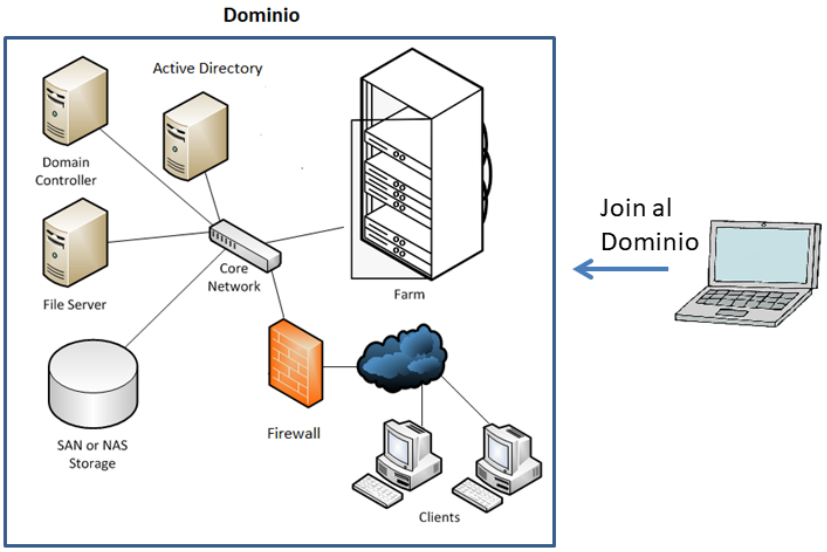

Fig 2.15 schematizzazione di una operazione di join al dominio

3.1 Active Directory: 3 punti

Descrivere AD (Active Directory) è sicuramente di grande interesse ma non è oggetto di questa stesura. Ci si limiterà a dire, per completezza espositiva, in queste poche righe che AD è stata creata per superare le limitazioni esistenti nel security database SAM (il security database di NT) relative alla gestione dei dati e in particolare alla:

- capacità di rappresentare molti tipi di dati ed estensibilità dei tipi;
- quantità di dati accettabili e scalabilità del database in dimensioni;
- sicurezza e delega;
- accesso distribuito;
- replica distribuita dei dati.

AD è un database LDAP (Lightweight Directory Access Protocol) che utilizza Kerberos V5 per l'autenticazione. E' distribuito, replicato, estendibile, e scalabile. Creato e utilizzato per rappresentare i dati dell'utenza, di servizi e dispositivi, nasce per soddisfare le esigenze di rappresentare su grande scala i dati di dominio, fornire un servizio di autenticazione univoco e distribuito per i domini enterprise, e grazie alla sua estensibilità di tipi consente di includere informazioni di natura disparata, utili ovviamente per tutti i servizi e utenti di dominio, viene usato infatti anche per integrare informazione come il database del DNS.

Oltre alla *AD on premises* che un sistemista può installare con le sue forze, è possibile usare AD in modalità cloud, commercialmente "Azure Active Directory".

In relazione ai servizi di autenticazione, Azure Active Directory fornisce i seguenti metodi di autenticazione:

- **Autenticazione in cloud** - Azure Active Directory gestisce il processo di autenticazione per l'accesso degli utenti, ed è possibile scegliere tra due opzioni:
    - **Sincronizzazione dell'hash delle password (PHS)** - La sincronizzazione dell'hash delle password consente agli utenti di usare gli stessi nome utente e

password usati in locale senza la necessità di implementare infrastrutture aggiuntive oltre a Azure AD Connect le hash password vengono sincronizzate tra la AD locale e Azure AD.

- **Autenticazione pass-through (PTA)** -Questa opzione è simile alla sincronizzazione dell'hash delle password, ma fornisce una convalida delle password mediante agenti software locali per organizzazioni con criteri di conformità e sicurezza avanzati.

- **Autenticazione federata** - Se si sceglie questo metodo di autenticazione, Azure AD trasferisce il processo di autenticazione a un sistema di autenticazione attendibile separato, ad esempio AD FS o un sistema di federazione di terze parti, per convalidare l'accesso dell'utente.

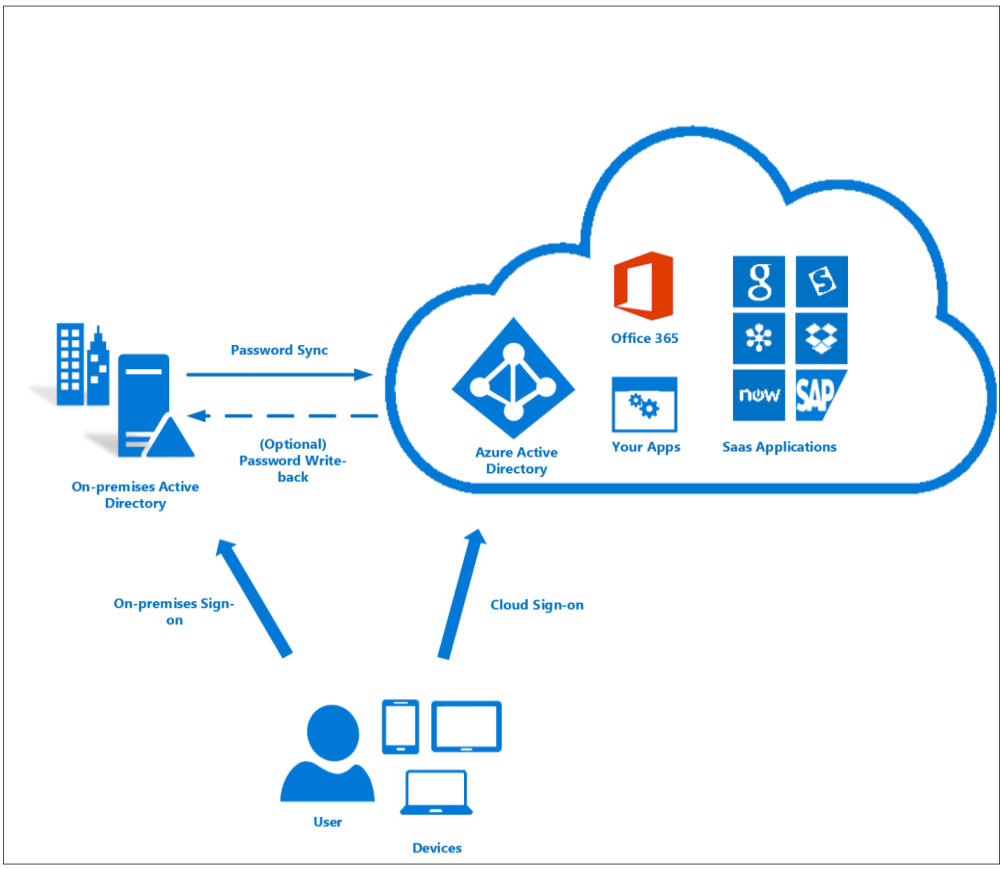

Fig 2.1Autenticazione cloud: sincronizzazione dell'hash delle password (PHS) tra Azure Active Directory e AD on Premises (immagine tratta da Microsoft Docs)

Per approfondimenti sulle molte caratteristiche di AD on premises si rimanda il lettore a *"Active Directory come directory service" di Stefano Pinardi, Emanuele Colombo, Alessandro Aruanno, Duke Italia editore, 70 pagine, ISBN:8886460155.*

Si chiude così questo doppio capitolo sull'architettura Widows, introduttivo e descrittivo dei processi e thread, e di alcuni aspetti architetturali relativi al concetto di autenticazione e Dominio di Windows.