Sicurezza su Grid

Corso: Sicurezza Informatica
Studente: Mattia Cinquilli
Professore: Stefano Bistarelli
AA: 2008/2009

Introduzione e Definizione di Computing Grid

La griglia computazionale e' un tipo di sistema parallelo e distribuito che consente la condivisione, selezione e aggregazione di risorse autonome geograficamente distribuite utilizzate a tempo di esecuzione, a seconda della loro disponibilita', capacita', prestazione, costo e qualita' del servizio richiesto dall'utente.
Dunque il Grid Computing altri non e' che l'applicazione infrastrutturale di quella logica di condivisione delle risorse che consente di utilizzare la potenza di elaborazione di una serie di computer collegati in rete via Internet, dividendo i processi di calcolo e di memoria secondo regole di distribuzione definite dai gestori della grid.
Cio' che rende possibile quest'infrastruttura intermediando fra diverse entita' e' il *middleware*. Questo e' un software di connessione formato da un insieme di servizi e di ambienti di sviluppo che consentono a piu' entita' che possono risiedere su uno o piu' elaboratori, di interagire attraverso una rete di connessione a dispetto di differenze nei protocolli di comunicazione, architetture dei sistemi locali, sistemi operativi, ecc.. Dunque, lo scopo del middleware e' quello di offrire servizi di comunicazione, astrazione, collaborazione ed un'ambiente di sviluppo delle applicazioni per permettere l'interoperabilita' e la connettivita' fra applicazioni distribuite su risorse eterogenee.

Definita da Ian Foster e Carl Kesselman nel 1998, nel libro "The GRID: A blueprint for a new computing infrastructure" come:
"...un sistema pensato per consentire ad una comunità di utenti di usare risorse di calcolo distribuite in Internet come se fossero di fronte ad un unico sistema di calcolo..."

La Grid permette dunque di virtualizzare risorse remote come se fossero locali, garantendo un accesso trasparente a risorse distribuite globalmente. Con risorse si intendoono sia i dati (di esperimenti scientifici, finanziari, ...) sia la potenza di calcolo (processori, cluster, supercomputer, ...). Inoltre l'infrastruttura della Grid e' costituita dai servizi per accedere alle risorse e dalle risorse stesse.

Dunque, in una Computing Grid "ideale" le infrastrutture sono generiche: non dipendono dalle applicazione che servono; le risorse non sono controllate centralmente, ma vengono amministrate localemente, e per rendere possibile questo e' fondamentale usare dei protocolli e delle interfacce che siano: standard e generici.
Ovviamente la qualita' dei servizi deve essere elevata.

Architettura Grid

Non e' possibile definire un'architettura grid che possa essere considerata come definita perche' le caratteristiche e l'architettura dipendono fortemente dal caso concreto. Ad esempio e' ben diverso avere risorse omogenee gestite amministrativamente in maniera centralizzata dall'organizzare risorse eterogenee e controllabili solo localmente.

In questo ultimo caso, che e' quello che ci interessa, una delle richieste a cui dovra' soddisfare la grid e' quella di assemblare risorse eterogenee, di essere scalabili nelle infrastrutture, di assicurare dinamicita' di uso delle risorse e di organizzazione di quest'ultime. E' tuttavia possibile definire come e' organizzata in generale una grid da un punto di vista concettuale.

Sono distinguibili 3 macro-livelli architetturali.

- Livello delle Applicazioni
  Ne fanno parte tutte le applicazioni dell'utente che interagiscono, direttamente o non, con la grid. Talvolta contiene l'interfaccia che consente all'utente di interagire con la grid e quindi anche l'ambiente di programmazione (API). Questo e' caratterizzato da un'assoluta portabilita' attraverso vari tipi di sistemi hardware-software e loro combinazioni in un contesto di eterogeneita' e dinamicita'. Inoltre tutto il meccanismo della gestione dei gruppi di lavoro e' parte integrante di questo livello.

- Livello Middleware
  Questo livello e' a sua volta scomponibile in due parti: un livello piu' vicino all'utente (High Level) ed uno piu' vicino alle risorse (Low Level).
  L'High Level e' costituito da:
  Knowledge Discovery: servizi di grid che forniscono un accesso consistente, pervasivo ed efficace a risorse computazionali, con un interesse rivolto allo sfruttamento della grid come sofisticato strumento di "Web computing";
  Sicurezza: la possibilita' di un efficace ed efficiente controllo di accesso alla griglia per avere ambienti di grid sicuri, ma anche per una cooperazione tra ambienti grid appartenenti a differenti organizzazioni;
  Resource Broker: servizio che fornisce un collegamento tra la richiesta di risorse e le risorse disponibili.

  Il Low Level e' composto da:
  Scheduling: si occupa di mappare costantemente le risorse della grid;
  Monitoring: questo servizio si incarica di controllare l'utilizzo delle risorse del sistema e di dare un supporto diagnostico in caso di guasti e sovraccarichi;
  Comunication: definisce i protocolli di comunicazione e autenticazione per le transazioni di rete abilitando lo scambio dei dati con il livello fabric. I protocolli di comunicazione permettono lo scambio di dati tra le risorse del livello inferiore, cioe' implementano i servizi di trasporto, routing e naming; mentre i protocolli di autenticazione forniscono un meccanismo di autorizzazione e protezione delle comunicazioni in uno scenario multi-istituzionale permettendo l'interoperabilita' tra le varie soluzioni locali.

- Livello Fabric
  Le risorse sono oggetti che hanno proprietari, che possono essere usate per un certo periodo di tempo e che possono essere rinnovabili oppure no. Sono gestite tramite lo Scheduling, il Knowledge Discovery e il Resource Broker. Questi permettono di allocare le risorse di cui ha bisogno un utente, sottraendole a quelle disponibili. I dati possono essere replicati per l'ottimizzazione delle risorse di memorizzazione, garantendo piu' prestazioni nell'accesso ai dati.
  Alcuni esempi di risorse possono essere spazio disco, banda di rete, tempo di CPU o semplicemente dati.

Gli Utenti vengono gestiti tramute le organizzazioni virtuali (VO, Virtual Organization) sono un insieme dinamico, multi-istituzionale e virtuale di entita' che condividono risorse. Ognuna ha una dimensione differente e persegue un diverso scopo con una diversa durata temporale. In alcune architetture le VO sono utilizzate per fornire agli utenti di un gruppo, senza una particolare caratterizzazione geografica, la potenzialita' di accedere alla risorse di un sistema distribuito, garantendone un accesso coordinato e controllato, offrendo all'utente la visibilita' di un unico sistema di calcolo logico, facilmente scalabile.

Ogni entita' mette a disposizione della griglia computazionale un insieme di risorse locali. I I membri di una stessa VO condividono alcuni privilegi della VO stessa, e ognuna di queste entita' puo' utilizzare le risorse della griglia computazionale combinandole nel modo piu' opportuno per risolvere i propri problemi. Inoltre, ogni entita' agisce sia da client che da server (cosi' come avviene nella tecnologia peer to peer).

Sicurezza su Grid

Poiche' non e' certamente possibile una condivisione incondizionata di risorse a livello di Internet, e' fondamentale che l'aspetto della sicurezza sia trattato in una Computing Grid. Per questo, vengono definiti tre livelli di sicurezza:

- politica di accesso: i fornitori di risorse e gli utenti devono definire con chiarezza e precisione a chi e' permesso di condividere risorse e per quali condizioni le risorse possono essere accedute;
- autenticazione: e' importante un meccanismo per la verifica dell'identita' di una risorsa e di un utente;
- autorizzazione: e' necessario un meccanismo per determinare se un operazione e' permessa, a seconda della relazione di politica di accesso delle risorse.

Quindi e' importante sapere chi e' autorizzato ad usare Grid e quali risorse in particolare; chi certifica che l'utente autentificato sia proprio quell'utente; quali sono le politiche d'uso delle risorse.

EGEE: un esempio di Computing Grid

Esistono varie comunità di ricerca in Europa, negli USA, in Asia e in altre nazioni, che sviluppano e raccordano tra di loro diverse Computing Grid.
La fisica delle alte energie (HEP, High Energy Physics) ha avviato il progetto WLCG (Worlwide LHC Computing Grid) il cui obiettivo e' quello di costruire e mantenere un'infrastruttura per le attivita' della comunita' fisica dell'esperimento LHC (Large Hadron Collider), in attivita' presso il CERN di Ginevra. WLCG sfrutta due progetti paralleli:

- Enabling Grid for E-sciencE (EGEE) in Europa
- Open Science Grid (OSG) negli USA

Enabling Grid for E-scienc e' il progetto finanziato dalla Comunita' Europea che ha come scopo la realizzazione di un'infrastruttura grid sicura, affidabile e robusta, che consenta di accedere a risorse geograficamente distribuite 24 ore al giorno. La base di partenza e' stata quella del preesistente LHC Computing Grid (LCG), e uno degli scopi e' di fornire a LCG nuove versioni del middleware.

Questo progetto raccoglie piu' di 50 nazioni con il fine comune di costruire un'infrastruttura Grid che fornisca servizi per scienziati 24/24h e 7/7gg disponibili indipendentemente dalla locazione geografica, utilizzando le piu' avanzate e recenti tecnologie Grid. Inoltre EGEE non sottovaluta l'interesse nell'attirare un ampio spettro di nuovi utenti ed utilizzi.

Problema: Computing Grid Security

In un ambiente computazionale multiorganico e' imperativo che tutti gli utenti e servizi interagiscano in un modo sicuro. I differenti servizi Grid e gli utenti devono essere in grado di 'fidarsi' l'uno dell'altro: cio' implica che l'uso delle risorse, che appartengono a domini multipli e distinti devono essere sotto controllo e i proprietari delle risorse hanno il diritto di decidere chi e chi non puo' usare le loro risorse; le stesse risorse (come i dati che sono in Grid) devono avere un proprietario. Inoltre dev'essere possibile trovare chi ha fatto cosa.

La sicurezza e' alla base di un sistema come Grid. Pero' Grid è estremamente dinamica: non ha un punto di controllo centrale e ogni provider di risorse ha le proprie policy (requisiti, politiche, tecnologie); inoltre un singolo utente con un'applicazione puo' utilizzare contemporaneamente risorse di piu' siti. Dunque sono un nodo centrale:

- *Autenticazione* ⇒ processo per stabilire una mutua fiducia
- *Autorizzazione* ⇒ capacita' di dire chi e' capace a fare qualcosa
- *Certificati* ⇒ provano l'identita' di un soggetto

Il Gruppo di lavoro GGF (Global Grid Forum) e l'OGSA (Open Grid Service Infrastructure) hanno raggruppato le sfide di sicurezza per la Computing Grid in 3 categorie:

- *Integration*: le infrastrutture di sicurezza esistenti non possono essere rimpiazzate, quindi non esiste una soluzione di sicurezza globale dove ogni dominio crea-gestisce-supporta la propria infrastruttura (eg: user account directory)
- *Interoperability*: i servizi Grid che interagiscono fra loro devono poter attraversare domini e hosts, garantendo l'interoperabilita' a diversi livelli:
  - Protocol messaggi che i servizi si scambiano (SOAP/HTTP)
  - Policy: policy differenti fra domini, specificate con una comune sintassi e semantica
  - Identity: identificare utenti attraverso domini diversi
- *Trust Relationship*: proteggere le risorse e proteggersi da chi offre le risorse attraverso il concetto di fiducia (Trust) e l'utilizzo di terze parti; organizzazioni di utenti che si fidano l'una dell'altra ed utenti si fidano l'uno dell'altro per identificare altri utenti.

Dunque, le esigenze di sicurezza di un sistema Grid sono:

Single sign-on: l'utente dovrebbe essere in grado di autentificarsi una sola volta per iniziare la computazione che acquisisce-usa-rilascia le risorse, senza nessun altra autenticazione dell'utente.
Protection of credential: le credenziali dell'utente (password, chiavi private, ...) devono essere protette.
Interoperability with local security solutions: l'accesso a risorse locali e' determinato dalle politiche/meccanismi di sicurezza locali, adottando soluzioni che prevedano un meccanismo di accesso interdominio e intradominio.
Uniform credential/certification infrastructure: accesso interdominio richiede almeno una via comune per esprimere/verificare l'identita' di un utente/risorsa.

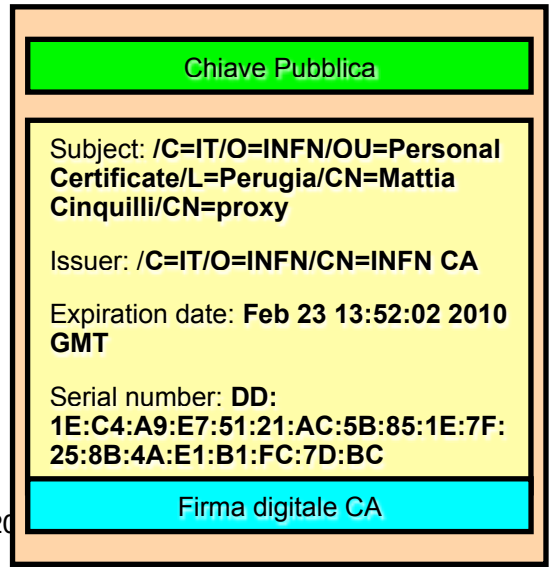
Grid consiste di piu' domini di fiducia: integrare collezioni eterogenee di utenti e risorse localmente amministrati, controllando le interazioni interdominio e l'associazione fra le operazioni interdominio e le politiche di sicurezza locale.
Esistono sia soggetti locali che globali: per ogni dominio esiste un'associazione parziale fra soggetti globali e locali: ogni utente di una risorsa ha due nomi, uno globale ed uno locale che e' potenzialmente differente per ogni risorsa; l'associazione (mapping) di un nome golbale in uno locale dipende dal sito; il nome globale permette il single sign-on.
Un soggetto globale autenticato, associato (mapped) in un soggetto locale e' uguale ad un soggetto locale autenticato: in un dominio "fidato" la combinazione delle politiche d'autenticazione Grid e l'associazione locale corrispondono alle politiche di sicurezza del dominio locale.
Il controllo sull'accesso avviene in base al soggetto locale: le politiche d'accesso rimangono quelle del dominio locale.
Un processo puo' lavorare a nome di un utente ed avere i suoi diritti: permette computazioni lunghe che possono acquisire risorse dinamicamente (single sign-on).

I meccanismi di sicurezza utilizzati prevedono l'utlizzo di:

- *CERTIFICATI X.509*. Standard ISO e IETF che collega credenziali a chiave pubblica (chiave pubblica e privata) ad un'identità. I certificati sono rilasciati da un insieme di ben definite Certification Authorities(CAs). Le credenziali sono divise in due parti: parte pubblica nel certificato (da condividere), parte privata che DEVE essere tenuta segreta.
- *PKI –Public Key Infrastructure*. Insieme di standards che definisce come i certificati e le CA debbano lavorare insieme.
- *GSS-API –Generic Security Services Application Program Interface*. Standard IETF definisce un'interfaccia unificata a meccanismi di sicurezza eterogenei (Kerberos, certificati X.509, etc..)

GSI Grid Security Infrastructure
Infrastruttura di sicurezza che collega insieme le tre componenti (certificati X.509, PKI e GSS-API) e aggiunge capacita' di delega delle credenziali (vedi piu' avanti...)
Una Certification Authority(CA) rilascia i certificati.
Ogni utente/servizio e' identificato da un certificato codificato in formato X.509 che contiene il subject name che identifica utente/servizio, la chiave pubblica, l'identita' della CA che ha rilasciato il certificato assieme alla sua firma digitale.

Struttura certificato X.509

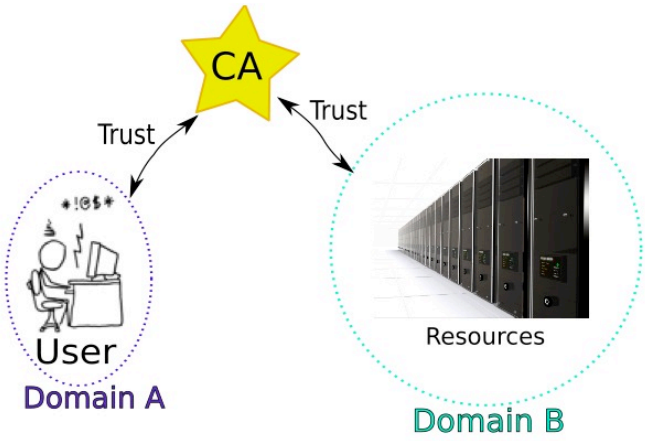


Certification Authorities (CA)
Chi garantisce che una chiave pubblica appertinga veramente a qualcuno? Le
Certification Authorities rilasciano una coppia di chiavi dopo aver verificato oltre ogni dubbio l'identita' del richiedente. L'entita' che ha l'obbligo di verificare l'identita' sono le Registration Authorities. Per provare che la chiave pubblica appartenga realmente a qualcuno e' necessario che la CA firmi la chiave pubblica dell'utente utilizzando la propria chiave privata. Cosi', una chiave pubblica firmata da una CA e' un certificato (le CA autofirmano i propri certificati).
Nel caso in cui un certificato venga compromesso la CA

revoca il certificato che non sara' mai piu' valido che viene incluso in una lista di certificati revocati regolarmente aggiornata (CRL: Certificate Revocation List).
Un certificato X.509 rilasciato da una CA e' composto da:

- ✓ Chiave pubblica del proprietario
- ✓ Identita' del proprietario
- ✓ Informazioni sulla CA
- ✓ Validita'
- ✓ Numero di serie
- ✓ Firma digitale della CA

I ceritificati hanno una data di scadenza: tipicamente hanno durata di un anno dal momento della creazione



Grid Authentication
L'autenticazione su Grid e' un'operazione fatta in comune (normalmente fra un utente ed un servizio) dove l'intero processo e' trasparente percio' l'utente non si accorge di tutti i passaggi della comunicazione necessaria per l'autentifica.
Vengono percio' eseguiti i seguenti passaggi perche' il servente puo' autentificare l'utente (la stessa procedura analoga avviene viceversa):

- L'utente invia la sua chiave pubblica al servente
- Il servente verifica la firma della CA
- Il servente invia una frase random all'utente
- L'utente calcola l'hash della frase e la cripta con la sua chiave privata
- L'hash criptata e' inviata al servente
- Il servernte decripta l'hash con la chiave pubblica del certificato dell'utente e la confronta con la propia hash della frase

Certificati Proxy e MyProxy
Il proxy di un utente e' un processo a cui e' dato il permesso di operare "a nome" dell'utente, cosi' che ogni processo d'autenticazione non debba richiederebbe la password della chiave privata dell'utente. I proxy altro non sono che dei certificati temporanei firmati con il certificato dell'utente, con una durata tipicamente corta (12 ore) e senza una password, che corrispondono a dei file contenti sia il certificato che la chiave privata.
Il file del proxy deve essere protetto dalla lettura, ma un proxy puo' essere usato per firmare un altro proxy (Proxy Delegation).

Un'operazione in Grid puo' avere la necessita' di un proxy valido per un tempo molto piu' lungo e alcune applicazioni Grid necessitano anche di qualche giorno (trasferimenti automatizzati di grandi quantita' di dati, jobs di analisi particolarmente lunghi). Ma il proxy ha un tempo di vita corto (esempio: 12 h) e avere un proxy lungo non e' una buona idea, quindi e' stato ideato il MyProxy server che permette di creare e memorizzare un certificato proxy di lunga durata cosi' che un servizio Grid possa contattarlo per rinnovare un proxy che sta per scadere. Ovviamente solo i servizi registrati sono autorizzati a chiedere/ricevere la delega e un servizio dedicato puo' rinnovare il proxy in modo automatico.

Virtual Organization Management System (VOMS)
Per diventare parte di una VO, un utente deve eseguire dei ben precisi passi:

- L'utente ottiene un ceritificato dalla CA
- L'utente si registra alla VO
- Normalmente avviene attraverso un'interfaccia web con il certificato utente caricato nel browser
- Il manager della VO approva la richiesta
- L'utente viene conosciuto come appartente alla VO anche dai servizi Grid

Il Virtual Organization Management System (VOMS) permette di estendere un proxy per includere che l'utente appartiene ad una specifica VO e ad uno o piu' gruppi della VO. Questo permette di definire dei ruoli speciali (o limitati) all'interno della VO, che consentano di avere dei jobs con priorita' speciale e/o permesso di leggere/scrivere in certe aree di storage. Dunque il server VOMS per una VO contiene tutti i gruppi e i ruoli che esistono e tutti gli utenti e a quali gruppi-ruoli essi appartengono.
I gruppi di VOMS sono gerarchici e i ruoli di VOMS sono sempre collegati ad un gruppo.

Alcuni possibili pericoli:

- Attacchi ai servizi di rete della Grid
- Codice utente vulnerabile, escalation di privilegi di utenti autenticati, accessi non autenticati guadagnati tramite jobs o codice errato
- Software di base vulnerabile (librerie incluse)
- Utilizzo degli account alla Grid non autorizzato/autentificato

Conclusioni
Le soluzioni di sicurezza sono abbastanza rigide e presentano dei colli di bottiglia per quanto riguarda la scalabilita', infatti le richieste degli utenti devono avvenire sempre attraverso un proxy e l'associazione fra soggetto globale-locale con l'aumentare degli utenti e' un limite.
Il sistema di sicurezza e' basato sui sistemi gia' esistenti e necessita' di migliorare i sistemi gia' presenti e sviluppare dei sistemi dedicati sfruttando l'esperienza maturata

Un altro elemento delicato e' la sicurezza degli Storage Element: questi contengono dei dati che sono accessibili da "chiunque" nella Grid, tramite particolari/dedicati protocolli, infatti e' come condividere il disco fisso del vostro computer su Internet. Per questo oltre essere d'estrema importanza gestire bene i permessi di lettura/scrittura, sono necessari dei protocolli d'accesso dedicati che siano particolarmente affidabili per autorizzazione e autentifica. Gia' esistono, ma attualmente sono in fase di migioraramento.