ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di LECCE

INFN/code-xx/xxx
giorno/mese/anno

CCR-24/2008/P

PROGETTO INFN-AAI: CONCEPTUAL DESIGN REPORT

AAI-WG

Abstract

Il progetto INFN-AAI ha come scopo principale quello di definire e dispiegare una Infrastruttura di Autenticazione ed Autorizzazione (AAI) unica per l'INFN, basata su Autenticazione Kerberos5 ed Autorizzazione attraverso un Directory Service LDAP. Tale Infrastruttura avrà una triplice valenza: offrire uno strumento utilizzabile per l'accesso alle applicazioni centralizzate; presentare l'INFN come unica entità nella partecipazione a federazioni di AAI; fornire alle singole sedi uno strumento che possa efficacemente sostituire i vari sistemi di Autenticazione ed Autorizzazione in uso, armonizzandoli in una unica Infrastruttura —integrata con quella nazionale— che permetterà di estendere le funzionalità dei sistemi di AA in produzione, garantendo la compatibilità con le applicazioni dispiegate nelle sedi, e fornendo supporto per il Single Sign-On (SSO).

In questo documento di descrizione concettuale (Concepual Design Report) oltre a evidenziare le motivazioni che hanno portato alla nascita del progetto, verrà effettuata l'analisi delle caratteristiche delle Infrastrutture esistenti nelle varie sedi, evidenziandone i limiti e la complessità della gestione. Verrà quindi illustrato il modello di AAI proposto per l'INFN che, oltre a fornire tutte le potenzialità e le funzionalità tipiche di una Infrastruttura di Autenticazione ed Autorizzazione unica, garantisce il mantenimento dell'autonomia dei Servizi di Calcolo e Reti delle singole sedi. Verrà infine analizzato un possibile piano di implementazione e una prima valutazione delle risorse umane, dei costi e delle attrezzature necessarie.

Pubblicato da **SIS–Pubblicazioni**
Laboratori Nazionali di Frascati

AAI-WG

Daniela Anzellotti[1], Silvia Arezzini[2], Enrico M.V. Fasanelli[3], Roberto Lulli[4], Simone Marini[2], Dael Maselli[5], Fulvio Ricciardi[3], Maurizio Siteni[6], Alessandro Spanu[1], Francesco M. Taurino[7], Emanuele Turella[5]

[1)]INFN-Sezione di Roma, Piazzale Aldo Moro, 2, I-00185 Roma, Italy
[2)]INFN-Sezione di Pisa, Largo B. Pontecorvo, 3, I-561270 Pisa, Italy
[3)]INFN-Sezione di Lecce, Via prov.le per Arnesano, I-73100 Lecce, Italy
[4)]INFN-Sezione di Roma2, Via Della Ricerca Scientifica, 1, I-00133 Roma, Italy
[5)]INFN-Laboratori Nazionali di Frascati Via E. Fermi 40, I-00044 Frascati, Italy
[6)]INFN-Sezione di Roma3, Via Della Vasca Navale, 84, I-00146 Roma, Italy
[7)]CNR/INFM ed INFN-Sezione di Napoli, Via Cintia, I-80126 Napoli, Italy

INDICE

1 INTRODUZIONE E FRAMEWORK 5
1.1 AAI e servizi che ne hanno bisogno 5
1.2 Situazione attuale nell'INFN 7
1.2.1 Stato delle AA nelle singole sedi 7
1.2.2 AA nel calcolo scientifico 19
1.2.3 AA nelle applicazioni centralizzate a livello nazionale 20
1.3 Ottimizzazione/Armonizzazione 27
1.3.1 Federazione di AAI locali 28
1.3.2 INFN-AAI 28
2 IL PROGETTO INFN-AAI 29
2.1 INFN-AAI 29
2.1.1 Obiettivi 29
2.2 Requisiti 30
2.3 Implementazione 32
2.3.1 Strumento SW 32
2.3.2 Architettura 35
2.4 Attività preliminari 41
2.4.1 Alpha-Testing 41
2.4.2 Stress Test 44
2.5 Proto AAI 45
3 PIANO ORGANIZZATIVO 47
3.1 Piano delle attività 47
3.1.1 ß-Test ed R&D 47
3.1.2 Fase Pilota 50
3.1.3 Produzione 50
3.1.4 Attività future 51
3.2 Milestones e tempi di attuazione 52
3.2.1 ß-Test ed R&D 52
3.2.2 Pilota e Produzione 54
3.3 Struttura organizzativa 54
4 ANALISI DEI COSTI 57
4.1 Infrastrutture 57
4.1.1 Infrastruttura di core 57
4.1.2 Infrastruttura locale 57
4.2 Risorse Umane 58
4.2.1 Gruppo di gestione 58

4.2.2 Supporto singole sedi 59
4.3 Riepilogo dei costi 60
5 ANALISI RISCHI 61
5.1 Rischi tecnologici 61
5.1.1 Software open source 61
5.1.2 Scalabilità del modello 61
5.1.3 Espandibilità del modello 61
5.2 Rischi organizzativi 62
5.2.1 Man-power 62
5.2.2 Formazione 62
5.2.3 Tempi di attuazione della INFN-AAI 63
5.3 Rischi economici 63
6 GLOSSARIO 64
7 RINGRAZIAMENTI 68
8 BIBLIOGRAFIA 69

1 INTRODUZIONE E FRAMEWORK

In questo capitolo verranno sinteticamente descritti i principali servizi informatici che possono utilizzare una AAI e le informazioni di cui tali servizi hanno bisogno (paragrafo 1.1). Verrà poi presentata (paragrafo 1.2) una fotografia dello stato attuale dei sistemi di AA in uso nell'INFN, considerando sia quelli utilizzati per i servizi informatici offerti all'utenza nelle varie sedi, che quelli relativi ai servizi centralizzati (come quelli forniti da DataWeb, il nuovo list-server basato su SYMPA[1)] e gestito dal CNAF ed il servizio TRIP[2)] di accesso alla rete wireless INFN). Verrà quindi evidenziato (paragrafo 1.3) come attraverso l'utilizzo di un **Servizio di Directory,** interrogabile attraverso il protocollo **LDAP**[3)] (ossia quello che viene comunemente chiamato "server LDAP") sia possibile ottimizzare i sistemi di AA in uso nelle varie sedi INFN e garantire l'accesso ai servizi centralizzati a livello nazionale.

1.1 AAI e servizi che ne hanno bisogno

In un qualunque ambiente informatico, tutti i servizi hanno bisogno sia di un sistema di Autenticazione che di un sistema di Autorizzazione. Nelle situazioni in cui non siano presenti infrastrutture centralizzate di AA, è sempre possibile (ed in alcuni casi necessario) configurare i vari servizi informatici in modo che usino un loro database interno per questo doppio importante scopo.

In una qualunque sede INFN vengono normalmente forniti i seguenti servizi:

- accesso interattivo a sistemi Unix e Windows
- relay di posta elettronica (SMTP server)
- accesso alle caselle di posta elettronica (IMAP/POP server)
- servizio di stampa
- applicazioni WEB (compreso l'accesso a pagine protette)
- accesso alla rete (wireless e wired)
- accesso a database locali
- servizio di mailing-list

Il login interattivo in un sistema Unix ha bisogno di informazioni relative all'utente (username, userID, password, home directory e shell di default) ed ai gruppi a cui l'utente appartiene (groupID). Tali informazioni si trovano nei file /etc/passwd ed /etc/group di ogni sistema. Esistono metodi standard per distribuire queste informazioni a gruppi di host (la più

utilizzata è NIS/YellowPages)

Il servizio di posta elettronica ha in realtà una doppia funzione: servizio di accesso alla casella di posta elettronica (POP/IMAP) e servizio di relay SMTP. Il servizio POP/IMAP ha bisogno di conoscere alcune informazioni in comune con quelle del login interattivo (username, userID e password) oltre alla posizione su disco delle caselle di posta elettronica dell'utente. Il servizio di relay SMTP dipende da informazioni relative al maildrop dell'utente (su quale host consegnare la posta) e agli alias (a quale utente corrisponde l'indirizzo di posta elettronica), nonché spesso anche dalla lista di reti autorizzate e dalla lista dei domini per i quali si gestisce il servizio. Tali informazioni devono essere replicate in tutti i mail exchanger di sede. Ancora più informazioni sono necessarie ai sistemi di gestione delle mailing list, che per poter autorizzare l'accesso agli archivi, l'iscrizione o l'utilizzo di una lista, devono poter accedere a particolari elenchi e alle caratteristiche della lista stessa. Tutte queste informazioni sono spesso in database locali ai server e, a differenza del servizio di login Unix, a meno che non si utilizzi una AAI, non esistono metodi standard per replicare tali informazioni sui vari server.

I server di gestione delle code di stampa oltre a richiedere l'Autenticazione (basata in generale su coppia username/password) possono limitare l'accesso alle stampanti in funzione di informazioni (come l'appartenenza ad un gruppo) che tipicamente sono memorizzare in un database locale. Inoltre possono contenere informazioni su configurazioni e formati di stampa, disponibili in appositi archivi.

L'accesso a pagine web protette è normalmente garantito attraverso la definizione di utenze all'interno di database locali, come i file .htaccess, o database SQL. Data la complessità sempre crescente e l'aumentare di pagine e sezioni di un singolo sito, o addirittura la creazione di diversi siti per gruppi o conferenze, si assiste ad una proliferazione di file .htaccess e di permessi in database.

Offrire accesso autenticato alle reti è diventato di fondamentale importanza per chi si occupa della gestione di una LAN. Il progetto TRIP aiuta in questo compito, ma alcune autorizzazioni, come per gli ospiti, sono legate a database ad hoc che devono essere sempre tenuti aggiornati.

Ulteriore archivio di utenze è, ove presente, l'Active Directory per la gestione degli utenti e dei computer con Microsoft Windows.

Come risulta evidente da quanto descritto finora, i sistemi di AA usati da questi servizi contengono molto spesso le stesse informazioni relative agli stessi utenti, ma duplicate in più

posizioni, in formati diversi e difficilmente sincronizzabili fra loro. La semplice modifica dei dati relativi ad una singola persona richiede l'aggiornamento di molti file su più macchine, con un alto rischio di errori.

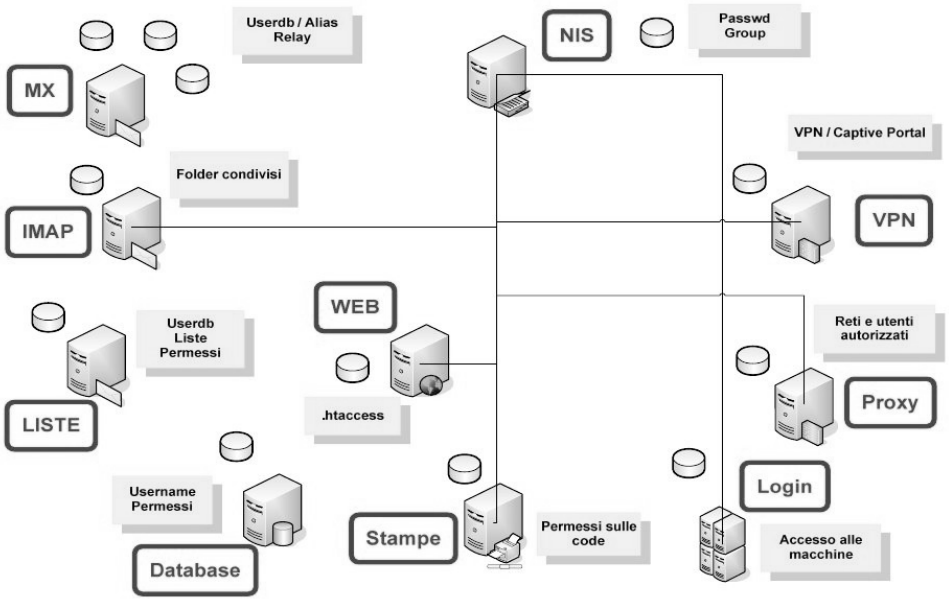

Figura 1: i servizi e gli archivi solitamente presenti in una sede

1.2 Situazione attuale nell'INFN

1.2.1 Stato delle AA nelle singole sedi

Allo scopo di acquisire informazioni sullo stato dei sistemi di Autenticazione ed Autorizzazione in uso nelle singole sedi è stato sottoposto, a tutti i Servizi Calcolo e Reti, un questionario che permettesse di capire, almeno a grandi linee, quali soluzioni sono in uso in questo momento nell'INFN.

All'indagine hanno risposto 31 sedi (sezioni, gruppi collegati e laboratori nazionali) alle

quali è stato chiesto di descrivere quali servizi fossero offerti in modo centralizzato e quali le soluzioni adottate per il controllo degli accessi.

Il *survey*, oltre a raccogliere dati sugli esistenti sistemi di Autenticazione ed Autorizzazione utilizzati per i principali servizi offerti (login, posta, applicazioni web, stampa, ecc.), ha posto l'attenzione sull'eventuale esistenza di un server LDAP o Windows AD, raccogliendo in questi casi dettagliate informazioni sulle caratteristiche fondamentali del Directory Server in produzione, quali BaseDN, schemi utilizzati, ed eventuali personalizzazioni.

L'analisi dei dati raccolti, oltre a fornire una fotografia della situazione attuale, offre informazioni utili a capire come effettuare il passaggio dalle singole AA di sede ad una infrastruttura di livello nazionale e come pianificare le operazioni evitando di distruggere l'infrastruttura esistente.

1.2.1.1 Servizi di base

La ricognizione effettuata mostra chiaramente come solo pochissime sedi abbiano in produzione una singola infrastruttura di AA a cui sono collegati tutti i servizi. Risulta evidente che nella maggior parte dei casi le informazioni sono distribuite su diversi sistemi che devono essere mantenuti aggiornati e sincronizzati tra loro.

Data la complessità dei dati raccolti, è stato necessario ridurre l'analisi a sei diverse categorie nelle quali sono compresi sistemi simili. L'analisi mostrata di seguito, quindi, considera i seguenti gruppi di servizi:

- servizi di posta elettronica (IMAP/POP/SMTP);
- applicazioni web (includendo in queste anche il controllo degli accessi a pagine protette);
- sistemi linux/unix
- sistemi windows
- servizi di stampa centralizzati (si sono considerati due servizi diversi se offerti per il mondo unix o per il mondo windows).

Nella prima colonna della seguente tabella (Tabella 1) osserviamo, per singola sede, il rapporto tra il numero dei sistemi di AA esistenti e il numero di servizi offerti che ne fanno uso. Nella seconda colonna è riportato il numero di sedi che si trovano in tale situazione.

n. sistemi di AA/ n. servizi offerti	n. Sedi
5/6	1
4/6	4
4/5	3
4/3	1
3/6	3
3/5	2
3/4	5
3/3	2
2/6	1
2/5	3
2/3	1
2/2	2
1/6	1
1/1	1

Tabella 1: Rapporto tra sistemi di AA e servizi e relativo numero di sedi.

È evidente che una tale situazione richiede uno sforzo continuo per mantenere la consistenza delle informazioni nelle diverse AA in produzione. Per questo alcune sedi hanno già iniziato il processo di ottimizzazione delle varie AA in una unica AAI di sede. È interessante notare come una sola sede riesca a fornire tutti i servizi utilizzando un'unica infrastruttura di AA. Si tratta in questo caso di una sede nella quale è utilizzato un Directory Server LDAP.

Una panoramica dei diversi servizi e dei relativi sistemi che consentono l'accesso controllato degli utenti viene fornita di seguito. Le informazioni sono in questo caso descritte per singolo servizio.

Posta elettronica

Su 31 sedi intervistate, 30 offrono un servizio di posta elettronica centralizzato, mentre una si appoggia al servizio offerto dall'università nella quale è ospitata.

Per l'Autorizzazione nelle diverse sedi INFN sono utilizzati principalmente sistemi LDAP, NIS o file locali. Windows AD, utilizzato per questo scopo in una sola sezione, è poi associato ad una Autenticazione Kerberos5[4)]. Nell'istogramma che segue è mostrato l'utilizzo dei diversi sistemi nelle sedi. La somma delle occorrenze è superiore al numero delle sedi perché una sede utilizza per l'Autorizzazione sia NIS che AD, mentre altre due hanno al momento sia utenti locali che LDAP, perché in fase di migrazione da un sistema di Autorizzazione all'altro.

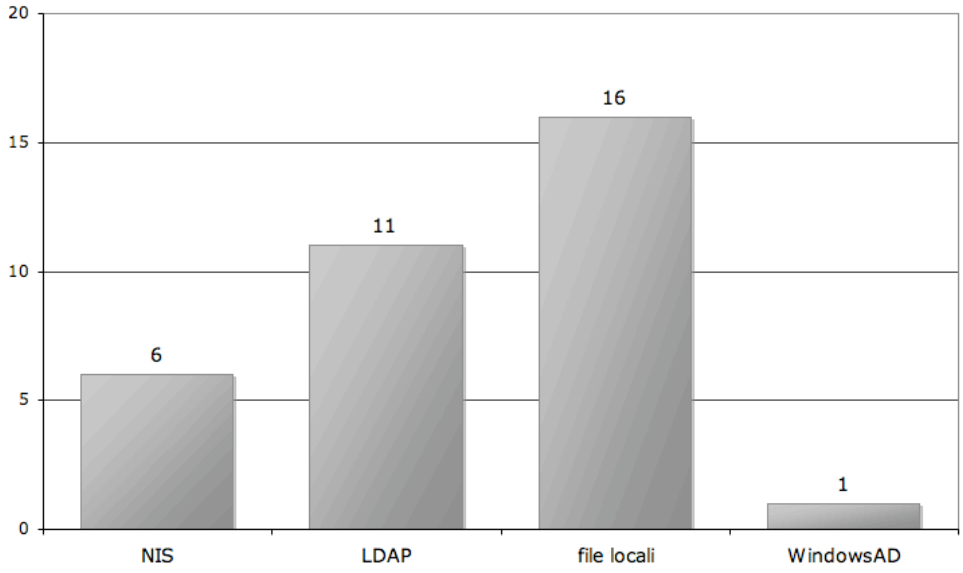

Figura 2: Infrastrutture di Autorizzazione per il servizio di posta (IMAP/POP/SMTP) nelle sedi INFN intervistate che offrono questo servizio (30 sedi)

Per l'Autenticazione, nelle diverse sedi INFN, sono utilizzati maggiormente file locali. Una notevole percentuale di sedi, inoltre, utilizza Kerberos5 o l'Autenticazione propria di LDAP. Pochi, infine, utilizzano i file di password distribuiti via NIS o ancora l'Autenticazione di Windows AD.

Nell'istogramma che segue è mostrato l'utilizzo dei diversi sistemi nelle sedi. La somma delle occorrenze è superiore al numero delle sedi perché, di nuovo, due sedi in fase di migrazione hanno sia utenti locali che LDAP, mentre una sede utilizza per alcuni dei suoi

utenti una Autenticazione Kerberos e per altri una Autenticazione LDAP.

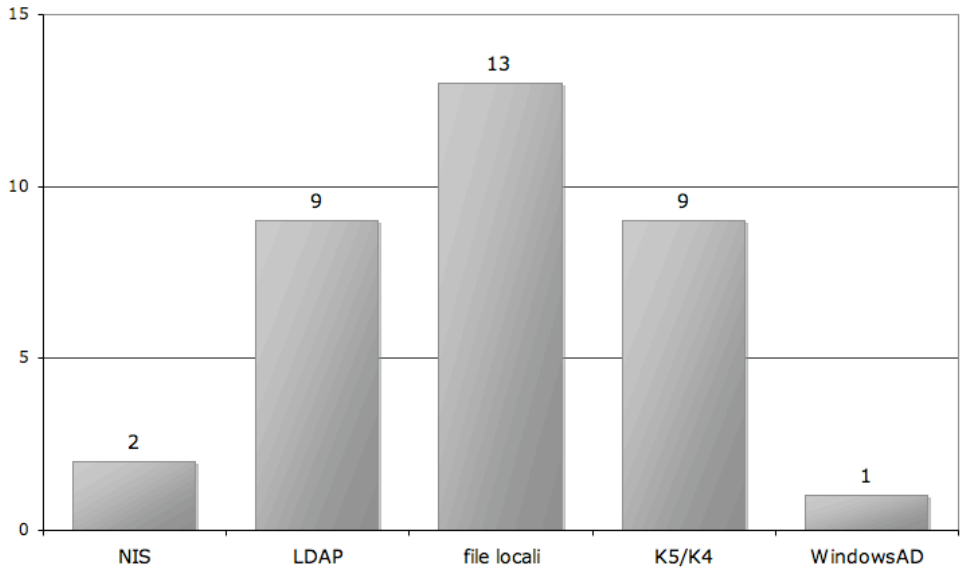

Figura 3: Infrastrutture di Autenticazione per il servizio di posta (IMAP/POP/SMTP) nelle sedi INFN intervistate che offrono questo servizio (30 sedi)

Sulle 30 sedi INFN che offrono il servizio di posta elettronica, infine, 13 consentono l'accesso anche tramite certificati X.509[5)], soluzione spesso implementata per consentire l'uso dei server di posta di sede anche quando si è connessi ad un nodo che non appartiene alla LAN (caso tipico è l'utente fuori sede che vuole inviare mail dal suo laptop).

Applicazioni Web

Nel valutare i sistemi di controllo degli accessi alle applicazioni web offerte dalle sedi INFN si è considerato anche il controllo delle credenziali per l'accesso a pagine web protette, siano esse relative a esperimenti, gruppi di lavoro o singoli utenti.

Su un totale di 28 sedi intervistate in merito, 26 offrono un servizio di accesso al web che necessita di credenziali. In questo caso per ciascuna sede sono implementati

contemporaneamente più metodi di AA che vanno dalla verifica di username e password del singolo utente, al controllo della network di appartenenza del nodo richiedente, fino all'accesso tramite certificato X.509, quest'ultimo utilizzato in 5 sedi. Alcune sedi inoltre utilizzano per il controllo delle applicazioni web sistemi proprietari o DB locali (sql, postgresql, ...). Infine ancora molto in uso è il metodo di Autorizzazione base, ossia tramite scrittura del file .htaccess nel ramo dell'albero offerto dal sito web, con una Autorizzazione del tipo "Basic Autentication". L'utilizzo di quest'ultimo sistema genera un proliferare di file all'interno dell'albero che difficilmente è possibile mantenere aggiornati nel tempo.

Gli istogrammi di seguito riportati descrivono l'uso dei metodi utilizzati per Autorizzazione e Autenticazione nelle varie sedi INFN. È evidente che nella maggior parte delle sedi più metodi sono in uso contemporaneamente.

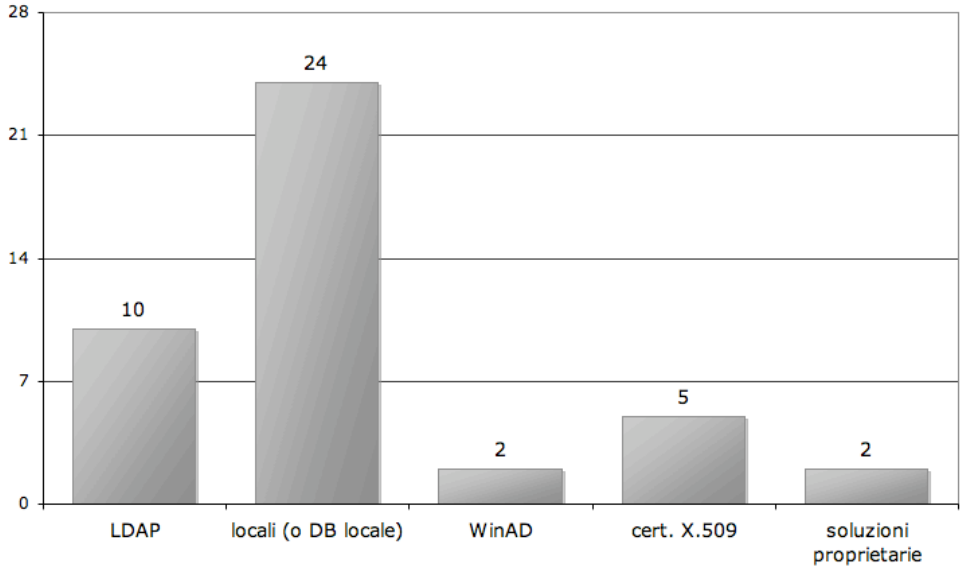

Figura 4: Infrastrutture di Autorizzazione per l'accesso ad applicazioni web e pagine web private, nelle sedi INFN intervistate che offrono questo servizio (26 sedi).

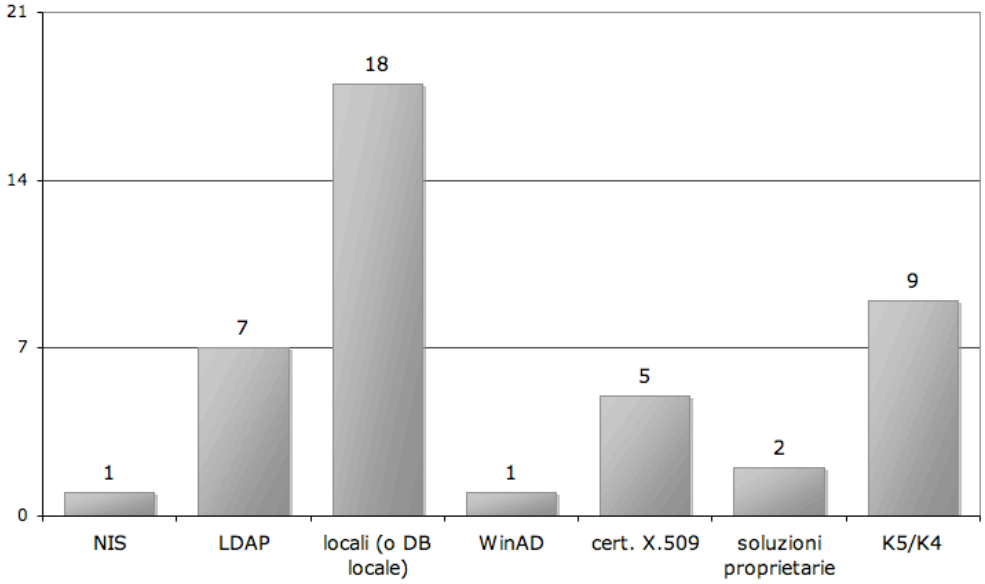

Figura 5: Infrastrutture di Autenticazione per l'accesso ad applicazioni Web e pagine web private, nelle sedi INFN intervistate che offrono questo servizio (26 sedi).

Sistemi linux/unix

Su un totale di 26 sedi intervistate sull'argomento, 25 offrono il servizio di accesso centralizzato a sistemi linux/unix. Nelle parti che seguono sono descritte le differenti soluzioni adottate per l'Autorizzazione e per l'Autenticazione degli utenti su detti sistemi.

Poco più della metà delle sedi utilizza per l'Autorizzazione un servizio LDAP, ma molte ancora hanno in produzione una infrastruttura NIS o si appoggiano a file di password locali. Il grafico a torta di seguito riportato mostra le percentuali di utilizzo dei sistemi di Autorizzazione implementati nelle diverse sedi INFN.

L'Autenticazione per l'accesso ai sistemi centralizzati di tipo linux/unix è, nella maggior parte dei casi, equamente demandata a server LDAP o Kerberos5. Meno del 30% delle sedi utilizza altri sistemi, quali NIS o file di password locali.

Nell'istogramma che segue è mostrato l'utilizzo dei diversi sistemi nelle sedi. La somma delle occorrenze è superiore al numero delle sedi: una sede, infatti, utilizza per alcuni dei suoi utenti una Autenticazione Kerberos e per altri una Autenticazione LDAP.

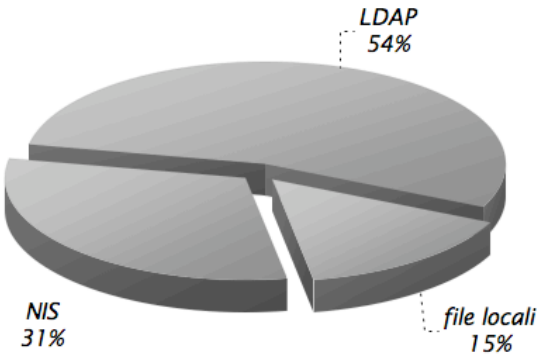

Figura 6: Infrastrutture di Autorizzazione per l'accesso ai sistemi linux/unix nelle sedi INFN che offrono un servizio di login centrale (25 sedi).

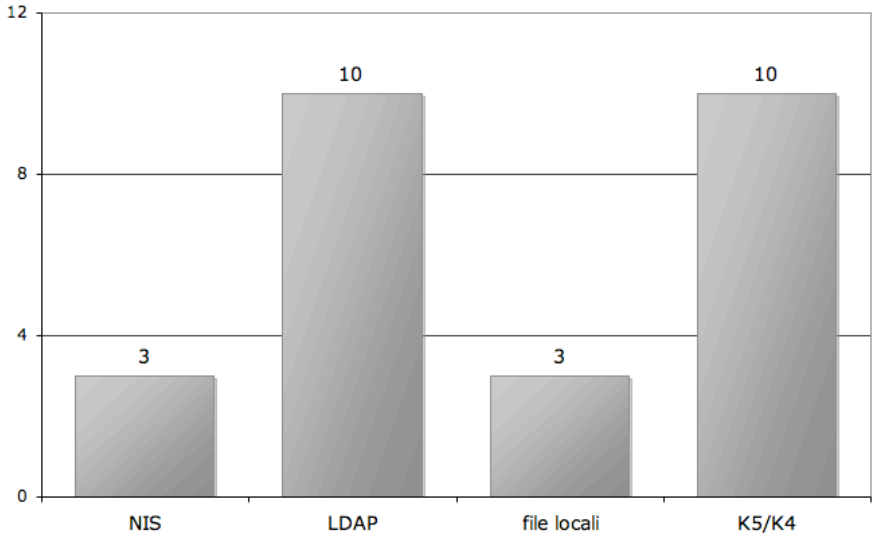

Figura 7: Infrastrutture di Autenticazione per l'accesso ai sistemi linux/unix nelle sedi INFN che offrono un servizio di login centrale (25 sedi)

Sistemi Windows

Per i sistemi Windows, seppure molto diffusi all'interno delle sedi INFN, non sempre è implementato un dominio Windows AD per il controllo degli accessi. Su 30 sedi intervistate sull'argomento, solo 11 hanno in produzione un dominio Windows AD equamente distribuiti tra domini nativi e compatibili NT, il cui utilizzo rimane principalmente circoscritto all'ambiente Windows di sezione. Come visto in precedenza sono rari i casi nei quali l'Active Directory Windows è utilizzato come infrastruttura di Autorizzazione o Autenticazione per i servizi centrali. Dove implementato, il servizio Windows AD è utilizzato per offrire condivisione di folder, installazione di software o accesso alle stampanti di rete o ancora per il controllo della login sui singoli nodi windows. In una delle sezioni in esame il servizio di Windows AD non è più utilizzato e se ne sta valutando la dismissione.

Nel grafico che segue è descritto l'utilizzo di Windows Active Directory nelle sedi dove questo è in produzione.

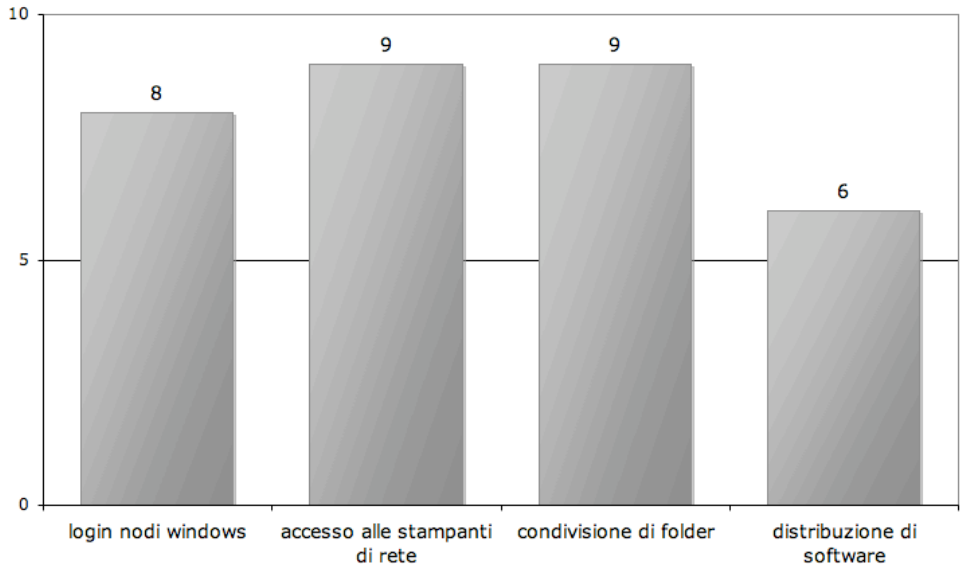

Figura 8: Utilizzo del dominio Windows AD nelle sedi ove questo è in produzione (11 sedi)

Servizio di stampa centralizzato

Su 28 sedi intervistate in merito, 23 offrono un servizio di stampa centralizzato. L'accesso delle stampanti di rete è controllato principalmente dalla verifica dell'appartenenza alla LAN di sede del nodo richiedente. In diverse sezioni questo metodo è utilizzato anche per consentire la stampa da nodi linux quando la gestione delle code di stampa è affidata a sistemi windows e viceversa. In alcuni casi la verifica dell'appartenenza alla LAN è associata ad altri metodi per il controllo dell'accesso, quali ad esempio username e password.

Il grafico di seguito riportato mostra la scelta dei metodi di controllo degli accessi ai sistemi di stampa centralizzati nelle varie sedi INFN.

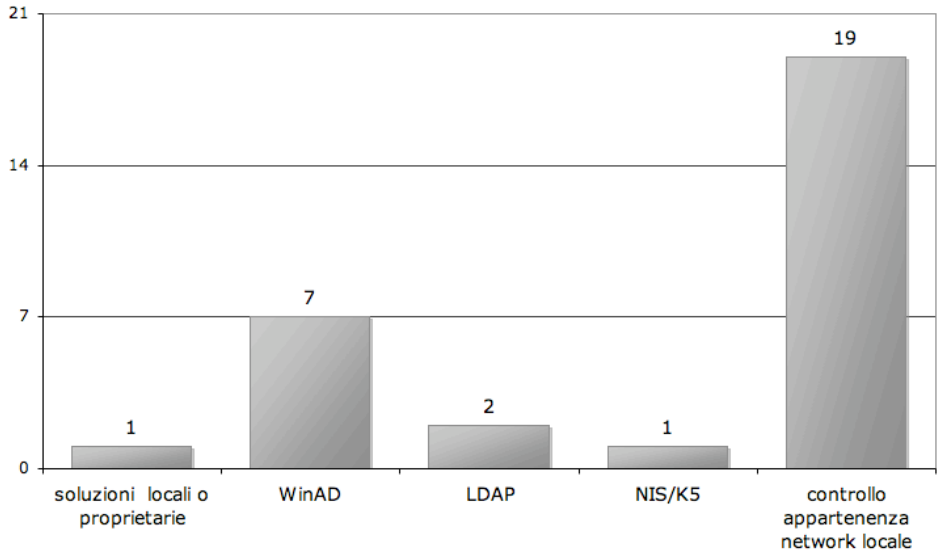

Figura 9: Sistemi di controllo degli accessi per il servizio di stampa centralizzato nelle sedi INFN che offrono questo servizio (23 sedi)

1.2.1.2 Utilizzo di LDAP e Kerberos5 nelle sedi INFN

Uso di Directory Server LDAP

Su 30 sezioni che gestiscono almeno un sistema di AA in sede, 14 hanno scelto un Servizio di Directory interrogabile via protocollo LDAP per implementare infrastrutture di Autorizzazione e Autenticazione per i vari servizi offerti.

Tutte le sedi intervistate utilizzano il software opensource OpenLDAP[6)], nelle diverse versioni fornite con le distribuzioni Linux RedHat (e quindi anche Scientific Linux), Debian e Suse.

La configurazione del software varia sensibilmente di sede in sede. Alcune sedi hanno definito classi di oggetti ad hoc, altre hanno assegnato ad attributi di classi di oggetti dei valori che non corrispondono allo standard previsto per quei dati attributi. In più, in alcuni casi, alcuni attributi standard sono utilizzati in modo non standard.

Anche il disegno dell'albero della Directory varia sensibilmente: alcune sedi hanno organizzato l'albero per servizi, altri distinguendo rami pubblici e privati, altri ancora dedicando diversi rami dell'albero al personale dipendente, associato o studente.

Il software OpenLDAP non offre supporto per gruppi dinamici o nidificati perciò, ove necessario, sono stati definiti gruppi statici.

In quasi tutte le sedi, al Directory Server sono agganciati il servizio di posta elettronica, le login unix e le applicazion web. In 4 sedi si utilizza LDAP per controllare l'accesso alla rete via Captive Portal o definendolo come backend del server RADIUS[7)] per TRIP.

Infine, singole sedi utilizzano il Directory Server per l'acceso alla rubrica interna, per il controllo dei permessi del sistema di code batch, come backend per samba per le login windows e come repository dei dati utilizzati dai servizi di rete come DNS e DHCP.

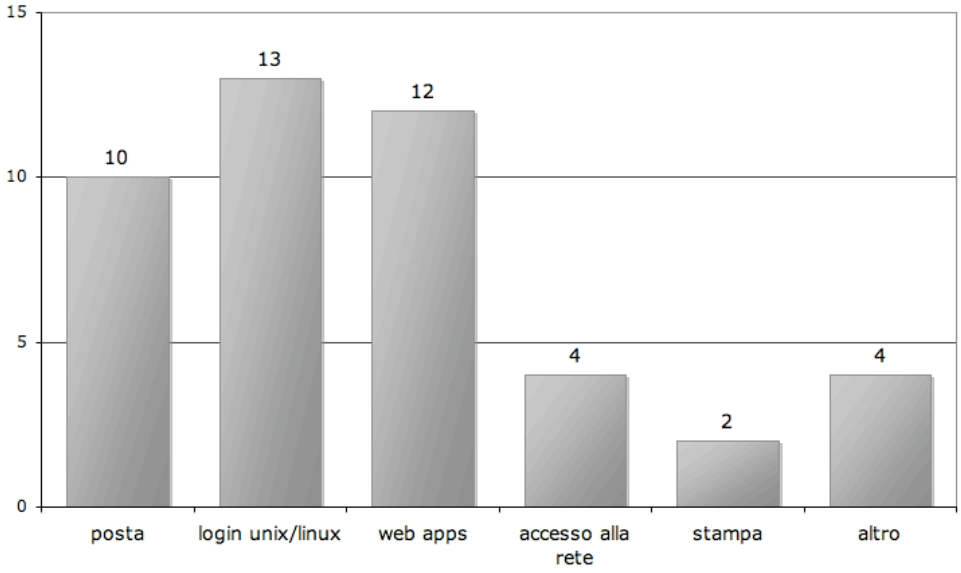

Figura 10: Utilizzo di un Directory Server LDAP nelle sedi INFN (14 sedi)

Il servizio di LDAP è utilizzato anche per l'Autenticazione in 10 sedi, mentre altre 4 delegano questo compito a server Kerberos5.

Uso di Autenticazione Kerberos

Da molti anni è in uso nell'INFN il file system distribuito AFS[8)] che, nelle ultime versioni del software, prevede una Autenticazione Kerberos5. Le sedi che già utilizzavano AFS, pertanto, sono naturalmente passate, nel tempo, ad una Autenticazione di questo tipo.

Su 30 sezioni che gestiscono almeno un sistema di Autenticazione in sede, 10 utilizzano il protocollo Kerberos5, e una è in procinto di migrare a questo dalla precedente versione (Kerberos4). Di queste 11 sedi, alcune afferiscono al REALM Kerberos nazionale INFN.IT, mentre altre hanno installato e configurato server Kerberos5 e REALM locali. In una sede il REALM locale Kerberos5 è in relazione di trust con il dominio nativo Windows AD.

Nelle varie sedi, i servizi che utilizzano una Autenticazione Kerberos5 sono costituiti fondamentalmente dalla posta elettronica, la login unix/linux e il controllo degli accessi per le applicazioni web. In un caso, il server Kerberos è utilizzato anche per il controllo dell'accesso

alle stampanti di rete.

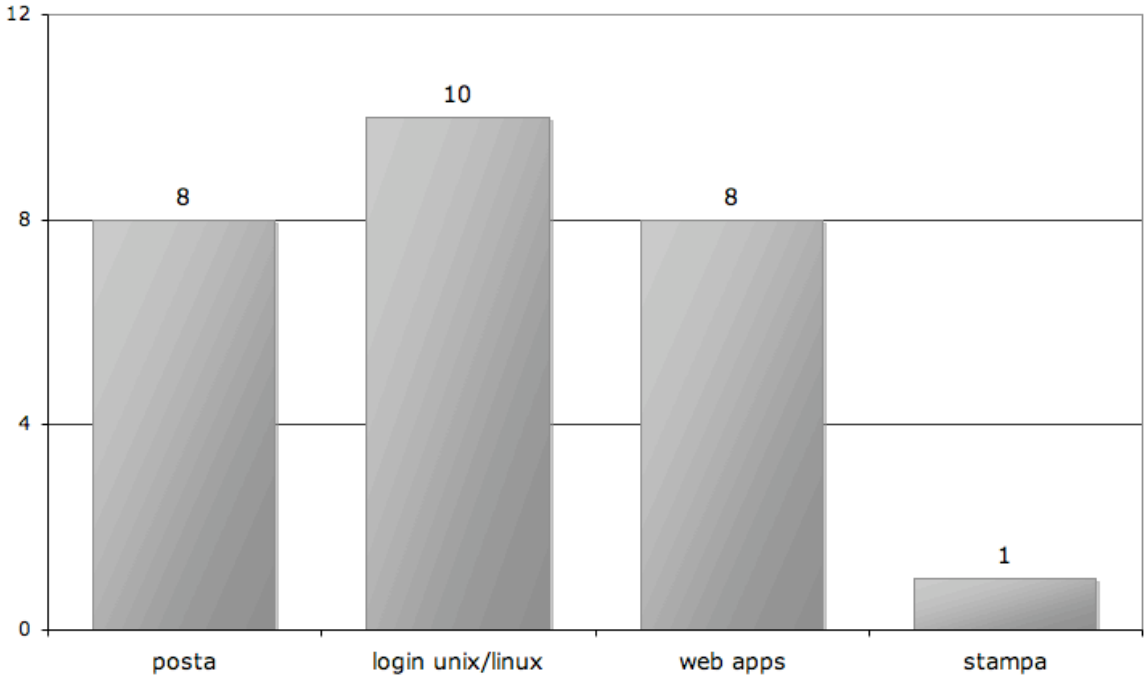

Figura 11: Utilizzo di Autenticazione Kerberos nelle sedi INFN (11 sedi)

1.2.2 AA nel calcolo scientifico

Con l'avvento di LHC e Grid il calcolo scientifico è sempre più spesso svolto su sistemi di calcolo dedicati. Nell'INFN sono in produzione diversi centri per il calcolo scientifico, distribuiti sul territorio, organizzati per "livelli" (i Tier).

I Tier2 dell'INFN sono strutture associate agli esperimenti, destinate a svolgere compiti di analisi dati, collaborando strettamente con il centro regionale italiano Tier1, situato al CNAF. Alcuni si appoggiano alle strutture del Servizio Calcolo e Reti della Sezione che li ospita, altri ne sono completamente disgiunti.

Nei Tier le infrastrutture di Autenticazione sono diverse a seconda dell'utilizzo delle risorse. Per l'accesso tramite Grid si utilizzano sistemi di Autenticazione basati su globus, altresì chiamate GSI (Grid Security Infrastructure). Il protocollo GSI mette a disposizione un servizio di Autenticazione basato su certificati X.509 e infrastruttura a chiave pubblica, con l'aggiunta di estensioni VOMS (Virtual Organization Membership Service) per associare i membri di una Virtual Organization in gruppi o per affidar loro ruoli e privilegi speciali.

L'utilizzo locale delle risorse invece prevede protocolli di tipo diverso per l'Autenticazione degli utenti locali, quali NIS, LDAP o Kerberos, riproducendo così situazioni simili a quanto descritto per le AA dei servizi di base delle sedi INFN.

Nei centri, infine, sono spesso presenti sistemi di AA per i differenti batch-systems, i server Wiki per la distribuzione delle informazioni e le mailing-list.

1.2.3 AA nelle applicazioni centralizzate a livello nazionale

Nel corso degli ultimi anni, sono state messe a disposizione degli utenti INFN un certo numero di applicazioni centralizzate. Alcune di carattere puramente "amministrativo", altre di supporto alle attività scientifiche e non.

Di seguito descriveremo le principali applicazioni, con particolare attenzione ai sistemi di Autenticazione ed Autorizzazione usati in ognuna di esse.

Applicazioni centralizzate fornite da DataWeb

Le applicazioni web centralizzate sono state realizzate per informatizzare i processi amministrativi e per coadiuvare l'attività di ricerca dell'INFN, per definizione dislocata sull'intero territorio nazionale. Fra questi processi si possono enumerare: richieste di fondi per affari internazionali, richiesta e registrazione di contratti di associazione, gestione dei corsi di formazione e dei relativi partecipanti, aggregazione e presentazione delle richieste finanziarie per la ricerca, aggregazione dei dati di consuntivo scientifico.

Gli utenti a cui sono rivolte le applicazioni

- sono un numero alto: il Portale INFN ne ha registrati più di tremila e ce ne sono una media di due in più ogni giorno;
- sono dislocati territorialmente e possono spostarsi o prestare servizio continuo in una struttura diversa da quella di afferenza;
- hanno ruoli amministrativi (funzioni d'ufficio) oppure partecipano all'attività di ricerca;

- sono organizzati secondo un organigramma ben definito;
- hanno competenze e ruoli diversi.

Schema di Autenticazione e Autorizzazione

Il problema del riconoscimento dell'utente e dell'attribuzione dei relativi permessi è stato risolto in diversi modi nel corso del tempo.

La prima soluzione è stata l'implementazione di un sistema "ciò che si conosce" tramite la creazione di credenziali per ogni applicazione ed ogni figura (impropriamente "ruolo") a cui l'applicazione era dedicata. Ad ogni credenziale corrisponde un insieme di permessi (di solito calcolati analizzando il formato del nome utente). In questo caso l'utente ha credenziali diverse:

- (sempre) per applicazioni diverse pur rivestendo lo stesso "ruolo"
- (spesso) per la stessa applicazione se riveste più "ruoli" contemporaneamente

Le problematiche che nascono sono:

- l'assegnazione degli accessi viene garantita dalla distribuzione di un insieme delle credenziali di accesso
- solitamente ne consegue che gli utenti si scambiano (e tramandano) le credenziali
- diventa impossibile aggiornare le password e distribuirle nuovamente a tutti gli utenti

Questo schema molto rudimentale è stato sostituito successivamente dall'implementazione del sistema "ciò che si è". Ogni utente ha un identificativo personale ed il sistema conosce, tramite il supporto di una apposita base di dati, la mappa dei "ruoli" ricoperti da ciascun utente: i "ruoli" possono rispecchiare quelli propri dell'organigramma aziendale oppure quelli definiti dal formalismo dell'applicazione web.

In questo ambiente, la funzione di attribuzione dei permessi dell'applicazione viene sviluppata prendendo a riferimento la base di dati dei ruoli: nel momento in cui l'utente si collega e si autentica vengono estrapolati i ruoli registrati per il suo identificativo, questi ruoli vengono utilizzati per filtrare gli accessi oppure, per ciascun ruolo, vengono assegnati un insieme di privilegi che, uniti, garantiscono l'accesso alle singole caratteristiche.

Recentemente è stato messo a disposizione CASSiO[9)]: una applicazione di Single Sign-

On che si occupa interamente dell'Autenticazione dell'utente. In Figura 12 è schematizzato il suo utilizzo da parte delle applicazioni centralizzate fornite da DataWeb.

La libreria di AA di cui fanno uso le applicazioni e che è schematizzata in Figura 13, è costituita da tre moduli traslucidi a cascata:

layer di Autenticazione: il primo modulo si occupa della richiesta dei parametri di Autenticazione e di bloccare l'esecuzione nel caso che non si riesca a identificare l'utente;

layer di Autorizzazione: a partire dall'identificativo utente, tramite ricerca in una base di dati di qualunque tipologia e struttura, viene prodotta la lista dei ruoli (reali o fittizi);

matrice dei permessi: questo modulo, in base ad una matrice di associazione, traduce la lista dei ruoli in una lista di permessi sulle singole sezioni dell'applicativo. Per ragioni di efficienza, manutenibilità o situazioni particolari non riconducibili a casi standard, viene inserito, sempre a cascata, un modulo aggiuntivo, spesso costituito da una rete multi-ingresso e multi-uscita, che esegue il mapping fra la struttura dati dei permessi e le flags utilizzate dalla funzione o dalla vista.

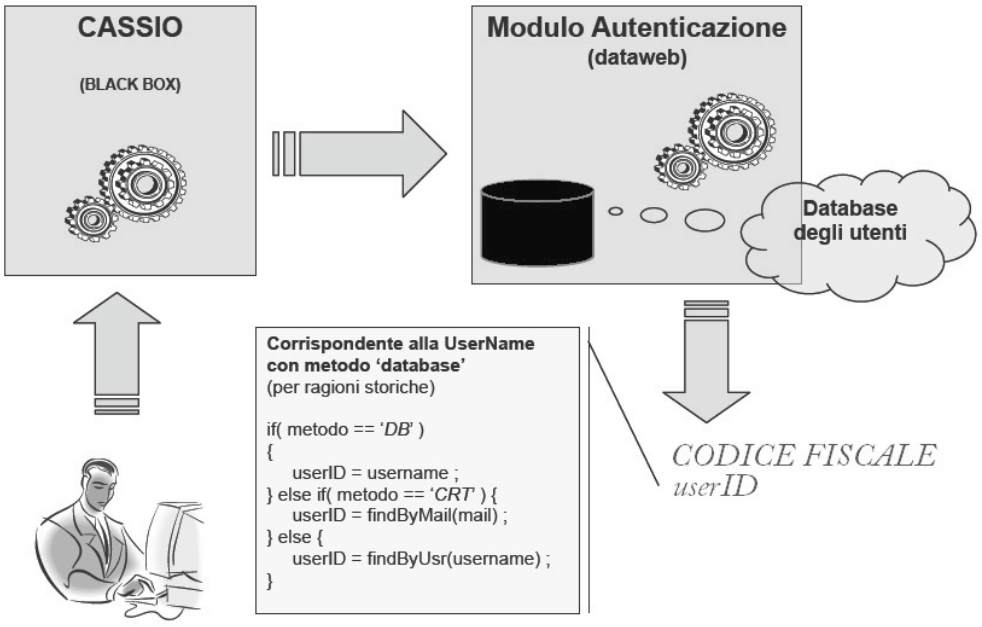

Figura 12: Schema di interfaccia tra CASSiO e le applicazioni centralizzate

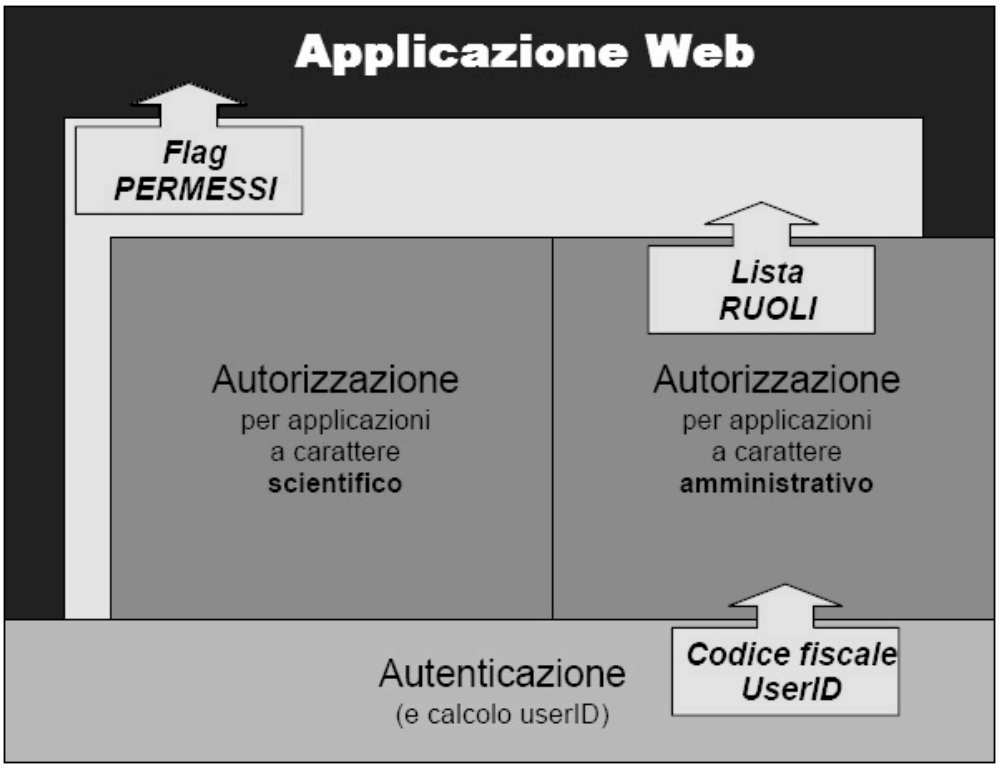

Figura 13: Schema delle librerie di Autenticazione ed Autorizzazione

Database di supporto (db-utenti)

Al momento i dati relativi all'identificazione dell'utente (distinzione della persona date le credenziali in un particolare sistema di accesso fra quelli disponibili in CASSiO) e alla memorizzazione dei relativi ruoli si trovano un database MySql condiviso fra le applicazioni. Questo database estende quello del Personale INFN (dipendenti, associati e ospiti). Nel db sono contenute una esiguo numero di tabelle relazionate che contengono:

- dati anagrafici degli utenti
- dati relativi all'Autenticazione di ciascun utente
- dati delle risorse disponibili (genericamente applicazioni web ed esperimenti di ricerca)
- tavole di relazione che registrano il ruolo per un utente data una risorsa

I ruoli descritti nelle tavole di cui sopra sono quelli che derivano dall'Organigramma Organizzativo dell'Istituto che prevede le seguenti entità:

- Sezioni
  - Consiglio
  - Uffici
  - Servizi
    - Reparti
- Laboratori
  - Comitati Scientifici
  - Consiglio
  - Uffici
  - Divisioni
    - Servizi
      - Reparti
  - Servizi
    - Reparti
- Gruppo Collegato
- AC
  - Consiglio
  - Direzioni
    - Uffici
  - Servizi
- Centro Nazionale (CNAF)
  - Consiglio
  - Servizi
- INFN
  - Giunta
  - Direttivo
  - Uffici Dirigenziali Generali
  - Commissioni
  - Comitati

Mailing list (SYMPA)

Da ottobre 2007 è in produzione un nuovo servizio di mailing-list basato su SYMPA che ha sostituito il precedente servizio basato su Majordomo.

Il software del nuovo list-server supporta tre tipi Autenticazione (database locale, certificati X.509 ed LDAP) ma in questo momento sono state abilitate solo le prime due modalità.

Il software è in grado di interfacciarsi con un server LDAP per l'Autenticazione (sostituendo il database interno degli account) e per l'Autorizzazione, estrapolando automaticamente la lista degli owner e dei moderator. Permette inoltre la definizione di mailing-list dinamiche, i cui membri sono definibili attraverso una query LDAP opportuna.

Accesso alla rete locale (TRIP)

Il progetto TRIP è nato con lo scopo di fornire un accesso semplice e sicuro alle reti wireless delle sedi INFN.

Esso prevede due modalità di accesso alla rete, ognuna destinata ad una tipologia di utenti: staff (dipendenti o associati INFN) e ospiti.

L'accesso alla rete wireless per un utente "staff" è basata su protocollo 802.1x che delega ad un RADIUS server le operazioni di Autenticazione ed Autorizzazione. L'architettura attuale prevede una gerarchia di RADIUS server che permette all'utente di usare le credenziali della propria sede di appartenenza. In questo modo è possibile accedere alla rete in una qualunque sede dell'INFN in cui sia stato implementato TRIP.

Il modello di Autenticazione radius proxy, insieme alla scelta del software freeRADIUS, fanno sì che ogni sede INFN sia libera di decidere di utilizzare il database più opportuno per la gestione delle credenziali per i propri utenti. Sono in produzione diversi scenari tra i quali:

- Database radius gestito localmente con file di password unix o file di testo users
- Autenticazione tramite PAM
- Autenticazione LDAP
- Autenticazione Kerberos e Autorizzazione LDAP

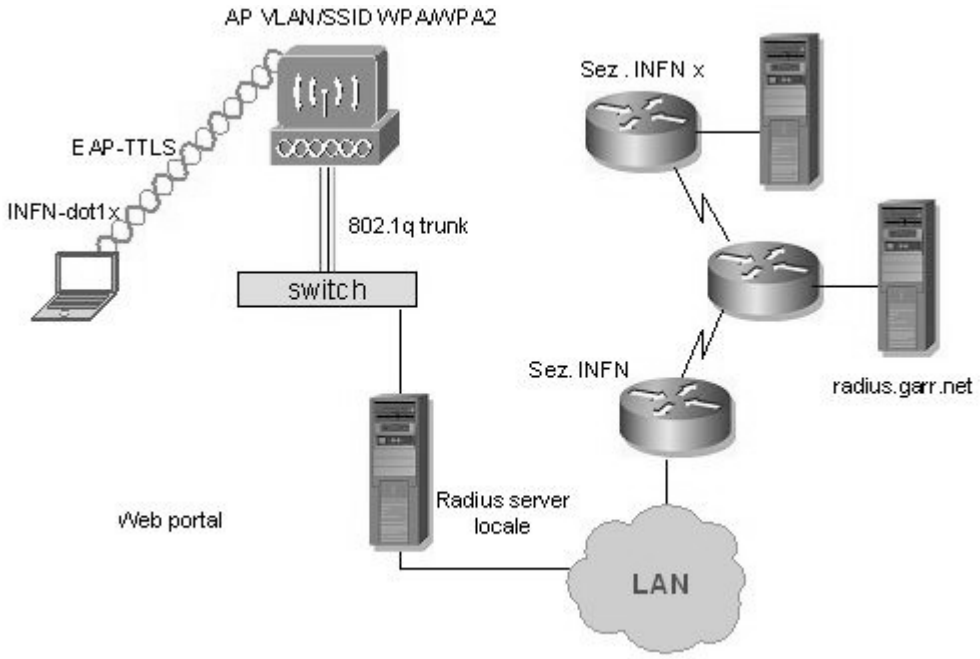

Figura 14: Schema di Autenticazione in TRIP per utenti “staff”

Per gli ospiti occasionali, invece è disponibile l'accesso attraverso un "captive portal" che effettua l'Autenticazione usando il database locale del server RADIUS o un certificato X.509 rilasciato dalla INFN-CA.

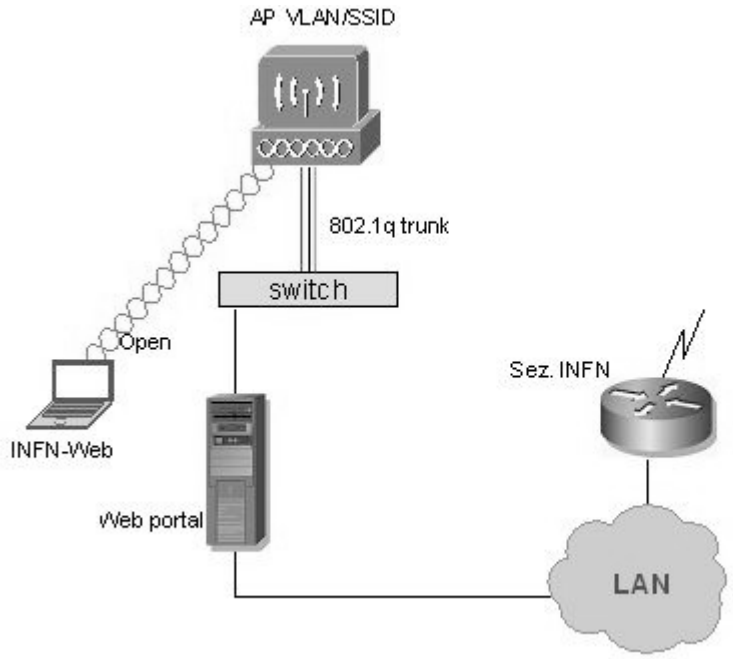

Figura 15: Schema di Autenticazione di TRIP per gli ospiti

1.3 Ottimizzazione/Armonizzazione

Dalle precedenti descrizioni risulta evidente che il paradigma "un servizio su ogni server", spesso implementato con grande attenzione alla fruibilità del servizio stesso invece che alla armonizzazione dei Sistemi di AA in una Infrastruttura comune utilizzabile dai vari servizi (anche semplicemente per necessità di compatibilità con i sistemi in uso nella sede), se da un lato ha fino ad ora disaccoppiato l'affidabilità dei servizi forniti da dipendenze con servizi esterni, dall'altro ha naturalmente dato origine a un insieme disomogeneo e vario di Sistemi di AA, nelle sedi dell'INFN.

Questo scenario rischia di ripetersi anche per i servizi centralizzati che, essendo numericamente in crescita, e non avendo a disposizione una unica AAI, sono costretti ad implementare ulteriori Sistemi di AA.

La razionalizzazione dei Sistemi di AA locali in corso in molte sedi, si può ben coniugare con l'analoga esigenza dei servizi centralizzati, all'interno della definizione di una INFN-AAI.

Una tale razionalizzazione potrebbe essere condotta in due modi: Federazione di AAI

locale o INFN-AAI

1.3.1 Federazione di AAI locali

Uno dei possibili approcci che conservi la totale autonomia delle sedi e nel contempo fornisca uno strumento utile per l'accesso a servizi centralizzati, è quello di costituire una federazione di AAI. Ne esistono varie implementazioni, anche se ormai lo "standard de facto" è la federazione che si basa sul protocollo Shibboleth[10)] e sul relativo software sviluppato all'interno dell'omonimo progetto di Internet2/MACE (Middleware Architecture Committee for Education).

Ovviamente un tale approccio richiederebbe che in ogni sede venga definita ed implementata una AAI, oltre ad almeno un servizio di IDentityProvider (IDP).

Inoltre, allo stato attuale, Shibboleth permette accesso autenticato e Single Sign-On solo per applicazioni Web.

1.3.2 INFN-AAI

L'approccio che invece proponiamo è quello di definire una architettura unica per una AAI a livello INFN, che comprenda nel disegno le AAI di ogni singola sede. Nonostante un tale approccio possa sembrare a prima vista in contraddizione con l'autonomia delle sedi, mostreremo che sarà possibile ottenere le due cose contemporaneamente.

Inoltre, essendo il progetto basato su una infrastruttura di Directory, la INFN-AAI potrà essere facilmente usata per partecipare a federazioni di AAI sia a livello nazionale (vedi progetto IDEM[11)] del GARR) che internazionale. Questo permetterebbe ad un qualunque utente dell'INFN di usufruire dei servizi offerti dalla federazione, senza aggravio per i Servizi di Calcolo e Reti della propria sede, in quanto la complessità aggiuntiva richiesta dalla partecipazione ad una federazione sarà gestita a livello centrale.

2 IL PROGETTO INFN-AAI

In questo capitolo verrà descritto il progetto INFN-AAI.

Il primo paragrafo è dedicato ad una beve descrizione nella quale verranno evidenziati gli obiettivi ed i requisiti che hanno portato alla definizione della proposta INFN-AAI. Successivamente verranno descritti i principali componenti software e l'architettura che è stata scelta. Inoltre saranno descritte le attività preliminari fin qui svolte, ed in particolare i risultati di un test relativo alla scalabilità dell'architettura proposta. Infine verrà descritta una implementazione prototipale della INFN-AAI ad uso esclusivo dei servizi centralizzati forniti da DataWeb.

2.1 INFN-AAI

Data la situazione attuale nelle sedi INFN, disegnare oggi una AAI che possa essere impiegata efficacemente (ossia alla quale facciano riferimento tutti i servizi che hanno bisogno di Autenticazione ed Autorizzazione) sia a livello di singola sede che a livello INFN (cioè di riferimento per tutti i servizi centralizzati) significa dover tenere in grande considerazione il fatto che molte sedi hanno già dei sistemi (ed alcune volte delle Infrastrutture) di Autenticazione ed Autorizzazione in produzione, e che i principali servizi informatici forniti, dipendono in modo cruciale da tali sistemi.

In sintonia con la scelta fatta dalle sedi dell'INFN che hanno implementato una AAI, ed in linea con le soluzioni adottate praticamente in tutti gli ambienti che necessitano di una AAI, il progetto si basa sulla implementazione di un Servizio di Directory opportunamente personalizzato, interrogabile via protocollo LDAP.

L'architettura definita è compatibile sia con Autenticazione Kerberos5 che con Autenticazione basata su hash di password (garantendo il supporto per tutti i meccanismi di hashing utilizzati nelle varie sedi: dal semplice "crypt" Unix ad MD5 e SHA1) memorizzate all'interno dell'albero della Directory, ed è in grado di fornire i dati necessari ai processi di Autorizzazione di qualunque servizio informatico fornito dalle sedi INFN.

2.1.1 Obiettivi

Per quanto sopra esposto, gli obiettivi che il progetto AAI si propone sono:

- La realizzazione di un'unica AAI per l'INFN utilizzabile contemporaneamente

dalle applicazioni di una singola sede e dalle applicazioni centralizzate nazionali, implementando tutte le funzionalità richieste in entrambi gli scenari e senza che questo ponga limiti all'autonomia di uno dei due.

- Disegnare la AAI in modo che possa supportare l'autenticazione verso le applicazioni web, centralizzate e non, attraverso certificato X.509.
- Disegnare la AAI in modo che possa essere integrata in federazioni di AAI.
- L'AAI dovrà offrire il servizio di Single Sign-On (SSO) per tutti, la possibilità cioè da parte di un utente di inserire una sola volta, per sessione di lavoro, le proprie credenziali accedendo a tutti i servizi disponibili, ovvero quelli che si appoggiano alla AAI. Questo dovrà avvenire in modo il più possibile trasparente per le sedi, senza che ci sia un aggravio effettivo di lavoro per gli amministratori locali.

2.2 Requisiti

2.2.1.1 Requisiti funzionali

In un ente strutturato praticamente e storicamente come l'INFN è assolutamente indispensabile garantire all'amministratore locale la completa autonomia nella gestione di Autenticazione ed Autorizzazione degli utenti per l'accesso alle risorse locali; quello che di seguito verrà più semplicemente indicato come *autonomia delle sedi*.

È fondamentale altresì garantire l'accesso autenticato a date informazioni, da parte dei gestori di queste, indipendentemente dalla loro "posizione relativa" all'interno dell'albero LDAP. Ovvero deve essere preservata la possibilità da parte di un utente che appartiene ad una particolare sede, quindi definito in un certo ramo dell'albero LDAP e autorizzato a gestire un certo attributo, di modificare tale attributo di una entry ovunque questa sia posizionata nell'albero stesso. Questo perché i ruoli (gli incarichi) che un dipendente può ricoprire all'interno dell'INFN interessano o possono interessare anche sedi diverse da quella di appartenenza: si pensi ad esempio al presidente di una commissione nazionale che dovrà poter modificare attributi di entry appartenenti a sedi diverse dalla propria.

È certamente tra i requisiti funzionali la possibilità di configurare tutti i servizi locali delle varie sedi in modo da utilizzare la INFN-AAI così da evitare inutili sforzi per mantenere la consistenza delle informazioni ed avere un reale beneficio da una infrastruttura di AA.

Allo stesso tempo è fondamentale fornire i vantaggi di una AAI alle applicazioni centralizzate garantendo un unico database per le informazioni, così da semplificare notevolmente il funzionamento dei meccanismi di AA delle applicazioni stesse. In particolare, con riferimento alla sezione 1.2.3:

- Per Data-Web può essere notevolmente semplificato il processo di AA che attualmente (fig. 12 e 13) fa utilizzo di un sistema complicato di più layer per la costruzione dei ruoli e della matrice di permessi in quanto il FDS, attraverso i "Roles", come spiegheremo più avanti, mette a disposizione dell'applicazione la possibilità di individuare i ruoli o di costruirli dinamicamente attraverso semplici query LADP.
- Per Sympa, abilitando il supporto per l'autenticazione LDAP, si potrà ottenere, come già riportato, la possibilità di estrapolare automaticamente le informazioni riguardanti i moderatori e gli amministratori nonché la possibilità di creare mailing-list in modo dinamico.
- Per quanto riguarda TRIP, si potrà evitare di usare la catena di proxy RADIUS, facendo puntare il server RADIUS ai server LDAP locali per l'autenticazioni degli utenti locali, e usare invece i server LDAP di core, per l'autenticazione degli utenti esterni. Disaccoppiando quindi l'autenticazione di un utente in viaggio, dalla effettiva raggiungibilià della sede di appartenenza.

2.2.1.2 Requisiti di integrazione

Come già affermato in precedenza, nelle sedi sono in produzione diversi servizi di AA, utilizzati dai principali servizi informatici forniti all'utenza. È necessario, pertanto, costruire una AAI nazionale che integri al suo interno almeno gli elementi delle AA di sede.

Dato che l'INFN-AAI fornirà supporto per SSO attraverso Autenticazione Kerberos5, le esigenze delle sedi che basano il loro sistema di Autenticazione su tale protocollo, sono automaticamente soddisfatte.

Per le sedi in cui sia Autenticazione che Autorizzazione sono basate su sistemi di tipo NIS (o YellowPages) o equivalenti, sarà necessario garantire, almeno nella fase iniziale, la possibilità di utilizzare l'autenticazione semplice di LDAP, attraverso l'inserimento nella Directory delle informazioni di Autenticazione ed Autorizzazione presenti nelle infrastrutture di sede.

La migrazione a Kerberos5 avverrà in modo automatico attraverso una procedura, descritta nei prossimi paragrafi, che sarà completamente trasparente per gli utenti.

2.2.1.3 Requisiti non funzionali

Un'infrastruttura di tale rilevanza per il funzionamento dei servizi offerti deve garantire massima **affidabilità**.

Per questo si prevede l'installazione di quattro server centrali, contenenti tutti i dati, in configurazione Multi-Master e collocati nelle sedi che offrono applicazioni centralizzate. L'affidabilità del sistema lato sede potrà essere garantita dalla presenza di almeno un server ReadOnly per ogni sede.

Uno dei problemi connessi alla distribuzione dei dati su area geografica è quello legato alla loro **disponibilità**. Infatti applicazioni centralizzate che richiedono dati distribuiti (si pensi ad un semplice phone-book di tutto l'INFN che fa riferimento ai dati presenti in ogni sede) rischiano di non poter funzionare se solo una delle sedi coinvolte non è raggiungibile per qualche motivo. L'architettura scelta, con i server contenenti tutti i dati, collocati nelle sedi che forniscono le applicazioni centralizzate, è appropriata ad evitare questo genere di problemi.

La disponibilità dei dati nelle singole sedi deve essere garantita dalla presenza di uno o più server ReadOnly.

In una AAI sono raccolti, per ogni utente, diversi tipi di dati che, rispetto all'azione di lettura, possono essere catalogati in pubblici, personali e sensibili, con corrispondenti vincoli di accesso. Inoltre all'interno di ognuna di queste categorie, rispetto all'azione di scrittura, devono essere rispettati ulteriori vincoli. Ad esempio, dati completamente pubblici come il numero di telefono o di FAX di un utente, devono essere accessibili da chiunque e possono essere modificati dall'utente a cui si riferiscono, mentre l'indirizzo e-mail dell'utente (che è pubblico) non dovrà essere modificabile dall'utente stesso, ma solo dall'amministratore del sistema di posta elettronica.

Saranno quindi utilizzate tecniche atte ad implementare una corretta politica di **protezione dei dati** presenti nella INFN-AAI, con modalità che saranno descritte di seguito.

La **sicurezza dei dati** sarà invece garantita dai sistemi di backup in produzione nelle sedi che ospiteranno i quattro server centrali.

2.3 Implementazione

2.3.1 Strumento SW

Per quanto detto nelle sezioni 2.1 e 2.2 in merito al tipo di servizio offerto dall'AAI e ai

requisiti richiesti, appare chiaro che lo strumento software per ottenere la realizzazione di una INFN-AAI debba supportare il protocollo LDAP e fornire un sistema di Autenticazione "forte" basato su Kerberos5.

Lo scenario dell'Open Source offre attualmente più strumenti per implementare un servizio di Directory, ma la possibilità di avvalersi di funzionalità importanti come la configurazione in Multi-Master e la definizione di gruppi dinamici o anche nidificati, insieme alla garanzia fornita da una grande comunità di sviluppo, ci hanno spinto a scegliere il Fedora Directory Server[12)].

Per la parte di Autenticazione Kerberos, tra la versione del software offerta dal KTH Svedese (Kerberos Heimdal[13)]) e quella prodotta dal MIT, si è scelto di utilizzare quest'ultima. Questo principalmente perché Kerberos MIT è più diffuso ed ha quindi una comunità di sviluppo più ampia, offrendo così maggiori garanzie di supporto. Prova ne è il neonato MIT Kerberos Consortium[14)] che annovera tra gli sponsor, esecutivi e non, nomi come la NASA, Sun Microsystems, Apple, Google, Microsoft (che ha basato AD su questa implementazione) e molti altri. Non ultimo, è disponibile uno strumento di conversione da MIT ad Hemindal e non il viceversa: questo ci garantisce la possibilità in futuro di poter cambiare.

2.3.1.1 Fedora Directory Server

Si tratta un Server LDAP che è stato sviluppato nel corso degli anni da grandi case di software (America Online, SUN Microsistem, RedHat) con lo scopo di fornire uno strumento di classe Enterprise.

Dal primo giugno 2005 RedHat ne ha rilasciata una versione OpenSource, distribuita da Fedora come Fedora Directory Server (FDS), che contiene le stesse caratteristiche del prodotto commerciale RedHat Enterprise Directory Server e si avvale della enorme comunità di sviluppo del progetto Fedora. Questo ci da sufficienti garanzie sulla continuità dello sviluppo e del supporto rivolto a questa soluzione per i prossimi anni. Le principali caratteristiche di FDS sono:

- la possibilità di installare server in configurazione "Multi-Master" con repliche a garanzia di alta affidabilità;
- elevata scalabilità;
- possibilità di sincronizzazione con Active Directory;
- metodi di Autenticazione e trasporto sicuri (SSLv3[15)], TLSv1[16)], and SASL[17)]);
- supporto per Autenticazione Kerberos5 attraverso SASL e GSS-API[18)]

- possibilità di aggiornare "a caldo" *schema*, configurazione ed ACI (Access Control Information);
- possibilità di definire gruppi dinamici o nidificati (*roles*)
- console grafica basata su java che permette di gestire completamente il Directory Server.

Ruoli

In FDS la gestione dei Gruppi può essere implementata tramite i *Ruoli*, attraverso i quali è possibile definire oltre ai gruppi statici, gruppi "dinamici" o anche nidificati.

I *Ruoli* sono definiti da una *entry* e possono essere di tre tipi:

Managed Roles: Permettono di definire Gruppi Statici. L'assegnazione di una *entry* a gruppi di questo tipo è definita singolarmente per ogni *entry*, nella quale si specifica il DN del ruolo che si vuole attribuire.

Filtered Role: Permettono di definire gruppi dinamici. È possibile infatti attribuire un *ruolo* ad una determinata entry a seguito della verifica, attraverso una query LDAP, del contenuto di un qualsiasi attributo di quella stessa entry. Ad esempio si può definire il ruolo "Nato a Roma" per tutti quelli che hanno la stringa H501 nel codice fiscale.

Nested Roles: Permettono di definire Gruppi di Gruppi. Ad esempio si può definire che il *ruolo* di PersonaleINFN sia assegnato a tutte le *entry* in cui è definito il *ruolo* DipendenteINFN o AssociatoINFN.

ACI

Il controllo degli accessi viene gestito attraverso le ACI (Access Control Information). L'ACI è un attributo amministrativo inseribile in una qualsiasi entry del DS, che viene ereditato dagli eventuali figli della entry in cui è inserito. Un'ACI è definita dal Target, ovvero il soggetto del permesso che può essere una *entry* o un singolo attributo di essa; dal Subject, che può essere una singola entry o un ruolo e costituisce l'identità da autorizzare; dalla Permission, ovvero l'operazione da concedere o negare.

Tramite ACI è possibile anche controllare il valore che viene inserito, concedendo l'inserimento ad esempio di un numero di telefono che inizi per 069403 solo da parte del personale dell'INFN di Frascati.

2.3.1.2 Kerberos5

È un protocollo di Autenticazione, nato negli anni '80 all'interno del progetto Athena al Massachusetts Institute of Technology (MIT), basato sull'uso di chiavi crittografiche "forti" con lo scopo di fornire un sistema sicuro di Autenticazione e scambio di informazioni tra client e server su reti "insicure". Le principali caratteristiche di Kerberos5 sono:

- la password dell'utente non viaggia mai sulla rete;
- la password dell'utente non viene mai memorizzata in nessuna forma sulla macchina client;
- la password dell'utente non viene memorizzata in chiaro neanche nel database dei server di Autenticazione;
- supporto nativo per il Single Sign-On;
- gestione centralizzata delle informazioni per tutti i sevizi;
- supporto per la mutua Autenticazione;
- supporto per la cifratura dei dati.

2.3.2 Architettura

Al fine di soddisfare il livello di affidabilità del servizio e disponibilità dei dati esposto in precedenza e sfruttando le caratteristiche di Fedora Directory Server, si è scelto di implementare, per ciò che riguarda il servizio di Directory, un'architettura basata su 4 server ReadWrite in configurazione Multi-Master, installati in numero di due per ognuno dei siti LNF e CNAF ed almeno un server ReadOnly per ogni sede. I server centrali conterranno i dati relativi a tutte le sedi e gruppi collegati oltre a quelli "top level" ovvero al livello dc=infn, dc=it.

L'unità minima replicabile in FDS è il database. Usando un database unico per tutto l'INFN, ogni modifica apportata da una qualsiasi sede verrebbe replicata in tutti i server (cioè i 4 master e gli slave di tutte le sedi) . Al fine di evitare operazioni di repliche non necessarie (la semplice modifica di un numero di telefono di un utente di una sede qualsiasi sarebbe replicato in tutti i server di tutte le sedi) si è scelto di definire un database per ciascuna sede, oltre al database relativo al livello dc=infn,dc=it, che conterrà tutte le informazioni che

devono essere condivise da tutte le sedi (come ad esempio ACI e *Roles*).

La presenza nelle sedi di uno o più server ReadOnly garantisce la piena funzionalità. I client di sede infatti contatteranno sempre il server ReadOnly locale che risponderà direttamente a tutte le operazioni di lettura e che, tramite il meccanismo di *referral,* provvederà a indirizzare il client verso uno dei 4 server di core per tutte le operazioni di scrittura. A modifica avvenuta il server provvederà a replicarla sugli altri tre server di core e sul server ReadOnly della relativa sede.

Il database top level, contenendo tutti i ruoli nonché tutte le ACI che dovranno avere validità in tutto l'albero INFN, deve essere replicato su tutti i server ReadOnly.

Nell'architettura finale le repliche dei database INFN e di sezione dai quattro server core verso le sedi sono schematicamente rappresentate in Figura 16.

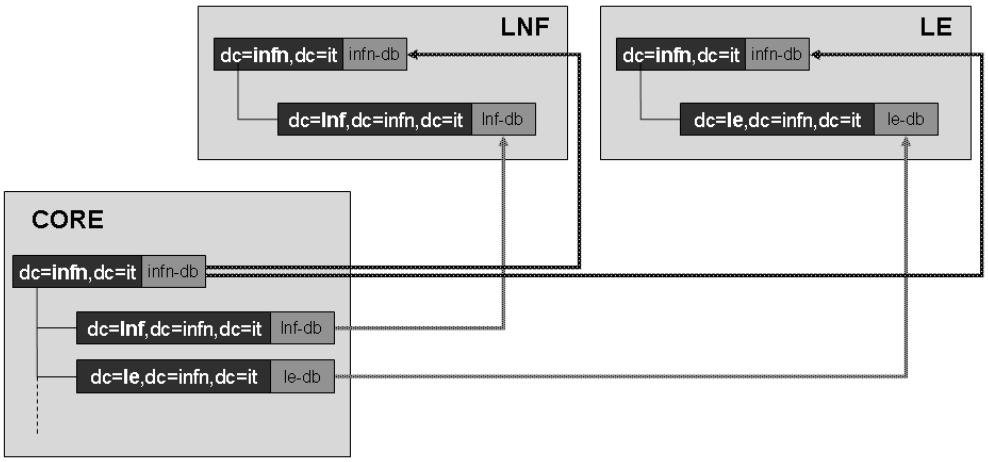

Figura 16: Schema dell'architettura dei server LDAP e della distribuzione di database

Infine, per garantire alle applicazioni centralizzate il completamento del processo di Autenticazione degli utenti, anche nel caso di irraggiungibilità dei server KDC delle sedi, l'architettura prevede l'installazione, in ognuna delle sedi che offrono servizi centralizzati, di un server KDC slave per ogni REALM kerberos. Data l'esigua quantità di risorse necessarie per il funzionamento di un server KDC, tutti i server slave potranno essere alloggiati in

macchine virtuali Xen, all'interno di una apposita "Xen KDC Farm" formata da un paio di server.

2.3.2.1 Autenticazione

La progettazione dell'Autenticazione, ovvero del processo delegato all'identificazione di un utente prima della successiva Autorizzazione all'uso dei servizi, ha tenuto conto della necessità di integrazione delle AA esistenti nell'INFN. Dato che FDS fornisce un sistema di Autenticazione basato su hash compatibili con quelli normalmente usati nei tradizionali sistemi di Autenticazione (crypt, MD5,SHA1), sarà possibile l'importazione automatica mediante i migration tools LDAP dei file contenenti gli hash criptati (etc/shadow o direttamente le mappe NIS). Di seguito, pertanto, sarà trattata in dettaglio solo l'Autenticazione Kerberos5.

Autenticazione Kerberos5

Per client kerberizzato si intende un software (ssh, browser web o di posta elettronica, lpr, AFS, ...) che essendo compilato con le librerie krb5 o più genericamente con le GSS-API, permette l'Autenticazione mediante l'uso di ticket Kerberos5 di cui l'utente dispone. Analogamente, per servizio kerberizzato si intende un processo capace di soddisfare una richiesta autenticata mediante l'uso di ticket Kerberos5. Queste precisazioni, all'apparenza scontate, sono d'obbligo, poiché si potrebbe erroneamente pensare, che qualsiasi applicazione in grado di autenticare l'utente chiedendogli le credenziali, che convaliderà mediante una richiesta ad un KDC Kerberos, sia un'applicazione kerberizzata, e che quindi sia in grado di offrire il SSO, funzionalità che invece solo le applicazioni kerberizzate garantiscono. In caso di applicazioni non kerberizzate, invece, l'utente che chiede di accedere al servizio deve digitare ogni volta le credenziali.

Il progetto della INFN-AAI prevede una situazione, in cui l'Autenticazione sia delegata ad una struttura cross-autenticata di REALM Kerberos5 distribuiti presso le sedi. Affinché questo sia possibile devono essere rispettati i seguenti punti:

1. nomi dei REALM corrispondenti ai domini DNS convertiti in maiuscolo;
2. un realm centrale, INFN.IT, con il compito speciale di aggregatore per le relazioni di trust su cui è basata la cross-Autenticazione;
3. ogni REALM di sede in relazione di fiducia bidirezionale con il REALM

INFN.IT. Grazie alla proprietà transitiva delle relazioni di fiducia, ogni sede si fiderà automaticamente di tutte le altre per ciò che riguarda l'Autenticazione. È ovvio tuttavia, che l'accesso alle risorse di una sede da parte degli utenti di un'altra sarà regolata da meccanismi autorizzativi;

4. il REALM INFN.IT dovrà contenere inoltre, i principal di Autenticazione per i servizi centrali;
5. ogni sede dovrà gestisce localmente un KDC Master in ReadWrite e, a sua discrezione, eventuali KDC slave di ridondanza. Dovrà inoltre garantire la propagazione del proprio database di Autenticazione verso i KDC slave presenti in ognuno dei luoghi dove sono dispiegati i 4 server ReadWrite di Autorizzazione (LNF, CNAF). Ciò è necessario al fine di garantire l'accessibilità ai servizi centrali anche qualora non sia disponibile il collegamento con la sede di appartenenza dell'utente.

Nei casi in cui si preveda un'intensa cooperazione tra due sedi, con conseguente condivisione di risorse, è possibile stabilire tra esse una relazione di fiducia diretta, al fine di evitare la perdita di efficienza causata dal dover contattare i KDC di INFN.IT.

Plugin di Autenticazione KRB5 per FDS

La necessità di consentire il funzionamento del sistema di Autenticazione con servizi ed applicazioni non kerberizzate (come ad esempio accesso da luoghi pubblici in cui l'Autenticazione GSS-API non sia configurata e né tanto meno configurabile) unita alla necessità di funzionamento in un ambiente Kerberos5 multi-REALM, ha richiesto lo sviluppo di un plugin di Autenticazione per FDS che sostituisca il comportamento di default della simple authentication LDAP (che prevede la verifica delle credenziali solo tramite il confronto degli hash immagazzinati nelle entry della directory). Tale plugin, scritto in codice C, ha il seguente comportamento:

- Verifica dell'esistenza della entry individuata dal DN con cui si tenta l'operazione di Bind;
- Individuazione del principal con cui tentare l'Autenticazione Kerberos:
    - se esiste l'attributo krbPrincipalName si utilizza come principal il valore di tale attributo;
    - se non esiste l'attributo krbPrincipalName si utilizza come principal quello

ottenuto dalla concatenazione dei dc che costituiscono il Distinguished Name, da sinistra verso destra e convertendo i dc in maiuscolo. Più precisamente, ipotizzando che l'utente abbia il DN uid=pippo,dc=le,dc=infn,dc=it:

- Principal = pippo@LE.INFN.IT

- Utilizzo delle API krb5 per validare le credenziali:
  - se si riesce a decriptare il ticket con la password proveniente dalla richiesta di Bind, il plugin restituisce OK
  - altrimenti si cerca la presenza dell'attributo userPassword e l'Autenticazione prosegue nella maniera standard.

È evidente che in una tale situazione, le credenziali viaggiano sulla rete ed è quindi necessario imporre una connessione crittografata tra client e server LDAP.

Migrazione a Kerberos 5

Le sedi che non utilizzano già Kerberos5 potranno migrare a tale sistema di Autenticazione con il minor aggravio possibile per gli amministratori ed in maniera completamente trasparente per gli utenti. Una volta installato e configurato il KDC del REALM relativo alla sede (operazione per la quale è previsto il supporto da parte del gruppo INFN-AAI), l'operazione di popolamento avverrà in modo automatico, grazie ad una funzionalità aggiuntiva del plug-in sopra descritto.

Sarà possibile infatti delegare al plug-in KRB5 il compito di creare le entry K5 corrispondenti agli utenti i cui Principal Kerberos non siano ancora inseriti nel KDC di riferimento della sede. Per far ciò, si sfrutta il fatto che quando un servizio tenta l'autenticazione LDAP, le credenziali arrivano in chiaro (ma protette con TLS) al plug-in. Quest'ultimo, la prima volta che l'utente si autentica con successo, si accorge che non esiste la entry K5 e la crea usando le credenziali che gli sono giunte. Con questa strategia, dopo un periodo transitorio che si conclude quando tutti gli utenti hanno effettuato almeno un'autenticazione con successo, il database Kerberos5 risulta completamente popolato.

Integrazione con l'Autenticazione di Windows Active Directory

Poiché un dominio Windows Active Directory utilizza nativamente Kerberos5 come sistema di Autenticazione, le sedi che ne fanno uso possono utilizzarlo direttamente come backend di Autenticazione per i loro utenti. Si possono presentare i seguenti casi:

- Il nome del dominio AD coincide con il dominio DNS della sede. In tal caso, il plugin KRB5 applicato al FDS, automaticamente utilizza il KDC presente sui domain controller per soddisfare una richiesta di Autenticazione LDAP;
- Il nome del dominio AD non coincide con quello del DNS (es. w2k.le.infn.it). In questa situazione è necessario inserire nelle entry degli utenti del FDS il valore dell'attributo UserPrincipalName relativo al dominio AD.

Peraltro, nell'ultimo caso è possibile stabilire una relazione di trust tra il REALM canonico del AAI e quello Active Directory. In questa maniera le risorse Windows di una sede saranno automaticamente disponibili agli utenti partecipanti all'AAI INFN, purché autorizzati.

2.3.2.2 Autorizzazione

La possibilità e le modalità di accesso alle informazioni e ai servizi rappresentano un punto cruciale nella nostra architettura.

Come gia anticipato FDS implementa lo strumento dei ruoli i quali offrono tutte le funzionalità dei gruppi ma con la grande differenza che i ruoli sono definiti come un attributo di una entry e soprattutto per ogni singolo ruolo possono essere definite delle ACI che determinano "chi" può modificarlo indipendentemente dalla posizione della entry nell'albero. Questo permette un controllo capillare delle autorizzazioni sia dal lato delle sedi sia dal lato delle applicazioni centralizzate. Inoltre l'utilizzo dei ruoli e di alcune classi di oggetti (objectClass) standard (come eduPerson, inetOrgPerson) e di altre definite ad hoc (come infnPerson), che intendiamo creare per supplire alla carenza di alcuni attributi nelle object class esistenti (vedi codice fiscale), permetteranno di dare collocazione nell'albero della INFN-AAI a tutte le informazioni presenti nelle AA gia esistenti nelle varie sedi.

Al fine di assicurare l'applicabilità dei ruoli su tutto l'albero della Directory è necessario che le entry di definizione dei ruoli stessi, siano inserite nel livello più alto dell'albero. Inoltre per facilitare sia la creazione di ACI opportune, sia la scrittura delle query LDAP delle applicazioni, prevediamo per i ruoli, la scelta di un naming che ricalchi

esattamente la struttura gerarchica dell'organigramma dell'INFN. Ad esempio se si definisco i ruoli cns1.atlas.resploc.sede1 e cns1.atlas.resploc.sede2 (responsabili locali di esperimento atlas) e cns1.atlas.respnaz (responsabile nazionale), si può definire una ACI che permetta la attribuzione di uno dei primi due, ad una data entry, solo da parte di chi possiede il terzo. In questo modo otteniamo che i responsabili locali dell'esperimento atlas siano aggiunti o rimossi solo dal responsabile nazionale qualunque sia la posizione relativa delle entry nell'albero LDAP

2.4 Attività preliminari

Per la definizione dell'architettura della INFN-AAI, sono state svolte un certo numero di attività preliminari che vanno dalla verifica della scalabilità del modello stesso, alla verifica della compatibilità con le esigenze di disponibilità e riservatezza dei dati contenuti nella INFN-AAI, alla definizione della struttura dell'albero della Directory (DIT).

Sono stati inoltre effettuati degli stress-test, in modo da analizzare la necessità di risorse da parte delle applicazioni ed evidenziare eventuali criticità.

2.4.1 Alpha-Testing

L'alpha testing ha previsto la verifica delle funzionalità dei software scelti, con una particolare attenzione alle caratteristiche che ne hanno determinato la scelta.

Data l'elevata esperienza precedentemente acquisita nei riguardi del protocollo Kerberos e delle sue implementazioni, si è scelto di concentrare gli alpha test su FDS, ed in particolare sono state verificate le seguenti funzionalità:

- Connessioni e Autenticazione basata su SSL/TLS con Certificati X.509
- Creazione albero INFN
- Repliche Multi-Master
- Integrazione MIT Kerberos
- Roles
- Gestione ACI
- Sincronizzazione Active Directory

Per l'occasione sono state predisposte una serie di macchine virtuali, in particolare 4 per il core Multi-Master, e una ogni due sedi INFN, per un totale di 22 macchine virtuali.

Tutti i test sono andati a buon fine; si riporta di seguito una sintetica descrizione di

quanto effettuato.

Albero INFN: l'albero LDAP per l'INFN è stato creato a partire dal suffix "dc=infn, dc=it". È stato quindi creato un sub-suffix per ogni sede del tipo "dc=SEDE, dc=infn, dc=it", ed associato a ciascuno di essi un distinto database, per un totale di 39 database.

Repliche Multi-Master: sono state configurate le repliche Multi-Master tra i server di core, con Autenticazione tramite certificato X.509. In tale configurazione, siccome per ogni database replicato è necessario definire una "istanza" di replica, su ogni server sono definite 39*3=117 istanze di replica.

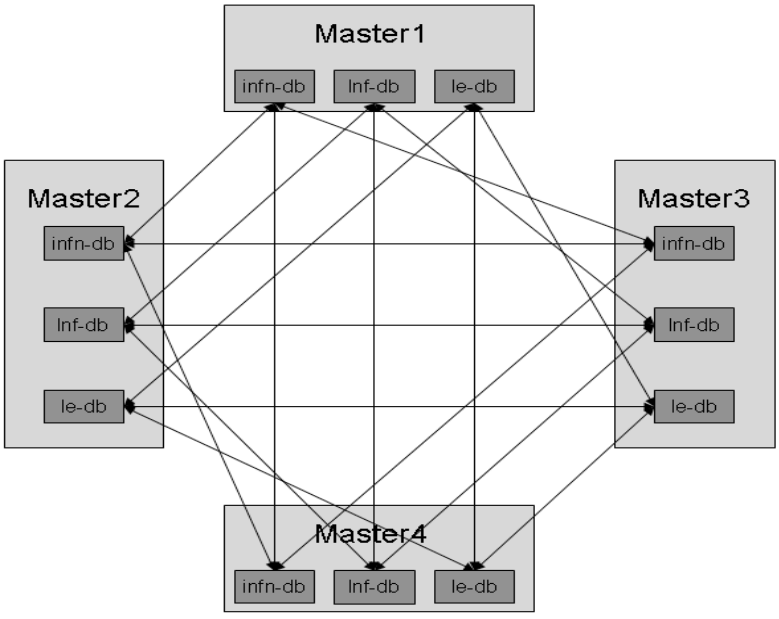

Figura 17: schema delle istanze di replica dei 4 server di core

È stata verificata la funzionalità delle repliche simulando dei crash di uno o più nodi coinvolti. Quando viene effettuato un aggiornamento su un Master, questo propaga le modifiche agli altri tre master. Nel caso uno o più server non fossero raggiungibili il master

tiene copia di tutti gli aggiornamenti che non è riuscito a propagare. Quando un server torna disponibile riceve quindi in modo automatico tutte le nuove informazioni e torna ad essere sincronizzato con gli altri master.

Repliche ReadOnly: si è poi provveduto a configurare anche le repliche ReadOnly dal core verso i server di sede. In questa modalità esiste una istanza di replica su ogni sever di core in direzione del server si sede, per ogni database da replicare. Segue uno schema che dovrebbe rendere l'idea.

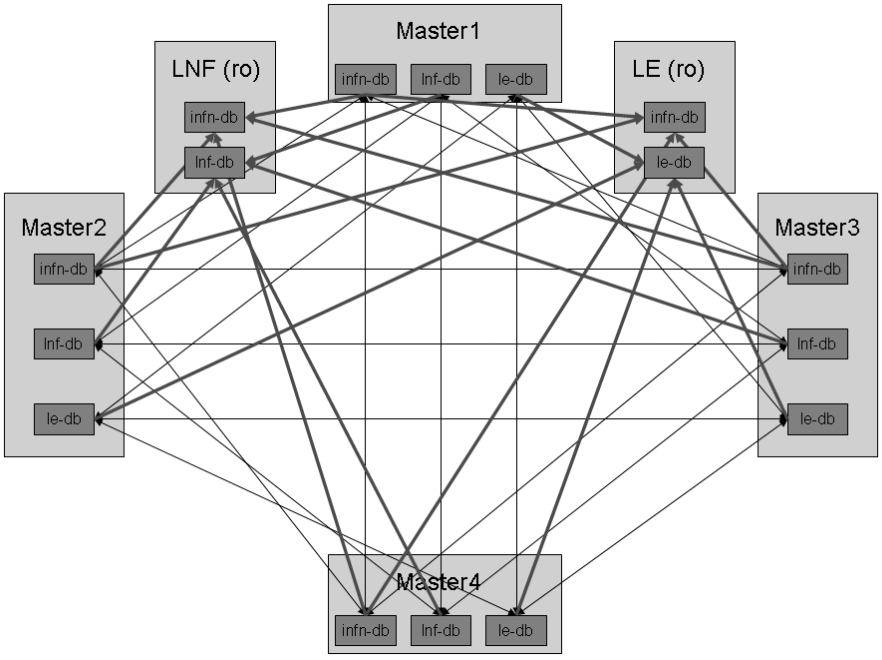

Figura 18: Schema delle repliche tra i master e con le sedi

Per la fase di Alpha Testing tuttavia si è scelto di inserire 2 database per ogni server periferico, per un totale di 174 istanze di replica in ogni server Master. Lo schema riportato in Figura 19 rappresenta tale architettura di test.

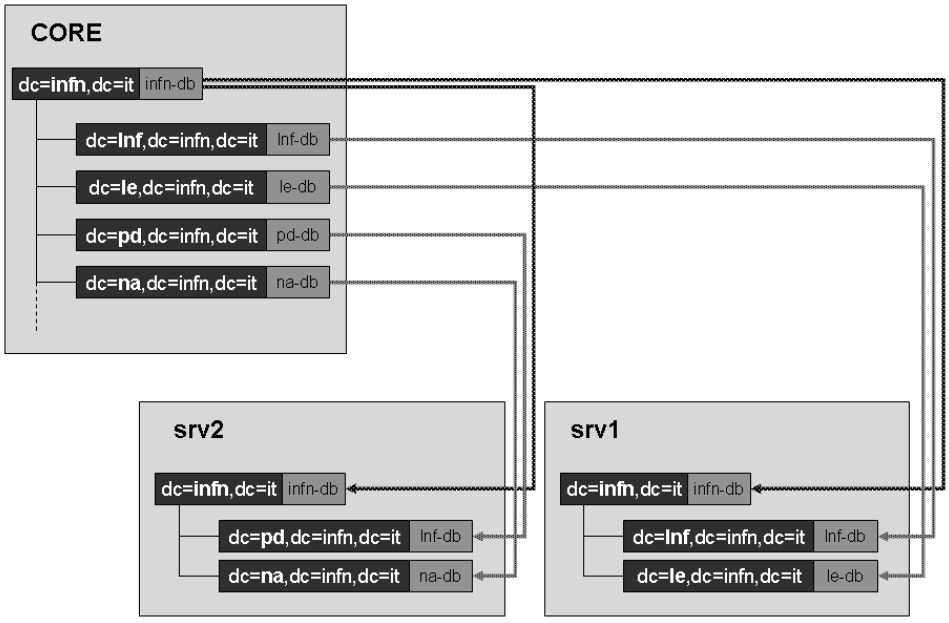

Figura 19: Schema dell'architettura usata nella fase di alpha-test

2.4.2 Stress Test

Per effettuare uno stress-test si è pensato di sottoporre i quattro server nella configurazione descritta, ad un elevato rate di query e monitorare l'utilizzo di risorse e il numero di query gestite in un lasso di tempo. In particolare si è proceduto in tale modo: 80 processi contemporanei eseguivano query di add, modify e delete distribuite in 100 modify, 5 add e 1 delete, selezionando in modo casuale uno dei 4 server Master. Si è notato che in tal modo si può generare una situazione di inconsistenza dei dati nei server Master, dovuta alla loro architettura implemetantiva: il database che gestisce gli aggiornamenti del Directory Server, chiamato changelog, ha come precisione del timestamp un secondo. Di conseguenza, se un client chiede l'aggiornamento della stessa entry con dati diversi a server diversi nello stesso secondo, i Master non sono in grado di discriminare quale sia l'informazione più aggiornata. Si consideri tuttavia che, secondo le specifiche LDAP, quando siano disponibili più server per la gestione delle informazioni riguardanti una stessa entry, si deve contattare il primo della lista e passare al secondo solo se il primo non risponde e non procedere quindi in

modo casuale. Questo rende di fatto impossibile il verificarsi del problema sopra citato.

Alla luce di quanto detto si è modificata la procedura di stress-test in modo che la selezione della sede avvenisse in modo random, ma fissando il mapping tra sede e server Master da interrogare, con uno schema del tipo infn-db -> master1, lnf-db -> master2, roma1-db -> master3, ecc. ecc.

Il risultato finale è stato di 357 Add, 7695 Modify e 68 Delete in 10 minuti. Circa 13,5 query/sec. I tempi di convergenza delle informazioni nei 4 server Master, con un simile carico, si aggirano nell'ordine di decine di secondi a patto che i nodi coinvolti abbiano caratteristiche di performance (in particolare di disk I/O) simili. È infatti comprensibile come se uno dei master non è in grado di gestire un rate di entry al pari degli altri nodi, questo non può essere in grado di terminare il job di stress-test nello stesso tempo degli altri ed avrà quindi un tempo di convergenza più elevato.

Inserendo nella configurazione dello stress-test le macchine di sede, ovvero aggiungendo le repliche ReadOnly per le singole sedi, il numero di repliche gestite dai server di core è salito da 117 a 174. Non si è notato alcun cambiamento rilevante nelle performance dell'intero sistema.

2.5 Proto AAI

Il gruppo Dataweb INFN, il quale si occupa di alcuni siti web dell'ente tra cui il Portale INFN, ha intenzione di migrare il proprio DB di Autenticazione ed Autorizzazione verso un sistema LDAP. Questo permetterebbe una gestione ottimizzata in particolare delle autorizzazioni, nonché per l'installazione di software di terze parti utilizzando le informazioni sulle username del portale INFN.

Dato lo sviluppo contemporaneo della INFN-AAI si è pensato di dare supporto a DataWeb predisponendo un sistema compatibile con INFN-AAI, in cui il database degli utenti corrispondesse a quelli attualmente in possesso dei Servizi di Calcolo delle sedi INFN. A questi dati, limitati a username e mail address, si aggiungeranno le definizioni dei ruoli del personale tramite i Roles di FDS; tali ruoli saranno strutturati secondo il modello definito dalla INFN-AAI ma in questa fase verranno gestiti direttamente da Dataweb. La struttura dei ruoli avrà un aspetto simile al seguente:

Informazioni di carattere "amministrativo"

- cns1.amm.member
- cns1.amm.president

- cns1.atlas.member
- cns1.atlas.resploc.sede
- cns1.atlas.respnaz
- cns1.atlas.referee

Informazioni di carattere "operativo"

- cns1.atlas.rivelatore.resp
- cns1.atlas.rivelatore.member

Informazioni relative alle sedi:

- struttura.divisione.servizio
- struttura.divisione.responsabile
- struttura.divisione.member

Per il motivo sopra citato, nonché per la natura attualmente mutevole della cosiddetta protoAAI, è ovvio che quest'ultima sarà ad uso solo degli strumenti del gruppo DataWeb che si impegna a adattare le proprie applicazioni ad eventuali cambiamenti del modello della INFN-AAI prima del suo dispiegamento.

Il sistema è costituito da due macchine virtuali su cui è installato Fedora Directory Server e dove sono stati creati i database corrispondenti alle sedi come da modello INFN-AAI. Tali database sono replicati su entrambe le macchine in modalità Multi Master in modo da garantirne la disponibilità.

Per permettere ai Servizi di Calcolo di popolare e tenere aggiornate le informazioni sugli utenti nei server LDAP è stata scritta un'applicazione chiamata Protoserv che tramite un interfaccia command-line accessibile via ssh permette un rapida e semplice gestione delle entry. Sono state scritte inoltre alcune procedure per il primo popolamento a partire dai file di configurazione dei mailserver.

I permessi della protoAAI permetteranno la lettura delle informazioni di tutto l'albero dai server del Dataweb e da parte delle singole sedi solo al ramo di loro competenza. L'inserimento di nuove entry e la modifica delle informazioni riguardanti le username e i mailaddress saranno permesse solo tramite Protoserv, mentre la modifica dei ruoli e la gestione delle password solo al gruppo Dataweb. L'Autenticazione avverrà tramite il sistema interno di FDS.

3 PIANO ORGANIZZATIVO

Come evidenziato nel capitolo 2, le attività fin qui svolte hanno dimostrato che il software scelto (FDS e MIT Kerberos5), nella configurazione prevista dall'architettura della INFN-AAI, fornisce tutte le funzionalità necessarie e può essere efficacemente utilizzato sia come AAI locale, che come AAI per i servizi centralizzati.

Definiti quindi i sistemi software da usare e l'architettura della INFN-AAI, possiamo passare alla definizione del piano di implementazione.

3.1 Piano delle attività

L'attenta analisi del *survey* ha messo in evidenza, oltre alla frammentarietà di soluzioni adottate nelle varie sedi, anche il fatto che molte applicazioni in produzione utilizzano sistemi di AA (o anche AAI) che, anche se tutte basate su Directory ed LDAP, non sono facilmente integrabili nella INFN-AAI (differente disegno del DIT, utilizzo non standard di classi di oggetti, ecc. ecc.)

Quindi, prima di definire in dettaglio i modi ed i tempi con cui le AAI locali in uso (e le applicazioni che ad esse fanno riferimento) possano essere integrate nella INFN-AAI, sarà necessario uno studio approfondito, sede per sede, e una fase di test per verificare le funzionalità incrociate.

Inoltre per riportare ad una unica AAI locale sedi in cui sono in uso domini Windows AD, sarà necessario un ulteriore periodo di R&D.

In definitiva, l'implementazione della INFN-AAI dovrà passare ancora attraverso le fasi di: pre-produzione, pilota e messa in produzione della INFN-AAI.

3.1.1 ß-Test ed R&D

La fase di pre-produzione conterrà fasi di:

- acquisto ed installazione dell'hardware;
- test (estensione degli alpha-test su una scala maggiore, test di scalabilità della "Xen KDC farm", e test sull'hardware finale);
- R&D (verifica della situazione delle sedi, produzione dei plug-in necessari e della GUI di amministrazione);
- produzione della documentazione necessaria.

Test

I test fino ad ora effettuati hanno dato tutti esiti favorevoli, nonostante siano stati svolti utilizzando macchine virtuali (anche per i server di core) e quindi su nodi con quantità di risorse molto più basse rispetto a quelle che avranno a disposizione i server in produzione.

Questo ci rende ragionevolmente confidenti del fatto che l'architettura proposta continui ad offrire prestazioni del livello richiesto anche se nei test svolti si è considerato un numero di istanze di repliche che è circa la metà di quelle che avremo in produzione.

Ciononostante riteniamo necessaria un'ulteriore fase di test con un numero maggiore di istanze di replica, poiché è ragionevole supporre che in molte sedi, per aumentare l'affidabilità locale, si vorrà installare più di un server ReadOnly.

Se si dovessero incontrare dei cali di prestazione, in funzione dell'aumento di istanze di replica, il disegno generale della architettura dell'INFN AAI potrebbe rimanere lo stesso, ma dovranno essere modificate le configurazioni dei server di sede. Infatti è possibile ridurre il numero di istanze di replica configurando nelle singole sedi invece che due server ReadOnly direttamente aggiornati dai server di core, un server "HUB" (che viene aggiornato dai server di core) più un server "foglia" (che verrà aggiornato dal server HUB di sede).

Una volta che si avrà a disposizione l'hardware definitivo, si potranno estendere i test di scalabilità su tali sistemi.

Sarà inoltre possibile verificare le prestazioni della "Xen KDC farm" che ospiterà gli slave KDC di tutte le sedi, ognuno in una macchina virtuale Xen.

R&D: verifica situazioni sedi

Sarà necessaria un'attenta verifica dell'implementazione AAI nazionale mirata alle sedi che hanno già in produzione un sistema di Directory LDAP. In particolare dovrà essere effettuato uno studio approfondito delle configurazioni attualmente in uso nelle diverse sedi e di come debbano essere modificate le configurazioni specifiche dei singoli servizi in produzione per poter utilizzare la nuova Infrastruttura nazionale.

Infine sarà necessaria una verifica del corretto funzionamento della nuova configurazione.

R&D: produzione dei plug-in necessari

Il plug-in KRB5, il cui funzionamento è già stato verificato durante la fase di alpha-test, dovrà essere modificato per aggiungere la funzionalità di creazione delle entry nei server KDC Kerberos. Sarà inoltre necessario scrivere un plug-in che impedisca la trasmissione di password in chiaro, obbligando l'uso di TLS (proprio del protocollo LDAPv3) per operazioni di Binding LDAP che richiedono la trasmissione di password.

R&D: GUI per gli utenti

Nonostante il software FDS abbia a corredo un'interfaccia grafica scritta in Java, essendo uno strumento pensato per gli amministratori della Directory, risulta complesso e poco fruibile da parte dell'utente. È pertanto prevista la produzione di GUI che possano essere facilmente usate da chiunque, garantendo accesso Autenticato.

Windows Active Directory

Secondo le specifiche di FDS, è possibile sincronizzare utenti, gruppi e password utente in modo bi-direzionale tra FDS e domini Microsoft Active Directory. Il processo non è semplice poiché FDS e Active Directory utilizzano funzioni hash diverse e questo fa si che le password dei due sistemi non siano compatibili. Inoltre non si conosce un meccanismo che consenta il recupero delle password in chiaro da Active Directory ma è possibile ovviare a questo intercettando le operazioni di cambio password durante le quali le informazioni passano necessariamente in chiaro. Lo strumento "Password Sync" fornito con FDS che va integrato in un sistema Active Directory sembra essere in grado di rilevare gli eventi di modifica delle password, estrarre le stringhe in chiaro e inviarle al server FDS utilizzando il protocollo LDAP su connessione SSL.

Quanto sopra descritto dovrà essere opportunamente verificato, con particolare attenzione alla effettiva compatibilità con le configurazioni dei domini Windows AD esistenti nelle sedi dell'INFN.

Documentazione e Formazione

Continuando l'attività fino ad ora svolta, sarà prodotta tutta la documentazione necessaria per semplificare l'implementazione delle AAI all'interno delle singole sedi e, al contempo, verranno riproposti, nei primi 4/6 mesi di realizzazione del progetto, almeno un paio di edizioni di tutorial su Kerberos5 e FDS già tenuti in varie occasioni e presenti nel

piano della Commissione Nazionale per la Formazione, e destinati ai referenti locali di AAI.

In tale piano sono anche previsti dei corsi di formazione avanzata sul software RedHat Directory Server per i membri del gruppo AAI, così da aumentarne le conoscenze sull'argomento in vista dell'impegno necessario per il supporto alle sedi.

3.1.2 Fase Pilota

Prima di dispiegare la INFN-AAI in tutte le sedi sarà necessario selezionarne un sottoinsieme, il più rappresentativo possibile, che partecipi ad una fase pilota in modo da verificare le funzionalità della Infrastruttura nel maggior numero di casi differenti.

Le sedi degli autori di questo CDR saranno candidate naturali, subordinatamente alle dovute verifiche di compatibilità con le attività di sede, da effettuare insieme ai responsabili dei Servizi di Calcolo e Reti delle sedi.

3.1.3 Produzione

Terminata la fase pilota, l'attività verrà indirizzata alla integrazione di tutte le sedi nella INFN-AAI.

Oltre all'attività di supporto alle sedi relativa al dispiegamento della parte locale della INFN-AAI, è prevista l'attività di supporto necessaria per il dispiegamento dei server KDC (sia quelli locali alle sedi che gli slave all'interno della Xen KDC Farm).

Nella Tabella 2, è offerto un quadro di insieme delle attività necessarie al completamento del progetto.

<table>
<tr><td colspan="6">INFN-AAI</td></tr>
<tr><td colspan="4">ß-Test ed R&D</td><td>Pilota</td><td>Produzione</td></tr>
<tr><td colspan="2">M2: Test di scalabilità su alpha-AAI estesa</td><td>M4: Test scalabi-lità Xen KDC farm</td><td rowspan="6">M7: da proto AAI ad INFN -AAI</td><td rowspan="6">M9: Sedi pilota in INFN-AAI</td><td rowspan="6">M10, M11, M12:
Tutte le sedi in INFN-AAI</td></tr>
<tr><td></td><td>M3: server di core</td><td>M3: Test su HW finale</td></tr>
<tr><td colspan="3">M1: Verifica sedi che usano LDAP</td></tr>
<tr><td colspan="3">M5: Krb5 plug-in new version</td></tr>
<tr><td colspan="3">M5: ForceTLS plug-in</td></tr>
<tr><td colspan="6">Formazione</td></tr>
<tr><td colspan="3">M6: Documentazione</td><td colspan="3">M6: Aggiornamento documentazione</td></tr>
<tr><td></td><td colspan="2">M5: GUI di amministrazione</td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3">M8: Integrazione Windows AD</td><td></td></tr>
</table>

Tabella 2: Riepilogo delle attività con indicazione delle milestones

3.1.4 Attività future

Federazioni di AAI

Uno dei "valori aggiunti" della INFN-AAI sarà quello di permettere di partecipare alle federazioni di AAI in fase di definizione in vari ambienti, sia nazionali (progetto IDEM del GARR) che internazionali. Tali federazioni, basate sul protocollo Shibboleth e relativo software implementativo, hanno lo scopo di garantire il SSO per le applicazioni Web.

Per partecipare a tali federazioni sarà quindi necessaria sia una fase di studio, che una fase di implementazione. È evidente che l'accesso alle funzionalità offerte da tali federazioni sarà disponibili agli utenti delle varie sedi a partire dall'adesione della sede alla INFN-AAI.

Autenticazione *dual factor*

Nell'INFN è in corso da tempo una attività di R&D sull'utilizzabilità di certificati X.509 protetti in "chiavi" USB.

Dato che la INFN-AAI prevede l'uso di Autenticazione Kerberos5, la completa funzionalità di tali sistemi potrà essere garantita dalla implementazione di PKINIT (estensione del protocollo Kerberos5 che permette di ottenere un ticket Kerberos a partire da un certificato X.509). Tale implementazione è ancora in fase embrionale nel software Kerberos5 di MIT, e quindi non ancora utilizzabile.

La prevista attività di studio e successiva integrazione nella INFN-AAI di sistemi di Autenticazione forte di tipo *dual factor* dipenderà quindi dalla effettiva disponibilità di un supporto per tali sistemi all'interno del software Kerberos.

GridShib[19)]

GridShib è un progetto che ha come scopo quello di integrare federazioni di AAI basate su Shibboleth con le tecnologie GRID, per permettere l'accesso alle risorse GRID attraverso il sistema di Autorizzazione basato su attributi, proprio delle federazioni di AAI.

È una tecnologia ancora immatura, e quindi non si prevede di dedicare risorse alla sua implementazione in questa fase del progetto. Tuttavia, essendo prevista la partecipazione di INFN-AAI a federazioni di AAI basate su Shibboleth, non dovrebbero sorgere ostacoli all'integrazione della tecnologia GridShib, una volta matura. Ovviamente tale integrazione richiederà una congrua fase di studio e test.

3.2 Milestones e tempi di attuazione

La definizione di tempi di attuazione, in assenza di certezze su man-power da poter dedicare, non può che essere approssimativa e soggetta in futuro a cambiamenti anche sostanziali. È comunque possibile definire una serie di traguardi intermedi o milestones, per il raggiungimento dei quali, si è fatto anche un esercizio di calcolo dei tempi di attuazione in base all'ipotesi di man-power a disposizione come dalla Tabella 2.

3.2.1 ß-Test ed R&D

M1: L'analisi approfondita sull'uso di LDAP nelle sedi richiede almeno una settimana di lavoro di una persona INFN-AAI che collabori con una persona dei servizi di calcolo della

sede in esame. Essendo 14 le sedi che necessitano di tale studio approfondito, il totale fa 14 settimane di una persona INFN-AAI (o poco meno di 5 settimane se le persone diventano 3). Lo studio dell'integrazione ed i testi relativi richiedono ulteriori 1.5 settimane per ogni situazione da studiare. Si prevede quindi che la fase di verifica della situazione nelle varie sedi si possa concludere in 35 settimane di lavoro (circa tre mesi di lavoro di 3 persone dedicate).

M2: Parallelamente si potrebbero concludere i testi di scalabilità, per i quali sarà necessario installare e configurare almeno una trentina di host (reali o virtuali). Supponendo che tale operazione possa essere condotta con l'aiuto di tutti i Servizi di Calcolo e Reti (e l'esperienza fatta durante l'alpha-test ci ha dimostrato che ciò è possibile anche se richiede tempo) questa fase potrebbe essere conclusa in circa 4 settimane di lavoro di una persona INFN-AAI (e di una frazione "variabile" di 4 settimane di lavoro di una persona in ognuna delle sedi coinvolte).

M3: L'acquisto, l'installazione e configurazione dell'hardware è soggetto ai "tempi tecnici". Una previsione "grossolana", ma vicina alla realtà (e comunque difficilmente "comprimibile"), può essere un paio di mesi dal finanziamento. Se tale previsione fosse rispettata, si potrebbero effettuare i test di scalabilità della configurazione di Fedora Directory Server, direttamente sull'hardware che dovrà poi andare in produzione.

M4: Parallelamente (con un impegno continuativo di almeno 3 settimane di lavoro di 3 persone) si potrebbe verificare la scalabilità della "Xen KDC Farm". Ossia la funzionalità dei circa 30 KDC Kerberos slave, distribuiti su altrettante macchine virtuali Xen all'interno di due server.

M5: Tutte le attività legate alla produzione del software necessario (plug-in specifici, GUI) potranno essere portate a termine in circa 4 mesi di lavoro di almeno un paio di sviluppatori (anche se non a tempo pieno)

M6: La documentazione, o almeno la parte che dovrà essere usata da coloro che dovranno dispiegare i server nelle sedi dovrà essere pronta entro 4 mesi dall'inizio delle attività. Qui l'impegno è ovviamente distribuito su tutti i partecipanti.

M7: Una volta completate tutte le sopraelencate attività, sarà possibile trasferire il contenuto della protoAAI dentro la struttura definitiva di INFN-AAI, ed agganciare a questa l'Autenticazione e l'Autorizzazione dei servizi centralizzati.

M8: La verifica dell'integrabilità con Windows AD richiederà tempi più lunghi e man-power con competenze specifiche dedicato a tale lavoro. Non essendo però l'integrazione di

Windows AD un requisito “bloccante”, sarà possibile procrastinare la chiusura di tale attività e fornire l’integrazione con Windows AD successivamente.

In definitiva, la fase di ß-Test e di R&D (con la sola esclusione dell’integrazione di Windows AD) potrebbe essere conclusa in 4/5 mesi di lavoro di 3 persone a tempo pieno. Si dovrà tenere inoltre conto della presenza indispensabile di una figura di coordinamento da individuarsi all’interno del gruppo di lavoro AAI della CCR (vedi struttura organizzativa) e di una discreta percentuale di tempo del personale tecnico e tecnologo del gruppo AAI-WG dell’INFN.

3.2.2 Pilota e Produzione

M9: La fase pilota potrà durare un paio di mesi durante i quali dovranno essere inserite nella INFN-AAI il maggior numero di sedi possibili, compatibilmente con le esigenze locali. Durante questa fase saranno verificate tutte le procedure di migrazione, la correttezza della documentazione, la funzionalità del Software scritto, la fruibilità dei servizi centralizzati e di tutte le funzionalità di una AAI. Alla fine di tale fase, il servizio INFN-AAI sarà a tutti gli effetti in produzione sia per le sedi che avranno partecipato alla fase pilota, che per i servizi centralizzati.

M10, M11, M12: Durante i successivi 6 mesi, saranno inserite nella INFN-AAi le rimanenti sedi. I tempi ed i modi saranno concordati direttamente con i responsabili locali, in funzione della complessità del lavoro da svolgere in sede per l’integrazione in INFN-AAI, e del man-power a disposizione in sede. Durante questa fase, prevediamo verifiche intermedie dell’avanzamento dei lavori, ogni 2 mesi.

3.3 Struttura organizzativa

In questa sezione viene descritta la struttura organizzativa relativa all'attuazione del progetto. L'intento è quello di identificare le varie componenti coinvolte ed i ruoli relativi, con particolare riferimento alle responsabilità connesse al progetto generale ed alle attività collegate.

INFN-AAI sarà un servizio nazionale che dovrà essere mantenuto nel tempo. Si cercherà quindi di illustrare le esigenze organizzative per il buon funzionamento del servizio, e verrà abbozzato uno scenario di struttura di gestione della INFN-AAI.

La struttura organizzativa sarà abbastanza semplice e prevederà un gruppo di gestione con responsabilità politico-decisionali, affiancato da uno staff tecnico con responsabilità

operative. A queste 2 unità sarà strettamente collegato il gruppo di responsabili locali costituito da un rappresentante per sede. La figura alla quale stiamo pensando è quella analoga all' Access Point Manger (APM) di ogni sede. Una figura ufficiale, incaricata dal Direttore e responsabile per la sede del servizio AAI. Questa figura, in maniera analoga a quanto accade per l'APM, avrà un indirizzo di posta elettronica ufficiale (aai_resp@dominio) al quale dovranno essere collegati un congruo numero di addetti in modo tale da non lasciare scoperto il servizio in caso di assenze più o meno programmate.

Il gruppo di gestione è identificabile, in prima analisi, con il corrispondente gruppo di lavoro di CCR, ma ne rappresenta la naturale evoluzione. Sarà guidato da un "coordinatore" affiancato da un vice. Saranno il coordinatore e il suo vice gli unici autorizzati a prendere decisioni relative all'infrastruttura, in maniera analoga a quanto oggi accade per l'infrastruttura AFS (dove sono 3 i responsabili).

All'interno del gruppo di gestione saranno identificati dei ruoli speciali affidati *ad personam* in base alle competenze specifiche. Intendiamo questi ruoli come i punti di interconnessione indispensabili tra la struttura e "il resto del mondo". In particolare saranno previste le figure di:

- addetto ai rapporti con i responsabili locali AAI
- addetto ai rapporti con il GARR (in particolare per la partecipazione alle federazioni di AAI)
- addetto ai rapporti con il servizio Data WEB
- addetto alla divulgazione dell'iniziativa

Lo staff tecnico opererà in stretta collaborazione con il gruppo di gestione riferendosi al coordinatore come al proprio responsabile.

Schema:

- Gruppo di gestione INFN-AAI (Gruppo di lavoro di CCR, storico) composto da: membri volontari provenienti da varie sedi, 1 coordinatore nominato dalla CCR, 1 vice nominato all'interno del gruppo stesso.
- Staff tecnico INFN-AAI composto da: 3 unità di personale appositamente assunte affiancate a membri del gruppo di gestione con incarichi temporanei (in particolare nelle fasi di startup)

- Gruppo responsabili locali AAI - INFN composto da un rappresentante per sede

È di basilare importanza notare che questa struttura dovrà essere opportunamente divulgata all'interno dell'Ente con seminari di formazione rivolti alla dirigenza politica ed amministrativa. La preoccupazione da più parti espressa su fallimenti dell'iniziativa nella sua globalità trova fondate motivazioni in una diffusa difficoltà a trasmettere l'importanza di questo genere di attività all'interno dell'INFN. È imprescindibile quindi, per il buon funzionamento dell'iniziativa, un forte coinvolgimento di vertici nazionali e locali. Ed è per questo che si ritiene basilare un processo di formazione e aggiornamento continuo sullo stato del progetto stesso.

Oltre ad iniziative dedicate (presentazioni), si terranno seminari nella forma del *webinar* con cadenze mensili e sarà continuamente aggiornato un sito web dedicato.

4 ANALISI DEI COSTI

In questo capitolo sarà effettuata, a grandi linee, un'analisi dei costi dell'operazione, con particolare riferimento al primo anno di attività, indicando anche il piano previsto dei costi per gli anni successivi.

4.1 Infrastrutture

4.1.1 Infrastruttura di core

1. Fase di start-up: ricordiamo che l'architettura proposta prevede l'installazione di quattro server in ognuna delle due sedi di core (LNF e CNAF). Due sono dedicati a fornire il servizio di Directory. Altri due (XKF: Xen KDC Farm) saranno dedicati ad ospitare le macchine virtuali che svolgeranno il servizio di KDC slave per tutte le sedi. In totale saranno quindi necessari in questa fase 8 server con elevate caratteristiche di affidabilità (doppio dual core, almeno 2 GB per core, alimentatori e ventole ridondate ed hot-swap, dischi velocissimi e con controller RAID con alte prestazioni).

Per quantificare, se prendiamo come esempio un server Dell PowerEdge 2950 con 5 anni di manutenzione on-site ed intervento entro le 4 ore, il cui costo è di circa 7.5K€, il costo totale per l'infrastruttura di core sarà di circa **60K€**.

2. Fase di produzione: nel corso degli anni, per la struttura di core del servizio di Directory potrebbero essere necessari modesti finanziamenti scaglionati nel tempo, in caso di necessità di ampliamento di spazio disco o RAM. Per quanto riguarda invece il servizio di "hosting" degli slave KDC delle sedi potrebbero essere necessari finanziamenti consistenti, per permettere l'acquisto di ulteriori 2 server (quindi **15**K€ secondo i listini attuali), in funzione del risultato dei test di scalabilità della "Xen KDC Farm".

4.1.2 Infrastruttura locale

1. Fase di start-up: vista l'esperienza fatta durante la fase di alpha-testing ed in alcune AAI di sede in produzione come Napoli, si suggerisce l'hosting dei server locali in macchine virtuali all'interno della infrastruttura di virtualizzazione (o consolidamento dei server) della sede. Il costo è quindi ridotto ad eventuali incrementi di spazio disco e RAM dei server di sede laddove esiste già una tale infrastruttura di consolidamento dei servizi, mentre nei casi in

cui tale processo di consolidamento non fosse ancora in atto, si tratterebbe semplicemente di un piccolo incremento di finanziamento rispetto alle previsioni.

2. Fase di produzione: modesti finanziamenti suddivisi nel corso degli anni successivi in caso di necessità di aggiornamento dell'hardware.

4.2 Risorse Umane

4.2.1 Gruppo di gestione

Per quanto concerne l'aspetto gestionale dell'infrastruttura INFN-AAI nazionale dobbiamo distinguere tra la fase di startup e la fase di gestione a regime. Il gruppo AAI farà evolvere il suo ruolo da quello di propulsione e supporto iniziale a quello di struttura politica di interconnessione tra le esigenze dell'ambiente e le esigenze tecniche dell'infrastruttura. Si prevede quindi una presenza ininterrotta, nel tempo, del gruppo AAI nella sua tradizionale formulazione come "gruppo di lavoro di CCR". Al suo fianco si dovrà prevedere da subito, però, uno staff tecnico, con precisi compiti operativi.

1. Fase di start-up

Il "Servizio INFN - AAI" dovrebbe essere composto da:

- Una unità di "staff" (anche composta da due persone al 50%)
- Almeno un articolo 15 (o contratto a progetto) dedicato
- Almeno due borse di studio (diplomato)

Questo gruppo operativo si occuperà della implementazione del servizio nazionale. Prevediamo 1 anno di tempo necessario per la completa implementazione della struttura, così suddiviso in due blocchi da 6 mesi ciascuno: i primi 6 mesi dedicati all'installazione e configurazione dell'infrastruttura server e all'aggancio delle realtà locali più facilmente integrabili (beta-testing, R&D e pre-produzione). I successivi 6 mesi saranno dedicati invece a percorsi personalizzati per portare le realtà locali più complesse alla convergenza di base nell'infrastruttura.

I costi in questa fase sono essenzialmente relativi al man-power ed alle attività di coordinamento del gruppo.

Per quanto riguarda il man-power, il costo dipende fortemente dalla tipologia di

contratto. Se infatti le 3 unità di personale aggiuntivo saranno inquadrate con un contratto a tempo determinato (art. 15 o contratto a progetto) ed assumendo un costo medio di 2.5K€ al mese, il costo per ogni unità di personale sarà di circa **30K€** l'anno, per un totale di **90K€**. Se invece si potrà accedere ad istituti come "borse di studio" il costo potrà essere inferiore.

Per quanto riguarda le attività di coordinamento, dato che la fase di start-up sarà caratterizzata da una intensa attività, per quanto si possa prevedere l'uso di strumenti di collaborazione remota, pensiamo di prevedere almeno 6 riunioni da 2 giorni l'una. Contando una media di 5 partecipanti ed un costo medio di 600€ per partecipante, il costo totale per le attività fin qui descritte sarà di **18K€** per missioni in Italia.

2. Fase di produzione

In fase di produzione si ritiene invece necessario un gruppo di gestione coordinato, almeno in fase iniziale, da un membro "storico" del gruppo originario e costituito da almeno 6 unità di personale ufficialmente dedicate per una frazione del loro tempo-lavoro, a questa attività. A questo gruppo di gestione dovrà affiancarsi uno staff tecnico costituito da almeno 2 unità di personale dislocato nelle sedi che ospitano i server e dedicato ufficialmente al supporto tecnico anche delle sedi periferiche.

L'attività di coordinamento di questo gruppo di gestione avrà bisogno di almeno 2 riunioni l'anno. Contando una decina di partecipanti, con i costi indicati nel punto precedente, la spesa annua sarebbe di **12K€** per missioni in Italia.

Si prevede inoltre la partecipazione a workshop internazionali (HEPiX) per cui sarà necessario prevedere una spesa di circa **4K€** per anno per missioni all'estero.

Al fine di garantire continuità operativa, , è necessario prevedere opportuni periodi di sovrapposizione dei contratti del personale appositamente reclutato. Ciò per permettere il naturale periodo di formazione dei nuovi assunti ed il conseguente passaggio delle consegne.

4.2.2 Supporto singole sedi

1. Fase di start-up

In questo periodo, i costi a carico del progetto saranno essenzialmente quelli delle spese relative ad i viaggi che il personale dello staff tecnico INFN-AAI dovrà effettuare per fornire supporto alla migrazione ad INFN-AAI.

Supponendo che sia necessario tale supporto solo nelle realtà più complesse e possa limitarsi ad un paio di settimane per ogni sede, si ottiene un costo di circa 2.4K€ per sede che, per 14 sedi (tante sono quelle che hanno implementato AA locali basate su LDAP) fa circa **34K€** per missioni in Italia.

2. Fase di produzione

In questa fase non sono previsti costi specifici per il supporto alle sedi. Tutte le attività prevedibili di coordinamento o aggiornamento saranno a carico delle singole sedi, come è ormai consuetudine, almeno per le attività legate ai Servizi di Calcolo e Reti.

4.3 Riepilogo dei costi

Si riporta sinteticamente nella Tabella 3, il riepilogo dei costi, previsti per i prossimi 5 anni.

Nella colonna "Altre spese" sono indicati i costi relativi alla produzione di documentazione e ad un eventuale potenziamento dell'hardware.

	Personale appositamente assunto	Personale INFN dedicato	Inventariabile	Missioni Interne	Missioni estere	Altre spese (consumo, potenziamento hardware)
1° anno	3 unità di personale	3.2 FTE (4*0.5+6*0.2)	60	52	4	3
2° anno	2 unità di personale	2.2 FTE (2*0.5+6*0.2)	15	12	4	3
3° anno	1 unità di personale	1.6 FTE (1*0.4+6*0.2)	0	12	4	2
4° anno	1 unità di personale	1.6 FTE	0	12	4	2
5° anno	1 unità di personale	1.6 FTE	0	12	4	2

Tabella 3: Riepilogo dei costi. Le cifre nelle 4 colonne a destra, sono espresse tutte in K€.

5 ANALISI RISCHI

5.1 Rischi tecnologici

Nel corso del lavoro di studio e sperimentazione, che in parte si concretizza in questo documento, sono emersi molti aspetti e problematiche per le quali sono state individuate possibili risposte. Per altre rimangono delle considerazioni e preoccupazioni, che riportiamo per consentire una valutazione più completa della proposta.

5.1.1 Software open source

Per individuare la piattaforma software la scelta è stata tra prodotti simili, commerciali e open-source. Le caratteristiche di FDS soddisfano le esigenze e i requisiti di progetto, oltre ad essere basata su standard. Trattandosi di un software open-source, rimangono insuperate tutte le questioni legate ad un prodotto per il quale non esiste un preciso riferimento, ma si può contare sulla collaborazione di una ampia comunità. In realtà Red Hat offre supporto per la versione commerciale di FDS (RedHat Enterprise Directory Server), per la quale è possibile sottoscrivere un contratto che garantisca l'assistenza software e la fornitura degli aggiornamenti. Il progetto INFN-AAI si basa sulla versione FDS free.

5.1.2 Scalabilità del modello

Nello scegliere l'architettura del modello molto ha pesato la possibilità di installare quattro server in configurazione Multi-Master nelle due sedi che offrono servizi centralizzati e prevedere in ogni sede uno o più di server di tipo ReadOnly. In una configurazione che coinvolge tutte le sedi saranno presenti oltre 30 server nelle sedi. A questi potrebbero aggiungersi ulteriori server ReadOnly se anche le realtà di calcolo scientifico volessero avvalersi delle funzionalità di questa infrastruttura. Come già evidenziato, sono previsti ulteriori test fatti su scala maggiore per accertare la scalabilità del modello.

5.1.3 Espandibilità del modello

Con la disponibilità di una AAI INFN le sedi, localmente, potranno sostituire le attuali AA alla base del funzionamento di tutti i servizi. L'analisi puntuale delle configurazioni di

ogni sede non ha evidenziato applicazioni o servizi che non possano utilizzare il protocollo LDAP. Una particolare attenzione deve però essere rivolta ai domini AD del mondo Windows per la cui completa integrazione è ancora necessario uno studio approfondito. Sarà pertanto necessario individuare personale con specifiche competenze sull'argomento che possa dedicarsi a questa attività.

5.2 Rischi organizzativi

5.2.1 Man-power

Il progetto INFN-AAI, come condotto fino ad ora, ha enormemente sofferto di scarsità di man power, dovuta al fatto che tutti i membri del gruppo, che hanno partecipato alle attività in modo volontaristico, erano già pesantemente impegnati nelle attività istituzionali dei Servizi di Calcolo e Reti di appartenenza.

È evidente che le future attività legate al progetto non potranno essere garantite con le stesse modalità volontaristiche.

La rivisitazione dei sistemi di AA locali necessariamente comporta un ulteriore carico lavorativo per i Servizi di Calcolo, nella stragrande maggioranza dei casi già alle prese con i problemi legati alla scarsità di personale. È dunque necessario sottolineare che questo processo di razionalizzazione comporta un iniziale ulteriore impegno, poi successivamente compensato dai benefici che ne deriveranno.

5.2.2 Formazione

Una speciale attenzione deve essere rivolta alla formazione. Una delle possibili concause perchè una sede ritardi la propria adesione alla INFN-AAI è la scarsa familiarità con protocolli e soluzioni non adottate localmente. Iniziative quali la programmazione di corsi, tutorial, giornate tematiche, devono essere cadenzate e ripetute. La realizzazione di mailing list, forum di discussione, sito web devono facilitare la circolazione di informazioni e di soluzioni implementative. Tutto questo comporta un ulteriore carico di lavoro per le persone che saranno coinvolte in queste attività.

5.2.3 Tempi di attuazione della INFN-AAI

Il progetto, che coinvolge tutte le sedi, prevede che l'adesione alla INFN-AAI possa avvenire in tempi diversi. Questo permette alle singole sedi una pianificazione delle attività locali e del necessario coordinamento con il gruppo di lavoro, ma può determinare una enorme dilatazione dei tempi necessari a considerare conclusa l'operazione. Inoltre in caso di partecipazione a federazioni di AAI, solo le sedi pienamente inserite nella INFN-AAI potranno usufruire dei relativi benefici.

5.3 Rischi economici

Gli investimenti economici previsti sono relativi ad acquisizione di hardware dedicato, attività di coordinamento del gruppo di gestione e del personale appartenente allo staff tecnico nella sua funzione di coadiutore della migrazione alla INFN-AAI delle varie sedi (missioni interne), nonché a specifici corsi di formazione.

Nel caso il progetto non dovesse essere attuato nella sua interezza, sarà sempre possibile utilizzare l'hardware acquistato e le ulteriori competenze acquisiste dal personale, all'interno delle attività istituzionali dell' INFN

6 GLOSSARIO

ACI - Access Control Information (LDAP): In una directory LDAP le ACI definiscono i diritti di accesso assegnati ad un determinato soggetto rispetto alle operazioni che puo' compiere sull'oggetto a cui le ACI sono applicate. Ogni entry in una directory LDAP ha associato un set di ACI.

AFS - Andrew File System: Un filesystem distribuito che si presenta con un name-space comune a tutti i nodi client. E' disponibile per un ampia gamma di sistemi eterogenei tra cui UNIX, Linux, MacOS X, e Microsoft Windows.

BaseDN (LDAP): La entry di piu' alto livello del Directory Information Tree in un directory server.

Bind (LDAP): Cosi' e' chiamata la prima operazione compiuta da un client quando effettua una connessione ad un server LDAP. L'operazione di Bind invia il Distinguished Name della entry e le credenziali utilizzate per l'autenticazione.

crypt: Funzione standard di encryption per unix/linux, ormai poco utilizzata.

DHCP - Dynamic Host Configuration Protocol: Protocollo di rete che offre una infrastruttura per fornire informazioni di configurazione ad un nodo su una rete TCP/IP.

DIT - Directory Information Tree (LDAP): E' la gerarchia di oggetti che forma la struttura ad albero della directory. Consiste dei Distinguished Name delle entry della directory. Un server LDAP puo' supportare piu' di un DIT.

DN - Distinguished Name (LDAP): Ogni entry in una directory LDAP ha un Distinguished Name che la identifica in modo univoco nella directory. Un DN e' composto di coppie attributo=valore, separate dalla virgola. Esempio: dc=roma1,dc=infn,dc=it.

DNS - Domain Name System: E' un servizio utilizzato per la risoluzione di nomi di host in indirizzi IP e viceversa, in una rete TCP/IP. Il servizio è realizzato tramite un database distribuito, costituito dai server DNS.

dual factor, autenticazione: Si basa sull'utilizzo contemporaneo di due metodi di autenticazione individuale; coniuga qualche cosa che l'utente conosce (ad esempio un PIN o una password) con qualcosa che possiede (ad esempio un Token o una smart-card).

FDS - Fedora Directory Server: E' un server LDAP sviluppato da Red Hat all'interno del progetto Fedora.

Grid: E' un sistema di calcolo distribuito costituito da un'infrastruttura altamente decentralizzata e di natura variegata, in grado di consentire ad un vasto numero di utenti autorizzati l'utilizzo di risorse provenienti da un numero indistinto di calcolatori.

GSI - Grid Security Infrastructure: Un insieme di tool, librerie e protocolli per consentire ad utenti ed applicazioni un accesso sicuro alle risorse. GSI e' basta su una infrastruttura a chiave pubblica, con Certification Authority e certificati X.509.

GSS-API - Generic Security Services Application Programming Interface: E' una API generica per effettuare autenticazione client-server. E' inclusa nella maggior parte delle distribuzioni Kerberos5 e questo fa si' che se una applicazione o un protocollo supporta GSS-API allora supporta anche Kerberos5.

hash, funzione di: L'hash è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta valore di hash, checksum crittografico o message digest.

IDEM - IDEntity Management: E' il nome del progetto pilota per la realizzazione dell'Infrastruttura di Autenticazione e Autorizzazione federata della rete GARR

IMAP - Internet Message Access Protocol: E' un protocollo standard per l'accesso a caselle di posta elettronica residenti su un server remoto, in una rete TCP/IP.

KDC - Key Distribution Center: E' il server di autenticazione in un ambiente Kerberos. Kerberos e' basato sulla funzione del KDC di distribuire ticket per l'accesso ai servizi. Puo' essere considerato logicamente composto di tre parti: il Database, il Ticket Granting Server (TGS) e l'Authentication Server (AS) propriamente detto.

LDAP - Lightweight Directory Access Protocol: E' un protocollo standard per l'accesso ai dati contenuti nei servizi di directory.

LHC - Large Hadron Collider: E' un acceleratore di particelle, attualmente nelle fasi finali di costruzione, presso il CERN di Ginevra.

MD5 - Message-Digest algorithm 5: E' una funzione di hash che produce un message digest di 128 bit.

MySQL: E' un Database Management System (DBMS) relazionale, composto da un client con interfaccia a caratteri e da un server.

NIS - Network Information Service: E' un semplice database amministrativo distribuito su rete, che permette a diversi calcolatori di condividere alcuni file di sistema, in una rete TCP/IP. I file sono semplici database a chiave singola.

OpenAFS: Implementazione open source di AFS.

OpenLDAP: Implementazione open source di LDAP, sviluppata dal progetto OpenLDAP.

PAM - Pluggable Authentication Modules: E' un metodo di Autenticazione sui

sistemi unix/linux che introduce un ulteriore livello nella procedura di Autenticazione: le applicazioni comunicano una richiesta di autenticazione al PAM che effettua l'autenticazione attraverso diversi metodi e restituisce quindi il responso alle applicazioni.

POP - Post Office Protocol: E' un protocollo standard per l'accesso a caselle di posta elettronica residenti su un server remoto, in una rete TCP/IP.

PostgreSQL: E' un completo database relazionale ad oggetti, con licenza libera.

Principal (Kerberos): Un principal e' il nome utilizzato per riferirsi alle entry nel database del server di Autenticazione Kerberos. Ad ogni utente, nodo o servizio in un REALM Kerberos e' associato un principal.

REALM (Kerberos): Indica un dominio amministrativo di autenticazione. Stabilisce i confini entro i quali un KDC Kerberos e' autoritativo per autenticare utenti, nodi o servizi. Un oggetto appartiene ad un REALM Kerberos se e solo se condivide un segreto (password/ticket) con il server di Autenticazione di quello stesso REALM. Se due oggetti appartengono a differenti REALM Kerberos e i due REALM sono tra loro in relazione di trust, allora l'autenticazione tra i due oggetti puo' avere luogo; questa caratteristica e' nota come Cross-Authentication.

referral (LDAP): E' la risposta che un server LDAP da a un client, contenente l'indirizzo (tipicamente una URL LDAP) di un altro server LDAP che puo' o deve contenere le informazioni richieste.

SASL - Simple Authentication and Security Layer: È un metodo per aggiungere supporto per l'autenticazione a protocolli connection-oriented in una rete TCP/IP.

Schema (LDAP): Un insieme di metadati (dati che riguardano altri dati) che descrivono l'uso degli oggetti all'interno di una determinata struttura.

SHA-1 - Secure Hash Algorithm: Una delle cinque funzioni di hash SHA. SHA-1 produce un message digest di 160 bit. Viene considerato il successore di MD5.

Shibboleth: E' composto di un protocollo e della relativa implementazione, basato su standard, per il Single Sign-On. E' pensato per l'accesso a servizi web che siano all'interno una organizzazione o forniti da organizzazioni diverse.

SMTP- Simple Mail Transfer Protocol: E' il protocollo standard per la trasmissione di e-mail in una rete TCP/IP.

SQL - Structured Query Language: E' un linguaggio creato per l'accesso a informazioni memorizzate nei database. E' divenuto negli anni uno standard per i software che utilizzano il modello relazionale.

SSL - Secure Sockets Layer: E' un protocollo che procura comunicazioni sicure in una

rete TCP/IP.

SSO – Single Sign-On: E' un metodo per il controllo degli accessi che consente ad un utente di autenticarsi una sola volta per accedere a tutte le risorse informatiche al cui uso e' abilitato.

suffix (LDAP) : Uno dei modi per indicare la entry di livello piu' alto in un Directory Information Tree.

SYMPA - SYsteme de Multi-Postage Automatique: E' un software open source per la gestione di mailing list.

TLS - Transport Layer Security: E' un protocollo che procura comunicazioni sicure in una rete TCP/IP.

VOMS - Virtual Organization Membership Service: E' un sistema per la gestione di autorizzazioni in un abiente di collaborazione multi-istituzionale. VOMS offre un database di ruoli e gruppi e strumenti per accedere e modificare il contenuto del database ai fini di generare credenziali per gli utenti quando necessario.

X.509: E' uno standard ITU-T per una Public Key Infrastructure (PKI) e Privilege Management Infrastructure (PMI). X.509 definisce, fra le altre cose, i formati standard per i certificati a chiave pubblica, le liste di revoca dei certificati, gli attributi contenuti nei certificati e gli algoritmi per la verifica dei certificati stessi.

7 RINGRAZIAMENTI

Si ringraziano i colleghi che hanno contribuito alla realizzazione dell'alpha-test, i responsabili dei Servizi di Calcolo e Reti delle sedi ed il Coordinatore del Servizio DataWeb che, mettendo a disposizione risorse di calcolo e tempo uomo, hanno permesso la realizzazione di tutto il lavoro necessario per la produzione di questo documento:

Stefano Zani e Massimo Donatelli (CNAF), Roberto Cecchini e Leandro Lanzi (sezione di Firenze), Alessandro Brunengo e Mirko Corosu (sezione di Genova), Massimo Pistoni e Fabrizio Murtas (Laboratori Nazionali di Frascati), Sandra Parlati Fabio Di Bernardini e Piero Spinnato (Laboratori Nazionali del Gran Sasso), Paolo Mastroserio (sezione di Napoli), Roberto Alfieri (gruppo collegato di Parma), Andrea Rappoldi e Carlo De Vecchi (sezione di Pavia), Marco Serra (sezione di Roma), Renata Kwatera (sezione di Roma2), Cristian Stanescu (sezione di Roma3).

8 BIBLIOGRAFIA

(1) Sympa (http://www.sympa.org/) è un mailing list server sviluppato e supportato dalla CRU (Comité Réseaux des Universités) francese (http://www.cru.fr/)

(2) TRIP (The Roaming INFN Physicist) è un progetto della CCR dell'INFN che ha lo scopo di fornire al personale INFN, un accesso alle reti wireless dell'INFN semplice e sicuro. La descrizione del progetto si trova in http://security.fi.infn.it/TRIP/ mentre altre informazioni si trovano in http://www.ccr.infn.it/

(3) LDAP: il protocolo LDAP e le sue estensioni sono descritti in una linga serie di RFC, alcuni relativi al "core", altri relativi alle estensioni.
LDAPv3 Core RFC:
LDAPv3 Technical Specification (RFC 3377)
LDAPv3 Protocol (RFC 2251)
LDAPv3 Attribute Syntax Definitions (RFC 2252)
LDAPv3 UTF-8 String Representation of Distinguished Names (RFC 2253)
LDAPv3 String Representation of LDAP Search Filters (RFC 2254)
LDAPv3 URL Format (RFC 2255)
A Summary of the X.500(96) User Schema for use with LDAPv3 (RFC 2256)
Authentication Methods for LDAP (RFC 2829)
LDAPv3 Extension for Transport Layer Security (RFC 2830)
IANA Considerations for LDAP (RFC 3383)
LDAPv3 Extension RFC:
LDAPv3 Use of Language Codes (RFC 2596)
LDAP v3 Server Side Sorting of Search Results (RFC 2891)
Storing Vendor Information in the LDAP root DSE (RFC 3045)
LDAP Password Modify Extended Operation (RFC 3062)
Named Subordinate References in LDAP (RFC 3296)

(4) Kerberos5: il protocollo Kerberos5 è descritto nell'RFC 1510

(5) X.509:
- [ITU-T Recommendation X.509][2] (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 08/05.
- "Internet X.509 Public Key Infrastructure: Certificate Management Protocols", RFC 2510, March 1999
- "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 4630.

(6) OpenLDAP: è una implementazione OpenSource di un Directory Server interrogabile via protocollo LDAP. Il sito web di riferimento è http://www.openldap.org/

(7) RADIUS (Remote Authentication Dial In User Service) è descritto nell' RFC 2865

(8) AFS (Andrew File System) è un filesystem distribuito, rilasciato in modalità OpenSource nel 2001. Il sito di riferimento è http://www.openafs.org/
(9) CASSiO (Cookie-based Authentication and Single-Sign-On) è una libreria di funzioni che permette alle applicazioni web di integrare molteplici sistemi di autenticazione. Sviluppato da Dael Maselli dell'INFN-LNF
(10) Shibboleth: http://shibboleth.internet2.edu/
(11) IDEM: http://www.idem.garr.it/index.php
(12) Fedora Directory Service: è la versione OpenSource di Red Hat Enterprise Directory Server.
Red Hat Directory Server Deployment Guide
Red Hat Directory Server Installation Guide
Red Hat Directory Server Configuration, Command and File Reference
Red Hat Directory Server Administrator's Guide
Red Hat Directory Server Schema Reference
(13) Heimdal: è una implementazione del protocollo Kerberos5. Il software è sviluppato presso il "Center for Parallele Computing" del Royal Institute of Technologies (KTH) svedese. Ilsito di riferimento è http://www.h5l.org/
(14) MIT Kerberos Consortium: http://www.kerberos.org/
(15) SSLv3: http://wp.netscape.com/eng/ssl3/
(16) TLSv1: RFC 2246
(17) SALS: RFC 4422
(18) GSS-API: RFC 2743
(19) GridShib: http://gridshib.globus.org/