Servizi Sistemistici, Sicurezza e Reti

Paola Tentoni
Servizi sistemistici e di rete

Abstract
L'articolo riporta esempi di servizi sistemistici CILEA per la gestione di sistemi o servizi complessi quali i DMS, per la loro integrazione con altre fonti informative aziendali e con i sistemi di autenticazione centralizzata, con riferimento anche ai problemi per la gestione della sicurezza come processo e delle reti in alta affidabilità.

This article describes CILEA's services for the management of complex systems (e.g. DMS) and for integrating these services with other informatics systems owned by customers and with central authentications Systems (CAS), indicating also solution for the security issues management and for high availability.

Keywords: Sistemi, DMS, Collaboration, Sicurezza ICT, CAS, Reti.

I Servizi sistemistici

Ogni realtà, per piccola che sia, ha ormai necessità di disporre di una rete locale, con accesso internet e sistemi informatici in grado di garantire, almeno, la condivisione organica d'informazioni e dati tra i gruppi di lavoro, il tutto inscindibile dalla gestione accurata delle autorizzazioni per l'accesso a tali informazioni.

Questo livello base, al crescere delle dimensioni e delle necessità organizzative, può spingere poi ad adottare anche strumenti molto complessi per la gestione documentale interna, non solo rivolti alla pura archiviazione, ma anche e soprattutto per l'automazione dei flussi documentali (*DMS - Document Management Systems*) [1] [2], o addirittura per la dematerializzazione dei documenti ufficiali, con problematiche di *conservazione* a norma di legge (protocollo informatico, firma digitale, conservazione sostitutiva).

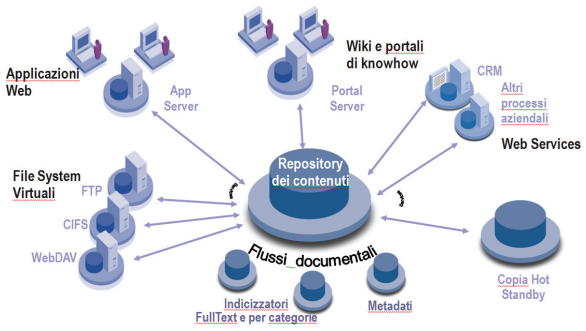

Fig. 1 – Esempio di "Piattaforma DMS"

Per questo motivo, l'informatizzazione di ogni ufficio, pubblico o privato, unita a un'agile comunicazione tra i gruppi interni o anche rivolta all'esterno, sono divenuti elementi imprescindibili per garantire elevati livelli di produttività e visibilità. Senza di essi non si può pensare, infatti, di competere efficacemente con i propri concorrenti in un mercato globale sempre più agguerrito e organizzato.

Quelli citati sono solo piccoli esempi che richiedono però grandi competenze da parte dei tecnici *ICT*, per l'adozione di soluzioni informatiche innovative, basate su piattaforme *Open Source* (predilette in campo accademico), o piuttosto proprietarie, per gli enti con minor capacità informatiche interne.

In questo caso non si parla più di semplici *"prodotti"* o *"pacchetti software"* ma di *"complesse piattaforme"* ben più articolate, spesso con ampie possibilità di programmazione e personalizzazione, che s'interfacciano e s'integrano, mediante *API*, con quanto già esistente in azienda, e con sistemi interni di autenticazione e autorizzazione basati su *SSO*, per evitare il proliferare di credenziali per i differenti applicativi.

Le necessità del mercato sono pertanto quelle di una robusta conoscenza dei sistemi operativi e software di base, con un riguardo speciale alla loro affidabilità: *High Availability*, *clustering*,

Disaster Recovery, sono richieste comuni alla gran parte dei servizi *ICT*.

Al sistema operativo si appoggiano poi i servizi applicativi in forma di *application server*, *web services* e sistemi di *backend* con *database relazionali* anche complessi.

CILEA con decenni di esperienza legati alla gestione diretta dell'*hardware*, del *software* di base e delle applicazioni, negli ambiti più vari e seguendone le evoluzioni nel tempo, offre anche oggi il proprio supporto sistemistico esperto, multipiattaforma, per chi vuole affidare in *outsourcing* completo o parziale i propri servizi o le proprie macchine o studiare soluzioni progettuali per specifiche esigenze.

Il supporto sistemistico di CILEA garantisce e offre ospitalità fisica, compresa di supporto sistemistico, *backup* centralizzato e controllo operativo. Lo stesso tipo di assistenza può essere attuato anche all'esterno della sede e presso il cliente, affiancando o sostituendo il personale tecnico di supporto del cliente.

In CILEA è attivo un complesso di circa sessanta *server* fisici, escludendo i nodi di super calcolo, alcuni dedicati a servizi di *Database Oracle* o *MSSQL* in *cluster*. Essi comprendono sia piattaforme *Intel*, sia *SUN*, alcune delle quali costituiscono nel loro insieme l'ambiente di virtualizzazione *VmWare* (otto nodi distribuiti in due *cluster* distinti) ospitanti circa 140 di *server* virtuali, tra produzione, sviluppo e collaudo.

Inoltre esiste un piccolo ambiente di virtualizzazione *SUN* basato su *M4000*, ospitante circa cinque *server* virtuali *Solaris* al proprio interno.

Tutti i server sono collocati nell'area protetta del *Data Center* (sala macchine) avente le seguenti particolari caratteristiche di sicurezza fisica e perimetrale:

- Accesso all'edificio sorvegliato h24.
- Ingresso alla sala server controllato da porta blindata con apertura a badge e telecamere di sorveglianza.
- Presidio tecnico operativo feriale dalle 7 alle 22.30 e sabato dalle 7.30 alle 13.30.
- Condizionamento costante (temperatura e umidità).
- Gruppo di continuità diesel e batterie tampone.
- Doppia linea di alimentazione ai rack.
- Servizi di *backup* centralizzato (robot e silos di cassette LTO4).
- Monitoraggio costante dei servizi, con allarmi automatici via mail/sms.
- Connettività internet con doppio provider (*GARR* e *InetBT*) per i servizi rivolti ad enti istituzionali.
- Controllo degli accessi ai server tramite firewall e *VPN*.
- Una *SAN* per l'accesso ai dati.

Le piattaforme operative, gli ambienti di virtualizzazione e i motori DB di cui CILEA ha esperienza diretta, alcuni dei quali con certificazione del fornitore, sono i seguenti:

- Sistemi Linux: Debian, Ubuntu, RedHat, CentOS
- SUN Solaris e container solaris
- Windows server 2003, 2008
- Virtualizzazione: VmWare Vsphere 4.x, ESX 3.x, MS HyperV.
- DB: Oracle, MSSQL, DB2, Postgres, MySQL.
- Sistemi di Disaster Recovery: Mirror MSSQL, DataGuard ORACLE, Mirror MySQL.

Oltre alla gestione delle piattaforme *hardware* e *software* di base, il gruppo sistemistico CILEA mette a disposizione tutta l'esperienza relativa alla personalizzazione e configurazione del *software* più strettamente applicativo, sia esso proprietario in ambiente *windows* o *open source* per ambienti *Linux*.

E' questo *software* che risponde alle citate esigenze di gestione del patrimonio e dei flussi documentali aziendali (piattaforme *DMS*), alla messaggistica interna ed esterna (email, liste di distribuzione, social forum, blog) e centralizzazione d'indirizzari, agende condivise, prenotazioni di risorse (*Collaboration Suite*) per facilitare la comunicazione e cooperazione dei gruppi di lavoro, secondo il paradigma dell'accesso sempre e ovunque (in mobilità), del risparmio del tempo e dei costi di trasferta.

La Sicurezza ICT

Sicurezza *ICT* significa non solo protezione fisica, garantita da un accesso controllato ai server e dal corredo di garanzie di continuità che abbiamo visto. Significa anche protezione logica, assicurata dalla configurazione opportuna di un insieme, complesso, di regole per l'accesso alle risorse *IP* e ai servizi: ci si affida innanzitutto ai *sistemi firewall* centralizzati o locali ai *server*, ma anche scadenze periodiche delle credenziali, controlli sui *log*, tassativi e

costanti aggiornamenti *software* e presenza di antivirus aggiornati.

CILEA ha da diversi anni sviluppato una collaborazione con il fornitore di una piattaforma di *firewall* (*StoneSoft*), del quale è divenuto partner [3].

La specificità di questa piattaforma era ed è rimasta quella di garantire l'alta affidabilità non solo attraverso configurazioni di *firewall* in *cluster*, ma anche fornendo la possibilità di bilanciare l'accesso ai servizi posti dietro al *firewall*, sia mediante *farm*, sia con architetture di doppio collegamento Internet. L'affidabilità è estesa anche alla possibilità di avere *VPN IPSEC multi-link*, a condizione di utilizzare lo stesso *software* di *firewall* ai due estremi della connessione.

Per alcuni servizi particolarmente critici commissionati dal MIUR (si veda Fig. 2), è stata adottata questa configurazione a doppio *provider* Internet, con presenza di *Disaster Recovery Site*, a garanzia della completa affidabilità dei servizi anche in relazione agli accessi da internet.

CILEA sta seguendo, inoltre, l'evoluzione delle piattaforme *firewall* verso il controllo di *IPv6*, che diverrà di estrema attualità nei prossimi anni, e verso le tecnologie cosiddette di "nuova generazione" (*next-generation*), che hanno come principio innovativo un diverso approccio nella definizione delle regole e nell'analisi, orientato al servizio, inteso come livello applicativo, non come coppia *porta/IP*. Inoltre ci si riferisce all'utente autenticato, sempre più mobile, non più identificato quindi solo dalla rete o reti *IP* di appartenenza.

Fa sempre parte della gestione del processo di sicurezza aziendale la fase d'identificazione e autorizzazione dell'utente che accede a una risorsa *ICT*. Questo processo ha richiesto una progressiva evoluzione verso sistemi centralizzati di gestione delle autorizzazioni, orientati a fornire funzioni di *SSO* verso tutti o quasi gli applicativi utilizzati.

Non esiste, infatti, solo il problema di "ricordare" le proprie credenziali nei diversi contesti applicativi, ma anche e soprattutto quello di "gestirle centralmente". Si deve garantire che ciascuno abbia accesso solo alle informazioni o dati che gli competono per il tempo previsto, mantenendo il controllo delle scadenze delle credenziali e della loro complessità, oltre alla verifica dei ruoli e della loro variazione nel corso della vita aziendale (in ottemperanza, ad esempio, alla legislazione sulla *privacy*).

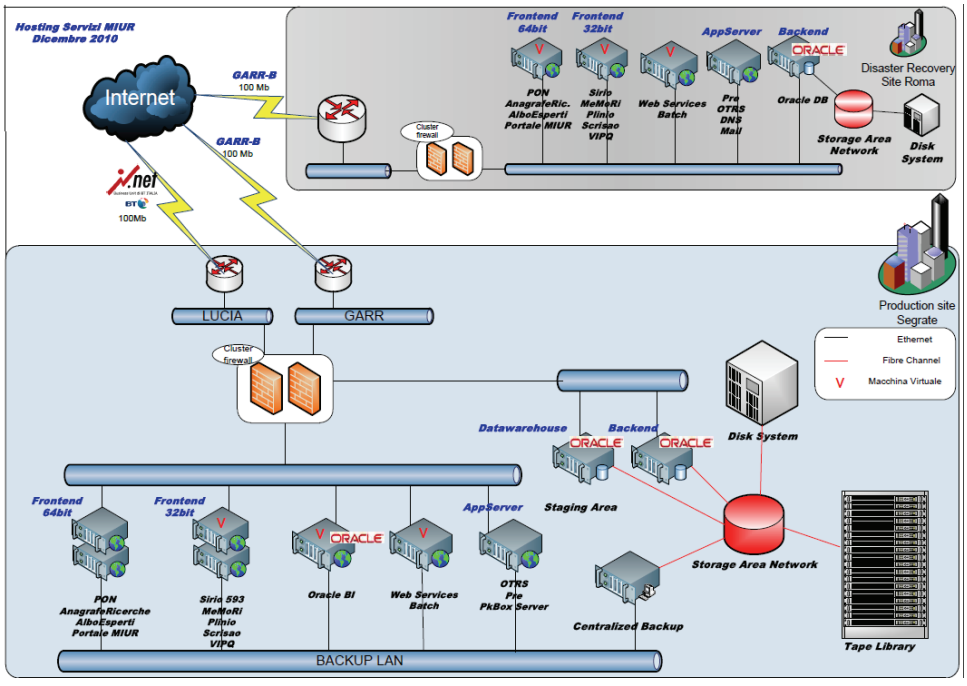

Fig. 2 – Architettura in alta affidabilità (con Disaster Recovery) e doppio provider Internet

Da qui la necessità per tutti gli enti di dotarsi di sistemi di *Directory* (*Open LDAP*, *Domini Active Directory*) per la catalogazione dei propri utenti interni, con l'interfacciamento di tali servizi verso sistemi di *SSO* (*CAS*, *Shibboleth*) e *identity provider* rappresentativi dell'ente e possibilmente inclusi in una federazione di respiro più ampio, come quella *GARR*, *progetto Idem*.

CILEA partecipa con un proprio *IdP* alla federazione, e offre anche servizi di *Service Provider* per l'accesso a proprie risorse. In quest'ottica fornisce supporto a chi volesse dotarsi di sistemi *IdP*, federandosi in *GARR-Idem*, o desiderasse integrare con *Shibboleth* le proprie applicazioni web, divenendo *service provider*. Analogamente è disponibile il supporto per la creazione di sistemi ridondati *Open LDAP*, o *Active Directory* per la gestione delle proprie utenze aziendali o studentesche.

Per quel che riguarda la legislazione sulla privacy, CILEA offre un sistema di raccolta per i *log* degli amministratori di sistema, con stoccaggio sui propri server di archiviazione (*DigA*), già attivo per conto di alcuni clienti esterni e multi piattaforma (*windows*, *linux*, *AS400*).

Le Reti

Anche l'infrastruttura di rete risente dei bisogni di affidabilità e performance, ancor più di servizi e server, essendo, di fatto, l'elemento su cui si basa l'utilizzo di qualunque strumento *ICT* e di comunicazione interna ed esterna (si pensi alla *telefonia VoIP*).

Dunque l'accesso alla rete interna (*LAN*, *WLAN*), le sue performance e *tuning*, e la connettività esterna sono indispensabili per qualsiasi attività lavorativa.

Le tecnologie di *networking* tengono conto, già da molti anni, del ruolo fondamentale dell'affidabilità e hanno fornito meccanismi di ridondanza a qualsiasi livello: *link*, apparati attivi, *slot* interni e alimentatori, *firewall in cluster*. Ovviamente queste tecnologie si portano dietro complicazioni architetturali e necessità di conoscenze sempre maggiori e articolate, soprattutto per la diagnosi dei problemi o per il *tuning*.

Un altro elemento che diviene importante e non opzionale, è quello del controllo automatico della rete e dei flussi circolanti, proprio per far fronte, in caso di necessità, a emergenze e rapide localizzazioni, correzioni o riparazioni di elementi mal funzionanti e/o disconnessi. Le stesse tecniche di diagnosi e analisi si possono utilizzare, in taluni casi, per opporsi ad attacchi informatici.

Anche in questi casi CILEA offre la sua esperienza sia in tema di configurazioni per l'alta affidabilità delle reti, sia per il *monitoring* dei flussi e dei suoi apparati.

Infine un elemento spesso trascurato, ma che ha particolare importanza per ambiti ove si custodiscano dati sensibili oltre che personali, è quello del controllo, mediante *security assessment* [4], da parte di terzi neutrali, dell'efficacia delle misure di sicurezza messe in campo a protezione di tali dati.

CILEA ha, infine, esperienza anche nell'esecuzione di *audit di sicurezza* [5], consigliati per confrontarsi con una valutazione esterna del rischio informatico. Per l'analisi ci si avvale di scansioni automatizzate delle vulnerabilità [6], ma anche di tecniche di analisi manuali per la ricerca di possibili debolezze, oltre che di interviste al personale ed esame dettagliato delle configurazioni dei singoli *server*. CILEA svolge tale attività, su richiesta, producendo una reportistica tecnica filtrata opportunamente dai falsi positivi. È parte della reportistica prodotta anche un *executive summary*, che riepiloga i risultati dell'analisi in forma chiara anche per personale meno tecnico.

Infine la discussione finale, insieme al cliente, è volta a verificare la comprensione del rischio e delle singole azioni di rimedio suggerite.

Bibliografia

[1] URL: http://www.siriusit.co.uk/siriuslabs/0-5-aug-2009/sharepoint-vs-alfresco-vs-nuxeo
[2] URL: A DMS Definition http://en.wikipedia.org/wiki/Document_management_system
[3] URL: http://www.stonesoft.com
[4] URL: Security Assessment definition http://en.wikipedia.org/wiki/Information_Technology_Security_Assessment
[5] URL: http://www.isecom.org/osstmm/, Open Source Security Testing Methodology Manual
[6] URL: SANS institute http://www.sans.org/security-resources/policies/Policy_Primer.pdf