Capitolato tecnico

Acquisizione di un servizio specialistico per la progettazione, migrazione e reingegnerizzazione della Server Farm della R.U. “Cyber Intelligence” dello IIT, mediante transizione da ambiente VMware ESXi a cluster Proxmox, comprensivo di reinstallazione dei server fisici, migrazione dei servizi e dei dati, documentazione tecnica e trasferimento di competenze, per la durata di – 12 mesi CIG …… – Importo € 30.000,00 non era 20000?(oltre IVA se dovuta).

Obiettivo del contratto

Creare un nuovo cluster proxmox reinstallando server esistenti migrandovi progressivamente i servizi o i dati ritenuti più rilevanti per le attività di ricerca, al fine di armonizzare la piattaforma tecnologica con quella adottata dalle altre unità di ricerca e tecnologiche dello IIT. Al termine del processo di migrazione, la nuova server farm sarà formalmente presa in carico per la gestione sistemistica dal personale dell'Istituto IIT.

Descrizione server farm

La server farm attuale comprende 7 server fisici alloggiati nei rack del datacenter IIT e virtualizzati principalmente con tecnologia vmware; ospitano circa 110 macchine virtuali, per la maggior parte linux Ubuntu, ma ve ne sono anche CentOS, Fedora, bsd e windows; la farm è articolata su più reti interne (fisiche e virtuali) il cui traffico è mediato da vps che agiscono come firewall/transparent firewall e reverse proxy; i servizi interni comprendono nfs (freenas), dns (bind), gestione centralizzata utenze (freeipa), monitoraggio (nagios), backup (ghettoVCB), svn, git e server openvpn; la farm eroga servizi ai ricercatori sia di tipo tradizionale (es. vm dedicate, web server, db sql) che BigData (es. elasticserch/kibana, spark/hadoop) ed in generale supporta la sperimentazione ed adozione di strumenti innovativi.

Descrizione HW

La farm si articola su 7 server fisici, le cui caratteristiche sono descritte di seguito:

server	Model	core	ram	storage	ssd
wafivm5	Dell R415	12	128GB	2TB	-
wafivm6	Dell R430	16	192GB	4TB	1TB
wafivm7	Fujitsu RX2530M2	24	256GB	6TB	1TB
wafivm8	Dell R430	20	256GB	8TB	-
wafivm9	Dell R430	20	256GB	8TB	512GB
freenas3	HP DL380 G5	4	24GB	32TB	-
freenas5	Supermicro	8	8GB	20TB	-

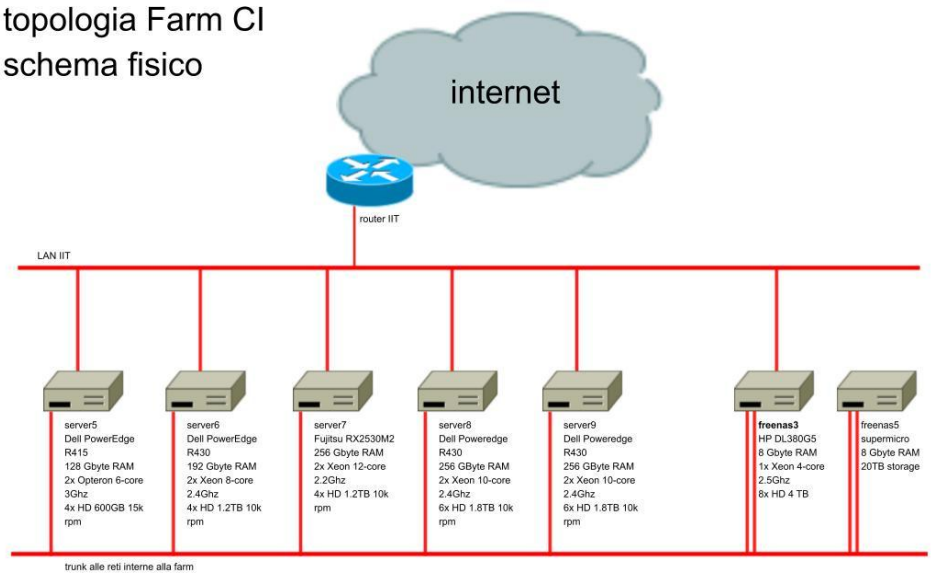
E' inoltre presente uno switch netgear XS716E collegato in trunk con i server.

Sui server sono installate le seguenti versioni di OS:

server	**Versione OS**
wafivm5	Esxi 5.5
wafivm6	Esxi 6.0
wafivm7	Esxi 6.0
wafivm8	Esxi 6.0
wafivm9	Esxi 6.5
freenas3	truenas 13
freenas5	truenas 13

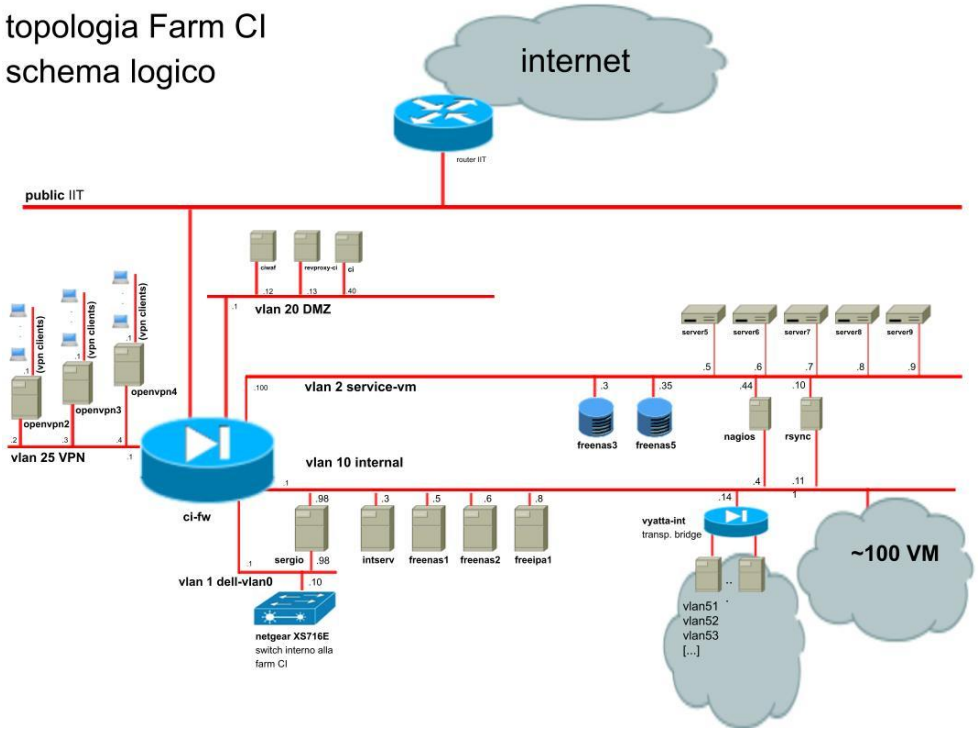
Topologia di rete

Lo schema fisico della rete della farm è riportato di seguito:



Ciascuno dei server vmware ha una interfaccia fisica attestata su rete pubblica (su switch gestiti da terzi) ed una o due interfacce fisiche collegate in trunk allo switch interno della farm.

Sui server vmware è configurata una topologia di rete logica basata su numerose vlan configurate in modo opportuno anche sullo switch interno, in modo da ottenere lo schema logico di rete descritto di seguito:



La comunicazione fra le vlan è mediata da istanze di VM vyatta.

Servizi interni

Di seguito sono descritti i principali servizi interni alla farm:

servizio	descrizione
Sso	gestione utenze personali basata su freeipa 4, per accessi ssh, vpn e web
Vpn	accessi vpn con permessi differenziati, basati su openvpn 2
Ssh	accessi ssh tramite bastion host in dmz
Git	servizio git interni, basato su gitlab ce 11
Nfs	servizio interno nfs ridondato su due vps con freenas 8
Backup	backup delle vm effettuato da esxi su nfs, basato su ghettovcb 2017 e su sistema custom di rotazione dei backups
monitoring	monitoring di oltre 400 servizi interni distribuiti su oltre 100 vm, basato su nagios 3
Firewall	la comunicazione fra vlan è mediata da più istanze di firewall/transparent firewall, basate su vyos 1.2 con configurazione da linea di comando
Waf	web application firewall implementato tramite reverse proxy e basato su apache2 e modproxy/modsecurity
siti web	l'infrastruttura ospita decine di siti web accessibili anche da internet e gestiti anche tramite virtual hosting su varie vm
db sql	l'infrastruttura ospita numerose istanza di db sql, principalmente mysql/mariadb in varie versioni
Elastic	l'infrastruttura ospita numerose istanze di elasticsearch/kibana, principalmente versione 7/8

La farm si articola su oltre 50 macchine virtuali, principalmente linux, che supportano le attivita' di ricerca della Research Unite Cyber Intelligence.

Descrizione servizio richiesto

Il gruppo di ricerca utilizza una server farm basata su vmware esxi, con hw e sw piuttosto obsoleto.
Il servizio richiesto ha l'obiettivo di reinstallare i server che saranno via via liberati creando un cluster proxmox sul quale saranno migrati progressivamente i servizi o i dati ritenuti più rilevanti per le attività di ricerca. La nuova server farm ricreata in logica proxmox sarà presa in carico per la gestione sistemistica dal personale dell'Istituto IIT.

Attività di migrazione verso Proxmox

Il fornitore dovrà operare in coordinamento con l'unità tecnologica CCN per definire l'architettura cui tendere. Successivamente, il fornitore è tenuto a procedere autonomamente alla valutazione preliminare, alla predisposizione di un piano operativo dettagliato e alla conseguente esecuzione delle attività di migrazione, che dovranno comprendere almeno le seguenti operazioni:

- censire le macchine virtuali ed i servizi presenti in ambiente vmware esxi
- definire le modalità di migrazione dei servizi o dei dati sul nuovo cluster proxmox

- reinstallare via via i server fisici che saranno liberati inserendoli nel nuovo cluster proxmox, tenendo conto delle caratteristiche dell'hw disponibile
- migrare progressivamente i servizi od i dati nel nuovo cluster proxmox
- verificare la funzionalità dei servizi migrati

Coordinamento e trasferimento conoscenze

Il fornitore dovrà:

- collaborare tecnicamente con il personale dello IIT durante tutte le fasi operative
- documentare sia in forma sinteticamente che in forma dettagliata, la nuova architettura HW/SW
- supportare il trasferimento delle conoscenze operative specifiche del nuovo cluster proxmox verso altri sysadmin.

Sulla infrastruttura da migrare sono presenti dati personali pubblici utilizzati per fini di ricerca, pertanto sarà necessario nominare un Responsabile Esterno del Trattamento, limitatamente ai compiti necessari per la migrazione dei servizi.

Criteri di valutazione dell'offerta tecnica

L'offerta tecnica presentata dovrà comprendere la descrizione:

- delle competenze ed organizzazione del team proposto
- delle modalità di presa in carico
- delle modalità di gestione del servizio
- del piano di miglioramento proposto per l'infrastruttura

L'offerta dovrà includere adeguata descrizione dell'esperienza maturata dal soggetto proponente e degli skill del team proposto per la gestione del servizio, che dovranno soddisfare i requisiti minimi di competenza previsti all'interno della sezione "Competenze minime richieste".

Caratteristiche tecniche minime

Si evidenziano le caratteristiche tecniche minime obbligatorie che devono essere trattate, a pena di esclusione, nella stesura della relazione tecnica:

#	Macro requisito	#	Dettaglio
RM1	qualità dei servizi professionali	RM1.1	esperienza di almeno 3 anni nella gestione di apparati HW in ambito datacenter
		RM1.2	esperienza di almeno 3 anni nella progettazione di architetture ICT complesse, integrazione di sistemi e documentazione
		RM1.	esperienza di almeno 3 anni nella gestione

		3	sistemistica e applicativa in ambito datacenter
		RM1.4	esperienza di almeno 3 anni nella gestione di ambienti virtualizzati in tecnologia vmware e proxmox
		RM1.5	esperienza di almeno 2 anni nella integrazione e gestione di ambienti in tecnologia Docker
		RM1.6	esperienza di almeno 2 anni nella gestione di tecnologie BigData ed in particolare di elasticsearch
RM2	sicurezza informatica e privacy	RM2.1	esperienza di almeno 3 anni nella gestione della sicurezza informatica in ambito datacenter e nel rispetto della normativa privacy vigente
RM3	esperienza in ambito ricerca ICT	RM3.1	esperienza di almeno 3 anni nella gestione di datacenter a supporto di attività di ricerca ICT
RM4	Competenze tecniche del team di lavoro	RM4.1	Vedi il paragrafo “Competenze minime richieste dei componenti del team di lavoro” all’interno dei Livelli di servizio

Modalità di erogazione

Il servizio di migrazione si intende erogato di norma da remoto via internet, tranne nelle occasioni in cui sia necessario o preferibile intervenire on-site; anche le interazioni con il gruppo di ricerca si intendono effettuate di norma da remoto, sfruttando strumenti di collaborazione e di teamworking online adottati dal gruppo
Gli strumenti di produttività individuale usati dal fornitore non saranno forniti dall’IIT, e non saranno riconosciuti costi aggiuntivi per eventuali interventi in sede.

Competenze minime richieste

Il Gruppo di Lavoro (GdL) dovrà comprendere persone che siano in grado di svolgere le attività previste nel presente capitolato e nell’offerta dell’aggiudicatario con la massima professionalità.

Il GdL dovrà essere composto almeno dalle seguenti professionalità con i seguenti livelli minimi di competenze di base:
- Il Gruppo di Lavoro (GdL) dovrà essere composto da persone dotate delle competenze individuate nel proseguo del paragrafo;
- I componenti del GdL potranno far parte dell’organico aziendale oppure essere collaboratori incaricati all’uopo, nei tempi e nei modi ritenuti opportuni dall’Aggiudicatario. In nessun caso potranno formarsi e derivare a carico del CNR oneri aggiuntivi di qualsiasi natura come conseguenza di azioni intraprese dall’Aggiudicatario per la realizzazione del servizio, ivi comprese le eventuali azioni per la formazione dei rapporti di collaborazione professionale con i componenti del gruppo di lavoro; la presentazione dei curricula dei componenti del GDL è obbligatoria e dovrà essere fornita prima della stipula del contratto.
- Prima della stipula del contratto l’operatore economico deve indicare il/i professionista/i che designati allo svolgimento dell’attività e dovranno fornire i loro CV e tutta la documentazione comprovante il

possesso dei requisiti dichiarati. La struttura appaltante si riserva di visionare e appurare le competenze dichiarate anche attraverso colloquio diretto con i designati.
- Il gruppo di lavoro presentato in sede di offerta tecnica non potrà essere modificato nei suoi componenti durante la fase di esecuzione del contratto senza la previa approvazione della stazione appaltante;
- I nuovi componenti che sostituiscono dovranno, in ogni caso, possedere requisiti o esperienza professionale equivalenti o superiori a quelli delle persone sostituite, da comprovare mediante l'esibizione di curricula adeguati;
- Il gruppo di lavoro dovrà essere composto da max. 3 professionisti. Sarà attribuito un punteggio preferenziale (come descritto all'interno della griglia dei criteri di valutazione al punto C4.2) agli operatori economici che offriranno il servizio attraverso la messa a disposizione di un unico professionista in maniera continuativa per tutta la durata di copertura del servizio, il quale avrà le competenze necessarie a garantire l'effettuazione dell'intero servizio a regola d'arte; si ritiene infatti, che tale fattispecie garantisca una maggiore efficacia e continuità nel tempo del servizio offerto. Il professionista unico individuato per l'espletamento dell'intero servizio dovrà possedere le skills minime individuate per ciascuno dei tre profili di seguito descritti.

Segue la composizione del gruppo di lavoro, con le relative skills minime richieste per ciascun profilo:

- Un responsabile di progetto, con i requisiti riportati in tabella:

Responsabile di progetto	
Titolo di Studio	Laurea in Ingegneria Informatica o Informatica o Scienze dell'Informazione
Esperienze Lavorative	• Almeno 3 di provata esperienza lavorativa nella conduzione di progetti complessi in ambito ICT • Almeno 5 anni di provata esperienza nella gestione di Operations ICT
Conoscenze	• Conoscenze ed uso di tecniche e prodotti SW per project management • Redazione di specifiche di progetto, stima di risorse e tempistiche • Analisi e progettazione, testing e documentazione di sistemi informativi

- Un amministratore di sistema senior, con i requisiti riportati in tabella:

Responsabile tecnico	
Titolo di Studio	Laurea in Ingegneria Informatica o Informatica o Scienze dell'Informazione

Esperienze Lavorative	• Minimo 5 anni di esperienza nelle ICT Operations in ambito datacenter • Minimo 5 anni di esperienza nella realizzazione di sistemi informativi • Analisi, progettazione ed integrazione di sistemi informativi • Partecipazione a gruppi di lavoro nell'ambito di progetti internazionali • Redazione di specifiche di progetto • Installazione e configurazione di macchine virtuali linux in datacenter virtualizzati con tecnologia vmware • Progettazione e gestione di architetture di rete fisiche e virtualizzate • Installazione e configurazione di middleware • Integrazione di prodotti e/o componenti • Redazione documentazione di progetto a supporto delle Operations • Esperienza ed attitudine al troubleshooting ed al problem solving • Autonomia nell'individuare, pianificare e progettare adeguamenti tecnologici infrastrutturali • partecipazione alla definizione delle misure di sicurezza e successiva implementazione in ambito datacenter
Conoscenze	• installazione, configurazione ed amministrazione di HW (server ed apparati di rete) in ambito datacenter • amministrazione ambienti virtualizzati in tecnologia vmware e proxmox • amministrazione sistemi linux (principalmente ubuntu) • amministrazione apparati di rete • amministrazione firewall/transparent firewall vyatta • amministrazione web application firewall basati su apache2/nginx • amministrazione database sql • amministrazione ambienti e middleware BigData, in particolare elasticsearch/kibana • amministrazione sistemi di SSO (freeipa) • amministrazione sistemi di monitoring (nagios) • amministrazione server vpn (openvpn) • amministrazione sistemi di backup vmware (ghettoVcb) • amministrazione di sistemi di revisione del codice (svn/git) • integrazione sistemi • amministrazione ambienti a microservizi (swarm docker)

- Un esperto in sicurezza informatica con conoscenza delle problematiche relative alla normativa Privacy, con i requisiti riportati in tabella:

Esperto in sicurezza informatica	
Titolo di Studio	Laurea in Ingegneria Informatica o Informatica o Scienze dell'Informazione
Esperienze Lavorative	• Almeno 5 anni di esperienza lavorativa nel settore della sicurezza informatica in ambito datacenter • analisi dei rischi legati alla sicurezza informatica e stesura di proposte per la loro mitigazione • supporto alle operations ICT su aspetti di sicurezza in ambito datacenter • gestione di incidenti ICT • analisi delle problematiche legate al rispetto della normativa Privacy e

	individuazione di soluzioni per garantirne il rispetto contenendo i costi ed l'impatto sulla produttivita' • almeno 2 anni di esperienza nel supporto a progetti di ricerca ICT, anche in ambito internazionale
Conoscenze	è gradita la certificazione CISSP in corso di validità o conoscenze equivalenti sui seguenti ambiti, declinate nell'ambito di Operations e progetti ICT: • Security and Risk Management • Asset Security • Security Architecture and Engineering • Communications and Network Security • Identity and Access Management • Security Assessment and Testing • Security Operations • Software Development Security

Per tutto il personale che costituisce il Gdl dovranno essere forniti i curricula che attestano il possesso dei requisiti precedentemente specificati.

Termini e luogo di consegna ed installazione

I termini di consegna dei servizi, sono da intendersi in giorni naturali e consecutivi decorrenti dal giorno successivo alla sottoscrizione del contratto.
La consegna e l'installazione dei beni e servizi della fornitura dovrà essere effettuata presso l'indirizzo indicato in tabella, in accordo con il Direttore esecutivo del Contratto:

# Prodotto	Luogo di consegna e installazione
	Istituto di Informatica e Telematica del Cnr di Pisa, via G. Moruzzi 1, 56124 Pisa

Valutazione delle proposte

La valutazione delle proposte terrà conto dei seguenti elementi migliorativi

- N d anni di esperienza nella gestione sistemistica ed applicativa in ambito datacenter
- possesso della certificazione CISSP in corso di validità
- N d anni di esperienza in attività progettuali riservate con LEA (Law Enforcement Agencies) o DIS
- N d anni di esperienza della gestione di datacenter a supporto di attività di ricerca ICT
- organizzazione del team per la fornitura del servizio. Sarà ritenuto elemento preferenziale la messa a disposizione di un solo referente che abbia competenze sufficienti per garantire il servizio

Non saranno prese in considerazione le proposte che non rispettano le richieste tecniche indicate ai paragrafi precedenti