

System Management

Riccardo Biella, Elia Perrone, Nicolas Sala, Kevin Dominguez

Semestre primaverile 2019

1 Esercitazione 01

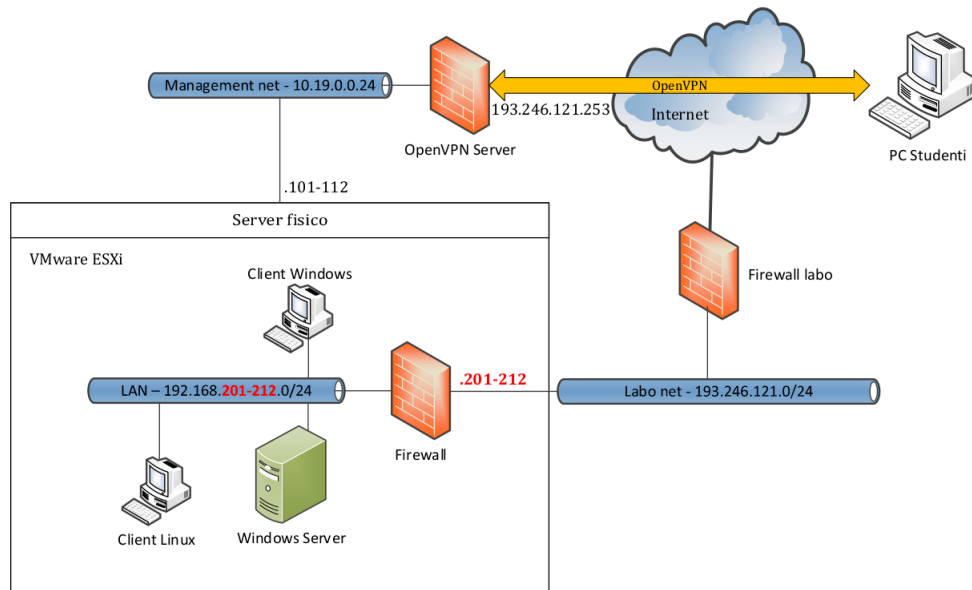


Figure 1: Schema di rete base

1.1 Specifiche del server utilizzato (Gateway GW2000h-GW170hq F1)

Il server utilizzato per le esercitazioni può contenere fino a quattro nodi, con le seguenti caratteristiche:

Mainboard	Processor type	Up to 2 Intel® Xeon® processors 5500/5600 series		
	Available processor with core and cache	Intel® Xeon® processor (Six-core) <ul style="list-style-type: none">• X5670/X5660/X5650/L5640: 12 MB L3 (Quad-core) <ul style="list-style-type: none">• E5640/E5630/E5620/X5667/L5630/L5609: 12 MB L3• X5570/X5560/X5550/E5540/E5530/E5520/L5530/L5520: 8 MB L3• E5507/E5506/E5504/L5506: 4 MB L3 (Dual-core) <ul style="list-style-type: none">• E5502: 4 MB L3		
	Chipset	Intel® 5520/5500 chipset		
	Graphics	BMC embedded: <ul style="list-style-type: none">• 16 MB video memory		
	Memory ¹	12 x 1333/1066 MHz DDR3 registered/unbuffered ECC memory Registered DIMM size: 1/2/4/8 GB <ul style="list-style-type: none">• Up to 96 GB registered DDR3 1333/1066 DIMMs when populated, 12 slots Unbuffered DIMM size: 1/2/4 GB <ul style="list-style-type: none">• Up to 48 GB unbuffered DDR3 1333/1066 DIMMs when populated, 12 slots		
	Expansion slots	PCIe ² x16 slot, supporting standard low-profile PCIe ² cards		
Security and service features	Onboard ports	Rear: <ul style="list-style-type: none">• 2 x Gigabit LAN ports (RJ-45)• Management port (RJ-45)• ID LED button• Optional DDR or QDR InfiniBand³ port³ Internal: <ul style="list-style-type: none">• 2 x 5-pin Intel® FPIO USB pin header for USB disk module		
	RAID ⁴	Integrated Intel® ICH10R Serial ATA host controller (6 x 3 Gb/s SATA ports) with RAID 0, 1, 5, support		
	LAN controller	Intel® 82574L dual-port Gigabit Ethernet controller		
		HDD mechanical lock	Administrator/user password	Device boot control
Subsystem availability	Power supply	2 x 1400 W 80 PLUS® Gold-level efficient easy-swap power supply (hot-pluggable)		
	System cooling	2 x CPU heat sinks, supporting Intel® Xeon® processors with up to TDP 95 W 4 x system fans with PWM control		
	Storage	Maximum capacity: Up to 6 TB (3 x 3.5" 2 TB SATA HDDs) 3.5" HDD capacity: 250/500/750 GB, 1 / 2 TB		
Chassis	Form factor	2U rack-mountable chassis, supporting 3 node configurations: GW170h F1, GW170hd F1 and GW170hq F1		
	Maximum nodes per chassis:	4		
	Dimensions	438 (W) x 724 (D) x 88 (H) mm (17.2 x 28.5 x 3.4 inches)		
OS support	Weight	35 kg (77 lbs.) maximum (all component slots and sockets fully populated) 30.9 kg (68 lbs.) minimum (HDD, power supply, processor installed)		
		Windows Server® 2008	Novell® SUSE® Linux® Enterprise Server 11	
		Windows Server® 2008 R2	Red Hat® Enterprise Linux® 5.4	
Server management utilities and applications		Windows Server® 2003	VMware ESXi® 4	
			VMware ESX® 4	
		Gateway Smart Console	BIOS update tool	
Warranty		Gateway Smart Server Manager	ID LED button	
		Gateway Smart Setup	Integrated Management Log	
			IPMI firmware update tool	
Regulatory compliance		3-year standard warranty or choose extended warranties and services ⁵		
	Emissions classification (EMC)	CE (Class A)		
	Industry standard compliance / safety	CB Nemko/GS		

1.2 Hardware utilizzato

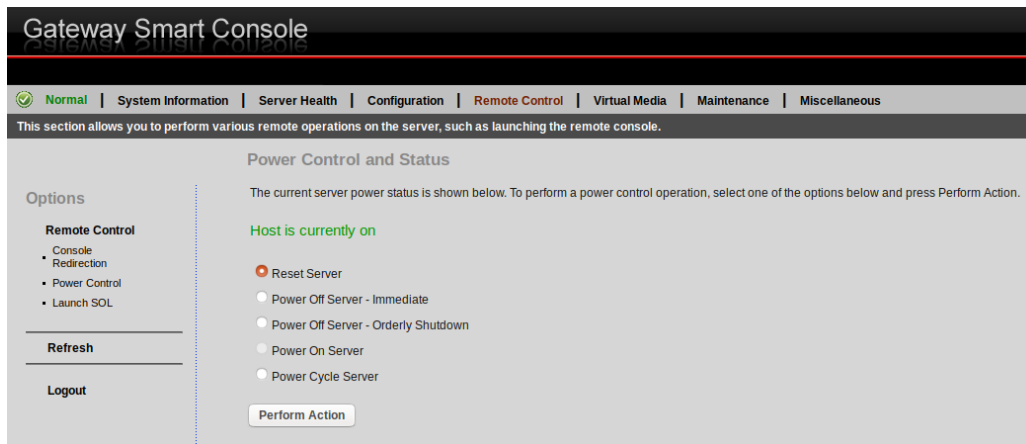
Ad ogni gruppo è stata assegnata la gestione di un nodo all'interno del rack, esso dispone di un disco rigido, un SSD ed una periferica USB mediante il quale sarà possibile installare un hypervisor sul server.

1.3 Interfaccia di gestione

La interfaccia di management del server, permette la gestione di numerosi aspetti della macchina, tra cui il controllo remoto, che utilizzeremo per lavorare sul server senza essere fisicamente presenti in laboratorio. L'interfaccia di gestione è raggiungibile all'indirizzo IP: 10.19.0.106, a seguito di una connessione tramite client vpn, con le credenziali seguenti:

username: grp6

password: System3m.Man_grp6



1.4 OpenVPN

1.4.1 Obiettivo

Connettersi tramite OpenVPN ed esplorare l'interfaccia di gestione del proprio server (10.19.0.101-112) (user: root password: superuser) e documentare azioni e informazioni disponibili. (Gli account OpenVPN sono gestiti dal docente, che distribuisce ad ogni gruppo un certificato personalizzato da importare nel proprio OpenVPN client – esempio di nome di un certificato: SystemManagement-udp-1194-grp5.ovpn e SystemManagement-udp-1194-grp5.p12).

1.4.2 Installazione OpenVPN - Ubuntu x64

1. apt-get install openvpn
Installiamo openvpn sulla nostra macchina
2. openvpn --version
Verifichiamo che l'installazione sia andata a buon fine
3. openvpn --config client.ovpn
Ci posizioniamo nella cartella (unzippata) che abbiamo scaricato da ICorsi, avviamo il client con il certificato corretto (.ovpn) che ci è stato fornito.

1.4.3 Problematiche

Il server mette a disposizione una finestra con la quale è possibile lavorare in modalità grafica stile desktop remoto. Tale applicazione fa scaricare un file .JNLP dal server (lanciando il controllo remoto dalla console di gestione). Qualora il certificato di sicurezza fosse scaduto, si dovrà procedere a creare il trust al server nella macchina client (che altrimenti ne blocca l'esecuzione): aggiungere l'IP del server nelle Exception Site List di Java. Utilizzando OpenJDK non è possibile sfruttare l'interfaccia grafica di gestione, per questo motivo abbiamo dovuto installare Oracle JRE.

1.5 VMware ESXi

1.5.1 Descrizione

VMware ESX Server è un prodotto per la virtualizzazione di livello enterprise offerto da VMware Inc., sussidiaria di Dell Technologies e ancor prima una divisione di EMC Corporation. ESX Server è un componente di un'offerta VMware più grande, VMware Infrastructure, che aggiunge servizi di amministrazione e di affidabilità al prodotto base.

1.5.2 Architettura

Il server ESX include un microkernel che si interfaccia direttamente con la macchina. Nelle versioni ESX 3 e precedenti all'avvio viene lanciato un kernel Linux (una versione modificata di Red Hat Enterprise Linux) che analizza l'hardware della macchina e alcuni componenti di gestione, per poi cedere il controllo al componente vmkernel sviluppato di VMware. Questo è un microkernel con tre interfacce verso l'esterno:

1. hardware
2. sistema guest
3. servizio console (servizio di gestione delle macchine virtuale che gira sul kernel che ha fatto partire vmkernel)

1.5.3 Installazione di VMWare

Dopo esserci collegati all'interfaccia di gestione della macchina, sulla scheda abbiamo Remot Control abbiamo scaricato il file .JNLP ed attraverso la sua esecuzione abbiamo installato l'ipervisor: abbiamo settato un Ip statico pubblico in modo da non dover accedere ogni volta tramite VPN. Abbiamo utilizzato per installare VMWare una chiavette collegata direttamente al server.

1.5.4 Altre opzioni di virtualizzazione

1. VirtualBox (Linux/Mac/Windows)
2. Parallels (Linux/Mac/Windows)
3. QEMU (Linux)
4. Windows Virtual PC (Windows)

2 Esercitazione 02

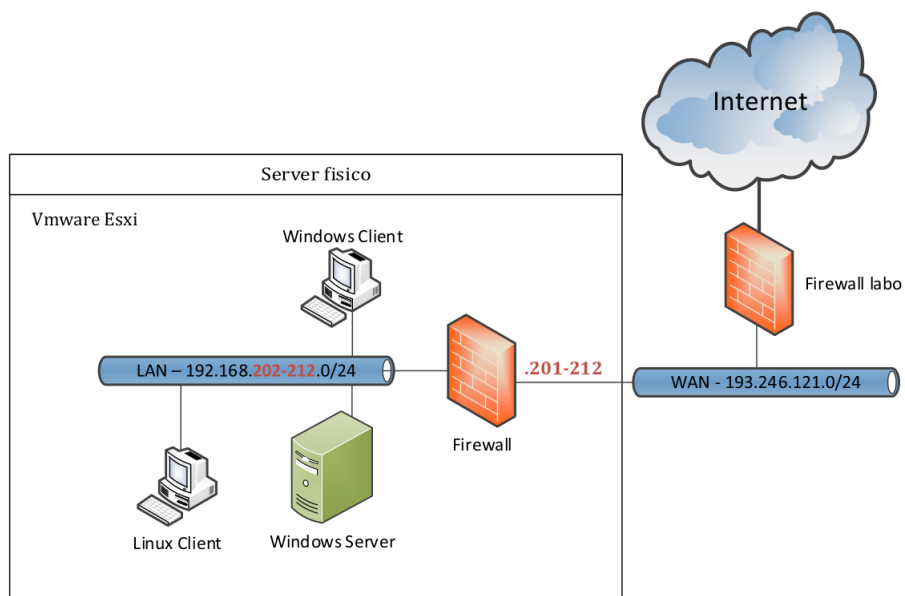


Figure 2: Schema di rete base

Sulla scheda virtual machine dell'interfaccia pubblica del server abbiamo cliccato su Create / Register VM per uplodare un'immagine di una nuova macchina virtuale

Abbiamo caricato:
kali Linux
Windows server 2012
Windows 10 x64

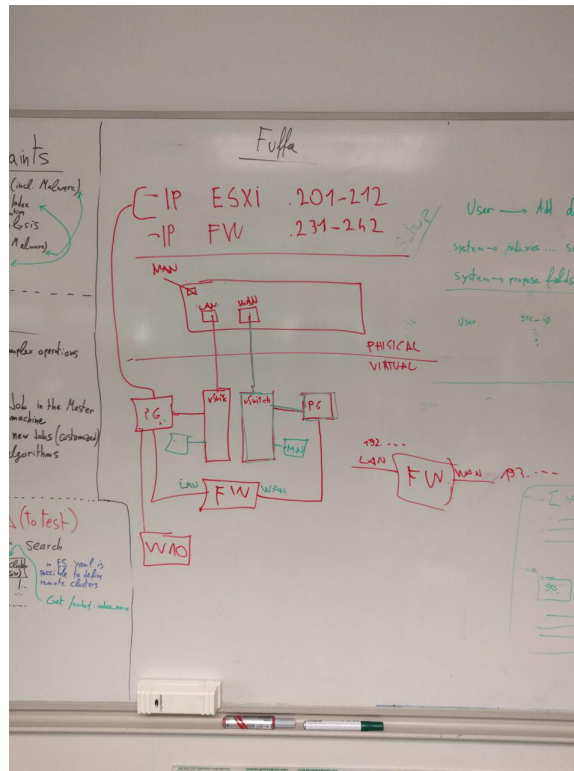


Figure 3: Schema di rete esercitazione 2

Nella foto possiamo osservare un virtual switch (quello verde) collegato ad un port group(verde) che sono quelli che abbiamo già, l'obiettivo dell'esercitazione è quello di creare un'altro virtual switch collegato all'interfaccia LAN e creare un port group nuovo collegato al nuovo virtual switch. I port group non sono altro che un'astrazione ad un livello più alto degli switch, su di essi possono risiedere le VLAN. Dobbiamo installare prima delle macchine anche un firewall che sarà collegato ai port group con due interfacce, una LAN e una WAN (è pubblica). Le macchine saranno poi collegate al nostro nuovo port group. Il firewall deve avere IP 236. Le nuove macchine installate verranno collegate al nuovo port group. Sul firewall bisogna installare un client VPN. L'obiettivo finale dell'esercitazione è quello di virtualizzare l'intera rete collegata alle interfacce LAN e WAN del server. Come ultimo passaggio dobbiamo spostare l'interfaccia di gestione di ESXi all'interno della rete (LAN).

2.1 Firewall utilizzato

pfSense è una distribuzione software open source basata su FreeBSD adatta per essere utilizzata come firewall/router. Ha lo scopo di fornire un firewall potente, sicuro e completamente configurabile utilizzando l'hardware di un comune PC. Nel cuore del sistema c'è FreeBSD e il firewall PF (Packet Filter) in prestito da OpenBSD da cui deriva appunto il suo nome, che ha il significato di "dare maggior senso per l'utente finale a PF".

Possiede le funzionalità basilari di un firewall di qualità:

2.1.1 Funzionalità

- Stateful Firewall con controllo granulare e possibilità di funzionare in maniera trasparente al layer 2 (in bridging)
- Network address translation
- HA (High Availability): grazie a CARP permette di configurare due firewall su due macchine identiche per replicarsi e autosostituirsi nel caso di guasto di una delle due (il software pfsync si occupa di

replicare lo stato firewall, la tabella delle connessioni e le regole del firewall, permettendo di passare al secondo firewall senza che le connessioni attive di rete cadano)

- Load Balancing: bilanciamento del carico di lavoro tra due o più server che si trovano dietro a pfSense (utilizzato normalmente per web server, mail server, ecc.)
- VPN server, su protocolli IPsec, OpenVPN e PPTP.
- PPPoE server
- Grafici RRD ed informazioni sullo stato in tempo reale.
- Captive portal
- Gestione uPnP e DNS dinamici

Grazie all'aggiunta di ulteriori moduli è possibile estendere le funzionalità di base ed integrarne di evolute come web proxying (con Squid), url filtering (Squidguard, DansGuardian), IDS (Snort) , antivirus (HAVP) ed altre ancora, fino alla gestione di messaggistica VoIP con FreeSWITCH.

Funzionalità	Windows Server 2012 Foundation	Windows Server 2012 Essentials	Windows Server 2012 Standard	Windows Server 2012 Datacenter
Active Directory Certificate Services	Solo autorità di certificato	Solo autorità di certificato ^(nota 4)	Si	Si
Active Directory Domain Services	Deve essere radice di foresta e dominio	Deve essere radice di foresta e dominio	Si	Si
Active Directory Federation Services	Si ⁽⁴⁷⁾	No	Si	Si
Active Directory Lightweight Directory Services	Si	Si	Si	Si
Active Directory Rights Management Services	Si	Si	Si	Si
Hyper-V	No	No	Si	Si
Modalità Server Core	No	No	Si	Si
Ruolo DHCP	Si	Si	Si	Si
Ruolo di server d'applicazioni	Si	Si ^(nota 4)	Si	Si
Ruolo server DNS	Si	Si	Si	Si
Ruolo server fax	Si	Si	Si	Si
Server Manager	Si	Si	Si	Si
Servizi di stampa e documento	Si	Si	Si	Si
Servizi UDDI	Si	Si	Si	Si
Servizi Web (Internet Information Services)	Si	Si ^(nota 4)	Si	Si
Windows Deployment Services	Si	Si	Si	Si
Windows Powershell	Si	Si	Si	Si
Windows Server Update Services	Si	Si	Si	Si

Figure 4: Schema di rete esercitazione 2