

System Management

Riccardo Biella, Elia Perrone, Nicolas Sala, Kevin Dominguez

Semestre primaverile 2019

Contents

1	Esercitazione 01	2
1.1	Specifiche del server utilizzato (Gateway GW2000h-GW170hq F1)	2
1.2	Hardware utilizzato	3
1.3	Interfaccia di gestione	3
1.4	OpenVPN	3
1.4.1	Obiettivo	3
1.4.2	Installazione OpenVPN - Ubuntu x64	3
1.4.3	Problematiche	3
1.5	VMware ESXi	4
1.5.1	Descrizione	4
1.5.2	Architettura	4
1.5.3	Installazione di VMWare	4
1.5.4	Altre opzioni di virtualizzazione	4
2	Esercitazione 02	5
2.1	Obiettivo e definizione di una struttura di rete	5
2.2	Rete LAN	6
2.3	Rete WAN	6
2.4	Firewall utilizzato	6
2.4.1	Versione utilizzata e requisiti minimi di sistema	6
2.4.2	Funzionalità	7
2.5	Installazione Windows Server 2012	7
2.5.1	Versione utilizzata e requisiti minimi di sistema	7
2.5.2	Tabella comparativa delle versioni	7
2.6	Configurazione dei servizi	8
2.7	Installazione di un sistema Windows 10	8
2.7.1	Versione utilizzata e requisiti minimi di sistema	8
2.8	Installazione di un sistema Linux	8
2.8.1	Versione utilizzata e requisiti minimi di sistema	8
2.9	Impostazione avvio automatico	8
3	Esercitazione 03	8
3.1	Creazione di una nuova macchina WinClient_02	8
3.2	Creazione di nuovi gruppi utente	8
3.3	Installazione di un sistema di backup	8
4	Esercitazione 04	9
4.1	Sistema di monitoring utilizzato: Nagios	9
4.1.1	Caratteristiche	9
4.2	Altri sistemi di monitoring	10
4.3	Punto 2-3-4	11
5	Esercitazione 05	11
5.1	Protocollo iSCSI	11
5.1.1	iSCSI vs Fibre Channel over Ethernet	11
5.2	Tabella comparativa dei sistemi di storage	12

1 Esercitazione 01

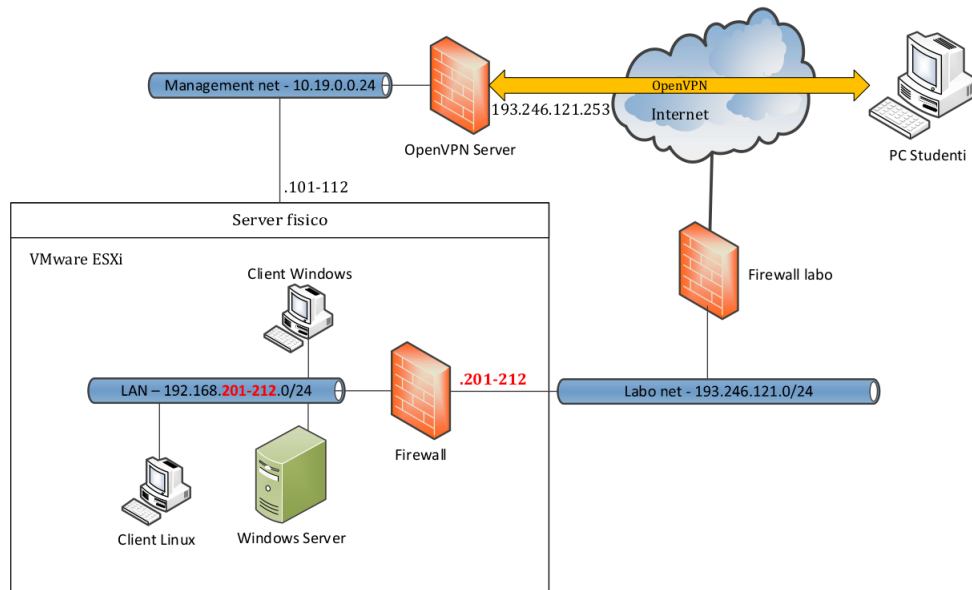


Figure 1: Schema di rete base

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 USB ports• Serial port• Video port		
	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 Chassis intrusion alert Power-on password Setup password		
Subsystem availability	Power supply	2 x 1400 W 80 PLUS ⁵ 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		
	Dimensions	Maximum nodes per chassis: 4 438 (W) x 724 (D) x 88 (H) mm (17.2 x 28.5 x 3.4 inches)		
	Weight	35 kg (77 lbs.) maximum (all component slots and sockets fully populated) 30.9 kg (68 lbs.) minimum (HDD, power supply, processor installed)		
OS support		Windows Server ⁶ 2008 Windows Server ⁶ 2008 R2 Windows Server ⁶ 2003		
		Novell ⁷ SUSE ⁸ Linux ⁹ Enterprise Server 11 Red Hat ¹⁰ Enterprise Linux ¹¹ 5.4 VMware ESXi ¹² 4 VMware ESX ¹³ 4		
Server management utilities and applications		Gateway Smart Console Gateway Smart Server Manager Gateway Smart Setup		
		BIOS update tool ID LED button Integrated Management Log IPMI firmware update tool		
Warranty		3-year standard warranty or choose extended warranties and services ⁵		
Regulatory compliance	Emissions classification (EMC)	CE (Class A)		
	Industry standard compliance / safety	CB Nemko/GS		

1.2 Hardware utilizzato

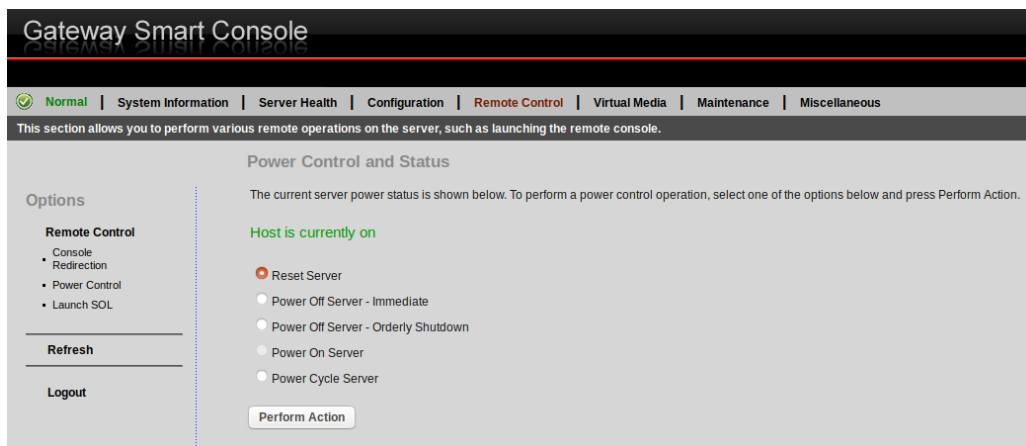
Ad ogni gruppo è stata assegnata la gestione di un nodo all'interno del rack, esso dispone di un disco rigido, un SSD ed una periferica USB mediante il quale sarà possibile installare un hypervisor sul server.

1.3 Interfaccia di gestione

L'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 Remot Control abbiamo scaricato il file .JNLP ed attraverso la sua esecuzione abbiamo installato l'hypervisor: abbiamo settato un IP statico pubblico in modo da non dover accedere ogni volta tramite VPN. Abbiamo utilizzato per installare VMWare una periferica USB 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

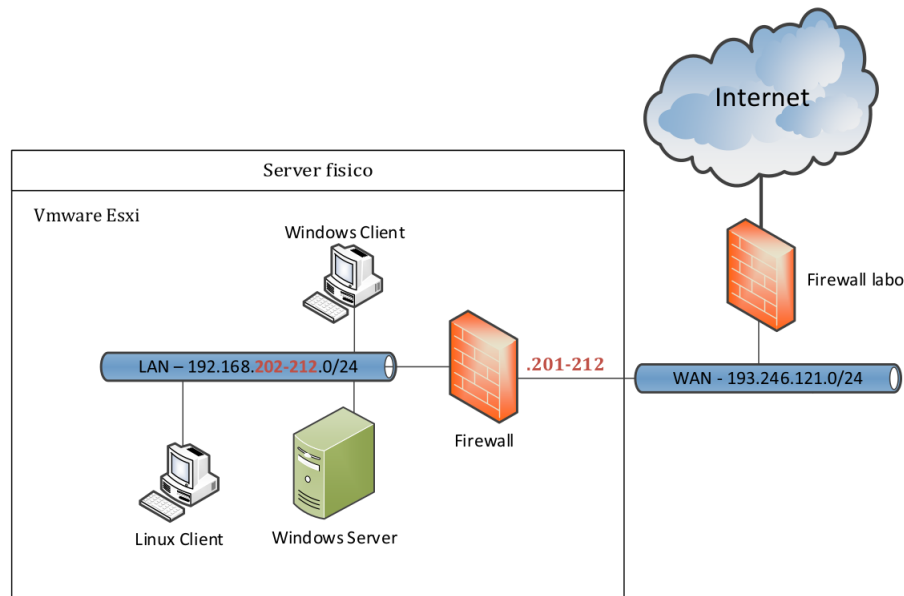


Figure 2: Schema di rete base

2.1 Obiettivo e definizione di una struttura di rete

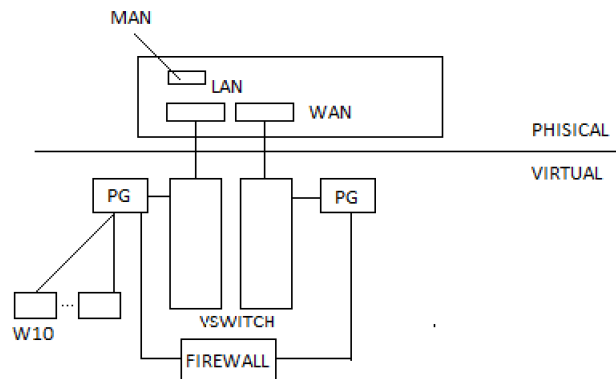


Figure 3: Struttura di rete

L'obiettivo finale dell'esercitazione è quello di virtualizzare l'intera rete collegata alle interfacce LAN e WAN del server. Nell'immagine è possibile osservare lo schema di rete che vogliamo realizzare. Nella parte superiore "Phisical", troviamo il server, con le sue interfacce MAN, LAN e WAN. Nella parte inferiore "Virtual" definiamo l'infrastruttura di rete che vogliamo virtualizzare. Si osservano due virtual switch, collegati a due port group, allo stato attuale disponiamo solo di un VS e di un PG, perciò dovremo creare un nuovo VS collegato all'interfaccia LAN e creare un nuovo port group nuovo collegato al VS creato. I port group non sono altro che un'astrazione ad un livello più alto degli switch, su di essi possono risiedere le VLAN. Nel corso dell'esercitazione procederemo ad installare alcune macchine virtuali client e server e un firewall che sarà collegato ai port group con due interfacce, una LAN e una WAN (pubblica). Le macchine virtualizzate saranno poi collegate al nostro nuovo port group. L'indirizzo IP assegnato al nostro firewall finisce in .236. Sul firewall installeremo poi un client VPN. Come ultimo passaggio dobbiamo spostare l'interfaccia di gestione di ESXi all'interno della rete (LAN).

2.2 Rete LAN

LAN Interface (lan, em1)	
Status	up
MAC Address	00:0c:29:98:8a:0e
IPv4 Address	192.168.206.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::20c:29ff:fe98:8a0e%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	7429531/14682699 (370.17 MiB/19.82 GiB)
In/out packets (pass)	7429531/14682699 (370.17 MiB/19.82 GiB)
In/out packets (block)	135/0 (11 KiB/0 B)
In/out errors	0/0
Collisions	0

Figure 4: Configurazione di rete LAN

2.3 Rete WAN

WAN Interface (wan, em0)	
Status	up
MAC Address	00:0c:29:98:8a:04
IPv4 Address	193.246.121.236
Subnet mask IPv4	255.255.255.0
Gateway IPv4	193.246.121.1
IPv6 Link Local	fe80::20c:29ff:fe98:8a04%em0
DNS servers	127.0.0.1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	19273028/12029270 (19.93 GiB/489.41 MiB)
In/out packets (pass)	19273028/12029270 (19.93 GiB/489.41 MiB)
In/out packets (block)	202802/0 (28.74 MiB/0 B)
In/out errors	0/0
Collisions	0

Figure 5: Configurazione di rete WAN

2.4 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".

2.4.1 Versione utilizzata e requisiti minimi di sistema

Versione: PFSense

Memoria RAM: 512 MB

2.4.2 Funzionalità

Possiede le funzionalità basilari di un firewall di qualità:

- 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.

2.5 Installazione Windows Server 2012

2.5.1 Versione utilizzata e requisiti minimi di sistema

Versione: Windows Server 2012 Standard Evaluation

Memoria RAM: 2 GB

Hard Disk: 60 GB

2.5.2 Tabella comparativa delle versioni

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]	Sì	Sì
Active Directory Domain Services	Deve essere radice di foresta e dominio	Deve essere radice di foresta e dominio	Sì	Sì
Active Directory Federation Services	Sì ^[47]	No	Sì	Sì
Active Directory Lightweight Directory Services	Sì	Sì	Sì	Sì
Active Directory Rights Management Services	Sì	Sì	Sì	Sì
Hyper-V	No	No	Sì	Sì
Modalità Server Core	No	No	Sì	Sì
Ruolo DHCP	Sì	Sì	Sì	Sì
Ruolo di server d'applicazioni	Sì	Sì ^[nota 4]	Sì	Sì
Ruolo server DNS	Sì	Sì	Sì	Sì
Ruolo server fax	Sì	Sì	Sì	Sì
Server Manager	Sì	Sì	Sì	Sì
Servizi di stampa e documento	Sì	Sì	Sì	Sì
Servizi UDDI	Sì	Sì	Sì	Sì
Servizi Web (Internet Information Services)	Sì	Sì ^[nota 4]	Sì	Sì
Windows Deployment Services	Sì	Sì	Sì	Sì
Windows Powershell	Sì	Sì	Sì	Sì
Windows Server Update Services	Sì	Sì	Sì	Sì

Figure 6: Versioni Windows Server 2012

2.6 Configurazione dei servizi

- **Active Directory:** Attraverso l'active directory abbiamo creato gli utenti del sistema e dei gruppi per l'assegnamento dei permessi (a livello di sistema operativo). Abbiamo poi creato cartelle per i profili utente sul disco C e aggiunto questi ultimi all'active directory.
- **Domain Controller:** Abbiamo creato il dominio korn.forest nel quale abbiamo inserito i vari client.
- **DHCP:** Abbiamo settato il server come DHCP, è stato necessario impostare l'ip range per gli indirizzi da distribuire, un default gateway e un default dns che corrisponde al server stesso. Inoltre è necessario ricordarsi di disabilitarlo dal firewall.
- **DNS:** Abbiamo creato un DNS associato al dominio appena creato. Nel nostro caso il DNS si occupa di eseguire un semplice forward, non introduce altre regole.

2.7 Installazione di un sistema Windows 10

2.7.1 Versione utilizzata e requisiti minimi di sistema

Versione: Windows 10 Home

Memoria RAM: 2 GB

Hard Disk: 60 GB

2.8 Installazione di un sistema Linux

2.8.1 Versione utilizzata e requisiti minimi di sistema

Versione: Kali Linux (con gnome)

Memoria RAM: 2048 MB

Hard Disk: 20 GB

2.9 Impostazione avvio automatico

Attraverso il menù actions delle VM abbiamo abilitato il riavvio automatico nel caso che il server fisico venga riavviato.

3 Esercitazione 03

3.1 Creazione di una nuova macchina WinClient_02

Abbiamo rinominato la macchina MS Windows client in WinClient_01, e dopo aver copiato la macchina WinClient_01, l'abbiamo clonato creando un nuovo client WinClient_02.

3.2 Creazione di nuovi gruppi utente

Abbiamo creato nuovi gruppi utente, come segue:

- Usgroup_A (usr01, usr02)
- Usgroup_B (usr01, usr02, usr03)
- Usgroup_C (usr04, Usgroup_A)

Utilizzando i client descritti in precedenza abbiamo verificato il funzionamento dei profili utenti appena creati.

3.3 Installazione di un sistema di backup

MANCA QUESTO PUNTO DELL'ESERCITAZIONE 3.

4 Esercitazione 04

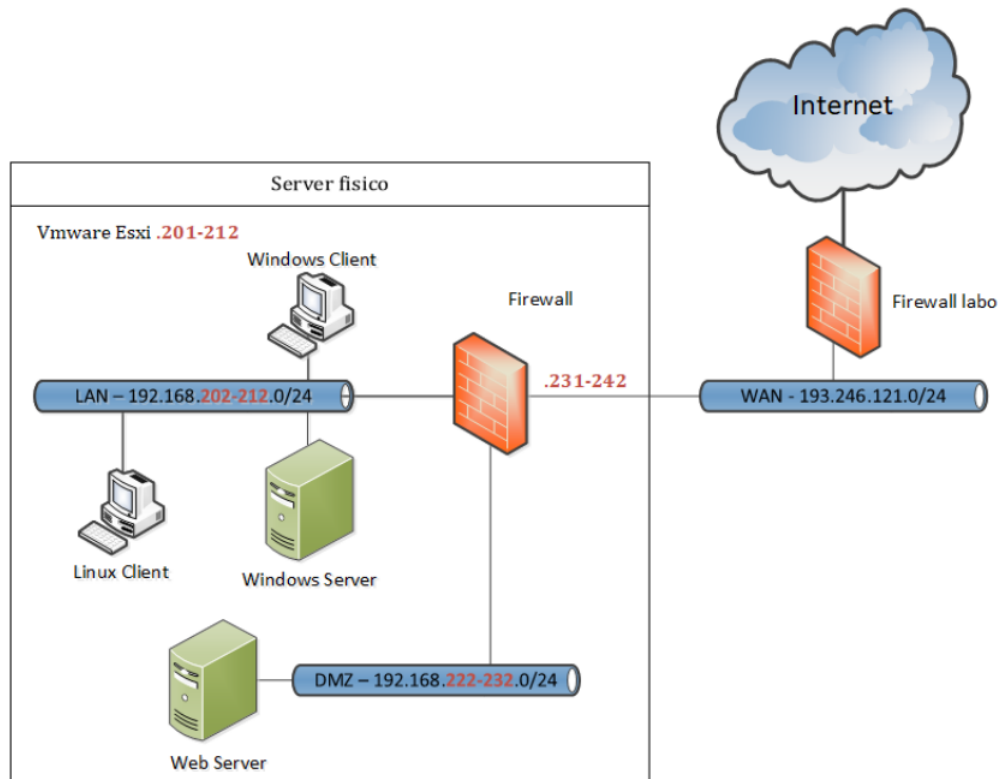


Figure 7: Configurazione di rete

L'infrastruttura realizzata sinora comprende una rete LAN e una rete WAN. Ad ognuna è assegnato un port switch virtuale che permette di creare la rete condivisa in VMWare dalle macchine virtualizzate e da quelle esterne. Abbiamo realizzato una nuova rete, una DMZ, nel quale abbiamo esposto un server di servizi web. Abbiamo aggiunto al FW un' interfaccia ethernet e l' abbiamo chiamata DMZ, abbiamo aggiunto poi un virtual switch e gli abbiamo associato l'interfaccia appena creata.

4.1 Sistema di monitoring utilizzato: Nagios

Nagios è un'applicazione open source per il monitoraggio di computer e risorse di rete. La sua funzione base è quella di controllare nodi, reti e servizi specificati, avvertendo quando questi non garantiscono il loro servizio o quando ritornano attivi. In origine Nagios è stato sviluppato per Linux, ma può funzionare correttamente anche su altre varianti di Unix.

4.1.1 Caratteristiche

- monitoraggio di servizi di rete (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH);
- monitoraggio delle risorse di sistema (carico del processore, uso dell'hard disk, log di sistema sulla maggior parte dei sistemi operativi, anche per Microsoft Windows);
- monitoraggio remoto supportato attraverso tunnel SSH o SSL;
- semplici plugin che permettono agli utenti di sviluppare facilmente nuovi controlli per i servizi in base alle proprie esigenze, usando bash, C++, Perl, Ruby, Python, PHP, C#, ecc.;
- controlli paralleli sui servizi;

- capacità di definire gerarchie di nodi di rete usando nodi "parent", permettendo la distinzione tra nodi che sono down e nodi non raggiungibili;
- notifiche quando l'applicazione riscontra problemi o la loro risoluzione (via email, cercapersone, SMS, o con altri sistemi per mezzo di plugin aggiuntivi);
- capacità di definire "event handler", ovvero azioni automatiche che vengono attivate all'apparire o alla risoluzione di un problema;
- rotazione automatica dei file di log;
- supporto per l'implementazione di monitoring ridondante;
- interfaccia web opzionale per la visualizzazione dell'attuale stato, notifiche, storico dei problemi, file di log, ecc.

4.2 Altri sistemi di monitoring





















	Product	Deployment	Bandwidth Monitoring	Dashboard	Internet Usage Monitoring	Network Diagnosis	Server Monitoring	Uptime Monitoring
	SolarWinds RMM ★★★★☆ (22 reviews)		✓	✓	✓	✓	✓	✓
	Datadog Cloud Monitoring ★★★★☆ (68 reviews)		✓	✓	✓	✓	✓	✓
	PRTG Network Monitor ★★★★☆ (84 reviews)		✓	✓	✓	✓	✓	✓
	Kaseya VSA ★★★★☆ (129 reviews)		✓	✓	✓	✓	✓	✓
	PA Server Monitor		✓	✓	✓	✓	✓	✓
	ManageEngine OpManager ★★★★☆ (21 reviews)		✓	✓	✓	✓	✓	✓
	NetFlow Analyzer ★★★★☆ (5 reviews)		✓	✓	✓	✓	✓	✓
	Atera ★★★★☆ (111 reviews)		✓	✓	✓	✓	✓	✓
	Opsgenie ★★★★☆ (109 reviews)		✓	✓	✓	✓	✓	✓
	EventLog Analyzer ★★★★☆ (2 reviews)		✓	✓	✓	✓	✓	✓

Figure 8: Sistemi di monitoring

4.3 Punto 2-3-4

MANCANO QUESTI PUNTI DELL'ESERCITAZIONE 4.

5 Esercitazione 05

Attivazione di una SAN e integrazione nel sistema sviluppato in laboratorio.

5.1 Protocollo iSCSI

In telecomunicazioni ed elettronica iSCSI (sta per "Internet SCSI") è un protocollo di comunicazione che permette di inviare comandi a dispositivi di memoria SCSI fisicamente collegati a server e/o altri dispositivi remoti (come ad esempio NAS o SAN). È un protocollo molto utilizzato in ambienti SAN poiché permette l'archiviazione dei dati su dischi virtuali, collegati attraverso la rete, dando l'illusione di disporre localmente di un disco fisico che invece si trova in realtà su un dispositivo di archiviazione remoto. Il client utilizza quindi un driver, detto initiator, che consente di inviare all'host dove sono fisicamente ospitati i dischi, detto target, i comandi che consentono di leggere e scrivere il disco virtuale. L'initiator tipicamente si identifica tramite un codice alfanumerico, detto IQN (acronimo inglese di "iSCSI Qualified Name", in italiano "Nome Qualificato iSCSI") al quale può essere associata una policy di accesso basata sull'indirizzo IP mittente. Il protocollo iSCSI supporta inoltre l'autenticazione tramite il protocollo CHAP.

5.1.1 iSCSI vs Fibre Channel over Ethernet

La differenza principale è che il protocollo Fibre Channel consente l'impacchettamento su TCP/IP, e attraverso l'infrastruttura di rete esistente rende possibile l'utilizzo di dispositivi a distanza. Di seguito riportiamo i punti di forza delle due soluzioni:

- iSCSI è sicuramente più adatto per le soluzioni di fascia bassa non richiedendo nessuna implementazione particolare della rete ethernet e operando su TCP/IP permette il suo utilizzo anche in ambito geografico. Esistono, inoltre, molte implementazioni software di server iSCSI e praticamente tutti i sistemi operativi attuale hanno un supporto per connessioni client iSCSI.
- FCoE è stato pensato per i CED in ambito locale dove la presenza di infrastrutture Fibre Channel è ampia. FCoE consente di utilizzare le stesse utility e funzionalità utilizzate su Fibre Channel oltre a fornire tutto il supporto per lo zoning. FCoE non ha bisogno di uno stack TCP/IP ed è quindi molto più efficiente di iSCSI.

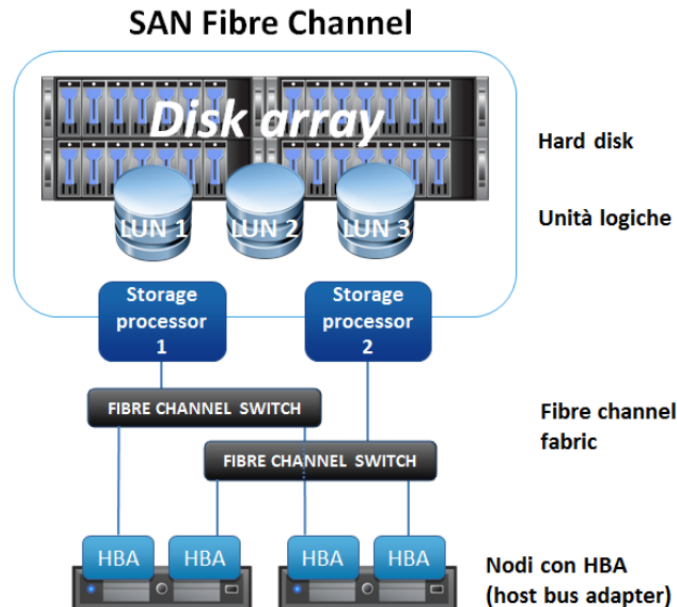


Figure 9: Sistemi di storage SAN

5.2 Tabella comparativa dei sistemi di storage

MANCA QUESTO PUNTO DELL'ESERCITAZIONE 5.