

Proposta evolutiva dell’infrastruttura IT

Indicazioni operative per una gestione più efficiente della rete e dei sistemi.

Redatto per: **Arancho Doc**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| © 2014 Progel SpA Tutti i diritti sono riservati.  Questo documento contiene informazioni proprietarie che sono coperte da copyright. Tutti i diritti sono riservati. Nessuna parte di questo documento può essere fotocopiata, riprodotta o tradotta in altra lingua senza il preventivo consenso scritto di Progel SpA  Le informazioni contenute nel presente documento rappresentano la posizione corrente di Progel SpA in merito all’oggetto discusso alla data della pubblicazione. Ogni procedura, politica od altra indicazione fornita si intendono accettati dal cliente al momento dell’applicazione delle stesse.  Dal momento che Progel SpA deve rispondere alle mutevoli condizioni di mercato e fornire indicazioni su strumenti non direttamente sotto il proprio controllo, le informazioni quivi esposte sono da ritenersi valide alla data di pubblicazione e nessuna garanzia esplicita o implicita viene fornita sull’accuratezza di quanto esposto dopo tale data.  Mythos è un marchio registrato Progel.  Altri prodotti o ditte menzionate possono essere marchi registrati dei rispettivi possessori.  Progel SpA • Via Due Ponti, 2 • 40050 Argelato (B0) • Italy • [www.progel.it](http://www.progel.it) • [info@progel.it](mailto:info@progel.it) • Tel. +39 051 6639411 • Fax +39 051 6639412  Registro delle Imprese di Bologna n. 03791100377 – Registro Ditte: 316517 – P.Iva 00662101203 CF 03791100377 – Capitale Sociale: 100.000 Euro I.V | | | | | |
| **Informazioni documento** |  | | | | |
| **Titolo** | Proposta evolutiva dell’infrastruttura IT | | | | |
| **Cliente** | **Arancho Doc** | | | | |
| **Area** | IT | | | | |
| **Riservatezza** |  | | | | |
| **Stato** | Release | | | | |
| **Versione** | 2 rev. 1 | | | | |
| **Ultimo Salvataggio** | 24/10/2014 | | | | |
| **File** | Aranchodoc\_Analisi Rete e Sistemi | | | | |
| **Autore** | Luca Bonora, Marco Lelli, Progel S.p.A. | | | | |
| **Distribuito a** | | | |  |  |
| **Destinatario** | | **Reparto o funzione** | **Società** | | |
| Daniele Sincich | | CIO | Arancho Doc | | |
| Daniela Gardenghi | | Responsabile IT | Arancho Doc | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versione** | **Autore** | **Modifiche** |
| 29-08-2014 | 1.0 | Luca Bonora | Prima stesura – indice generale – Rete locale passiva |
| 08-09-2014 | 1.1 | Luca Bonora | Revisione bozza |
| 19-09-2014 | 1.2 | Marco Lelli | Integrazione con analisi sistemi |
| 22-09-2014 | 1.3 | Marco Lelli | Revisione bozza |
| 29-09-2014 | 1.4 | Luca Bonora | Revisione bozza |
| 02-10-2014 | 1.5 | Marco Lelli | Revisione bozza |
| 07-10-2014 | 1.6 | Luca Bonora | Revisione bozza |
| 13-10-2014 | 1.7 | Luca Bonora | Revisione bozza |
| 13-10-2014 | 1.8 | Marco Lelli | Revisione bozza |
| 14-10-2014 | 1.9 | Marco Lelli | Revisione bozza |
| 20-10-2014 | 1.10 | Marco Lelli | Revisione generale |
| 23-10-2014 | 2.0 | Luca Bonora | Approfondimenti network |
| 24-10-2014 | 2.1 | Marco Lelli | Revisione finale per consegna a cliente |

# Sommario

[Sommario 3](#_Toc401915283)

[1 Introduzione 5](#_Toc401915284)

[1.1 Esigenze del cliente 5](#_Toc401915285)

[1.2 Obiettivi 5](#_Toc401915286)

[2 Generalità 6](#_Toc401915287)

[2.1 Ambito 6](#_Toc401915288)

[2.2 Sedi 6](#_Toc401915289)

[3 Assessment ed analisi 8](#_Toc401915290)

[3.1 Rete Locale 8](#_Toc401915291)

[3.1.1 Architetura di rete passiva 8](#_Toc401915292)

[3.1.2 Architettura di rete - apparati attivi 9](#_Toc401915293)

[3.1.3 Indirizzamenti di rete e VLAN 11](#_Toc401915294)

[3.1.4 Analisi rete Wifi 13](#_Toc401915295)

[3.2 Rete Geografica 14](#_Toc401915296)

[3.2.1 Architettura 14](#_Toc401915297)

[3.2.2 Firewall 16](#_Toc401915298)

[3.2.3 Navigazione internet 18](#_Toc401915299)

[3.2.4 Pubblicazione servizi Internet, Accelerazione e Bilanciamento 19](#_Toc401915300)

[3.2.5 Sistema di monitoraggio 22](#_Toc401915301)

[3.3 Hardware 23](#_Toc401915302)

[3.3.1 Server 23](#_Toc401915303)

[3.3.2 Storage 25](#_Toc401915304)

[3.3.3 Necessità del cliente 26](#_Toc401915305)

[3.3.4 Criticità rilevate 26](#_Toc401915306)

[3.3.5 Proposta evolutiva 27](#_Toc401915307)

[3.4 Sicurezza dei sistemi informativi 27](#_Toc401915308)

[3.4.1 Account 27](#_Toc401915309)

[3.4.2 Patching 28](#_Toc401915310)

[3.4.3 Antivirus 28](#_Toc401915311)

[3.4.4 Necessità del cliente 29](#_Toc401915312)

[3.4.5 Criticità rilevate 30](#_Toc401915313)

[3.4.6 Proposta evolutiva 30](#_Toc401915314)

[3.5 Sistema di Identity 31](#_Toc401915315)

[3.5.1 Architettura Logica 31](#_Toc401915316)

[3.5.2 Architettura fisica 31](#_Toc401915317)

[3.5.3 Necessità del cliente 32](#_Toc401915318)

[3.5.4 Criticità rilevate 32](#_Toc401915319)

[3.5.5 Proposta evolutiva 34](#_Toc401915320)

[3.6 Sistema di Posta Elettronica 34](#_Toc401915321)

[3.6.1 Architettura 34](#_Toc401915322)

[3.6.2 Necessità del cliente 35](#_Toc401915323)

[3.6.3 Criticità rilevate 36](#_Toc401915324)

[3.6.4 Proposta evolutiva 36](#_Toc401915325)

[3.7 Server Virtualization 36](#_Toc401915326)

[3.7.1 Hyper-V 36](#_Toc401915327)

[3.7.2 VMWare 37](#_Toc401915328)

[3.7.3 Necessità del cliente 38](#_Toc401915329)

[3.7.4 Criticità rilevate 38](#_Toc401915330)

[3.7.5 Proposta evolutiva 39](#_Toc401915331)

[3.8 Backup & Recovery 39](#_Toc401915332)

[3.8.1 Altaro 39](#_Toc401915333)

[3.8.2 Acronis 40](#_Toc401915334)

[3.8.3 Veeam 41](#_Toc401915335)

[3.8.4 Windows Backup 41](#_Toc401915336)

[3.8.5 Sedi remote 41](#_Toc401915337)

[3.8.6 Necessità del cliente 42](#_Toc401915338)

[3.8.7 Criticità rilevate 42](#_Toc401915339)

[3.8.8 Proposta evolutiva 42](#_Toc401915340)

[3.9 Licensing 43](#_Toc401915341)

[3.9.1 Necessità del cliente 43](#_Toc401915342)

[3.9.2 Criticità rilevate 43](#_Toc401915343)

[3.9.3 Proposta evolutiva 44](#_Toc401915344)

[4 Conclusioni 45](#_Toc401915345)

[4.1 Percorso evolutivo proposto 45](#_Toc401915346)

[5 Appendici 47](#_Toc401915347)

[5.1 A - Switch 47](#_Toc401915348)

[5.1.1 blq-swc01 47](#_Toc401915349)

[5.1.2 blq-swc02 49](#_Toc401915350)

[5.1.3 blq-swc03 51](#_Toc401915351)

[5.1.4 blq-swc04 54](#_Toc401915352)

[5.1.5 blq-swc05 (SWITCH\_ISCSI\_1002) 60](#_Toc401915353)

[5.2 B - Accesso 67](#_Toc401915354)

[5.3 C - VPN 74](#_Toc401915355)

[5.4 D – Configurazioni Sistema di Monitoraggio 76](#_Toc401915356)

[5.5 E – Configurazioni cluster Hyper-V 83](#_Toc401915357)

[5.6 F – Configurazioni BLQ-VH03 87](#_Toc401915358)

[6 Allegati 91](#_Toc401915359)

[7 Sigle ed acronimi 92](#_Toc401915360)

# Introduzione

Arancho Doc, nato dalla fusione di IC DOC e Arancho, è uno dei principali protagonisti nel settore dell’industria linguistica internazionale.

L’azienda offre al proprio parco clienti servizi linguistici incentrati nelle seguenti aree: traduzione, localizzazione, terminologia, desktop publishing e project management.

## Esigenze del cliente

La richiesta dell’azienda è quella di effettuare un’assessment del proprio ambiente negli ambiti di rete e sistemi e ricevere indicazioni strategiche di evoluzione che permettano di migliorare in termini di efficienza.

Per quanto riguarda la rete locale, ma soprattutto geografica, il desiderio è di semplificare al massimo l’architettura, attraverso l’accentramento a Bologna dei servizi forniti per le sedi distaccate.

Stanno infatti cambiando le logiche di implementazione: inizialmente ICDOC aveva una logica di decentramento con server virtuali nelle varie sedi, mentre le attuali direttive aziendali hanno una direzione completamente opposta.

Anche i sistemi seguiranno questa logica di accentramento, ed anche in questo caso c’è desiderio di semplificarne l’architettura.

L’evoluzione tecnologica ha avuto infatti una velocità differente rispetto agli investimenti e agli sforzi finora compiuti dall’azienda per l’ambito tecnologico, questo genera inefficienze e incapacità di utilizzare la tecnologia per valorizzare e rendere più efficiente il business.

## Obiettivi

Obiettivo principale di questo documento è quello di riprodurre una fotografia della situazione al momento dell’assessment, di fornire un’analisi dei dati raccolti e di evidenziare criticità e proposte evolutive.

# Generalità

## Ambito

In questo documento verranno analizzati i principali temi architetturali, esclusivamente per la sede di Bologna, in merito a:

* Architettura Telematica (rete passiva)
* Rete locale attiva Wired
* Rete locale attiva Wireless
* Connettività internet
* Hardware
* Sicurezza dei sistemi informativi
* Sistema di Identity
* Sistema di posta elettronica
* Licensing.

Le seguenti tematiche verranno invece affrontate sia in merito alla sede di Bologna che di quelle remote:

* Rete geografica e connettività internet
* Server Virtualization
* Backup & Recovery.

## Sedi

Arancho Doc è organizzata su più sedi operative. La sede principale si trova a Bologna, ma sono presenti uffici in altre località e nazioni.

Di seguito l’elenco delle sedi e uffici censiti:

* Bologna (circa 50 postazioni)
* Mirandola (circa 10 postazioni)
* Rimini (10 Postazioni)
* Barcellona (circa 10 postazioni)
* Zurigo (3 postazioni)
* Praga (3 postazioni)
* Helsinki (circa 10 postazioni).

Si possono poi includere numerosi professionisti che si collegano in VPN o tramite servizi pubblicati (ad esempio il Terminal Server).

Sono circa 1500 le persone che possono effettuare l’accesso dall’esterno, ma il trend di connessioni contemporanee va dalle 2 alle 10 sessioni.

# Assessment ed analisi

## Rete Locale

Al CED sono presenti 3 rack suddivisi come:

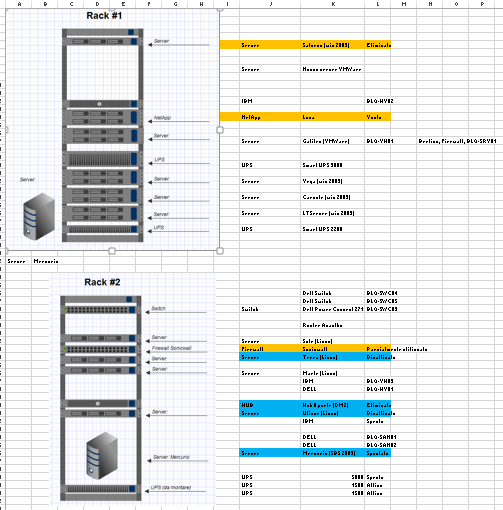
* Armadio 1: Nodi Hypervisor, Server Fisici (Caronte e LTServer)
* Armadio 2: Nodi Hypervisor, SAN e switch iSCSI, Connettività Acanto e firewall SonicWall
* Armadio 3: Apparati telematici, switch di rete locale e connettività geografica Fastweb.

### Architetura di rete passiva

La rete passiva della sede di Bologna è centralizzata nell’ armadio 3 presente nell’unico locale CED.

SI tratta di cablaggio UTP cat 6 Biticino non certificato. L’impianto è stato realizzato nel 2005.

I tre armadi non hanno collegamenti strutturati tra di loro, ma vengono utilizzate patchcord volanti.



Il cliente non dispone degli schemi del rack 3.

#### Necessità del cliente

Il cliente si dichiara soddisfatto dell’attuale architettura di rete passiva anche se l’impianto non risulta certificato.

#### Criticità rilevate

Le criticità rilevate riguardano:

* L’interconnessione fra gli apparati: fra i rack sono stesi cavi volanti in modo completamente destrutturato
* La certificazione dell’impianto è assente. Il documento di certificazione permette:
  + Di garantire che la posa dei cavi è stata effettuata a regola d’arte
  + Di garantirne il corretto funzionamento per molti anni
  + Se la certificazione è rilasciata dal produttore stesso del cablaggio i principali produttori certificano l’impianto per molti anni (fino a 25 anni in caso di AMP o Brandrex)

Secondo me il terzo punto elenco è inutile...può essere incluso nella frase che introduce i punti elenco. In questo modo. Poi vedi tu.

* La certificazione dell’impianto è assente.

Il documento di certificazione, se rilasciata dal produttore stesso del cablaggio, dura fino a 25 anni in caso di AMP o Brandrex e permette di:

* + Garantire che la posa dei cavi è stata effettuata a regola d’arte
  + Garantirne il corretto funzionamento per molti anni

#### Proposta Evolutiva

Al fine di migliorare l’ordine e l’usabilità del CED si consiglia di predisporre fra gli armadi una distribuzione orizzontale di cavi attraverso cablaggio strutturato (patch panel).

Si ritiene inoltre importante provvedere alla certificazione dell’impianto di rete telematica, al fine di garantire una solida base di partenza per evoluzioni future e nella quale identificare facilmente eventuali problemi di connessione.

### Architettura di rete - apparati attivi

#### Design e Switch

Gli switch sono tutti dislocati nel CED. L’unica eccezione è un Access Point con 4 porte Ethernet al quale sono collegate due stampanti, che risulta dislocato direttamente negli uffici.

Gli Switch attualmente utilizzati sono:

* Due DELL Powerconnect 2748, 48 porte GigabitEthernet
  + Porte in uso circa il 90 %
* Due DELL Powerconnect 2848, 48 porte GigabitEthernet
  + Porte in uso circa il 90 %
* Due DELL Powerconnect 5524, 24 porte GigabitEthernet
  + Per entrambi le porte in uso sono il 60%
  + Utilizzati per iSCSI, VLAN per i cluster, connessioni internet verso i carrier Acantho e Fastweb.
* Un DELL Powerconnect 2716, 24 porte GigabitEthernet
  + Porte in uso 10
  + Utilizzato per la DMZ
* Un 3COM 2920, 20 porte GigabitEthernet + 4 SFP
  + Porte in uso 8
  + Utilizzato per connessioni in DMZc

Agli switch si accede in http mediante login Admin e password di default.

È possibile raggiungere gli switch con nome FQDN, ad esempio ***blq-swc01.aranchodoc.corp*** al quale corrisponde **192.168.0.250.**

In Appendice A sono riportate le configurazioni rilevate negli switch.

#### Necessità del cliente

Il cliente si dichiara soddisfatto dell’attuale architettura di rete locale attiva.

#### Criticità rilevate

Le criticità rilevate riguardano:

* La presenza di switch eterogenei. Avere switch eterogenei:
  + Non permette l’implementazione di funzionalità specializzate tipicamente personalizzate da ogni produttore
  + Potrebbe avere effetti indesiderati principalmente dovuti ai diversi modi di implementazione per i protocolli in uso
* L’utilizzo delle porte degli switch principali risulta essere circa il 90% delle porte disponibili. E’ nostro parere che in un impianto di rete le porte libere dovrebbero essere mediamente il 30% della disponibilità complessiva. Questo per garantire:
  + Una buona scalabilità dell’impianto stesso, in grado di supportare evoluzioni dei sistemi informativi
  + Di non sovraccaricare le performance richieste agli switch
* La totale assenza di sicurezza nella gestione dell’account di amministrazione, ed in particolare
  + Login in chiaro
  + Login di default
  + Stessa login amministrativa per tutti gli utenti
* La rete locale risulta implementata in modalità piatta (unico layer 2) a scapito dei protocolli e della sicurezza locale.

#### Proposta Evolutiva

Al fine di superare le criticità rilevate si consiglia di:

* Rivedere l’architettura di Core
  + Inserendo un numero maggiore di porte disponibili
  + Inserendo gli switch in stack per garantire l’alta affidabilità dell’architettura
* Organizzare una struttura di autenticazione che permetta di
  + Gestire account di tipo personale
  + Non far passare la login in chiaro all’interno della rete
* Implementare una coerente architettura di VLAN
  + Uniformando le VLAN sugli switch
  + Valutando se servono altre VLAN da implementare
  + Per fare ordine nell’utilizzo dei dispositivi.

### Indirizzamenti di rete e VLAN

#### Indirizzi di rete e VLAN

Di seguito le VLAN e le relative classi IP rilevate nelle varie sedi:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sede | VLAN | Utilizzo | IP | Subnet |
| Bologna | 1 | Inside | 192.168.0.0 | 255.255.255.0 |
| Bologna | 2 | DMZ | 10.0.0.0 | 255.255.255.0 |
| Bologna | 3 | iSCSI 1 | 10.0.1.0 | 255.255.255.0 |
| Bologna | 1002 | iSCSI2 | 10.0.2.0 | 255.255.255.0 |
| Bologna | 4 | Fastweb | 85.18.169.113 | 255.255.255.252 |
| Bologna | 5 | Acanto | 77.89.9.49 | 255.255.255.250 |
| Bologna | 11 | HertBeat | 10.0.254.1 | 255.255.255.250 |
| Bologna | 12 | CSV | 10.0.254.16 | 255.255.255.250 |
| Bologna | 13 | live migration | 10.0.254.32 | 255.255.255.250 |
| Rimini | 1 | Inside | 10.1.2.0 | 255.255.255.0 |
| Mirandola | 1 | inside | 10.2.1.0 | 255.255.255.0 |
| Praga | 1 | inside | 10.4.1.0 | 255.255.255.0 |
| Helsinki | 1 | inside | 10.3.1.0 | 255.255.255.0 |
| Zurigo | 1 | inside | 192.168.208.0 | 255.255.255.0 |
| Bamberg | 1 | inside | 10.6.1.0 | 255.255.255.0 |

Nelle sedi remote non sono presenti architetture di VLAN o di DMZ.

Nelle sedi di Barcellona, Praga ed Helsinki esiste una sottorete 192.168.1.0/24, utilizzata unicamente per raggiungere la rete di management del router di rete geografica locale.

In queste sedi si accede a tale rete attraverso uno specifico server dotato di una doppia scheda di rete, con una NIC in inside ed una nella rete di management.

#### Sede di Bologna

Seguono le tabelle delle reti implementate nella sede di Bologna

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **BLQ-SWC04 - Dell PC5524** | | | | **BLQ-SWC05 - Dell PC5524** | | | |
| **SWC Port** | VLAN | IP | DEVICE | PORT/CBL | VLAN | IP | DEVICE | PORT/CBL |
| **1** | 3 | 10.0.1.11 | BLQ-SAN01 | C0-P0 | 1002 | 10.0.2.11 | BLQ-SAN01 | C0-P1 |
| **2** | 3 | 10.0.1.21 | BLQ-SAN01 | C1-P0 | 1002 | 10.0.2.21 | BLQ-SAN01 | C1-P1 |
| **3** | 3 | 10.0.1.12 | BLQ-SAN02 | C0-P0 | 1002 | 10.0.2.12 | BLQ-SAN02 | C0-P1 |
| **4** | 3 | 10.0.1.22 | BLQ-SAN02 | C1-P0 | 1002 | 10.0.2.22 | BLQ-SAN02 | C1-P1 |
| **5** | 3 | 10.0.1.30 | HV01 | 1 | 1002 | 10.0.2.30 | HV01 | 5 |
| **6** | 3 | 10.0.1.31 | HV02 | HV02-1 | 1002 | 10.0.2.31 | HV02 | HV02-3 |
| **7** | 3 | 10.0.1.32 | BLQ-HV03 | HV03-4 | 1002 | 10.0.2.32 | BLQ-HV03 | HV03-6 |
| **8** | 3 | 10.0.1.33 | VH03 | 2 | 1002 | 10.0.2.33 | VH03 | 3 |
| **9** | 3 | 10.0.1.34 | BLQ-VH04 |  | 1002 | 10.0.2.34 | BLQ-VH04 |  |
| **10** | 3 |  |  |  | 1002 |  |  |  |
| **11** | 3 |  |  |  | 1002 |  |  |  |
| **12** | 3 | 10.0.1.1 | LUNA |  | 1, 1002 | 10.0.2.1 | LUNA e0a |  |
| **13** |  |  |  |  |  |  |  |  |
| **14** |  |  |  |  |  |  |  |  |
| **15** | 4 | 85.18.169.113 | Fastweb GTW |  | 5 | 77.89.9.49 | Acantho GTW | Giallo |
| **16** | 4 | 85.18.169.114 | BLQ-VH03 | VH03-4 | 5 | 77.89.9.50 | BLQ-VH03 | VH03-7 |
| **17** |  |  |  |  |  |  |  |  |
| **18** |  |  |  |  |  |  |  |  |
| **19** | 11 12 13 | 10.0.254.1 10.0.254.17 10.0.254.33 | HV01 | 2 | 11 12 13 | 10.0.254.1 10.0.254.17 10.0.254.33 | HV01 | 7 |
| **20** | 1 11 12 13 | 192.168.0.121 10.0.254.2 10.0.254.18 10.0.254.34 | HV02 | HV02-5 | 1 11 12 13 | 192.168.0.121 10.0.254.2 10.0.254.18 10.0.254.34 | HV02 | HV02-7 |
| **21** | 11 12 13 | 10.0.254.3 10.0.254.19 10.0.254.35 | BLQ-HV03 |  | 11 12 13 | 10.0.254.3 10.0.254.19 10.0.254.35 | BLQ-HV03 |  |
| **22** | 3, 11, 12, 13 |  | SWC06 | Link P5 |  |  |  |  |
| **23** |  |  |  |  |  |  |  |  |
| **24** | 1 | 192.168.0.138 | SWC03 | Link P13 | 1 | 192.168.0.139 | SWC03 | Link P15 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **BLQ-SWC03 - Dell** | | | | **BLQ-SWC06 - 3COM** | | | |
| **SWC Port** | VLAN | IP | DEVICE | Cable | VLAN | IP | DEVICE | PORT |
| **1** | 1 | 192.168.0.249 | SWC01 | Link P6 | 1 | 192.168.0.251 | LAN |  |
| **2** | 1 |  | SWC04 | Link P24 |  |  |  |  |
| **3** | 1 |  | SWC05 | Link P24 |  |  |  |  |
| **4** |  |  |  |  | 2 | DMZ | SWC03 | 11 |
| **5** |  |  |  |  | 3, 11, 12, 13 |  | SWC04 | Link P22 |
| **6** |  |  |  |  | 4, 5 |  | BLQ-VH03 |  |
| **7** | 1 |  | HV01 | M | 2 | DMZ | HV02 | 0 |
| **8** | 1 |  | VH03 | 9 | 5 |  | Sonicwall |  |
| **9** |  |  |  |  | 4 |  | Fastweb | Disc. |
| **10** |  |  |  |  |  |  |  |  |
| **11** | 2 | DMZ | SWC06 | 4 |  |  |  |  |
| **12** | 2 |  |  |  | 2 |  | BLQ-HV01 |  |
| **13** | 2 |  |  |  | 2 |  | BLQ-HV02 |  |
| **14** | 2 |  |  |  | 2 |  | BLQ-HV03 |  |
| **15** | 2 | DMZ | VH03 | VH03-1 | 2 |  | BLQ-VH03 |  |
| **16** | 2 | DMZ | HV01 | HV01-3 | 2 |  | SWC03 | 11 |

#### Necessità del cliente

Il cliente si dichiara soddisfatto dell’attuale architettura di rete locale attiva.

#### Criticità rilevate

Le criticità rilevate riguardano l’impatto sui vari switch dell’architettura di VLAN. Si rimanda quindi al punto precedente per la proposta evolutiva: 3.1.2.4.

### Analisi rete Wifi

#### rete Wifi Uffici

In tutte le sedi è presente una copertura WiFi.

Nelle sedi remote è erogata direttamente mediante il router ADSL che è tipicamente un router della tipologia Small Office con antenna WiFi (nelle sedi italiane si tratta di un TPLINK).

Nella sede centrale esistono invece due impianti WiFi:

* Per gli utenti interni l’accesso è implementato mediante access point di marche diverse D-LINK e 3COM
* Per i visitatori l’accesso è implementato mediante un unico access point guest integrato nel router di rete geografica situato in DMZ.

Agli utenti guest non viene data la possibilità raggiungere le reti degli utenti interni ma solo la navigazione Internet.

#### Necessità del cliente

Il cliente si dichiara in generale soddisfatto dell’attuale architettura di rete WiFi.

#### Criticità rilevate

Le criticità rilevate riguardano:

* La presenza di una doppia architettura di Access Point per tenere separati gli impianti interni e guest; La soluzione adottata seppur riconoscibile come valenza storica è stata superata dalle nuove tecnologie che ne permettono la perfetta controllabilità e gestibilità in un unico impianto di rete WiFi
* L’integrazione nel router di rete geografica dell’unica fonte WiFi per i Guest e per le sedi remote, ed in particolare
  + Un single point of failure
  + La copertura WiFi è decrescente allontanandosi dal router
* Totale assenza di gestione centralizzata delle connessioni WiFi.

#### Proposta Evolutiva

Al fine di superare le criticità rilevate si consiglia di rivedere l’architettura dell’impianto WiFi:

* Implementando un impianto che permetta di avere sugli stessi apparati e con la medesima copertura sia SSID interni che guest
* Implementando una architettura di apparati che permetta di tenere traccia degli accessi WiFi siano essi interni o guest
* Inserendo un numero sufficiente di access point atto a garantire una copertura completa sia in sede che nelle sedi remote
* Centralizzare nella sede di Bologna il controllo remoto degli access point delle sedi remote

Al fine di superare le criticità rilevate si consiglia di rivedere l’architettura dell’impianto WiFi:

* Implementando un impianto che permetta di avere sugli stessi apparati e con la medesima copertura sia SSID interni che guest
* Implementando una architettura di apparati che permetta di tenere traccia degli accessi WiFi siano essi interni o guest
* Inserendo un numero sufficiente di access point atto a garantire una copertura completa sia in sede che nelle sedi remote
* Centralizzare nella sede di Bologna il controllo remoto degli access point delle sedi remote

In questo paragrafo c’è un solo punto elenco per capoverso,con i suoi sottopunti...che senso ha fare un solo punto elenco? L’ho cambiato come vedi.

## Rete Geografica

### Architettura

La rete geografica è implementata fra le varie sedi mediante connessioni ad internet in modalità full mesh.

Ogni sede ha una doppia connessione ad internet. Fanno caso a se le sedi di Zurigo e Bamberg.

La sede di Bamberg non presenta la connessione di backup.

La sede di Zurigo ha una connettività diretta via ethernet, sfruttando il provider che si trova al piano superiore nello stesso edificio di quello di Arancho Doc. Ci si aspetta che il provider abbia nativa la connessione di backup. Non è chiaro però se la utilizza anche per dare servizio ad Arancho Doc

Ove presente, la connessione ad internet di riserva è tipicamente molto scadente e senza garanzia di banda minima garantita (BMG).

Tali connessioni secondarie vengono utilizzate per:

* Garantire la raggiungibilità dalla sede centrale e fare troubleshooting
* Garantire servizi minimi come ad esempio la posta elettronica (non per gli applicativi o il Terminal Server)

La seguente tabella riassume le caratteristiche delle linee utilizzate nelle varie sedi:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sede** | **Carrier principale** | **Banda Linea Principale** | **BMG** | **Carrier Secondario** | **Linea secondaria** | **BMG** |
| Bologna | Fastweb (F.O.) | 100 Mb | 2 | Acantho | 10 Mb | 1 Mb |
| Rimini | Pensareweb Ponte radio | 35 Mb | non nota | Fastweb SHDSL | 4 Mb | 512 Kb |
| Mirandola | Acantho Ponte Radio | 10 Mb | 1 | Fastweb HDSL | 2 Mb | 512 |
| Barcellona | Colt Fibra Ottica | 10 Mb | 100% | Telefonica ADSL | 7 Mb | non nota |
| Praga | GTS Fastwethernet | 4 Mb | non nota | GTS ADSL | 4m/380k | non nota |
| Helsinki | Teliassonera SHDSL | 8 Mb | 4 Mb | Elisa ADSL | 20Mb/1Mb | non nota |
| Zurigo | Dataway Fastwethernet | 100Mb | non nota | X | X | X |
| Bamberg | Ufficio in un albergo | 100Mb | non nota | X | X | X |

I router di connettività Internet sono di proprietà dei carrier a meno dei router ADSL che sono di proprietà di Arancho Doc.

La porta LAN dei router della linea principale è collegata ad una VLAN “Outside” che viene esposta al firewall PFSense, ospitato come VM, su di un Hypervisor VMWare ESXi.

Le porte LAN dei router delle linee secondarie sono invece collegate direttamente alla rete locale con un indirizzo dedicato.

Nella sede di Barcellona il router ADSL del carrier instaura una connessione PPoE con il firewall mediante la LAN interna.

#### Necessità del cliente

Il cliente in merito all’architettura di rete geografica lamenta:

* Difficoltà di utilizzo della linea di backup
* Un’ architettura non uniforme per le varie sedi remote
* Si sente obbligato al mantenimento dell’architettura ESXi per garantire la presenza dei firewall PFSense virtuali
* Parte del personale IT non ha sufficiente competenza rispetto ai firewall PFSense.

#### Criticità rilevate

Le criticità rilevate riguardano:

* Linea di backup inadeguata per permettere connessioni veloci e backup affidabili
* Assenza di contratti per la linea di backup nella sede di Zurigo e Bamberg
* Assenza di banda minima garantita per alcune sedi
* Architettura complicata nella gestione della linea di backup tramite l’utilizzo del firewall PFSense :
  + Il disegno dell’architettura non è chiaro all’attuale IT
  + Il firewall PFSense non risulta di semplice configurazione (anche perché manca formazione)

#### Proposta Evolutiva

Al fine di superare le criticità rilevate si consiglia di procedere con un progetto di revisione della rete geografica di Arancho Doc, perseguendo i seguenti obiettivi:

* Rivedere la capacità delle linee in uso nelle varie sedi geografiche
* Implementare una nuova architettura di VPN che permetta di automatizzare l’utilizzo della linea di backup garantendo la connessione in caso di caduta della linea principale
* Centralizzare il controllo delle VPN Lan to Lan nella sede centrale di Bologna
* Semplificare l’architettura complessiva della soluzione
* Procedere con un piano di formazione che permetta all’attuale IT di:
  + Conoscere l’architettura implementata
  + Di fare troubleshooting nel caso si presentino dei problemi

### Firewall

I firewall presenti nella sede di Arancho Doc sono di due tipi:

* Appliance fisica SonicWall (attualmente in dismissione per sostituzione con appliance virtuale)
* Appliance PFSense ospitato come VM su una architettura di Hypervisor VMWare ESXi dislocati nelle varie sedi

Ai Firewall si accede in http con utente Admin.

La soluzione firewall delle varie sedi risulta eterogenea ed è riassunta nella tabella dell’Appendice C.

I firewall vengono utilizzati come apparati di frontiera, per pubblicare i servizi degli Application Server e dei Terminal Server.

Non è stata attivata nessuna configurazione in alta affidabilità.

Le configurazioni sono riportate in Appendice B.

#### Necessità del cliente

Il cliente in merito all’architettura di firewall lamenta:

* Complessità di architettura delle VPN;
* Connessioni in VPN molto lente ed elevata frequenza di perdita di connessione
* Poca competenza di alcune persone dell’IT nell’utilizzo e nella personalizzazione della soluzione implementata con PFSense
* Obbligo di mantenere una doppia architettura di hypervisor, dove una è quasi unicamente dedicata alla soluzione firewall PFsense:
  + L’appliance PFSense ha supporto nativo solo per la piattaforma VMWare mentre l’attuale scelta dell’IT è di investire sulla piattaforma Microsoft Hyper-V
* Obbligo nelle sedi remote di mantenere una architettura di server ad oggi altrimenti inutile.

#### Criticità rilevate

Le criticità rilevate sono le seguenti:

* L’architettura dei firewall non è in alta affidabilità
* Non sono gestiti account personali per l’accesso ai firewall.

#### Proposta Evolutiva

Al fine di superare le criticità rilevate e soddisfare le esigenze del cliente si consiglia di procedere allo studio progettuale di revisione dell’architettura di Firewall.

L’obiettivo di questo progetto sarà quello di permettere la sostituzione degli attuali Firewall con una soluzione omogenea per tutte le sedi garantendo scalabilità di modelli in base alle singole esigenze.

I firewall considerati dovranno rispondere all’esigenza di permettere una più semplice configurazione ed un efficiente e ben noto processo di formazione dei responsabili IT.

La soluzione di firewall proposta da Progel è da ricercarsi nella famiglia di prodotti Cisco ASA.

La famiglia di dispositivi di sicurezza Cisco ASA consente di proteggere reti aziendali di tutte le dimensioni. Offre agli utenti un accesso ai dati altamente sicuro, ovunque, in qualsiasi momento e con qualsiasi dispositivo. Questi dispositivi sono il frutto di più di 15 anni di leadership nella sicurezza di rete e nella tecnologia firewall di Cisco, con oltre 1 milione di appliance di sicurezza implementate nel mondo e moltissime realizzazioni eseguite da Progel.

Tra gli altri vantaggi, il software Cisco ASA permette di:

* + Integrare funzionalità come [IPS](http://www.cisco.com/en/US/products/ps5729/Products_Sub_Category_Home.html) e [VPN](http://www.cisco.com/en/US/netsol/ns1049/index.html)
  + Supportare le aziende nell'aumento delle capacità e delle prestazioni attraverso il raggruppamento in cluster (caratteristica che permette anche l’alta affidabilità richiesta in Arancho Doc)
  + Offrire una elevata disponibilità per applicazioni con elevata resilienza
  + Facilitare il routing dinamico e VPN site-to-site sulla base del contesto

### Navigazione internet

La navigazione internet avviene localmente ad ogni sede in maniera diretta senza utilizzo di proxy.

#### Necessità del cliente

Il cliente non ha espresso esigenze specifiche in merito alla navigazione degli utenti in internet.

#### Criticità rilevate

Si considera l’assenza di Proxy una criticità.

Un server proxy è un servizio che si interpone fra uno o più client e uno o più server per consentire l'accesso ad Internet (o più in generale ad un altro servizio di rete). Tipicamente il proxy è utilizzato per la navigazione in internet e si interpone fra la rete aziendale e la rete esterna. Il proxy intercetta le richieste dei client e le inoltra (a “proprio nome”) ai server.

Questo meccanismo consente numerose funzionalità inerenti la sicurezza, il controllo degli accessi, le prestazioni e il controllo del traffico.

* La sicurezza è migliorata:
  + Perché le richieste verso server (esterni) avvengono attraverso il proxy, quindi un solo e ben identificato punto di interfaccia verso l'esterno, facile da manutenere, controllare e gestire. I client sono “schermati” dal proxy.
  + Il proxy è anche in grado di monitorare il traffico bloccandolo quando è ritenuto dannoso (virus e affini).
* Le prestazioni:
  + I proxy svolgono funzioni di cache. I risultati delle richieste dei client (pagine web) vengono memorizzate localmente, sul server proxy, successive richieste degli stessi dati sono soddisfatte usando i dati in cache locale e non con ulteriore traffico verso la rete pubblica.
  + L’accesso ad Internet è quindi meno utilizzato e la velocità di presentazione di pagine web migliorata perché buona parte dei dati richiesti sono su una memoria locale.
* Controllo Accessi:
  + Il proxy è in grado di autorizzare le connessioni in funzione della risorsa richiesta (una particolare pagina web, un sito). L’autorizzazione può essere concessa o negata alla utenza che viene identificata attraverso autenticazione. Solo gli utenti autorizzati possono usare Internet e le relative risorse.
* Controllo del traffico:
  + Il proxy, essendo interessato a tutto il traffico client/server, è in grado di operare sul tipo di contenuto in funzione di politiche aziendali, quindi bloccare particolari siti o pagine web, ma anche negare traffico potenzialmente pericoloso come virus o non desiderato (content filtering).

#### Proposta Evolutiva

Al fine di superare le criticità rilevate e aumentare il livello di sicurezza della navigazione Internet si consiglia l’utilizzo di un’architettura proxy centralizzata nella sede di Bologna.

La soluzione proposta da Progel è da ricercarsi nella famiglia BlueCoat ProxySG. Si tratta di una soluzione ampiamente consolidata di un leader riconosciuto a livello mondiale.

La soluzione BlueCoat può essere implementata sia in modalità appliance virtuale che mediante appliance fisica, sia on cloud che on site.

Si attiverà quindi una fase di analisi congiunta assieme al cliente, per identificare quale soluzione risponda al meglio rispetto alle evoluzioni della propria architettura.

### Pubblicazione servizi Internet, Accelerazione e Bilanciamento

#### DNS

Su tutti i Domain Controller è replicato il servizio DNS, quindi tutte le sedi tranne quella di Zurigo (che non ha server DC) utilizzano un server DNS locale per la risoluzione dei nomi.

Nella sede di Bologna i server DNS sono due BLQ-SRV01 e MIL-SRV01.

La gestione dei DNS pubblici viene erogata tramite il servizio NO-IP di Aruba per l’Italia e CHNET per la Svizzera.

Le richieste di risoluzione per i nomi Internet vengono reindirizzate dai server DNS interni ai server DNS di Google: 8.8.8.8 e 8.8.4.4

Di seguito le zone rilevate relative ai domini AD locali:

* aranchodoc.corp
* icdoc.local

Di seguito le zone relative ai domini pubblici:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Description: http://adam/pics/puce-up.png**[**Name**](http://adam/front/contract.php?itemtype=Contract&sort=1&order=DESC&start=0&field%5b0%5d=view&contains%5b0%5d=&searchtype%5b0%5d=contains&field2%5b0%5d=view&contains2%5b0%5d=&searchtype2%5b0%5d=contains) | [**Entity**](http://adam/front/contract.php?itemtype=Contract&sort=80&order=DESC&start=0&field%5b0%5d=view&contains%5b0%5d=&searchtype%5b0%5d=contains&field2%5b0%5d=view&contains2%5b0%5d=&searchtype2%5b0%5d=contains) | [**Type**](http://adam/front/contract.php?itemtype=Contract&sort=4&order=DESC&start=0&field%5b0%5d=view&contains%5b0%5d=&searchtype%5b0%5d=contains&field2%5b0%5d=view&contains2%5b0%5d=&searchtype2%5b0%5d=contains) | [**Number**](http://adam/front/contract.php?itemtype=Contract&sort=3&order=DESC&start=0&field%5b0%5d=view&contains%5b0%5d=&searchtype%5b0%5d=contains&field2%5b0%5d=view&contains2%5b0%5d=&searchtype2%5b0%5d=contains) | [**Start date**](http://adam/front/contract.php?itemtype=Contract&sort=5&order=DESC&start=0&field%5b0%5d=view&contains%5b0%5d=&searchtype%5b0%5d=contains&field2%5b0%5d=view&contains2%5b0%5d=&searchtype2%5b0%5d=contains) | [**Expiration**](http://adam/front/contract.php?itemtype=Contract&sort=12&order=DESC&start=0&field%5b0%5d=view&contains%5b0%5d=&searchtype%5b0%5d=contains&field2%5b0%5d=view&contains2%5b0%5d=&searchtype2%5b0%5d=contains) | [**Initial contract period**](http://adam/front/contract.php?itemtype=Contract&sort=6&order=DESC&start=0&field%5b0%5d=view&contains%5b0%5d=&searchtype%5b0%5d=contains&field2%5b0%5d=view&contains2%5b0%5d=&searchtype2%5b0%5d=contains) |
| [**adconnex.com**](http://adam/front/contract.form.php?id=14) | Root entity | Domain Registartion + DNS Management |  | 12-10-2013 | 12-10-2014 | 12 month |
| [**arancho.com**](http://adam/front/contract.form.php?id=2) | Root entity | Domain Registartion + DNS Management |  | 28-08-2013 | 28-08-2014 | 12 month |
| [**aranchodoc.ch**](http://adam/front/contract.form.php?id=3) | Root entity | DNS Management |  | 07-12-2013 | 07-12-2014 | 12 month |
| [**aranchodoc.co.uk**](http://adam/front/contract.form.php?id=13) | Root entity | Domain Registration + Redirect |  | 26-11-2012 | 26-11-2014 | 24 month |
| [**aranchodoc.com**](http://adam/front/contract.form.php?id=4) | Root entity | Domain Registartion + DNS Management |  | 26-11-2013 | 26-11-2014 | 12 month |
| [**aranchodoc.es**](http://adam/front/contract.form.php?id=12) | Root entity | Domain Registration + Redirect |  | 26-11-2013 | 26-11-2014 | 12 month |
| [**aranchodoc.eu**](http://adam/front/contract.form.php?id=11) | Root entity | Domain Registration + Redirect |  | 26-11-2013 | 26-11-2014 | 12 month |
| [**aranchodoc.fi**](http://adam/front/contract.form.php?id=5) | Root entity | DNS Management |  | 07-12-2013 | 07-12-2014 | 12 month |
| [**aranchodoc.it**](http://adam/front/contract.form.php?id=9) | Root entity | Domain Registration + Redirect + PEC |  | 26-11-2013 | 26-11-2014 | 12 month |
| [**aranchodoc.jp**](http://adam/front/contract.form.php?id=21) | Root entity | Domain Registartion + DNS Management |  | 26-12-2013 | 26-12-2014 | 12 month |
| [**aranchodoc.net**](http://adam/front/contract.form.php?id=10) | Root entity | Domain Registration + Redirect |  | 26-11-2013 | 26-11-2014 | 12 month |
| [**aranchodoc.org**](http://adam/front/contract.form.php?id=7) | Root entity | Domain Registration + Redirect |  | 26-11-2013 | 26-11-2014 | 12 month |
|  |  |  |  |  |  |  |
| [**donatello.cz**](http://adam/front/contract.form.php?id=8) | Root entity | DNS Management |  | 23-12-2013 | 23-12-2014 | 12 month |
| [**icdoc.com**](http://adam/front/contract.form.php?id=15) | Root entity | Domain Registartion + DNS Management |  | 16-10-2013 | 16-10-2014 | 12 month |
| [**lifelingua.com**](http://adam/front/contract.form.php?id=16) | Root entity | Domain Registartion + DNS Management |  | 03-05-2013 | 03-05-2014 | 12 month |
| [**linguapool.ch**](http://adam/front/contract.form.php?id=22) | Root entity |  |  | -- |  |  |
| [**linguateam.es**](http://adam/front/contract.form.php?id=23) | Root entity | Domain Registration + Redirect |  | 31-01-2014 | 31-01-2015 | 12 month |
| [**linguateam.it**](http://adam/front/contract.form.php?id=24) | Root entity | Domain Registration + Redirect |  | 31-01-2014 | 31-01-2015 | 12 month |
| [**linguateams.com**](http://adam/front/contract.form.php?id=17) | Root entity | Domain Registartion + DNS Management |  | 03-05-2013 | 03-05-2014 | 12 month |
| [**motorlingua.com**](http://adam/front/contract.form.php?id=18) | Root entity | Domain Registartion + DNS Management |  | 03-05-2013 | 03-05-2014 | 12 month |
| [**technicalingua.com**](http://adam/front/contract.form.php?id=19) | Root entity | Domain Registartion + DNS Management |  | 03-05-2013 | 03-05-2014 | 12 month |

La maggior parte dei server utilizzati sono appartenenti ad uno dei due domini AD, fatta eccezione per alcuni server presenti in DMZ che attualmente non partecipano al dominio.

I servizi erogati dai server in DMZ vengono pubblicati direttamente con un server di reverse NAT Apache.

#### Servizi Erogati

I servizi erogati attraverso Internet utilizzano un meccanismo di alias che punta di volta in volta all’IP di Fastweb o di Acantho.

Il funzionamento è il seguente:

* Il client su internet richiede ad esempio **adconnex.aranchodoc.com**
* Il server DNS di NO-IP ha l’alias **adconnex** con **blq.aranchodoc.com**
* Al nome **blq.aranchodoc.com** corrisponde l’IP di Fastweb
* In caso il personale IT desideri fare manutenzione o ci si trovi in un caso di guasto della linea Fastweb è prassi modificare manualmente la risoluzione del nome con l’IP gestito da Acantho

Marte è il server Linux con O.S. Debian 5 che fa da reverse proxy per gli applicativi attraverso Apache e che eroga inoltre il servizio di relay di posta elettronica.

Tale server è posizionato all’interno della rete locale con IP 192.168.0.113.

Seguono i servizi erogati dalla sede di Bologna:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Servizio** | **Server** | **IP Privato** | **Port** | **Nota** | **Nota 1** |
| ADCONNEX | MADRID | 10.0.0.11 | 80,443 | Portale, SQL Server in DMZ; non ha connessione verso l'interno |  |
| FTS | VEGA | 192.168.0.108 | 80 | File Transfer System |  |
| BLQRDS01 | BLQ-RDS01 | 192.168.0.123 | 389 e altre per vari servizi | RDP, RDA (Remote Desktop Application) | Esposto direttamente in internet non in reverse Proxy |
| SITECORE-FTP | BLQ-FTP02 | 10.0.0.7 | 21 | FTP server | Esposto direttamente in internet non in reverse Proxy |
| SITECORE-FTP | BLQ-FTP01 | 192.168.0.112/10.0.0.3 | 21 | FTP Server vecchio | Esposto direttamente in internet non in reverse Proxy |

Non sono presenti sistemi di bilanciamento locale per la gestione dei carichi.

Non sono presenti sistemi di accelerazione applicativa o di banda internet.

#### Necessità del cliente

Il cliente non ha espresso esigenze specifiche in merito alla ripubblicazione dei servizi in internet, alla gestione del bilanciamento di servizi locali o di linee internet

#### Criticità rilevate

Le criticità rilevate riguardano:

* L’assenza di un sistema gestito di ripubblicazione
  + Attualmente ci si affida al solo sistema di NAT del firewall che non permette una inspection a livello applicativo
* L’assenza di sistemi di bilanciamento locale che non permette di avere sistemi applicativi in bilanciamento di carico o in alta affidabilità
* L’assenza di sistemi di accelerazione di banda applicativa
* La mancanza di gestione di un sistema di bilanciamento efficiente delle linee internet.

#### Proposta Evolutiva

Al fine di superare le criticità rilevate si consiglia di ripubblicare i servizi mediante opportune appliance che permettono di mettere in sicurezza gli applicativi espletando il ruolo di firewall inspection L4-L7.

In questo modo è possibile garantire la capacità di evidenziare comportamenti malevoli, derivanti da eventuali attacchi che sfruttino bachi dei servizi erogati, per compromettere i dati aziendali o causarne denial of service.

La soluzione proposta da Progel è la soluzione Kemp Loadmaster.

Kemp presenta una soluzione relativamente nuova sul mercato internazionale ma consolidata per quantità di installato.

Il sistema di bilanciamento LoadMaster gestisce automaticamente ed in modo intelligente il traffico generato dagli utenti e dalle applicazioni, assicurando l’integrità delle rispettive infrastrutture web. I prodotti KEMP ottimizzano tali infrastrutture rispondendo alle esigenze di alta disponibilità, alte prestazioni, scalabilità flessibile, intuitività e sicurezza con una particolare attenzione ai costi di implementazione.

Il prodotto Kemp LoadMaster è completamente certificato Microsoft ed è disponibile sia mediante appliance fisica, che virtuale, sia on cloud (sulla piattaforma Azure) che on site.

Per quanto riguarda la gestione della soluzione di alta disponibilità delle linee internet e DNS la soluzione proposta da Progel è il Radware Linkproof. Si tratta di una soluzione leader di mercato che permette di bilanciare su più connessioni internet i servizi erogati come la navigazione o la pubblicazione dei servizi erogati.

L’utilizzo di questa soluzione permetterà ad Arancho Doc di utilizzare contemporaneamente le linee Fastweb e Acantho garantendo come effetto immediato la somma delle due disponibilità di banda oltre ad una backup automatico.

### Sistema di monitoraggio

Per tenere sotto controllo lo stato di salute degli apparati esiste un apposito sistema di monitoraggio: Zabbix 2.2.1 (IP 192.168.0.148 zabbix.aranchodoc.corp).

Il sistema, che gestisce 33 sistemi, è erogato come VM su piattaforma VMware ESXi nella sede di Bologna. L’accesso avviene mediante http e tramite gli utenti di dominio del personale IT.

Al momento dell’analisi risultava in corso di attivazione la gestione degli allarmi mediante mail.

In appendice D sono riportate le principali configurazioni rilevate.

#### Necessità del cliente

Il cliente ha la necessità di avere un unico ed efficiente sistema di monitoraggio atto a mantenere sotto controllo tutto il sistema informativo aziendale.

#### Criticità rilevate

Il sistema di monitoraggio scelto da Arancho Doc risulta essere sufficiente per le esigenze del cliente, anche se non completamente configurato al momento della raccolta dati.

#### Proposta Evolutiva

Progel condivide con i clienti l’importanza di un ottimo sistema di monitoraggio che opportunamente configurato è il primo punto di visione ed allerta dei propri sistemi.

L’importanza che Progel da al monitoraggio è tale per cui non è possibile proporre ai propri clienti soluzioni open source la cui implementazione e sviluppo è affidato a privati e a blogger.

La soluzione proposta da Progel è la soluzione HP IMC (Intelligent Management Center).

Si tratta di una gestione completa che HP ha implementato per garantire il monitoraggio dei fault, il salvataggio delle configurazioni, la gestione degli apparati, il monitoraggio delle prestazioni ed altre funzionalità progettate per la gestione completa di infrastrutture di rete.

La soluzione HP IMC è modulare ed è possibile personalizzarla in base alle specifiche esigenze. Come soluzione di monitoraggio evoluta in Arancho Doc si consiglia l’implementazione della suite standard che oltre a garantire tutte le principali funzionalità di monitoraggio e raccolta dati permette di gettare le basi per moduli specifici che in futuro potrebbero risultare utili.

## Hardware

L’assessment dell’hardware è stato eseguito tramite visita on-site nel datacenter di Bologna e tramite compilazione foglio di raccolta dati da parte del cliente.

### Server

Di seguito la lista dei sistemi server presenti presso le sedi di Arancho Doc:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server Name** | **Critical level High/Medium/Low** | **Physical/Virtual** | **Role / Description** | **Operating System** | **Datacenter** |
|  |  |  |  |  |  |
| **BLQ-HV01** | High | Physical | Hyper-V node |  | BLQ |
| **BLQ-HV02** | High | Physical | Hyper-V node |  | BLQ |
| **BLQ-HV03** | High | Physical | Hyper-V node |  | BLQ |
| **Caronte** | High | Physical | Legacy app (web + sql) server | Windows 2003 | BLQ |
| **Vega** | Medium | Physical | File system IcDoc | Windows 2003 | BLQ |
| **Sole** | High | Physical | App server linux ( adrenalin ) | Debian 5 | BLQ |
| **Marte** | High | Physical | Reverse NAT , smtp2 server | Debian 5 | BLQ |
| **Mercurio** | Low | Physical | Domain controller IcDoc | Windows 2003 | BLQ |
| **BLQ-FTP02** | Medium | Virtual | New FTP server | Windows 2008 | BLQ |
| **Berlino** | High | Virtual | CAT Tool server - fino al 30/8/2014 | Windows 2008 R2 | BLQ |
| **Berlino2** | High | Virtual | CAT Tool server - dal 1/9/2014 | Windows 2008 R2 | BLQ |
| **BLQ-RDS01** | High | Virtual | Remote application server | Windows 2008 R2 | BLQ |
| **BLQ-SRV01** | Medium | Virtual | Domain controller AranchoDoc + DNS | Windows 2008 R2 | BLQ |
| **BLQ-SRV04** | High | Virtual | File System Server | Windows 2008 R2 | BLQ |
| **BLQ-SRV06** | High | Virtual | CAT Tool server | Windows 2008 R2 | BLQ |
| **Londra** | High | Virtual | ERP server ESA | Windows 2008 R2 | BLQ |
| **Madrid** | High | Virtual | AD Connex server, DMZ | Windows 2008 R2 | BLQ |
| **MIL-SRV01** | Medium | Virtual | Domain controller | Windows 2008 R2 | BLQ |
| **MIL-SRV02** | High | Virtual | Exchange server | Windows 2008 R2 | BLQ |
| **Roma** | High | Virtual | CAT Tool server | Windows 2008 R2 | BLQ |
| **Adam** | Medium | Virtual | Help desk sw |  | BLQ |
| **BLQ-FTP01** | Medium | Virtual | FTP server |  | BLQ |
| **BLQ-FWL01** | High | Virtual | Firewall | FreeBSD | BLQ |
| **Trust** | Medium | Virtual | server trusting ICDOC & Aranchodoc,corp domain |  | BLQ |
| **Vtiger** | High | Virtual | CRM server | Debian 6 | BLQ |
| **Zabbix** | Medium | Virtual | Inventory system tool server |  | BLQ |
| **HEL-ESX01** | High | Physical | Hypervisor | VmWare ESX 4.1 | HEL |
| **HEL-SRV01** | High | Virtual | DC, DNS, DHCP, Fileserver, Printserver | Windows 2008 R2 | HEL |
| **HEL-FWL01** | High | Virtual | Firewall | FreeBSD | HEL |
| **Plunet** | Low | Virtual | Vecchio gestionale | Windows 2003 | HEL |
| **PRG-ESX01** | High | Physical | Hypervisor | VmWare ESX 4.1 | PRG |
| **PRG-SRV01** | High | Virtual | DC, DNS, DHCP, Fileserver, Printserver | Windows 2008 R2 | PRG |
| **PRG-FWL01** | High | Virtual | Firewall | FreeBSD | PRG |
| **BCN-ESX02** | High | Physical | Hypervisor | VmWare ESX 4.1 | BCN |
| **BCN-SRV01** | High | Virtual | DC, DNS, DHCP, Fileserver, Printserver | Windows 2008 R2 | BCN |
| **BCN-FWL01** | High | Virtual | Firewall | FreeBSD | BCN |
| **BCNESX01** | High | Physical | Hypervisor | VmWare ESX 4.0 | BCN |
| **BCN01** |  | Virtual | Vecchio server | Windows 2003 | BCN |
| **RIM-ESX01** | High | Physical | Hypervisor | VmWare ESX 4.1 | RIM |
| **RIM-SRV01** | High | Virtual | DC, DNS, DHCP, Fileserver, Printserver | Windows 2008 R2 | RIM |
| **RIM-FWL01** | High | Virtual | Firewall | FreeBSD | RIM |
| **Database update** |  | Virtual | Gestione timbrature | Windows XP | RIM |
| **Licenze Trados 1** |  | Virtual | Server licenze trados | Windows 2003 | RIM |
| **Licenze Trados 2** |  | Virtual | Server licenze trados | Windows 2003 | RIM |
| **RIM01** |  | Virtual | Vecchio server Arancho con contabilità | Windows 2003 | RIM |
| **RIM02** |  | Virtual | Vecchio server Arancho con gestionale | Windows 2003 | RIM |
| **RIM-HV01** | High | Virtual | Server Hyper-V per backup offsite | Hyyper-V Server 2012 | RIM |
| **MIRESX01** | High | Physical | Hypervisor | VmWare ESX 4.1 | MIR |
| **MIR-SRV01** | High | Virtual | DC, DNS, DHCP, Fileserver, Printserver | Windows 2008 R2 | MIR |
| **MIR-FWL01** |  | Virtual | Firewall | FreeBSD | MIR |

Non c’è un solo vendor hardware di riferimento, sono presenti sistemi IBM, HP, Dell, e MAXDATA.

### Storage

Nella sede di Bologna sono presenti tre sistemi storage: 2 Dell PowerVault MD3200i (BLQ-SAN02) ed 1 NetApp FAS2050 (LUNA).

Il primo dei due storage Dell (SAN01) contiene 12 HDD da 1 TB 7.2k impostati in modalità Disk Pooling. Si tratta di una modalità proprietaria di questo specifico storage che gestisce in maniera dinamica l’allocazione dell’array e che ha prestazioni similari a quelle di un RAID 6.

Su questo storage è ospitata una LUN da 4TB utilizzata in modalità disk pass-through dal File Server BLQ-SRV04. Contiene i dati di archivio.

Il secondo dei due storage Dell (SAN02) contiene 8 HDD da 600 GB in RAID 10 e 4 HDD da 4TB 7.2k in RAID 5.

Sul RAID 10 sono definite due LUN (CL01-Quorum, CL01-VIRTUAL) utilizzate dal cluster Hyper-V e che ospitano la maggior parte delle VM.

Sul RAID 5 sono definite le seguenti LUN:

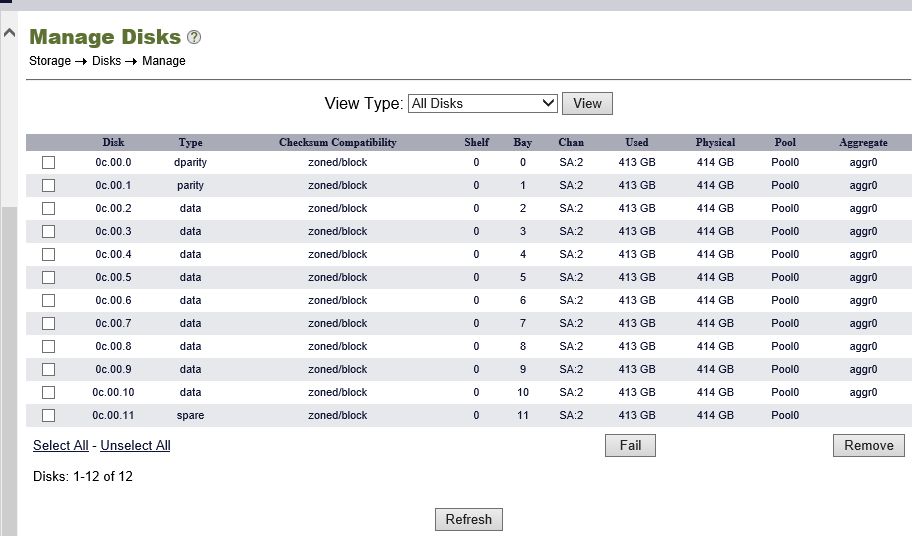
-Backup del volume su SAN01 (BCK01), tramite Windows Backup di BLQ-SRV04

-Disco per VMWare (500GB) (VMWDS01)

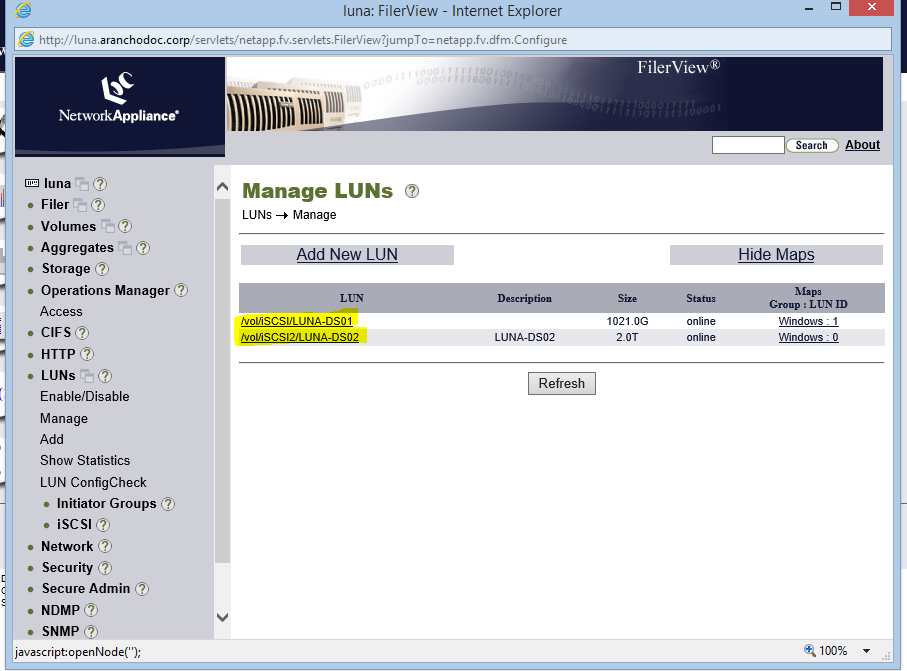
-1 LUN 500GB (CL01-virtual02)

-1 LUN 1TB per cluster (CL01-Volume5).

Lo storage NetAPP (LUNA) contiene invece 12 HDD da 500 GB SATA.



Su questi dischi sono definite due LUN, utilizzate dal cluster Hyper-V (LUNA-DS01, LUNA-DS02)



### Necessità del cliente

Il cliente si dichiara soddisfatto dell’attuale configurazione storage, ma ha intenzione di dismettere il NetAPP FAS2050, dato che ha una capacità limitata e che non è più sotto copertura in caso di guasti.

É in corso un’operazione per dismettere l’hardware più datato, ma non è chiaro quando si riuscirà a terminarla. I sistemi interessati sono:

* VEGA – Server Maxdata con Windows 2003 – Vecchio File Server IC DOC
* MERCURIO – Server HP ML350 con SBS 2003 – DC ed ex posta di IC DOC
* CARONTE – Server Maxdata con Windows 2003 – Applicativo DADAR con criticità massima
* MARTE – Server Dell PowerEdge 2950 con Linux Debian 5 – Reverse Proxy ed relay SMTP applicativo.

Nell’ottica della centralizzazione, c’è il desiderio di consolidare i dati delle sedi remote su quella di Bologna e di eliminare di conseguenza i sistemi delle relative sedi.

### Criticità rilevate

Il parco hardware non uniforme comporta un sovraccarico amministrativo nella gestione: diversi supporti tecnici in caso di guasti, siti differenti in caso di aggiornamenti e diversi software di management.

É stato fatto un tentativo di portare il sistema più critico (CARONTE) sull’ambiente di virtualizzazione, ma a seguito di test prestazionali insoddisfacenti il cliente ha deciso di interrompere la migrazione.

Questo risultato evidenzia la necessità di un approfondimento sull’ambiente di virtualizzazione ed il relativo storage per verificare la presenza di eventuali colli di bottiglia prestazionali e/o configurazioni errate.

### Proposta evolutiva

Consigliamo caldamente di effettuare una “vendor selection” ed identificare un vendor hardware univoco con il quale instaurare un rapporto consolidato che snellisca le operazioni di crescita, mantenimento e supporto del parco server aziendale.

Concordiamo con la scelta di dismettere lo storage Netapp FAS 2050, soprattutto a causa del supporto scaduto.

Per raggiungere l’obiettivo sarà necessario che il personale IT di Arancho Doc identifichi quali dati risiedano al suo interno, elimini eventuali dati inutilizzati ed inoltre verifichi quale possa essere una posizione alternativa per i dati utili.

## Sicurezza dei sistemi informativi

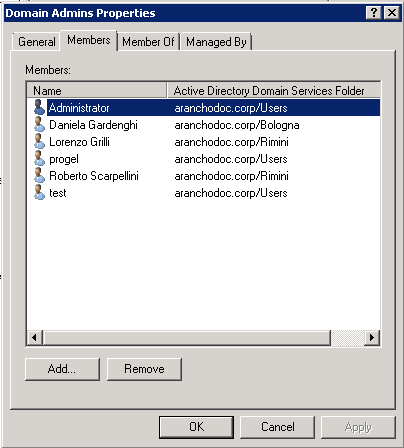
L’aspetto della sicurezza aziendale rispetto ai sistemi informativi, se sottovalutato, può portare a diverse perdite quali: furto di dati, malfunzionamento dei sistemi, distruzione di dati e sovraccarico del reparto IT per riparare i danni subiti.

Risulta quindi importante valutare quali varchi di sicurezza siano presenti ed investire risorse nella loro chiusura.

Di seguito quanto rilevato durante l’analisi dell’architettura di Arancho Doc.

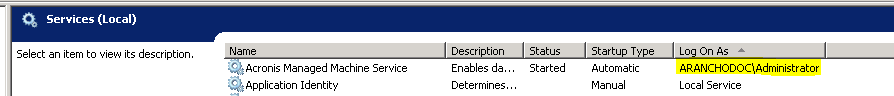
### Account

Gli amministratori di rete, ad eccezione di Daniele Sinchich, utilizzano un account personale che fa parte anche dei Domain Admins



L’utente built-in “*Administrator”* viene utilizzato da tutti i membri dell’IT per l’accesso ai server aziendali.

Lo stesso utente viene inoltre utilizzato per avviare servizi sui vari server.



Per quanto riguarda le postazioni client è stato rilevato che, da direttive aziendali, si è deciso che tutti gli utenti siano anche amministratori della loro postazione di lavoro.

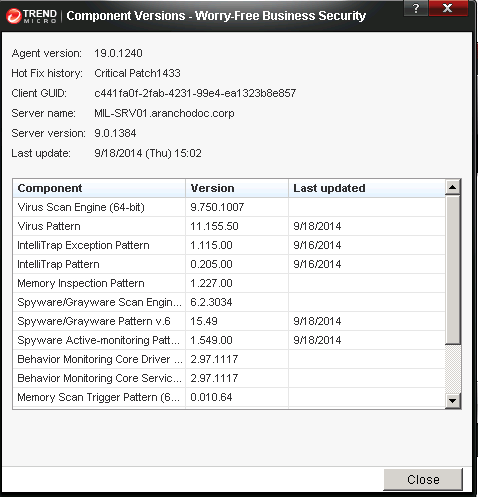
### Patching

Non è presente nessuna strategia di patching dei sistemi, l’installazione delle fix avviene a discrezione dell’operatore ogni volta che interviene su un qualsiasi sistema per manutenzione.

### Antivirus

Il server di gestione antivirus è MIL-SRV01, su di esso è presente Trend Micro Worry Free Business Security versione 9.

I componenti di detection del software Antivirus risultano correttamente aggiornati:



Il software si occupa della detection dei virus a livello file system sulle postazioni di lavoro e sui sistemi server. Incorpora inoltre un modulo per Exchange che si occupa della detection di virus e spam nei messaggi di posta elettronica.

Un ulteriore anti-spam e anti-malware viene utilizzato attraverso il modulo Trend Micro Hosted Email Security. Si tratta di un relay SMTP in-the-cloud che verifica le mail in entrata ed in uscita dalla posta aziendale.

Non è stato rilevato alcun sistema di Web Filtering, la navigazione Internet non risulta pertanto controllata.

### Necessità del cliente

Negli scorsi anni il personale IT aveva iniziato un’attività di rimozione dei diritti amministrativi agli utenti sulle loro postazioni, in modo da aumentare il livello generale di sicurezza. Tale attività è stata interrotta e i permessi amministrativi ristabiliti a seguito delle nuove direttive fornite dopo la fusione aziendale.

Al personale IT piacerebbe riprendere questa tematica per ristabilire un sufficiente livello di sicurezza nel parco client.

### Criticità rilevate

L’account built-in *Administrator* è uno dei principali bersagli degli attacchi informatici in ambito security: si tratta infatti di un account noto e con i massimi diritti sull’ambiente. Il furto di questa identità consente pieno controllo di tutto l’ambiente.

Il fatto che ne venga fatto un uso frequente, che la relativa password sia nota a più persone e che non scada, aumenta il relativo rischio di furto di identità.

Non è inoltre best-practice utilizzare tale account per avviare servizi applicativi: è infatti buona norma usare specifici “Account di Servizio” dedicati, con password complessa, nessuna scadenza, ma nessun utilizzo interattivo.

La mancata strategia di patching aumenta nei sistemi il rischio di lasciare aperti dei varchi di sicurezza che possano essere sfruttati da virus o da attacchi informatici.

Anche il mancato filtro sulla navigazione aumenta il rischio di lasciare aperti tali varchi. Le moderne minacce virali, sono infatti complesse e prevedono vari punti di ingresso, tra cui quello web.

Un esempio eclatante sono le minacce di phishing, dove l’utente viene invitato via mail a cliccare su di un “fake link” che lo porta su siti web dedicati al furto di identità.

### Proposta evolutiva

Ci sentiamo di consigliare, se possibile, la ripresa delle operazioni di rimozione dei diritti amministrativi sulle postazioni degli utenti, in modo da abbassare il rischio di attività dannose, generate da malware che si impossessino della sessione utente.

Per quanto riguarda gli amministratori IT ci sembra opportuno consigliare l’adozione della strategia della doppia identità. Si tratta di utilizzare un utente personale “User” per le attività quotidiane, ed un utente personale “Admin” per la connessione ai sistemi server.

Le problematiche legate all’utente built-in “*Administrator”* possono essere gestite con differenti strategie. Quella più semplice è di cambiarne la password con una complessa e dismetterne l’impiego per l’accesso ai sistemi server.

Tale account non dovrebbe inoltre essere impiegato per l’avvio di servizi applicativi ma sostituito con specifici “Service Account”.

Ci sono poi strategie più avanzate per la gestione di questo utente quali la rinomina, la creazione di un utente “Administator” fake e la sua disabilitazione, ma che consigliamo di prendere in esame solo dopo aver applicato la strategia base di cui sopra.

Per quanto riguarda l’applicazione delle fix sui sistemi, ci sembra opportuno che venga applicato un metodo strutturato e basato sul tool WSUS di Microsoft.

Attraverso tale strumento sarà possibile applicare in maniera sistematica e precisa le fix sui sistemi, gestendo eventuali eccezioni quali sistemi ad applicazione manuale e sistemi da escludere per motivi applicativi.

Per quanto riguarda il sistema di protezione dai malware, ci sentiamo di consigliare l’adozione di un meccanismo di web filtering, in modo da inibire gli accessi, volontari o meno, a tutti quei siti che potrebbero comportare una minaccia per i sistemi ed i dati aziendali.

## Sistema di Identity

Il cuore di un sistema informatico è il suo sistema di Identity, attraverso il quale vengono gestiti gli accessi degli utenti, assegnati i relativi permessi di utilizzo delle risorse e distribuite le policy aziendali.

Presso Arancho Doc il sistema di Identity è basato su Microsoft Active Directory alla versione 2008 R2.

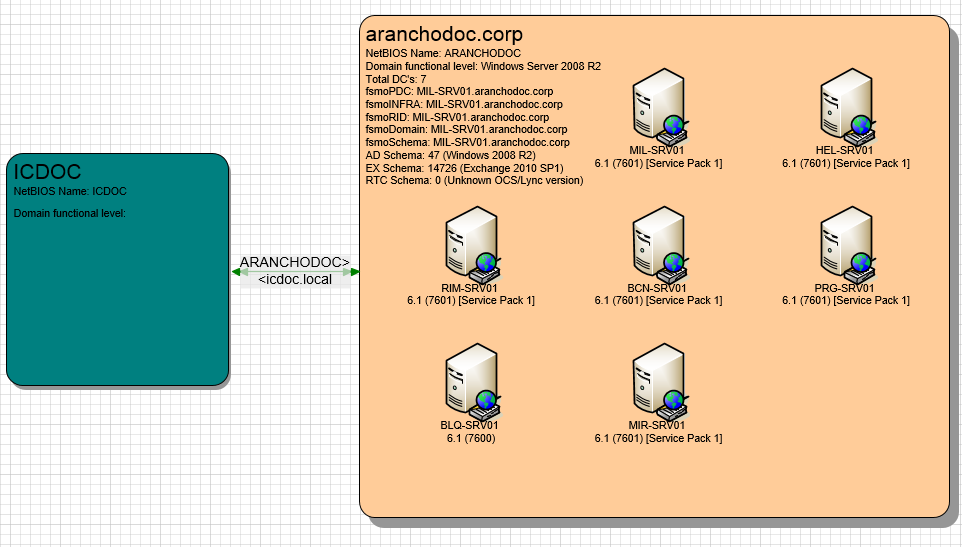
### Architettura Logica

L’architettura logica di Active Directory è basata su due domini: ***aranchodoc.corp***, dominio principalein trust con un vecchio dominio SBS 2003, ***ICDOC***, in fase di dismissione.

I servizi di dominio sono erogati attraverso 7 Domain Controller: MIL-SRV01, HEL-SRV01, RIM-SRV01, BCN-SRV01, PRG-SRV01, BLQ-SRV01, MIR-SRV01.

Tutti i ruoli FSMO sono erogati attraverso il DC MIL-SRV01, tutti i server sono anche Global Catalog.

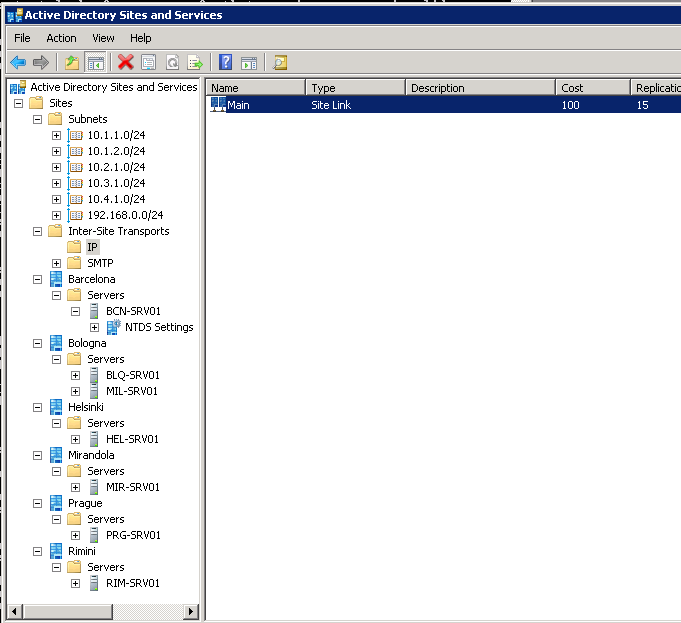
Il Domain Functional Level è a livello Windows 2008 R2, quindi sono erogate tutte le funzionalità disponibili per l’attuale versione dei DC.



### Architettura fisica

Sono presenti 6 site AD: Barcelona, Bologna, Helsinki, Mirandola, Prague, Rimini.

Ogni site ha un Domain controller, ad eccezione di Bologna che ne ha due.



Per la replica è stato creato un unico site link, definendo pertanto un’architettura di replica detta *Full Mesh*, dove tutti i DC replicano tra di loro.

Nella sede di Bologna sono servite indicativamente 40 utenze, in quella di Mirandola e Rimini indicativamente 10 ciascuna, mentre altre 30 utenze sono servite complessivamente attraverso gli altri 3 siti.

### Necessità del cliente

La trust con il dominio ***ICDOC*** doveva già essere dismessa da tempo ed è desiderio del cliente la sua rimozione a seguito della dismissione del sistema SBS2003. L’operazione è legata allo spostamento di un software di rilevazione presenze che non è stato portato a termine per mancanza di tempo.

Rispetto al dominio ***aranchodoc.corp*** è desiderio del cliente semplificarne l’architettura, andando a potenziare i link geografici e rimuovendo i DC dalle sedi periferiche. L’intenzione sarebbe quella di accentrare quanto più possibile sulla sede di Bologna ed assegnare alla sede di Rimini il ruolo di sito secondario, eliminando gli altri DC.

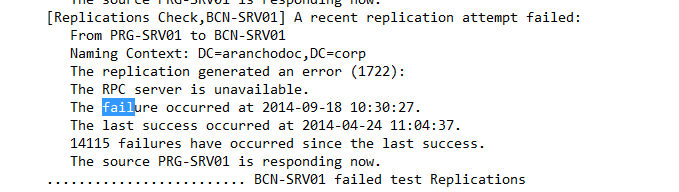
### Criticità rilevate

Sui DC è stata rilevata la presenza di software di terze parti e/o servizi applicativi. E’ buona norma lasciare che i DC eseguano solo il loro compito, oltre ai normali servizi di infrastruttura, quali DNS e DHCP. Questa strategia semplifica notevolmente il mantenimento e l’eventuale aggiornamento del sistema di directory, nonché la gestione ordinaria e straordinaria.

A livello di architettura logica, è stata rilevata una discrepanza tra l’architettura *Full Mesh* impostata tramite l’unico Site Link “Main” e la reale architettura di rete.

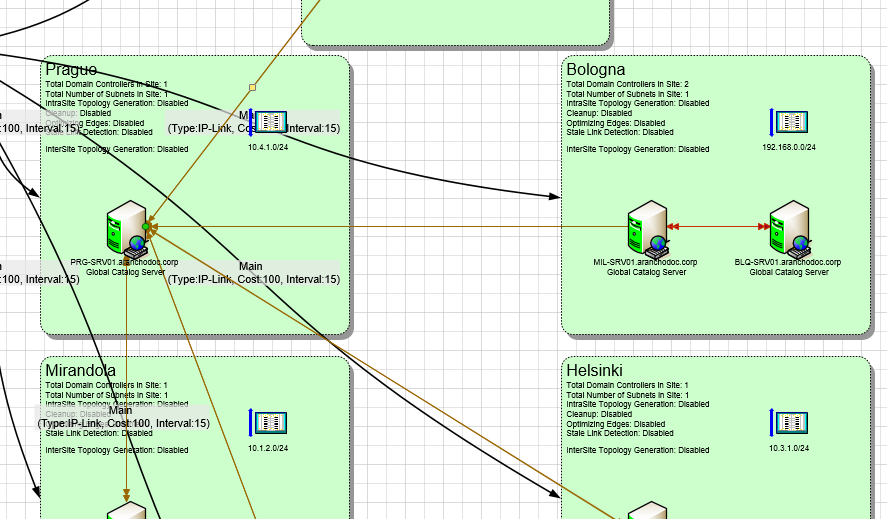
L’architettura *Full Mesh* prevede infatti che tutte le sedi possano contattare tutte le altre, mentre sul campo è stato rilevato che questo non è sempre vero.

Ad esempio sono stati rilevati problemi di replica tra siti, in corso anche da molti mesi:



Il motivo principale di questi problemi è legato al fatto che i meccanismi di replica di AD, basandosi sull’architettura impostata, hanno eletto uno dei siti come centro stella, ma in maniera casuale.

Attualmente il centro stella per le repliche è diventato il sito di Praga:



É importante inoltre segnalare come la presenza di Writable DC sulle sedi remote comporta un possibile buco di sicurezza. Il motivo è legato alla scarsa sicurezza fisica che spesso si trova nei locali che ospitano i DC.

Esiste infatti il rischio che, a fronte del furto di un server, vengano compromesse tutte le identità aziendali attraverso un meccanismo di Brute Force Attack.

Per ovviare a questo tipo di problema, Microsoft ha introdotto a partire da Windows 2008 R2 il ruolo di Read Only Domain Controller (RODC).

Segnaliamo infine che ad uno dei Domain Controller (BLQ-SRV01) non sia stato applicato il Service Pack 1 di Windows 2008 R2 come invece fatto per gli altri DC.

### Proposta evolutiva

Consigliamo come prima cosa l’allineamento di BLQ-SRV01 allo stesso livello di Service Pack degli altri DC: SP1.

Ci sentiamo poi di consigliare una review della definizione dei Site Link, con una modalità a centro stella su Bologna che rispecchi la volontà di accentramento dei sistemi. I site link dovranno rispecchiare la reale connettività geografica.

Successivamente, dopo aver verificato che i meccanismi di replica saranno nuovamente funzionanti, sarà possibile, se le linee lo consentiranno, la rimozione del ruolo locale di DC nelle sedi remote.

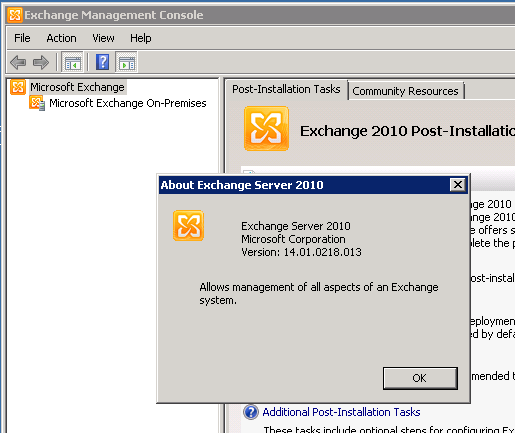
Ove non sarà possibile rimuovere i DC consigliamo la conversione dei Writable DC in RODC.

Consigliamo poi di proseguire nelle operazioni di dismissione del dominio ICDOC, in modo da eliminare un Hardware obsoleto e semplificare l’infrastruttura di Identity.

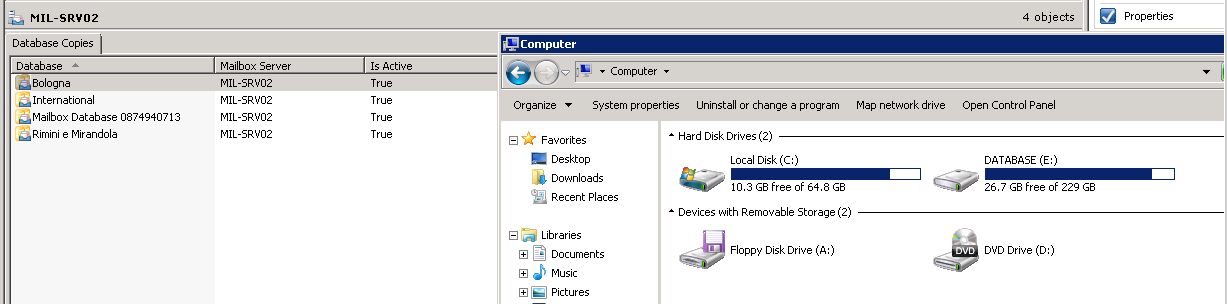
## Sistema di Posta Elettronica

### Architettura

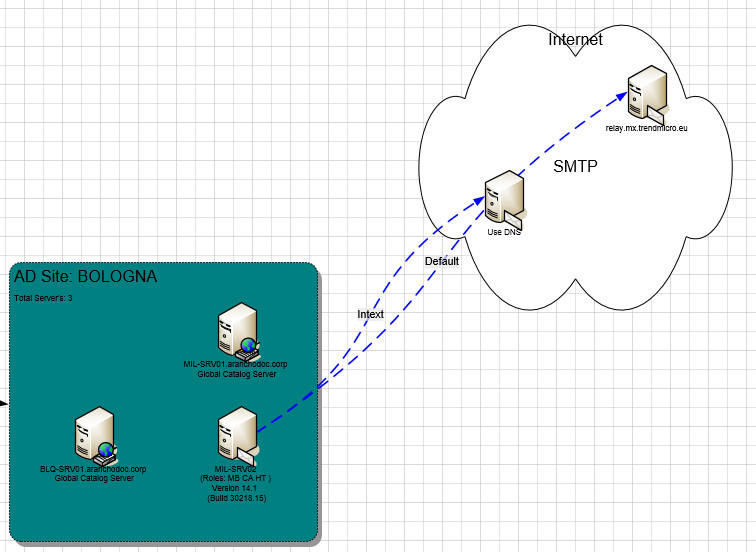
Il sistema di posta elettronica di Arancho Doc è basato su di un unico server Microsoft Exchange 2010 Sp1, **MIL-SRV02**. Si tratta di una Virtual Machine erogata dal cluster Hyper-V.



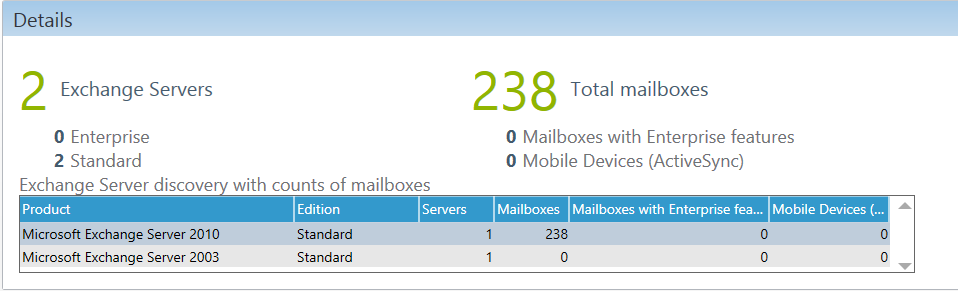
Il server gestisce 4 DB di posta per circa 200 GB di caselle postali.



La ricezione e spedizione dei messaggi avviene attraverso l’SMTP server in cloud relativo a Trend Micro Hosted Email Security.



Da una verifica effettuata tramite utility MAP di Microsoft, è stato rilevato che sul server sono presenti 238 mailbox.



L’altro server Exchange 2003 rilevato è in realtà il server SBS 2003 non più usato per la posta ed in fase di completa dismissione.

Come già visto nel capitolo “Antivirus”, sul server è presente un agent Trend Micro per la scansione dei messaggi.

### Necessità del cliente

Il cliente è soddisfatto del proprio servizio di posta elettronica ma lo considera un servizio critico per l’azienda.

Per questo ha espresso tra i propri desideri quello di aumentarne la resilienza attraverso un meccanismo di alta affidabilità o di failover geografico.

### Criticità rilevate

La versione di service pack rilevata (SP1) risale all’anno 2010, mentre l’ultimo service pack (SP3) è del 2013, al quale sono succeduti diversi Update Rollup, tra i quali il più recente è l’UR7: <http://support.microsoft.com/kb/2961522>

Il sistema risulta quindi scoperto di circa 4 anni rispetto a bug e vulnerabilità, un lasso di tempo troppo ampio per un sistema considerato critico.

### Proposta evolutiva

La prima azione che ci sentiamo di consigliare è sicuramente un’attività di aggiornamento del software per allinearlo all’ultimo service pack ed alle ultime hotfix.

Per incrementarne la resilienza consigliamo poi di valutare gli scenari di alta disponibilità offerti da Microsoft Exchange 2010 attraverso il meccanismo di DAG: <http://technet.microsoft.com/en-us/library/dd979781(v=exchg.141).aspx>

In alternativa ci sentiamo di consigliare la valutazione del passaggio dei servizi di messaging allla modalità cloud based, tramite il servizio Microsoft Office 365:

<http://products.office.com/en-us/business/explore-office-365-for-business>

Quest’ultima soluzione consentirebbe di avere un sistema di messaging costantemente aggiornato ed efficiente, senza gravare in alcun modo sul personale IT interno all’azienda.

## Server Virtualization

La virtualizzazione dei Server è uno dei temi più caldi degli ultimi anni, non c’è azienda dotata di reparto IT che non abbia approcciato questa tecnologia, grazie alla quale è possibile ottimizzare l’impiego delle risorse hardware, che ne semplifica la gestione e che rende possibili scenari prima impensabili.

Arancho Doc ha affrontato questa tematica scegliendo di adottare le soluzioni di Server Virtualization dei due principali vendor: Microsoft Hyper-V e VMWare.

### Hyper-V

Il principale ambiente Hyper-V è presente nella sede di Bologna ed è costituito da un cluster Hyper-V 2012 a tre nodi, BLQ-CL01.

Il sistema operativo dei tre nodi è Hyper-V Server 2012, si tratta di un’edizione free del sistema operativo Windows Server 2012 con diverse limitazioni:

* Licensing: non è compresa alcuna licenza per i sistemi operativi delle VM guest.
* Funzionalità: il sistema è dotato solo di Hypervisor e servizio di failover clustering, mancano invece tutte le altre funzionalità comprese nell’OS base, tra cui spiccano le interfacce di gestione.

Nella seguente tabella sono riepilogati i parametri principali dei nodi Hyper-V:

|  |  |  |  |
| --- | --- | --- | --- |
| **Server Name** | **Model** | **RAM** | **CPU** |
| **BLQ-HV01** | Dell PowerEdge R620 | 64GB | Intel Xeon E5-2630 2.30GHz |
| **BLQ-HV02** | IBM System x3650 M3 | 64GB | Intel Xeon E5620 2.40GHz |
| **BLQ-HV03** | Dell PowerEdge T710 | 96GB | Intel Xeon X5550 2.67GHz |

L’elenco completo dei parametri rilevati sul cluster Hyper-V è riportato inappendice E.

Oltre al cluster **BLQ-CL01** è stato rilevato un server Hyper-V nella sede di Rimini: **RIM-HV01**

Si tratta però di una configurazione anomala e non supportata, dove l’hypervisor Microsoft è installato in una VM ospitata su di un hypervisor VMWare.

A questo articolo VMware i dettagli della configurazione:

<http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2044876>

Questa la frase più significativa:

*“Hyper-V functionality inside VMware is experimental and is unsupported”*

### VMWare

La tecnologia VMware è stata adottata da Arancho Doc precedentemente rispetto ad Hyper-V ed è impiegata in tutte le sedi, comprese quelle remote.

Questi i sistemi rilevati:

* BLQ-VH03 – ESXi 5.0.0 – Sede di Bologna
* HEL-ESX01 – ESXi 4.1 – Sede di Helsinki
* PRG-ESX01 – ESXi 4.1 – Sede di Praga
* BCN-ESX02 - ESXi 4.1 – Sede di Barcellona
* BCNESX01 – ESXi 4.0 – Sede di Barcellona
* RIM-ESX01 – ESXi 4.1 – Sede di Rimini
* MIRESX01 – ESXi 4.1 – Sede di Mirandola

Anche in questo caso la scelta fatta riguarda versioni free dell’Hypervisor, quindi dotate di un set ridotto di funzionalità.

Il dettaglio delle configrazioni rilevate su BLQ-VH03 è riportata all’appendice F.

Le VM ospitate sull’ambiente di Bologna sono costituite da alcuni client e diverse macchine con distribuzioni Linux, tra cui il firewall PFsense.

Sulle sedi remote sono presenti i sistemi Windows Server di sede (DC, File server, ecc..) oltre al firewall PFsense.

### Necessità del cliente

Il cliente si dichiara soddisfatto dei risultati ottenuti con Microsoft Hyper-V ed ha iniziato una transizione delle VM verso tale ambiente. L’operazione si è interrotta a causa di problemi rilevati nella migrazione delle macchine firewall PFsense.

Il fulcro del problema è il sistema operativo della VM PFsense: FreeBSD versione 8.3.

Basandosi sull’intenzione del cliente di centralizzare i sistemi attualmente presenti nelle sedi remote, la presenza di una VM firewall (PFsense) risulta di fatto un vincolo alla dismissione dei relativi hypervisor VMware.

Si rende quindi necessaria una valutazione di dettaglio per capire quale sia la strategia migliore che consenta di sostituire il firewall software.

Il cliente ha inoltre espresso dei dubbi rispetto alla capacità dell’attuale ambiente di virtualizzazione Hyper-V di accogliere il carico dei sistemi provenienti dalle sedi periferiche.

### Criticità rilevate

Il cluster Hyper-V risulta costituito da nodi piuttosto variegati, per quanto riguarda Vendor e caratteristiche tecniche:

* BLQ-HV01 – Dell R620 – CPU Xeon E5-2630 – 64GB RAM (rack mounted)
* BLQ-HV02 – IBM x3650 M3 – CPU Xeon E5620 – 64GB RAM (rack mounted)
* BLQ-HV03 – Dell T710 – CPU Xeon X5550 – 96GB RAM (tower)

Sebbene questo tipo di configurazione sia consentita non segue le best practices in materia e, da esperienza diretta sul campo, espone al rischio di incorrere in diversi problemi:

* In caso di fail o manutenzione del nodo BLQ-HV03 (che ha 32 GB in più degli altri) c’è il rischio di “overcommit”, una situazione nella quale i nodi rimanenti non hanno abbastanza RAM per mantenere attive tutte le VM.
* Per poter migrare le VM tra nodi con processori di generazioni diverse (E5-xxxx vs E/X5xxx) è necessario limitare il set di istruzioni delle VM, con un potenziale calo prestazionale delle VM.
* Spostando una VM tra nodi con schede di rete differenti, potrebbero esserci comportamenti imprevisti che causano la mancata comunicazione della VM sulla rete. Il problema è solitamente legato ad implementazioni leggermente differenti delle stesse tecnologie da parte dei diversi vendor nei propri driver e firmware.

Come ulteriore criticità è stato rilevato che il disco **BLQ-SAN02-Volume5** risulta occupato oltre il 90%.

Testo alternativo generato dal computer:
BLQ-SAN02-V01u,ne5 
Volu— (I) 
DS02-VoIume5 (CftCIusterStorzgeWoIume5) 
CSVFS GB 1 024 GB 

Infine, come già riportato nel capitolo ***3.4 Hardware*** un tentativo di P2V della macchina CARONTE è fallito a causa delle scarse prestazioni rilevate in ambito virtuale.

### Proposta evolutiva

La presenza di più hypervisor moltiplica gli sforzi in termini di know-how, gestione, licenze e software.

Ci sembra pertanto coerente l’aver identificato Microsoft Hyper-V come hypervisor di riferimento per l’azienda e ci sembra quindi opportuno intensificare gli sforzi per cercare di portare tutto il parco VM su tale ambiente.

In particolare per quanto riguarda la distribuzione Linux FreeBSD, è stato rilevato che esiste il supporto da parte di Microsoft sulla base di determinati requisiti:

<http://blogs.technet.com/b/openness/archive/2012/08/09/available-today-freebsd-support-for-windows-server-hyper-v.aspx#.VB_kQu8cR9M>

Ribadiamo la necessità di una verifica approfondita sull’attuale ambiente virtuale Hyper-V al fine di evidenziare eventuali colli di bottiglia e/o errate configurazioni che possano giustificare le scarse prestazioni rilevate nel tentativo di migrazione della macchina CARONTE.

Ci sembra comunque opportuno, dopo aver effettuato l’hardware selection di cui al capitolo ***3.4 Hardware*** e aver effettuato una valutazione puntale sul carico di lavoro che sarà raggiunto con la centralizzazione dei sistemi remoti, effettuare la sostituzione degli attuali nodi Hyper-V con sistemi omogenei e opportunamente dimensionati. Il dimensionamento deve poter accogliere il carico di lavoro stimato e mantenere un 50% di risorse libere per crescita futura.

## Backup & Recovery

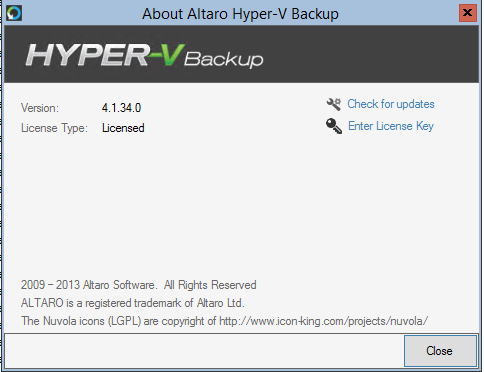
Le strategie di Backup & Recovery, spesso sottovalutate, se correttamente implementate posso consentire ad un’azienda di uscire rapidamente da una situazione disastrosa quale un incendio o la completa perdita di una sala CED per cause ambientali.

Arancho Doc ha attualmente implementato ben quattro soluzioni differenti di B&R: Altaro Hyper-V Backup, Acronis, Veeam e Windows Backup.

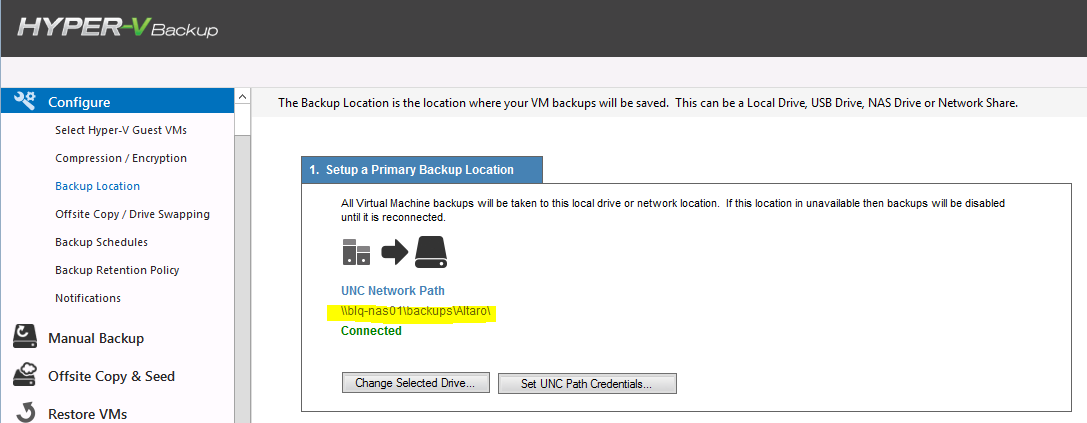
### Altaro

Si tratta di un software specifico per Microsoft Hyper-V, in grado di salvare le VM onsite ed offsite: <http://www.altaro.com/>

La versione rilevata è la 4.1.34.0, per la quale è stata acquistata regolare licenza d’uso.



Il salvataggio avviene via rete su di un NAS IOMEGA con un retention di 2 settimane.



Oltre alla copia sul NAS è impostata una copia offsite verso la sede di Rimini.

### Acronis

Si tratta di un software da tempo sul mercato, specializzato nell’image backup dei sistemi fisici.

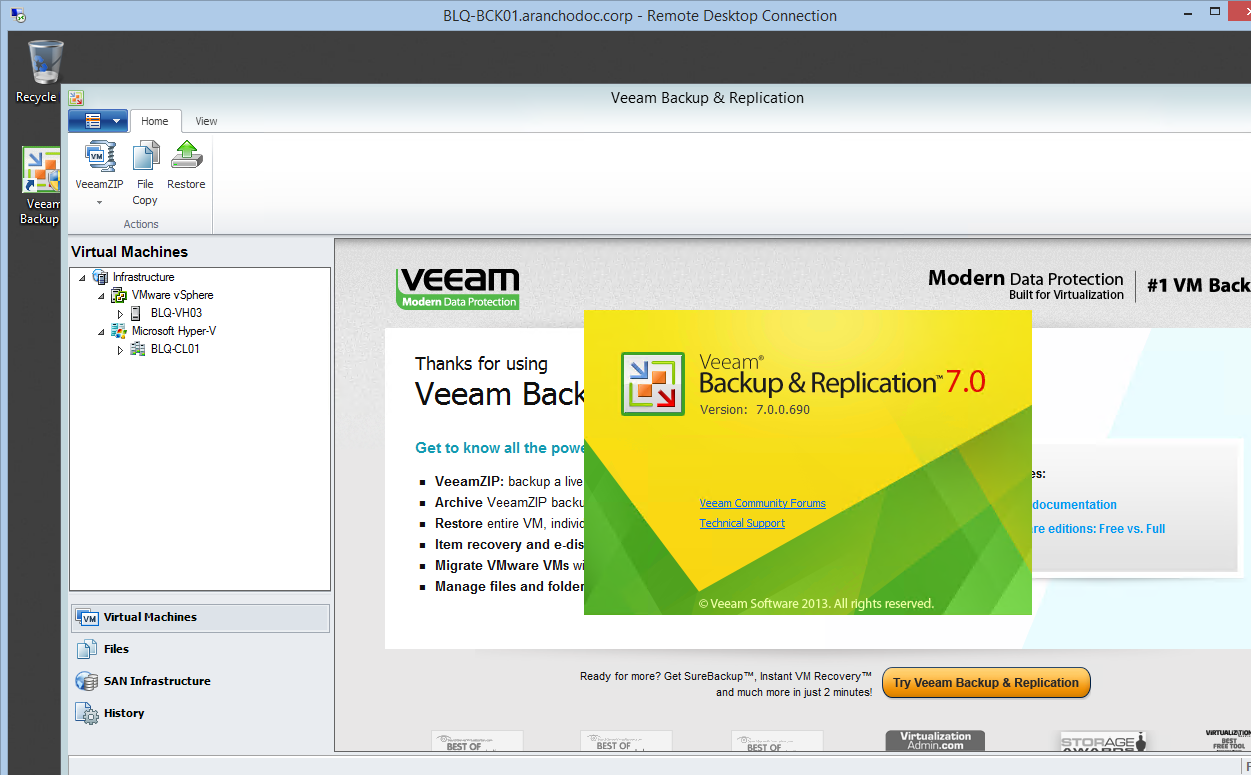
Viene impiegato per salvare il sistema CARONTE verso il NAS IOMEGA con una retention di circa 60 giorni. Non esistono meccanismi di backup offsite.

E’ stato inoltre impiegato per eseguire il P2V dei vari sistemi verso l’ambiente Hyper-V e il relativo agent risulta ancora installato sulle VM.

### Veeam

Si tratta di un software nato per la virtualizzazione, in rapida crescita e che consente salvataggio di ambienti virtuali sia Microsoft che Vmware. E’ stato recentemente esteso con funzionalità di Item Level Recovery e tape backup.

La versione rilevata a Bologna è la 7.0, con licenza free.



Viene utilizzato per salvare sul NAS IOMEGA le VM presenti su VMware, ma per la natura free della licenza, i salvataggi vanno effettuati manualmente.

Non esistono strategie di backup offsite.

### Windows Backup

Viene impiegato sul File Server per salvare i dati verso un altro volume connesso all’ambiente virtuale.

La retention è di circa 10 giorni, ma è variabile sulla base del volume dei dati salvati.

Non esistono strategie di backup offsite, inoltre il backup rimane all’interno dello stesso ambiente storage.

### Sedi remote

Sulle sedi remote sono presenti dei file server che effettuano una copia dei dati su NAS locale.

Non è configurato alcun backup a livello di VM.

Anche in questo caso non esiste una strategia di backup offsite.

### Necessità del cliente

Il cliente dichiara che finora le strategie di backup messe in atto hanno sempre soddisfatto le richieste di restore che si sono presentate.

Il cliente avrebbe comunque il desiderio di poter migliorare la retention dei propri salvataggi arrivando ad un risultato complessivo di 30 giorni.

La VM considerata più critica è quella di posta elettronica, la quale viene però salvata una sola volta alla settimana per problemi di tempo.

Il cliente dichiara che per salvare la VM in questione (circa 200GB) sono necessarie dalle 10 alle 15 ore.

Come eventuale sede per l’offsite dei backup si è identificata quella di Rimini.

### Criticità rilevate

Dall’analisi delle informazioni raccolte è evidente che manca una visione d’insieme delle strategie di Backup & Recovery, in termini di scelte tecnologiche, modalità e retention.

Risulta inoltre mancante un documento di Recovery che funga da guida per le varie situazioni che richiedano ripristino dei dati.

Il fatto di avere diverse soluzioni di backup comporta inoltre un sovraccarico amministrativo per il personale IT.

### Proposta evolutiva

Ci sembra opportuno intraprendere un percorso di review dell’ambiente di backup nella sua interezza con l’obiettivo di raggiungere i seguenti risultati:

* Semplificare la gestione
* Aumentare ed uniformare la retention dei dati
* Ottenere una strategia comune per il mantenimento offsite dei salvataggi
* Redigere e mantenere una documentazione di recovery che semplifichi tutte le procedure di ripristino, compreso un eventuale Disaster Recovery.

Il percorso sarà composto dalla seguente sequenza di operazioni:

* Effettuare una software selection, per identificare possibilmente un prodotto univoco di B&R che supporti le scelte effettuate in termini di hypervisor, applicativi e sistemi operativi.
* Dimensionare ed acquistare lo storage di backup primario, sulla base del volume di dati, della retention e delle performance necessarie.
* Identificare una modalità operativa per effettuare l’offsite dei salvataggi, scegliendo tra:
  + Backup su storage disco in altra sede (Rimini)
  + Backup su tape con trasporto offsite dei nastri
* Dimensionare ed acquistare il device identificato per il backup offsite
* Redigere un documento di recovery.

## Licensing

La verifica delle licenze è stata effettuata unicamente in ambito Microsoft, non sono stati pertanto valutati altri vendor.

La situazione rilevata è piuttosto variegata, in parte derivata dalla fusione delle due aziende (Arancho e IC Doc) ed in parte derivata da acquisti fatti senza una linea guida generale.

Sono infatti presenti licenze acquistate a volume, licenze OEM, licenze retail.

Questo il report delle licenze acquistate a volume, come riportato sul sito di licensing Microsoft del cliente:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Pool di prodotti*** | ***Famiglia di prodotti della licenza*** | ***Versione licenza*** | ***Quantità effettiva*** |
| *Applications* | *Office Professional* | *Plus 2010* | *1* |
| *Servers* | *Exchange Server - Standard* | *2010* | *1* |
| *Servers* | *Exchange Server Standard CAL - User CAL* | *2010* | *100* |
| *Servers* | *SQL - Device CAL* | *2012* | *1* |
| *Servers* | *SQL Server - Standard* | *2012* | *1* |
| *Servers* | *Windows Remote Desktop Services - User CAL* | *2008* | *5* |
| *Servers* | *Windows Server - Standard* | *2012* | *1* |
| *Servers* | *Windows Server - Standard* | *2008 Release 2* | *6* |
| *Servers* | *Windows Server - User CAL* | *2008* | *90* |

Oltre a queste licenze il cliente dichiara di conoscere:

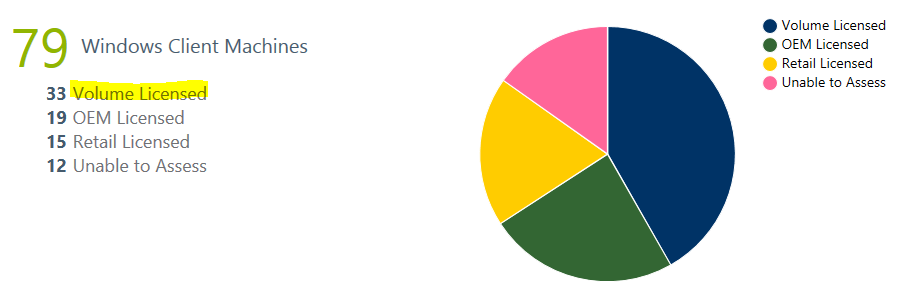
* 1 Licenza OEM Datacenter Windows 2008 R2 (associata ad uno dei nodi del cluster, su cui però c'è Hyper-V 2012)
* Molte licenze retail di Office Home and Business 2010 (25-30)
* 2 licenze retail di windows 7 ultimate
* 2 licenze retail di access 2010
* 1 licenza SQL associata al software di contabilità.

### Necessità del cliente

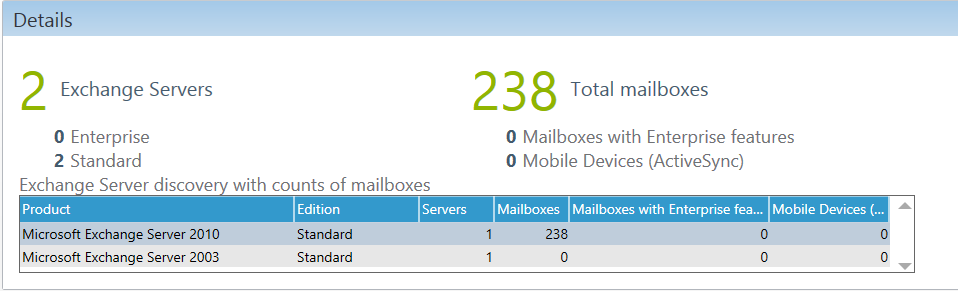
Il cliente è consapevole del fatto che non c’è un tracking preciso e che probabilmente ci sono situazioni di licenze scoperte.

### Criticità rilevate

Da una rapida verifica emergono già alcune incongruenze, ad esempio risultano 33 client licenziati a Volume, per i quali mancano le corrispettive licenze nella tabella sopra:



C’è una evidente incongruenza anche tra le CAL di posta licenziate (100) e le mailbox rilevate in produzione (238):



### Proposta evolutiva

Ci sentiamo di consigliare caldamente un assessment mirato per avere un quadro più chiaro della situazione licenze e poter sopperire ad eventuali lacune. In questo modo sarà possibile evitare di incorrere in problemi legali e/o penali.

Progel si rende disponibile a fornire eventualmente aiuto per effettuare l’assessment delle licenze.

# Conclusioni

L’analisi dei dati raccolti ha evidenziato la presenza di un’infrastruttura IT piuttosto variegata ed articolata, nella quale spesso convivono tecnologie diverse per rispondere a problemi simili.

Questa situazione è in parte legata alla recente fusione, durante la quale ogni azienda ha portato la propria eredità tecnologica nella nuova realtà, ma rende la gestione dell’infrastruttura più complessa.

Questa complessità risulta piuttosto elevata se rapportata al numero complessivo di utenze servite (meno di 100) e soprattutto se rapportata al numero di persone del reparto IT che si occupano di gestire l’ambiente (2 persone).

Ci sentiamo pertanto di consigliare il perseguimento di due obiettivi generali che possano guidare le future scelte in termini di infrastruttura IT: razionalizzazione e semplificazione.

Ottenere risultati in questi ambiti consentirà a sua volta di guadagnare in efficienza e risparmiare sui costi.

## Percorso evolutivo proposto

Per perseguire questi obiettivi, ci sembra opportuno che venga intrapreso un percorso evolutivo, basato sulle indicazioni fornite ai capitoli precedenti per ogni area oggetto di analisi.

Di seguito il percorso che ci sentiamo di suggerire come il più adegato.

La prima area su cui agire riguarda l’infrastruttura di rete, andando ad agire sul cablaggio strutturato degli armadi e relativa certificazione, sulla razionalizzazione della rete locale e Wifi, sull’aumento dell’efficienza dei link geografici.

Una volta ottenuta una solida base di rete, sarà possibile passare ad affrontare le tematiche legate ai sistemi.

Il primo aspetto da affrontare per quanro riguarda i server è sicuramente quello della dismissione dei sistemi obsoleti, partendo dal vecchio dominio SBS ***ICDOC.***

Una volta razionalizzati i server sarà poi la volta di effettuare una scelta in termini di hypervisor.

Tale scelta si intreccerà molto probabilmente con una scelta legata al sistema di firewall, dato che l’attuale firewall PFsense sembra avere difficoltà ad essere ospitato in ambito Microsoft Hyper-V.

Prima di poter quindi proseguire con le attività di razionalizzazione degli hypervisor potrebbe essere necessario affrontare un progetto che consenta di rivedere la propria soluzione firewall.

Una volta identificato l’hypervisor di riferimento il percorso proseguirà trattando queste tematiche:

* Hardware selection, per identificare su quale vendor investire ed acquisire un parco di hypervisor omogeneo
* Storage, per ospitare il nuovo ambiente virtuale e per l’accentramento dei dati attualmente presenti nelle varie sedi.
* Backup, per identificare il sistema (hardware e software) più adeguato a salvare il nuovo ambiente virtuale.

Si tratta di tre tematiche strettamente collegate tra di loro e che saranno affrontate in un progetto comune.

Una volta ottenuta quindi una solida base infrastrutturale in termine di rete e sistemi, sarà possibile affrontare i rimanenti ambiti:

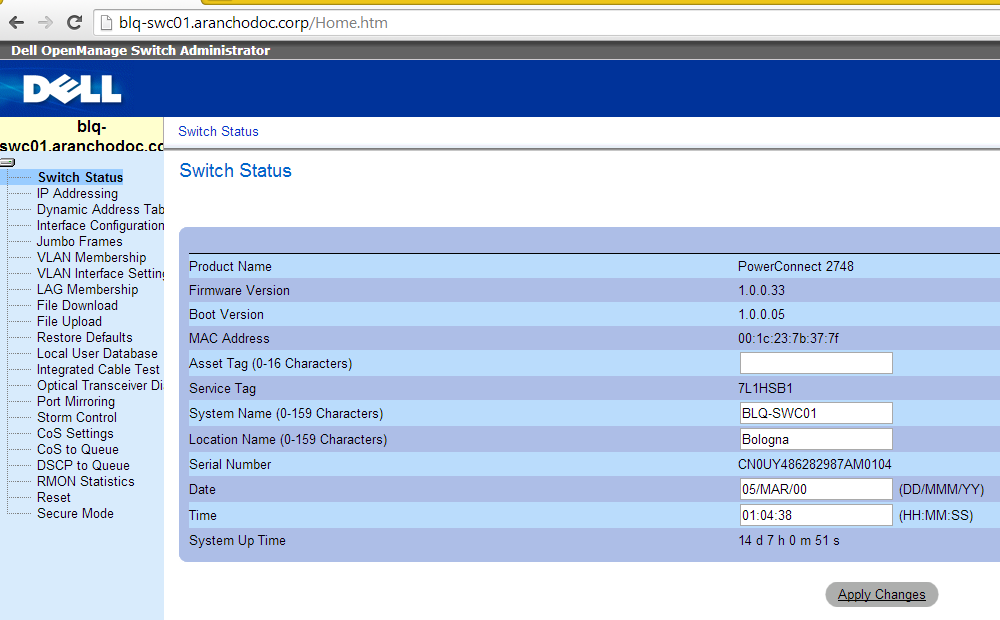
* Posta elettronica
  + Rendendo l’attuale sistema più efficiente
    - Aggiornando il sistema che risulta scoperto in termini di bug e vlnerabilità
    - Portandolo in alta affidabilità tramite meccanismi di DAG
  + In alternativa traslocando la posta in cloud tramite servizio Microsoft Office 365
* Navigazione Internet
  + Aumentandone sicurezza e controllo tramite un meccanismo di proxy
* Pubblicazione dei servizi su Internet
  + Aumentando la sicurezza dei servizi pubblicati attraverso apposito software di Firewall Inspection
* Monitoring
  + Verificando che l’attale software Zabbix sia coerente rispetto alle nuove scelte tecnologiche
  + Valutando come alternativa il software proposto da Progel: HP IMC
* Sicurezza dei sistemi informativi
  + Aumentando la sicurezza degli account amministrativi
  + Attivando un meccanismo strutturato di patching dei sistemi
  + Attivando un meccanismo di web filtering
* Licensing
  + Effettuando un assessment puntuale al fine di regolarizzare aventuali lacune

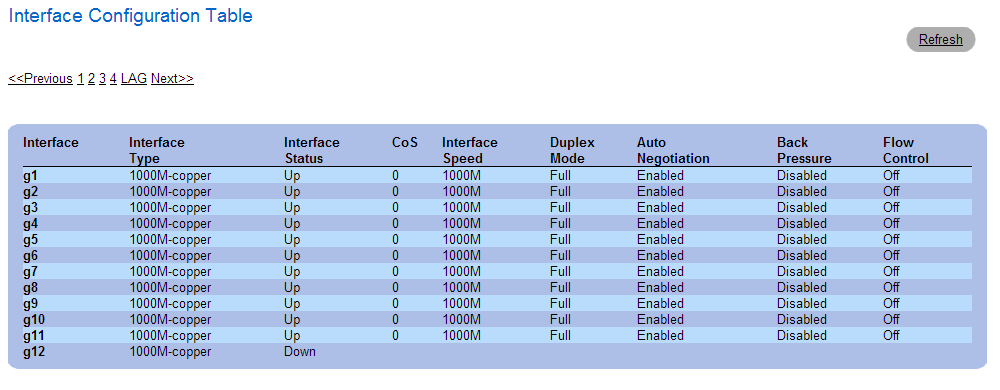
# Appendici

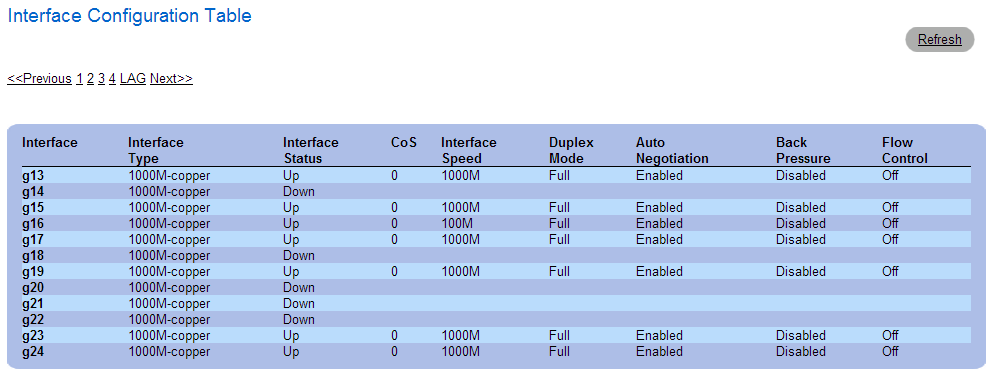
## A - Switch

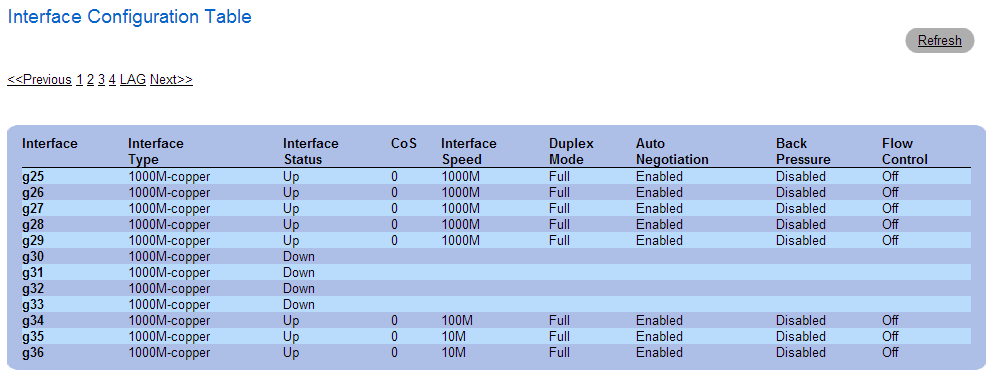
Seguono le configurazioni di massima degli switch di rete

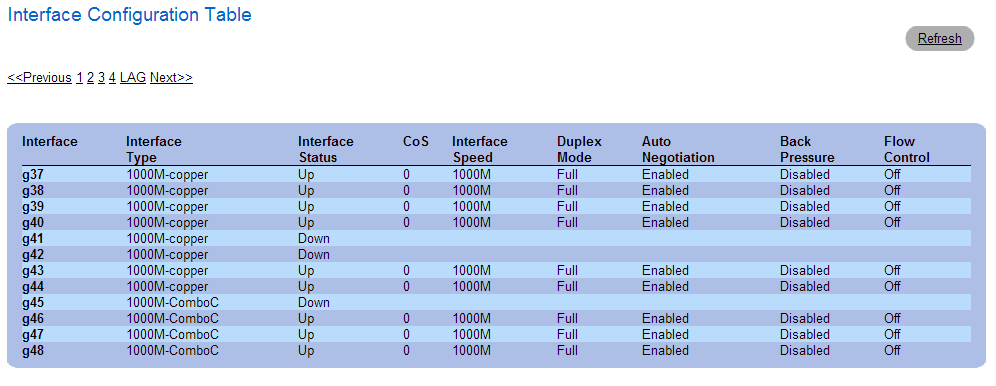
### blq-swc01

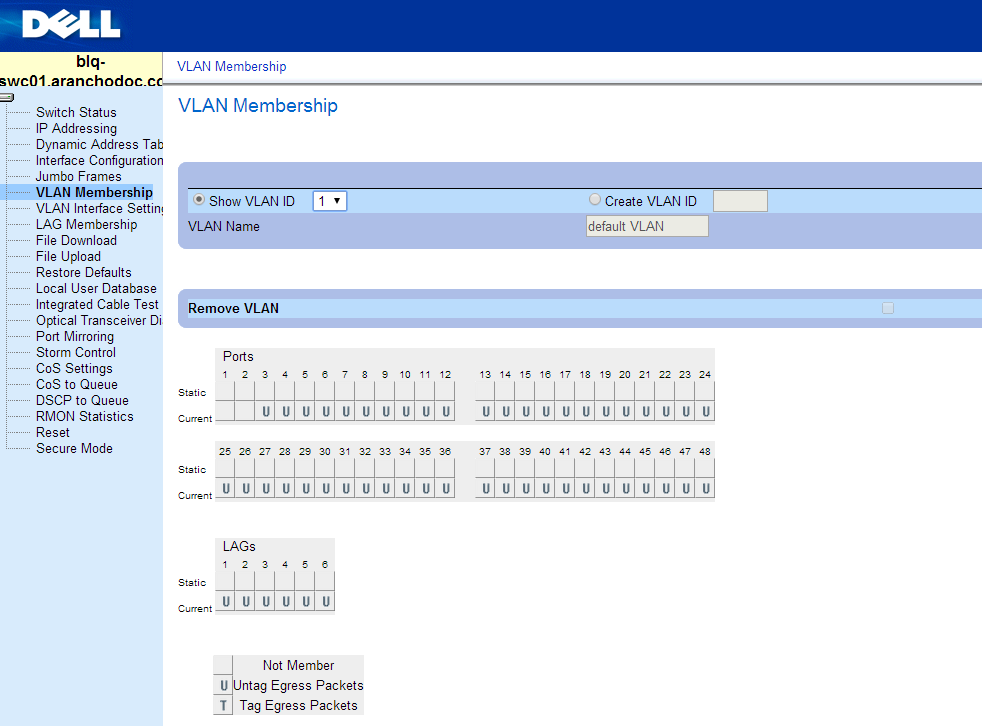






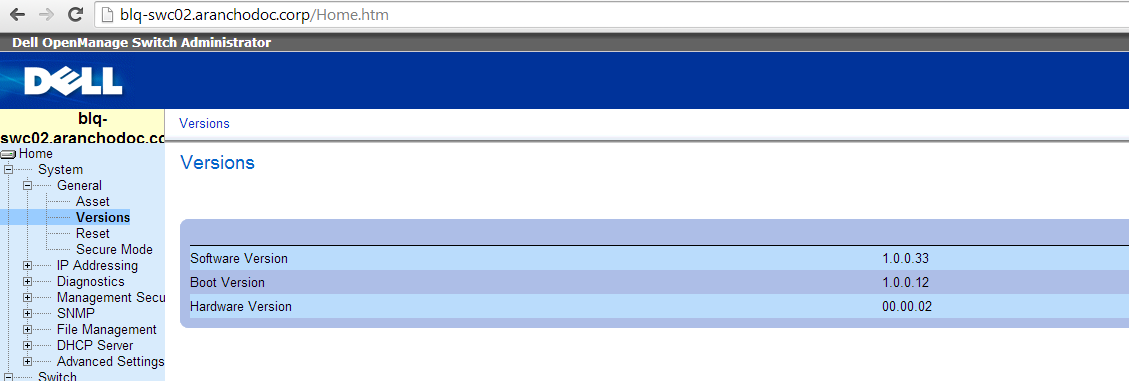


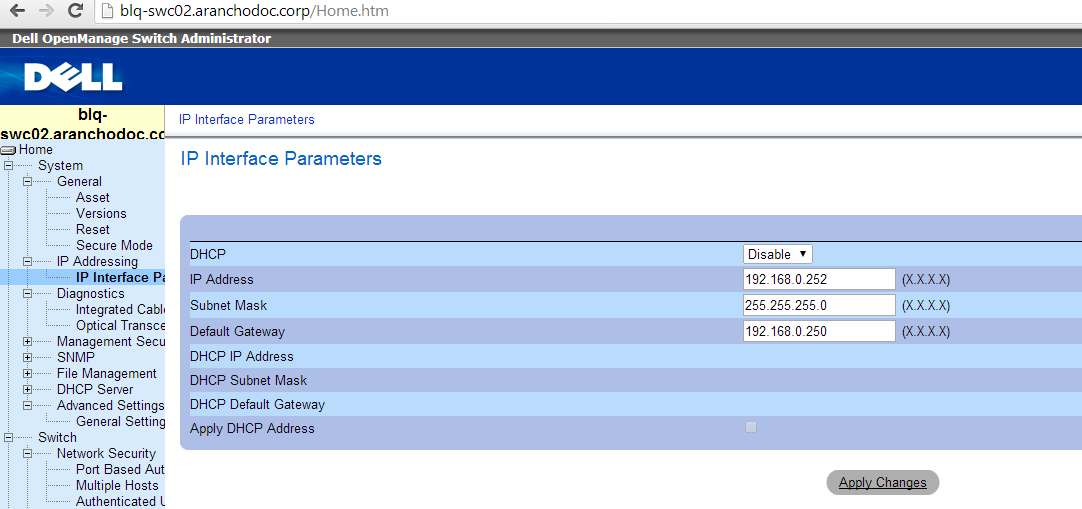


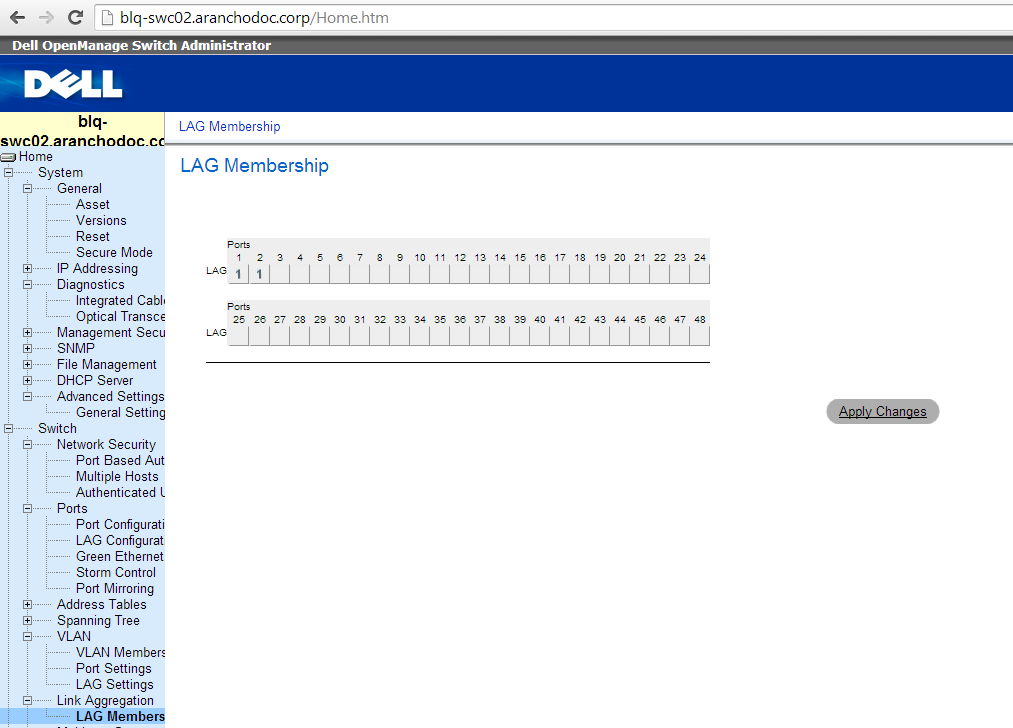


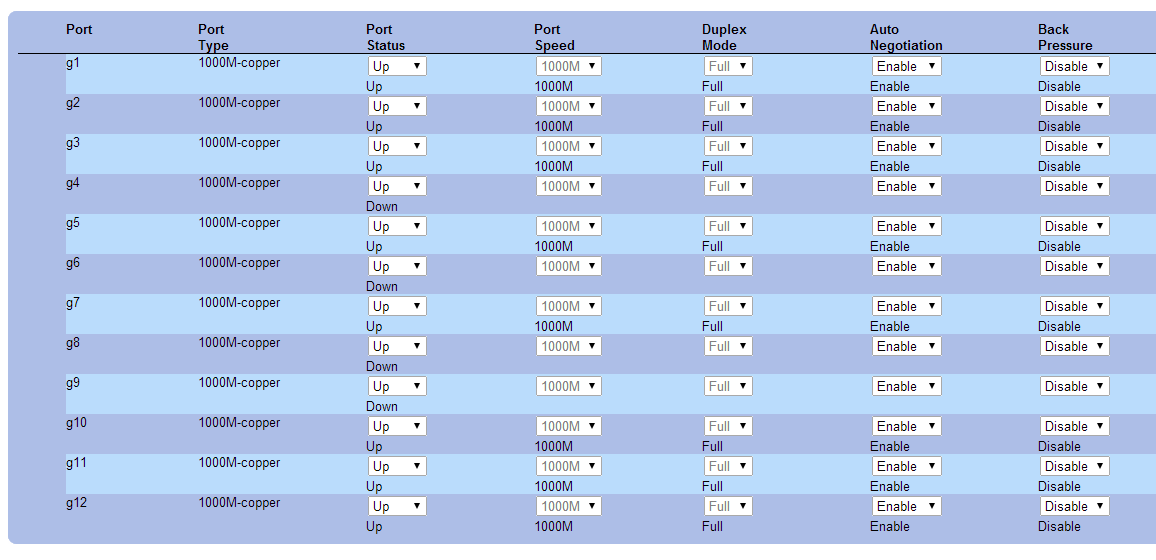
### blq-swc02

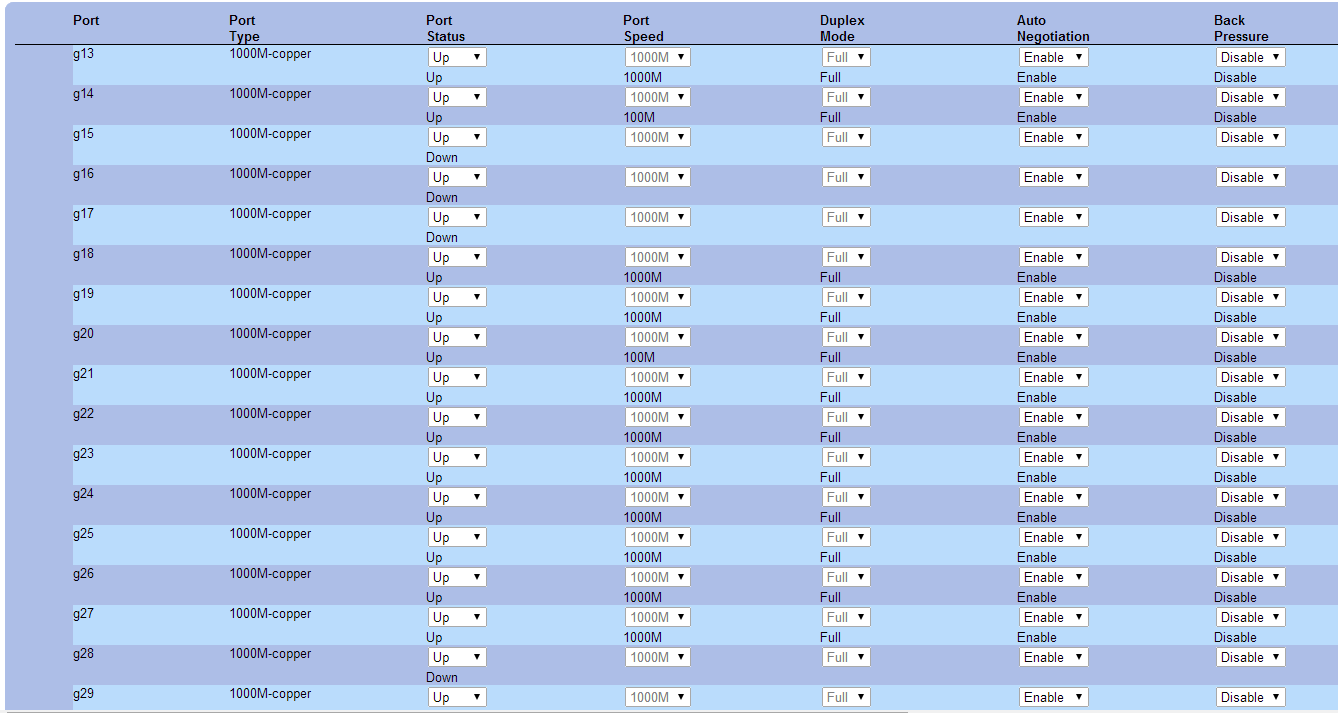


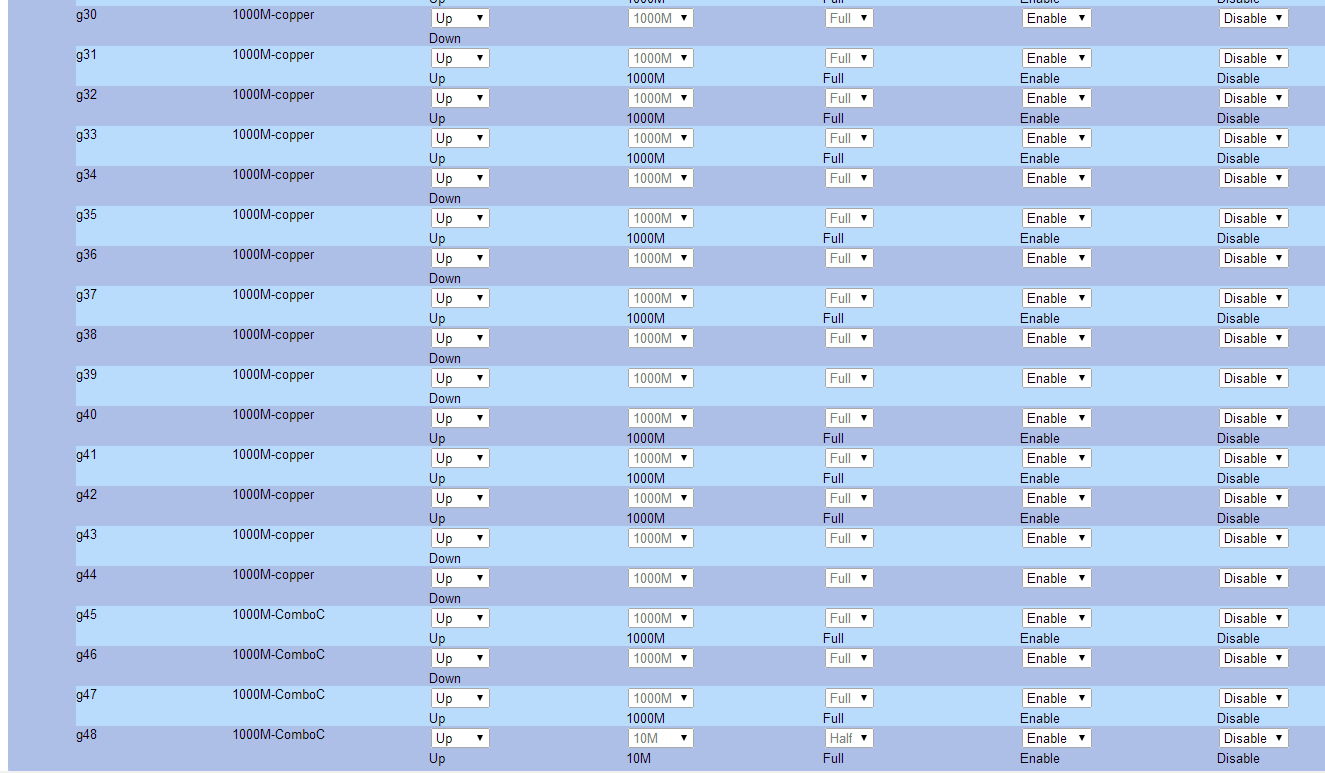




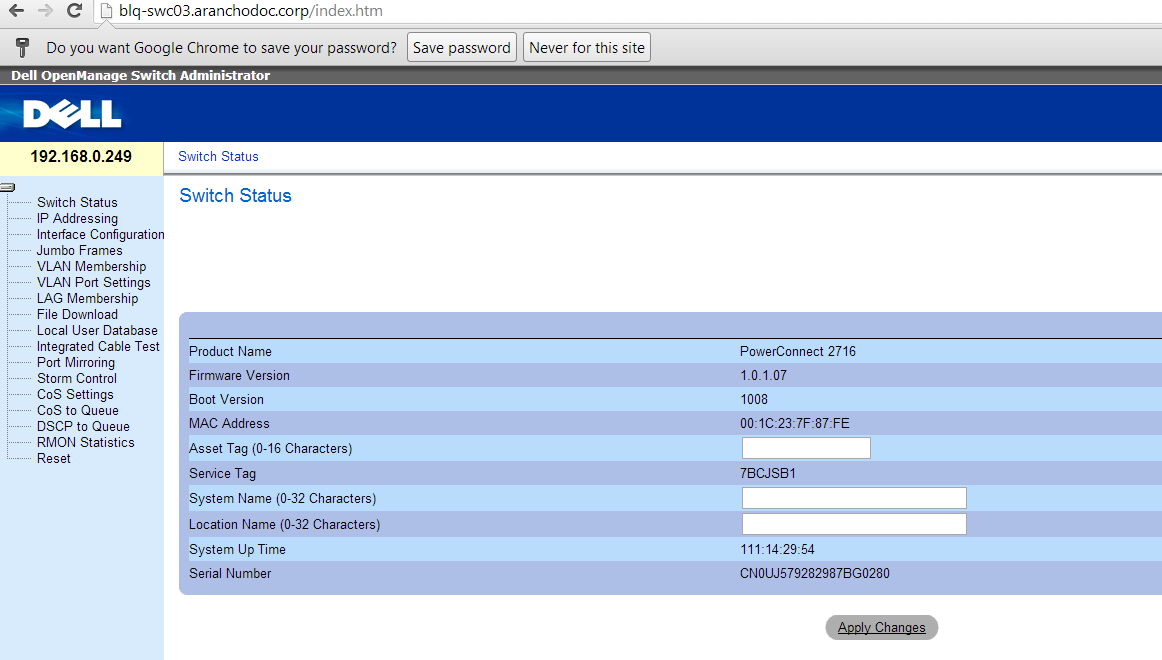


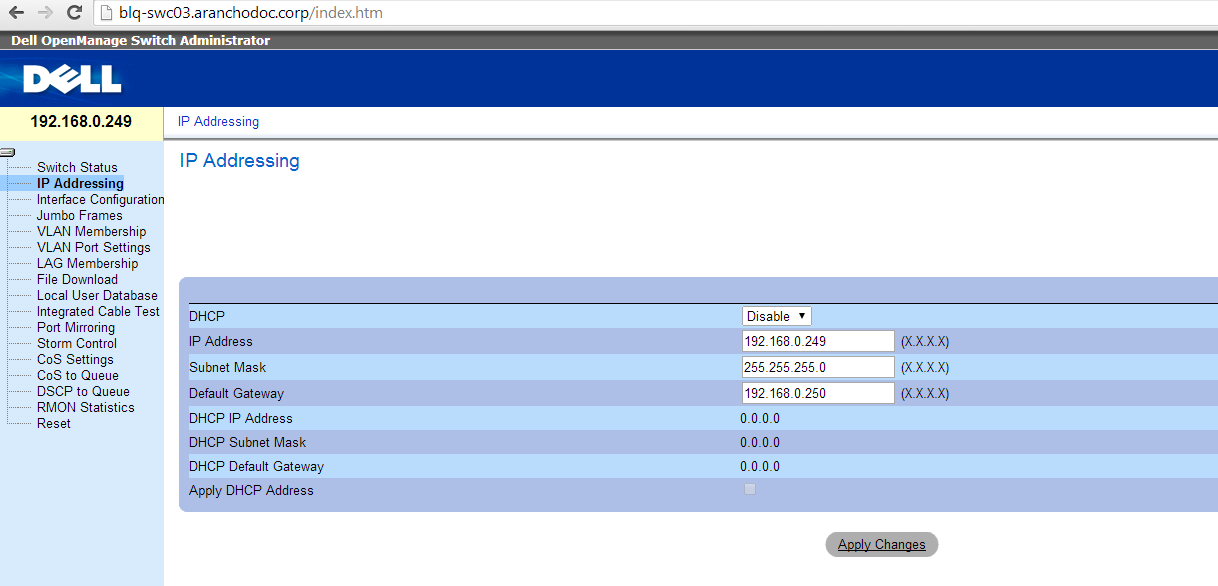


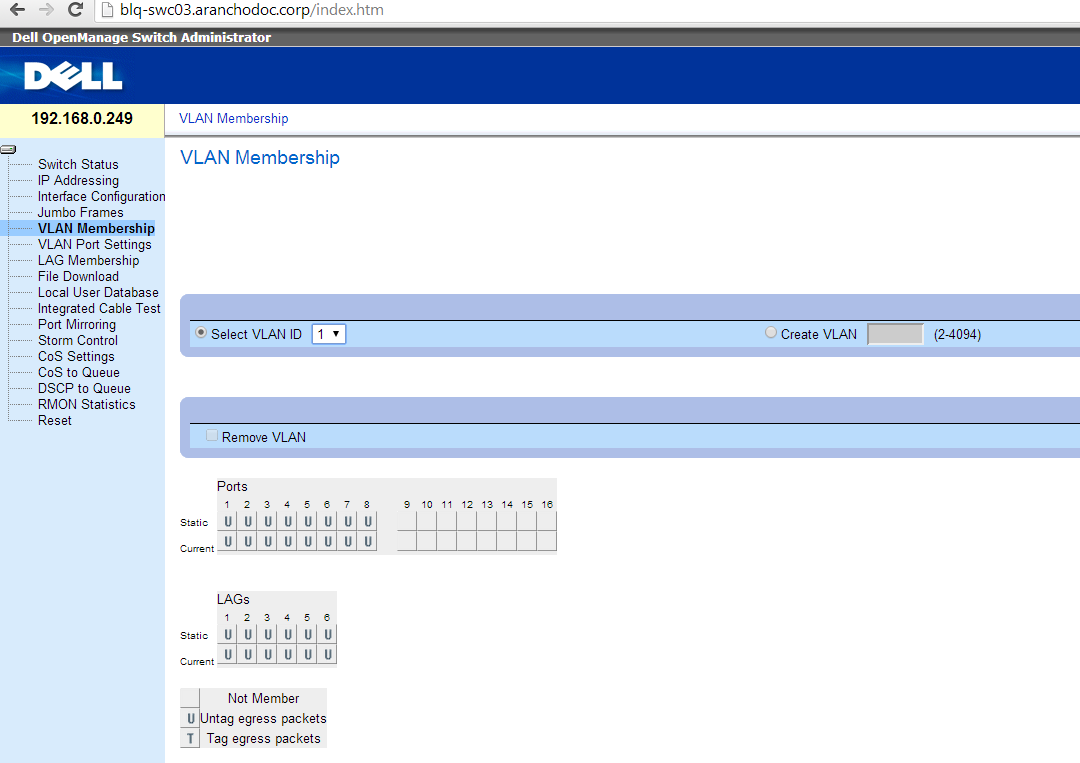


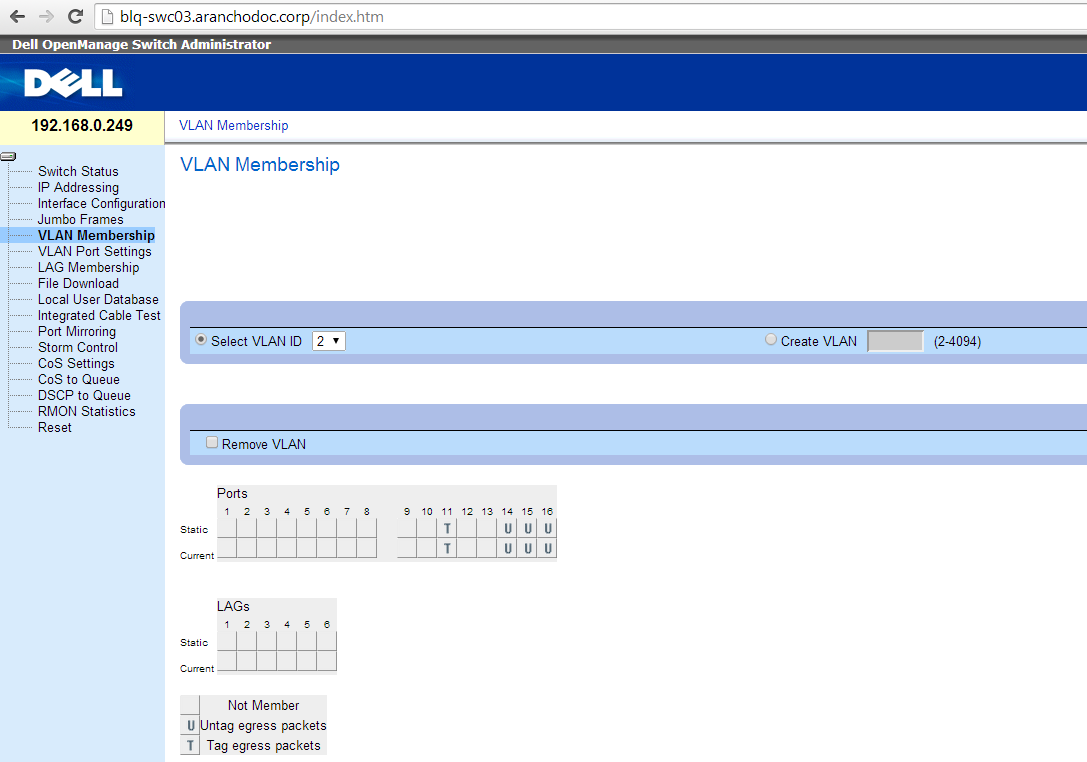


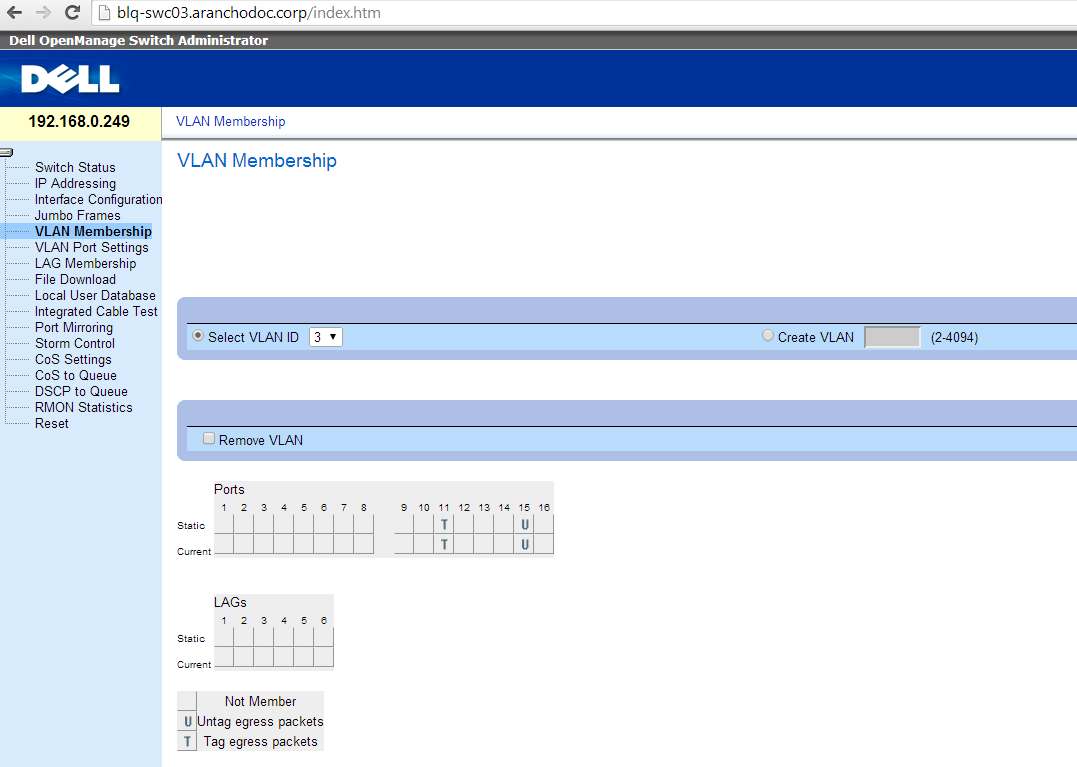
### blq-swc03

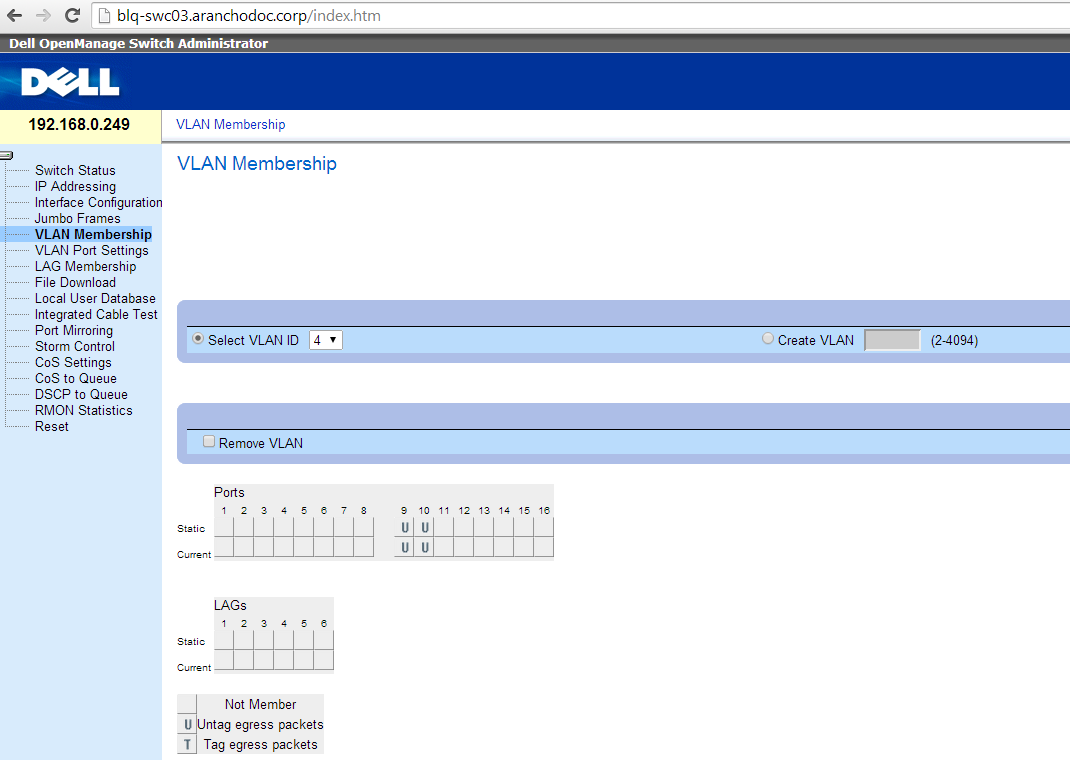


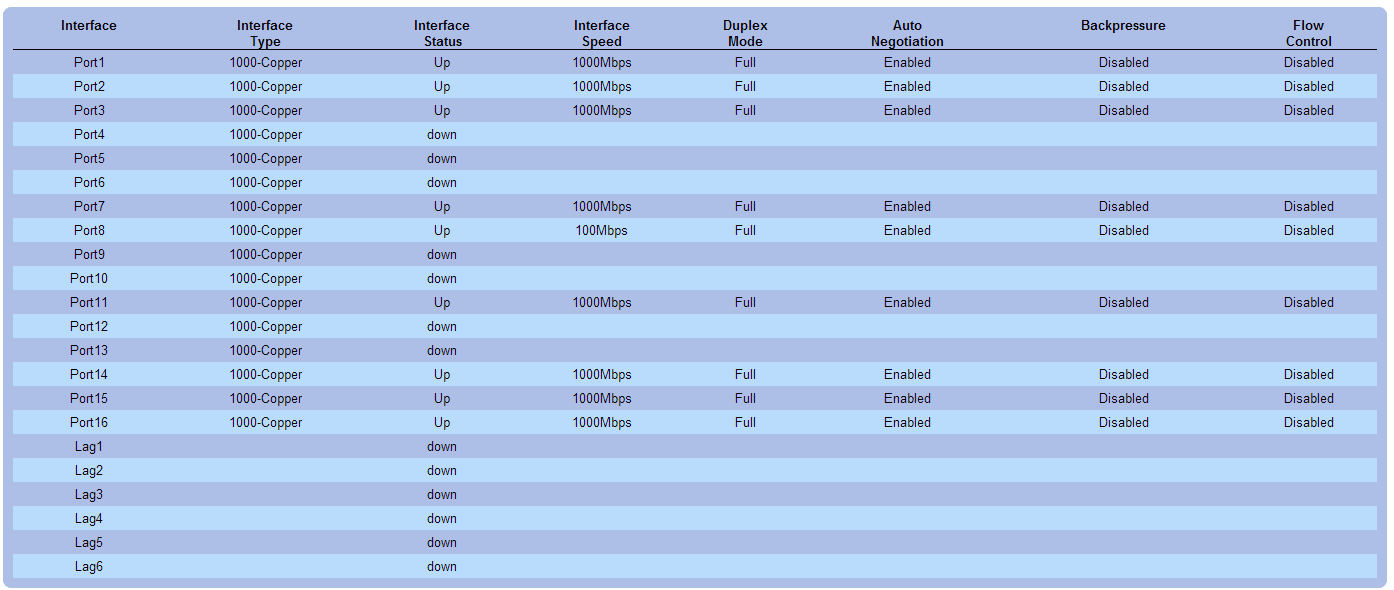












### blq-swc04

BLQ-SWC04# sh ver

Unit SW version Boot version HW version

------------------- ------------------- ------------------- -------------------

1 4.1.0.8 1.0.0.14 00.00.02

BLQ-SWC04# sh interfaces status

Flow Link Back Mdix

Port Type Duplex Speed Neg ctrl State Pressure Mode

-------- ------------ ------ ----- -------- ---- ----------- -------- -------

gi1/0/1 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/2 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/3 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/4 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/5 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/6 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/7 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/8 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/9 1G-Copper -- -- -- -- Down -- --

gi1/0/10 1G-Copper -- -- -- -- Down -- --

gi1/0/11 1G-Copper -- -- -- -- Down -- --

gi1/0/12 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/13 1G-Copper -- -- -- -- Down -- --

gi1/0/14 1G-Copper -- -- -- -- Down -- --

gi1/0/15 1G-Copper Full 100 Disabled On Up Disabled On

gi1/0/16 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/17 1G-Copper -- -- -- -- Down -- --

gi1/0/18 1G-Copper -- -- -- -- Down -- --

gi1/0/19 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/20 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/21 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/22 1G-Copper -- -- -- -- Down -- --

gi1/0/23 1G-Copper -- -- -- -- Down -- --

gi1/0/24 1G-Copper Full 1000 Enabled On Up Disabled Off

te1/0/1 10G-Fiber -- -- -- -- Down -- --

te1/0/2 10G-Fiber -- -- -- -- Down -- --

Flow Link

Ch Type Duplex Speed Neg control State

-------- ------- ------ ----- -------- ------- -----------

BLQ-SWC04#

BLQ-SWC04# sh vlan

Vlan Name Tagged Ports UnTagged Ports Type Authorization

---- ------------ ------------------ ------------------ --------- -------------

1 1 gi1/0/19-48, Default Required

te1/0/1-2,

gi2/0/1-48,

te2/0/1-2,

gi3/0/1-48,

te3/0/1-2,

gi4/0/1-48,

te4/0/1-2,

gi5/0/1-48,

te5/0/1-2,

gi6/0/1-48,

te6/0/1-2,

gi7/0/1-48,

te7/0/1-2,

gi8/0/1-48,

te8/0/1-2,Po1-32

3 iSCSI 1001 gi1/0/1-8, permanent Required

gi1/0/12-13

4 Fastweb gi1/0/15-16 permanent Required

11 LiveMig gi1/0/19-21 permanent Required

12 CSV gi1/0/19-21 permanent Required

13 Cluster HB gi1/0/19-21 permanent Required

14 Test permanent Required

BLQ-SWC04#

BLQ-SWC04# sh interfaces counters

Port InUcastPkts InMcastPkts InBcastPkts InOctets

---------------- ------------ ------------ ------------ ------------

gi1/0/1 1932289411 16 139 116089244974 606

gi1/0/2 8083985 7 129 945806918

gi1/0/3 217139168 32 1023 942342501261 02

gi1/0/4 4227634429 16 762 169287295655 644

gi1/0/5 2799187751 1080725 1048412 510721036335 26

gi1/0/6 3721259329 1432324 1351735 630613663767 83

gi1/0/7 1788140455 253445 808467 548480484006 19

gi1/0/8 471836184 27460 319821 547348032131

gi1/0/9 0 0 0 0

gi1/0/10 0 0 0 0

gi1/0/11 0 0 2 692

gi1/0/12 2651183811 5 79002 728933045850 57

gi1/0/13 2559431896 113776 125761 157771183136 88

gi1/0/14 0 73340 413819 68694609

gi1/0/15 2074877085 50551 190702 333486132709 4

gi1/0/16 2543725327 660 1635505 718479963226 2

gi1/0/17 0 0 2 128

gi1/0/18 0 0 0 0

gi1/0/19 928080205 2204148 6605332 201390167603 64

gi1/0/20 3012921840 2687358 3622737 131143390730 39

gi1/0/21 3866482589 1478993 1891167 988130247101 9

gi1/0/22 856609677 7058398 1376335 887823510384

gi1/0/23 1190933 64086 14626 237776222

gi1/0/24 2959446109 143986491 337531406 479687557674 4

te1/0/1 0 0 0 0

te1/0/2 0 0 0 0

Port OutUcastPkts OutMcastPkts OutBcastPkts OutOctets

gi1/0/1 3357508825 4394916 5011123 183036528218 92

gi1/0/2 8260346 4394800 5009978 1483111769

gi1/0/3 3052789292 4356749 4643491 484927866747 80

gi1/0/4 2737308689 4354993 4635420 510283093402 77

gi1/0/5 4114720231 2906948 3436682 157805815206 443

gi1/0/6 1964409353 2765293 3399360 222071930289 008

gi1/0/7 138262450 2856303 1784435 552892336268 19

gi1/0/8 639441265 4151790 4091605 647149842116

gi1/0/9 0 0 0 0

gi1/0/10 0 0 0 0

gi1/0/11 0 2 0 136

gi1/0/12 2045186851 3120412 2529552 673039728401 31

gi1/0/13 2430489809 332896 781897 169925473734 80

gi1/0/14 0 109020 0 7413360

gi1/0/15 2543523138 1013877 1628019 718471902899 4

gi1/0/16 2071837718 1063799 190692 333473597174 1

gi1/0/17 0 2 0 136

gi1/0/18 0 0 0 0

gi1/0/19 477397255 103799648 336611675 139892412537 71

gi1/0/20 1154035630 86913778 282442913 207802780933 61

gi1/0/21 4079615003 74868001 240754417 604815813182 1

gi1/0/22 1520664795 2054269 3493725 154400936696 5

gi1/0/23 471933475 30591791 97265114 61239270147

gi1/0/24 1303505671 3405077 1766248 171758157377 90

te1/0/1 0 0 0 0

te1/0/2 0 0 0 0

BLQ-SWC04# sh system

Unit Type

---- ----------------------

1 PowerConnect 5524

Unit Main Power Supply Redundant Power Supply

---- ----------------- ----------------------

1 OK

Unit Fans Status

---- ------------------

1 ON

Unit Temperature (Celsius) Temperature Sensor Status

---- ------------------------- -------------------------

1 50 OK

Unit Up time

---- ---------------

1 08,16:37:43

BLQ-SWC04# sh run

no spanning-tree

port jumbo-frame

vlan database

vlan 3-4,11-14

exit

voice vlan oui-table add 000181 Nortel\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 0001e3 Siemens\_AG\_phone\_\_\_\_\_\_\_\_

voice vlan oui-table add 00036b Cisco\_phone\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 00096e Avaya\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 000fe2 H3C\_Aolynk\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 001049 Shoretel\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 0060b9 Philips\_and\_NEC\_AG\_phone

voice vlan oui-table add 00907a Polycom/Veritel\_phone\_\_\_

voice vlan oui-table add 00e0bb 3Com\_phone\_\_\_\_\_\_\_\_\_\_\_\_\_\_

iscsi target port 860 address 0.0.0.0

iscsi target port 3260 address 0.0.0.0

iscsi target port 9876 address 0.0.0.0

iscsi target port 20002 address 0.0.0.0

iscsi target port 20003 address 0.0.0.0

iscsi target port 25555 address 0.0.0.0

hostname BLQ-SWC04

username admin password encrypted 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 pr

ivilege 15

snmp-server location Bologna

snmp-server community Dell\_Network\_Manager rw view DefaultSuper

clock timezone GMT 1

clock summer-time GMT recurring eu

sntp anycast client enable

sntp broadcast client enable

clock source sntp

sntp unicast client enable

sntp unicast client poll

sntp server 192.168.0.117 poll

!

interface vlan 1

ip address 192.168.0.138 255.255.255.0

!

interface vlan 3

name "iSCSI 1001"

!

interface vlan 4

name Fastweb

!

interface vlan 11

name LiveMig

!

interface vlan 12

name CSV

!

interface vlan 13

name "Cluster HB"

!

interface vlan 14

name Test

!

interface gigabitethernet1/0/1

switchport general allowed vlan add 1001 untagged

switchport access vlan 3

!

interface gigabitethernet1/0/2

switchport general allowed vlan add 1001 untagged

switchport access vlan 3

!

interface gigabitethernet1/0/3

switchport general allowed vlan add 3 untagged

switchport access vlan 3

!

interface gigabitethernet1/0/4

switchport access vlan 3

!

interface gigabitethernet1/0/5

switchport access vlan 3

!

interface gigabitethernet1/0/6

switchport access vlan 3

!

interface gigabitethernet1/0/7

switchport access vlan 3

!

interface gigabitethernet1/0/8

switchport access vlan 3

!

interface gigabitethernet1/0/9

switchport access vlan 1001

!

interface gigabitethernet1/0/10

switchport access vlan 1001

!

interface gigabitethernet1/0/11

switchport access vlan 1001

!

interface gigabitethernet1/0/12

switchport access vlan 3

!

interface gigabitethernet1/0/13

switchport general allowed vlan add 1001 untagged

switchport access vlan 3

!

interface gigabitethernet1/0/14

switchport access vlan 1001

!

interface gigabitethernet1/0/15

speed 100

no negotiation

switchport access vlan 4

!

interface gigabitethernet1/0/16

switchport access vlan 4

!

interface gigabitethernet1/0/17

switchport access vlan 1001

!

interface gigabitethernet1/0/18

switchport access vlan 1001

!

interface gigabitethernet1/0/19

switchport mode general

switchport general allowed vlan add 11-13 tagged

switchport general allowed vlan add 1 untagged

!

interface gigabitethernet1/0/20

switchport mode general

switchport general allowed vlan add 11-13 tagged

switchport general allowed vlan add 1 untagged

!

interface gigabitethernet1/0/21

switchport mode general

switchport general allowed vlan add 11-13 tagged

switchport general allowed vlan add 1 untagged

!

interface gigabitethernet1/0/22

switchport general allowed vlan add 3,11-13 tagged

!

asset-tag 01-A0201 unit 1

ip route 0.0.0.0 0.0.0.0 192.168.0.250

Default settings:

Service tag: 2J0VTS1

SW version 4.1.0.8 (date 28-Aug-2012 time 11:17:36)

Gigabit Ethernet Ports

=============================

no shutdown

speed 1000

duplex full

negotiation

flow-control on

mdix auto

no back-pressure

interface vlan 1

interface port-channel 1 - 32

spanning-tree

spanning-tree mode RSTP

qos basic

qos trust cos

eee enable

### blq-swc05 (SWITCH\_ISCSI\_1002)

SWITCH\_ISCSI\_1002# sh ver

Unit SW version Boot version HW version

------------------- ------------------- ------------------- -------------------

1 4.1.0.8 1.0.0.14 00.00.02

SWITCH\_ISCSI\_1002# sh system

Unit Type

---- ----------------------

1 PowerConnect 5524

Unit Main Power Supply Redundant Power Supply

---- ----------------- ----------------------

1 OK

Unit Fans Status

---- ------------------

1 ON

Unit Temperature (Celsius) Temperature Sensor Status

---- ------------------------- -------------------------

1 40 OK

Unit Up time

---- ---------------

1 111,17:18:40

SWITCH\_ISCSI\_1002# sh ver

Unit SW version Boot version HW version

------------------- ------------------- ------------------- -------------------

1 4.1.0.8 1.0.0.14 00.00.02

SWITCH\_ISCSI\_1002# sh interface status

Flow Link Back Mdix

Port Type Duplex Speed Neg ctrl State Pressure Mode

-------- ------------ ------ ----- -------- ---- ----------- -------- -------

gi1/0/1 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/2 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/3 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/4 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/5 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/6 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/7 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/8 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/9 1G-Copper -- -- -- -- Down -- --

gi1/0/10 1G-Copper -- -- -- -- Down -- --

gi1/0/11 1G-Copper -- -- -- -- Down -- --

gi1/0/12 1G-Copper -- -- -- -- Down -- --

gi1/0/13 1G-Copper -- -- -- -- Down -- --

gi1/0/14 1G-Copper -- -- -- -- Down -- --

gi1/0/15 1G-Copper Full 100 Enabled On Up Disabled Off

gi1/0/16 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/17 1G-Copper -- -- -- -- Down -- --

gi1/0/18 1G-Copper -- -- -- -- Down -- --

gi1/0/19 1G-Copper Full 1000 Enabled On Up Disabled On

gi1/0/20 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/21 1G-Copper Full 1000 Enabled On Up Disabled Off

gi1/0/22 1G-Copper -- -- -- -- Down -- --

gi1/0/23 1G-Copper -- -- -- -- Down -- --

gi1/0/24 1G-Copper Full 1000 Enabled On Up Disabled Off

te1/0/1 10G-Fiber -- -- -- -- Down -- --

te1/0/2 10G-Fiber -- -- -- -- Down -- --

Flow Link

Ch Type Duplex Speed Neg control State

-------- ------- ------ ----- -------- ------- -----------

SWITCH\_ISCSI\_1002#

SWITCH\_ISCSI\_1002# sh vlan

Vlan Name Tagged Ports UnTagged Ports Type Authorization

---- ------------ ------------------ ------------------ --------- -------------

1 1 gi1/0/19-48, Default Required

te1/0/1-2,

gi2/0/1-48,

te2/0/1-2,

gi3/0/1-48,

te3/0/1-2,

gi4/0/1-48,

te4/0/1-2,

gi5/0/1-48,

te5/0/1-2,

gi6/0/1-48,

te6/0/1-2,

gi7/0/1-48,

te7/0/1-2,

gi8/0/1-48,

te8/0/1-2,Po1-32

11 11 gi1/0/19-22 permanent Required

12 12 gi1/0/19-22 permanent Required

13 13 gi1/0/19-22 permanent Required

1002 ISCSI\_1002 gi1/0/1-18 permanent Required

SWITCH\_ISCSI\_1002# sh interfa counters

Port InUcastPkts InMcastPkts InBcastPkts InOctets

--------------- ------------ ------------ ------------ ------------

gi1/0/1 255981356 0 25 380926486280 06

gi1/0/2 1942084 0 26 232589528

gi1/0/3 1297390802 7 36 289292880398 98

gi1/0/4 3143163826 0 25 261888540177 18

gi1/0/5 2116430147 674041 506489 105059622038 8

gi1/0/6 2156416129 315852 95597 171505848710 06

gi1/0/7 414738480 82143 269965 142187830125 3

gi1/0/8 4272758602 0 32265 185927274727 94

gi1/0/9 0 0 0 0

gi1/0/10 0 0 0 0

gi1/0/11 0 0 0 0

gi1/0/12 0 0 0 0

gi1/0/13 0 0 0 0

gi1/0/14 0 0 0 0

gi1/0/15 973957884 0 57791 275993534706

gi1/0/16 1292411343 10 31396 884970399195

gi1/0/17 0 0 0 0

gi1/0/18 0 0 0 0

gi1/0/19 3633309705 422592 694418 218654420549 48

gi1/0/20 3507327257 468130 862543 659692174458 9

gi1/0/21 840334390 462639 986716 338718817989

gi1/0/22 0 0 0 0

gi1/0/23 0 0 0 0

gi1/0/24 3889606885 32774195 77138825 249914062175 4

te1/0/1 0 0 0 0

te1/0/2 0 0 0 0

gi1/0/1 687756416 1393810 993590 296871971589 6

gi1/0/2 2065845 1393810 993589 359549562

gi1/0/3 2648486270 1393804 993536 265494706414 82

gi1/0/4 1325792719 1393810 993590 869767384302 2

gi1/0/5 3999137376 719128 486386 175063974924 71

gi1/0/6 450387159 1077958 898018 718725112692 95

gi1/0/7 486926054 1311667 723650 151276742652 6

gi1/0/8 4058377814 1393808 961345 231998640598 2

gi1/0/9 0 0 0 0

gi1/0/10 0 0 0 0

gi1/0/11 0 0 0 0

gi1/0/12 0 0 0 0

gi1/0/13 0 0 0 0

gi1/0/14 0 0 0 0

gi1/0/15 1292411803 1393810 935824 885131223341

gi1/0/16 973958599 1393808 962193 276154968646

gi1/0/17 0 0 0 0

gi1/0/18 0 0 0 0

gi1/0/19 3087548141 24037694 78844999 368587748398 0

gi1/0/20 2831539940 24026042 78820155 197796483378 03

gi1/0/21 3704246745 24031450 78695766 101542146611 75

gi1/0/22 0 0 0 0

gi1/0/23 0 0 0 0

gi1/0/24 1447484674 708921 360464 765376659302 5

te1/0/1 0 0 0 0

te1/0/2 0 0 0 0

SWITCH\_ISCSI\_1002# sh syetm

% Unrecognized command

SWITCH\_ISCSI\_1002# sh system

Unit Type

---- ----------------------

1 PowerConnect 5524

Unit Main Power Supply Redundant Power Supply

---- ----------------- ----------------------

1 OK

Unit Fans Status

---- ------------------

1 ON

Unit Temperature (Celsius) Temperature Sensor Status

---- ------------------------- -------------------------

1 40 OK

Unit Up time

---- ---------------

1 111,17:20:14

SWITCH\_ISCSI\_1002# sh running-config

no spanning-tree

port jumbo-frame

vlan database

vlan 11-13,1002

exit

voice vlan oui-table add 000181 Nortel\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 0001e3 Siemens\_AG\_phone\_\_\_\_\_\_\_\_

voice vlan oui-table add 00036b Cisco\_phone\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 00096e Avaya\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 000fe2 H3C\_Aolynk\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 001049 Shoretel\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

voice vlan oui-table add 0060b9 Philips\_and\_NEC\_AG\_phone

voice vlan oui-table add 00907a Polycom/Veritel\_phone\_\_\_

voice vlan oui-table add 00e0bb 3Com\_phone\_\_\_\_\_\_\_\_\_\_\_\_\_\_

iscsi target port 860 address 0.0.0.0

iscsi target port 3260 address 0.0.0.0

iscsi target port 9876 address 0.0.0.0

iscsi target port 20002 address 0.0.0.0

iscsi target port 20003 address 0.0.0.0

iscsi target port 25555 address 0.0.0.0

hostname SWITCH\_ISCSI\_1002

username admin password encrypted 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 pr

ivilege 15

snmp-server community Dell\_Network\_Manager rw view DefaultSuper

sntp anycast client enable

sntp broadcast client enable

clock source sntp

sntp unicast client enable

sntp unicast client poll

sntp server 192.168.0.117 poll

!

interface vlan 1

ip address 192.168.0.139 255.255.255.0

!

interface vlan 1002

name ISCSI\_1002

!

interface gigabitethernet1/0/1

switchport access vlan 1002

!

interface gigabitethernet1/0/2

switchport access vlan 1002

!

interface gigabitethernet1/0/3

switchport access vlan 1002

!

interface gigabitethernet1/0/4

switchport access vlan 1002

!

interface gigabitethernet1/0/5

switchport access vlan 1002

!

interface gigabitethernet1/0/6

switchport access vlan 1002

!

interface gigabitethernet1/0/7

switchport access vlan 1002

!

interface gigabitethernet1/0/8

switchport access vlan 1002

!

interface gigabitethernet1/0/9

switchport access vlan 1002

!

interface gigabitethernet1/0/10

switchport access vlan 1002

!

interface gigabitethernet1/0/11

switchport access vlan 1002

!

interface gigabitethernet1/0/12

switchport access vlan 1002

!

interface gigabitethernet1/0/13

switchport access vlan 1002

!

interface gigabitethernet1/0/14

switchport access vlan 1002

!

interface gigabitethernet1/0/15

switchport access vlan 1002

!

interface gigabitethernet1/0/16

switchport access vlan 1002

!

interface gigabitethernet1/0/17

switchport access vlan 1002

!

interface gigabitethernet1/0/18

switchport access vlan 1002

!

interface gigabitethernet1/0/19

switchport mode general

switchport general allowed vlan add 11-13 tagged

switchport general allowed vlan add 1 untagged

switchport access vlan 13

!

interface gigabitethernet1/0/20

switchport mode general

switchport general allowed vlan add 11-13 tagged

switchport general allowed vlan add 1 untagged

switchport access vlan 1002

!

interface gigabitethernet1/0/21

switchport mode general

switchport general allowed vlan add 11-13 tagged

switchport general allowed vlan add 1 untagged

!

interface gigabitethernet1/0/22

switchport mode general

switchport general allowed vlan add 11-13 tagged

switchport general allowed vlan add 1 untagged

switchport access vlan 1002

!

ip route 0.0.0.0 0.0.0.0 192.168.0.250

Default settings:

Service tag: JD0VTS1

SW version 4.1.0.8 (date 28-Aug-2012 time 11:17:36)

Gigabit Ethernet Ports

=============================

no shutdown

speed 1000

duplex full

negotiation

flow-control on

mdix auto

no back-pressure

interface vlan 1

interface port-channel 1 - 32

spanning-tree

spanning-tree mode RSTP

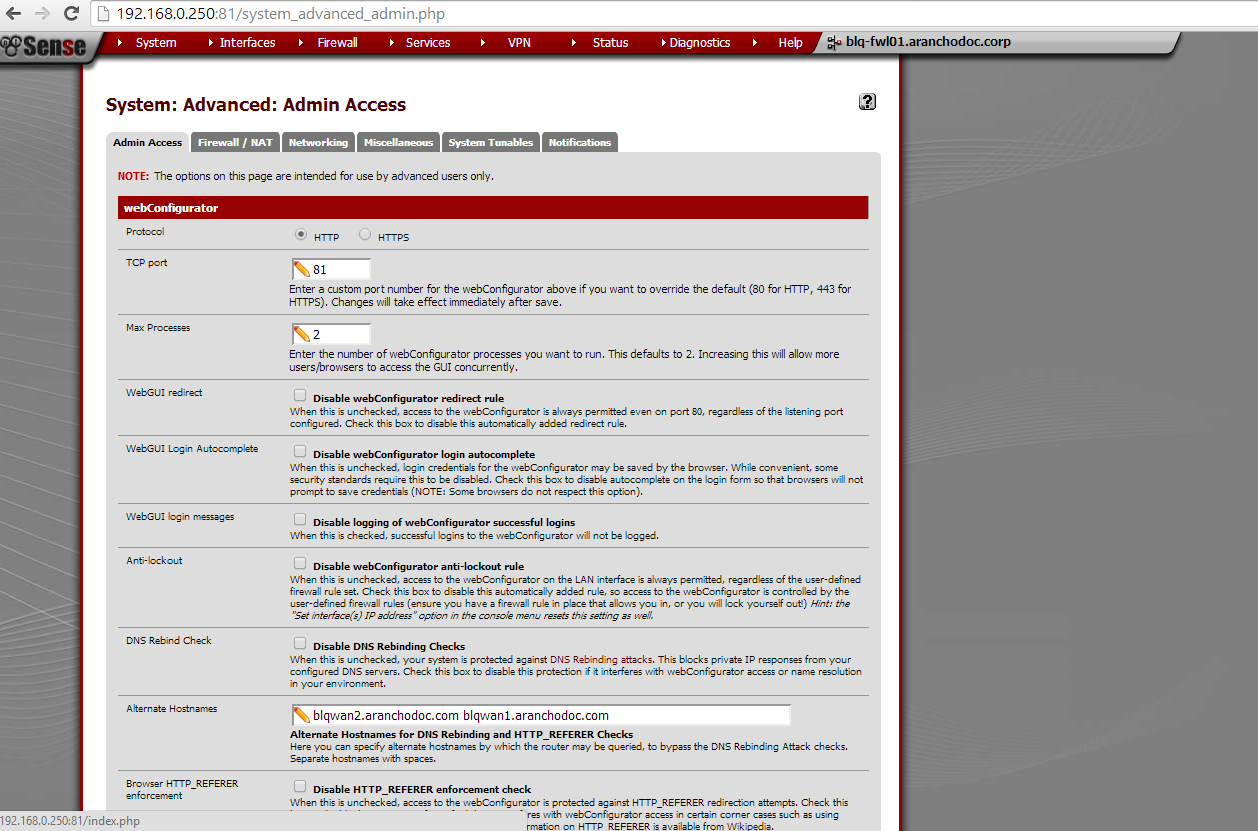
qos basic

qos trust cos

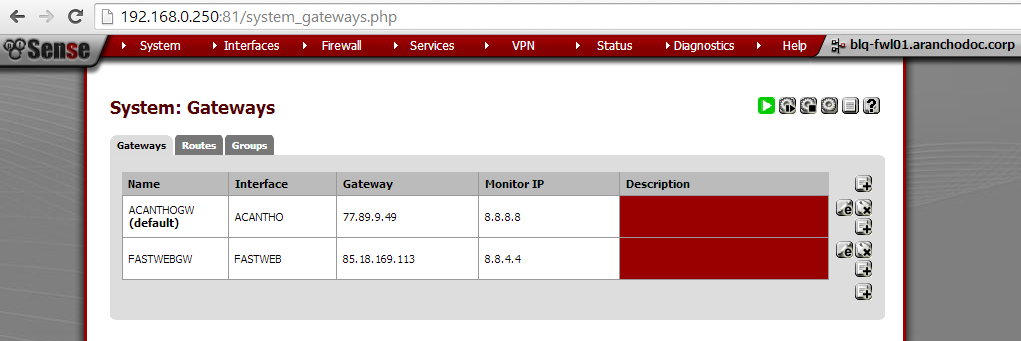
eee enable

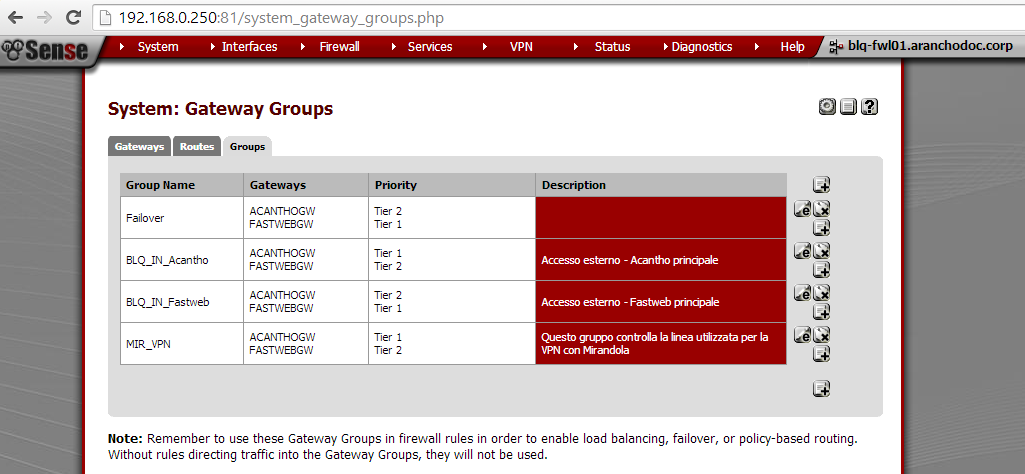
## B - Accesso

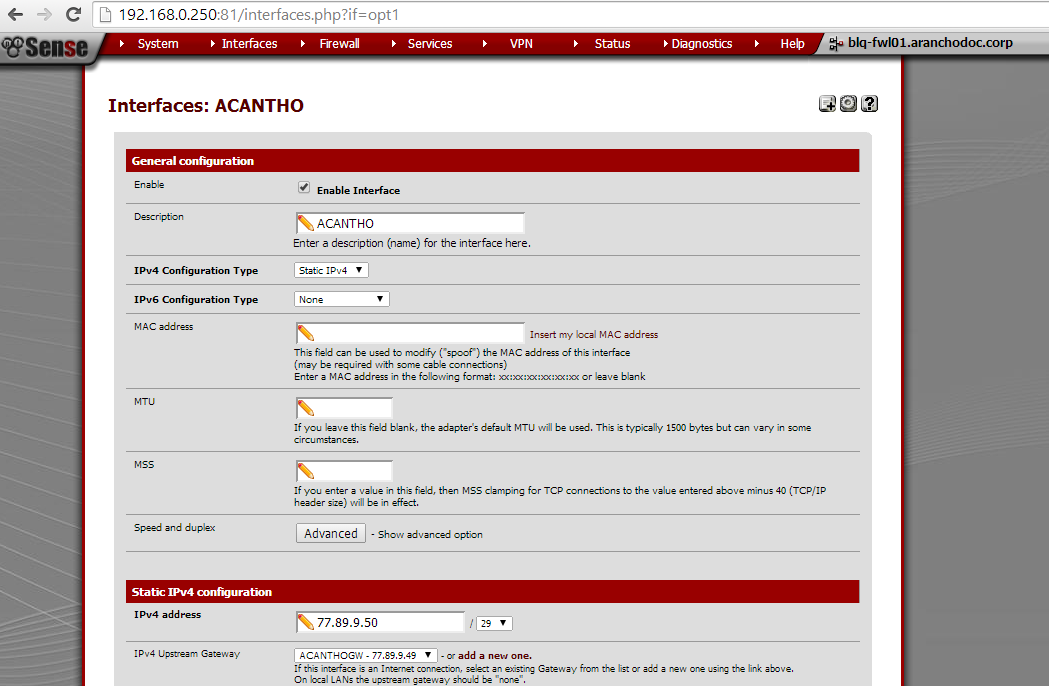
Accesso

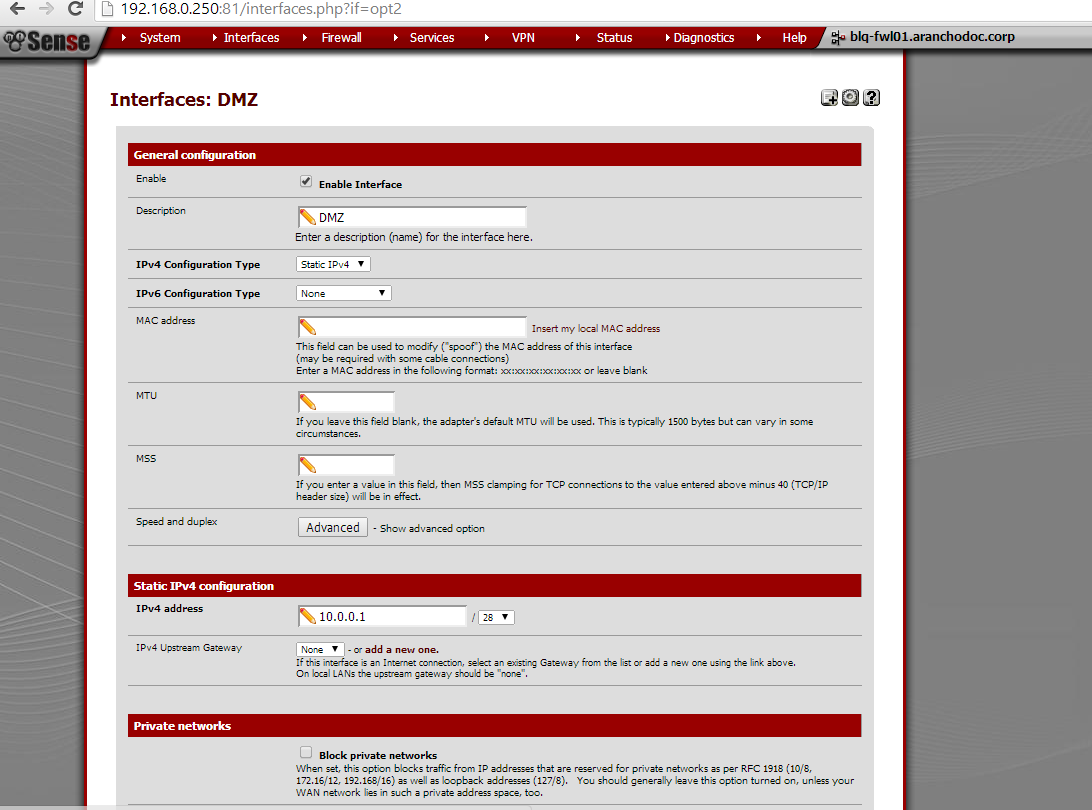


Esistono due trigger per verificare la raggiungibilità delle linee Fastweb e Acantho:

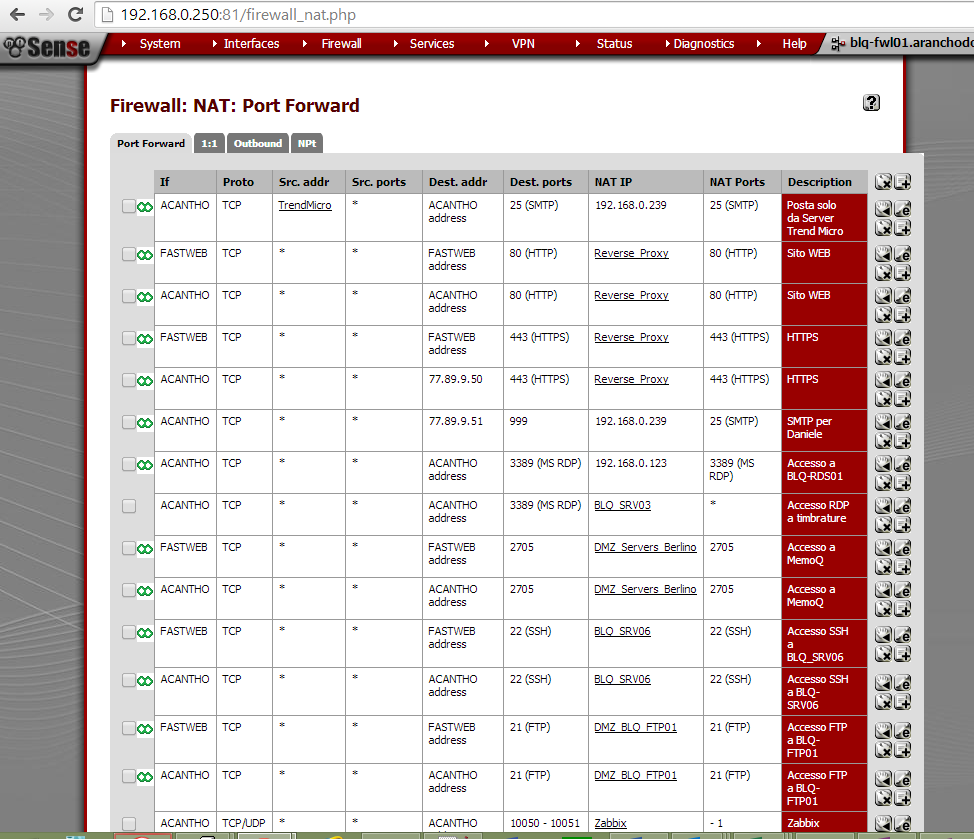




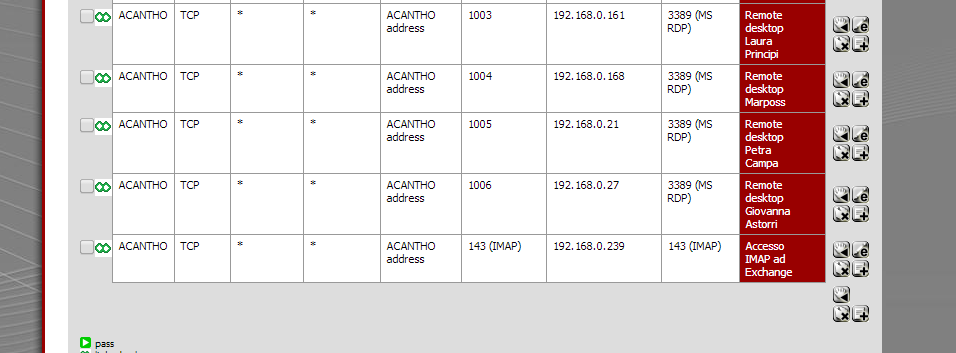




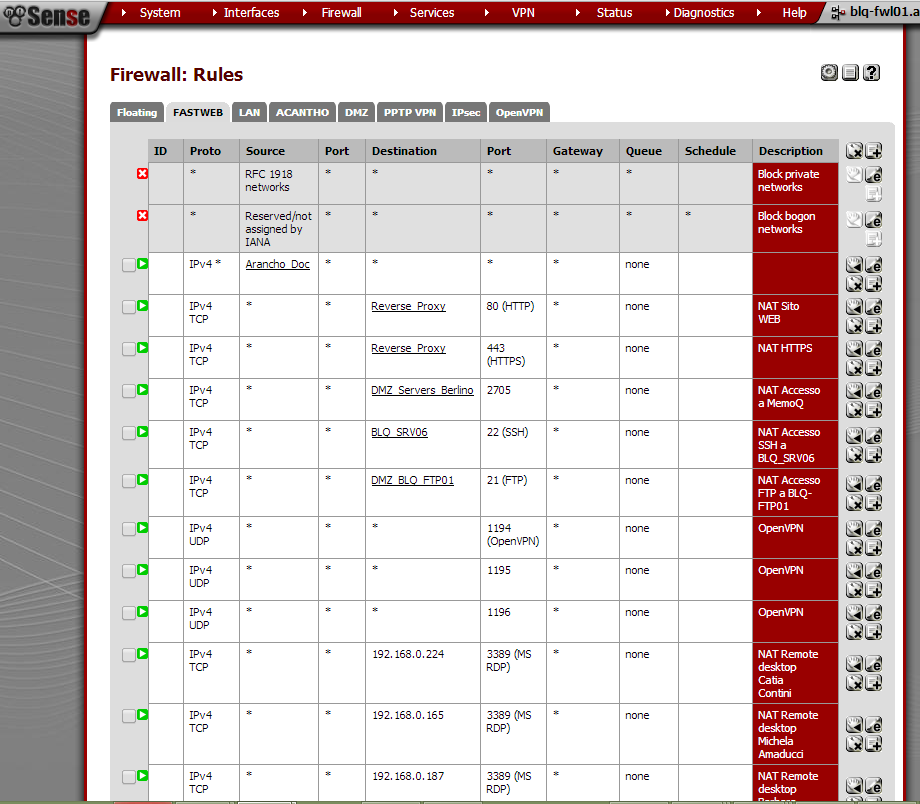
NAT

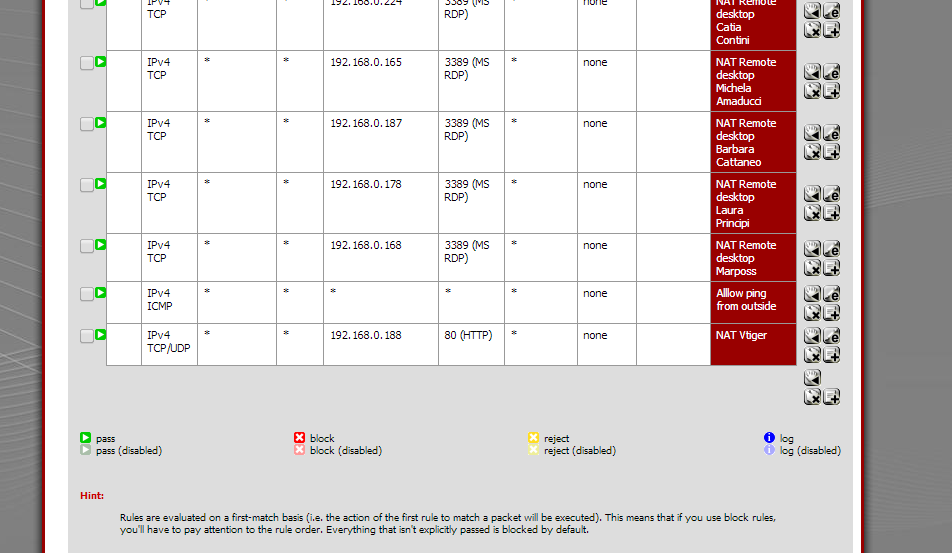




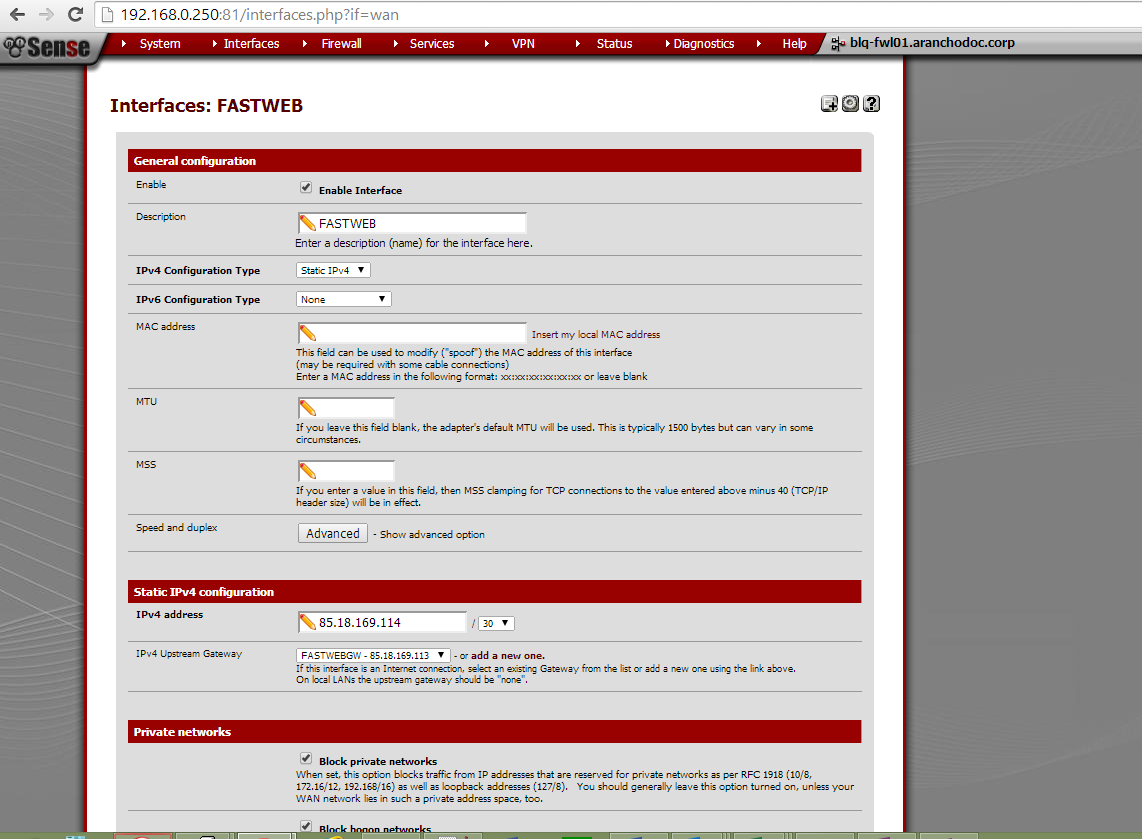


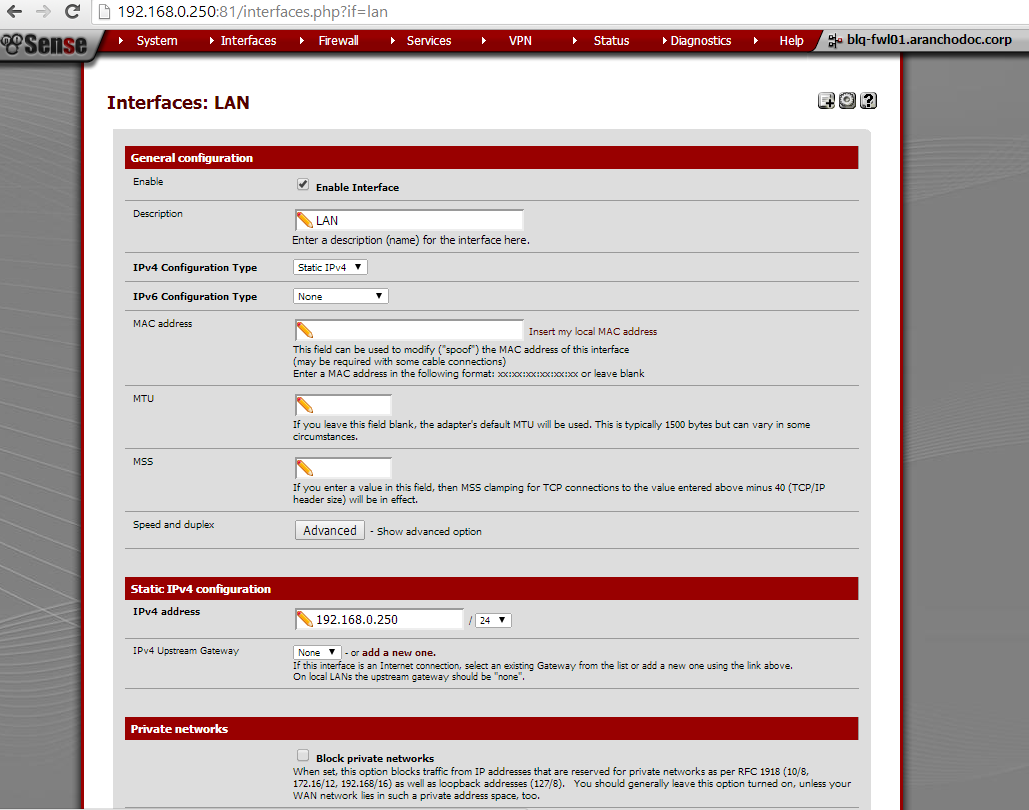
RULES



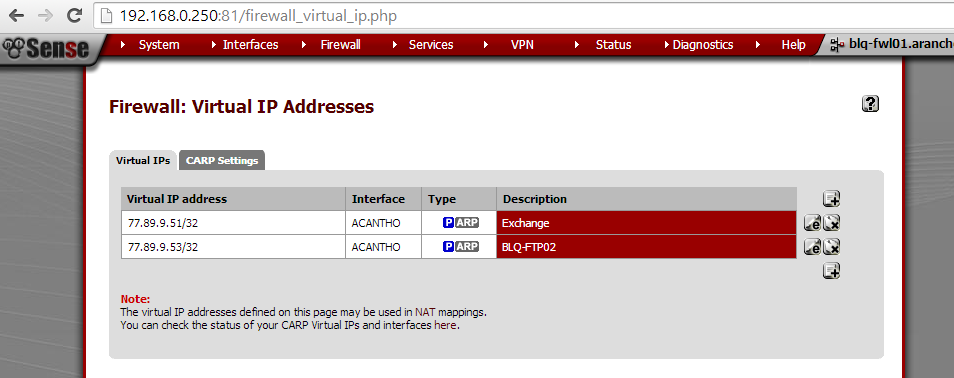


Interfacce





VIP



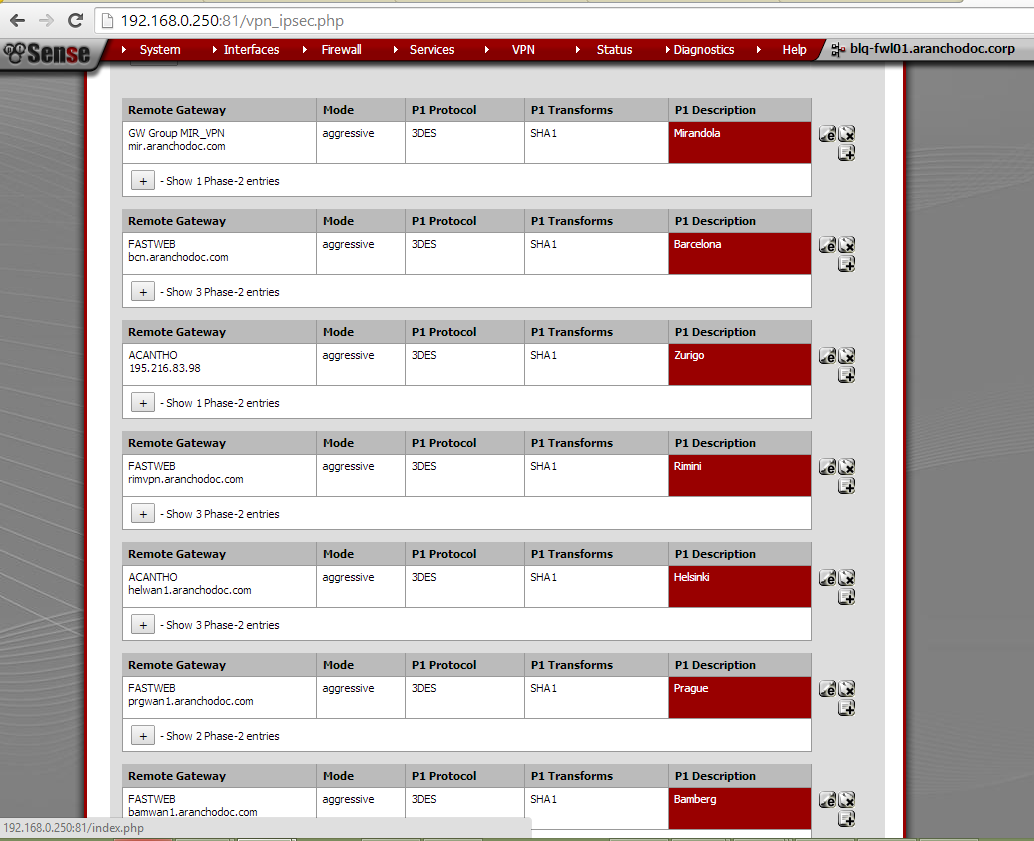
OPENVPN



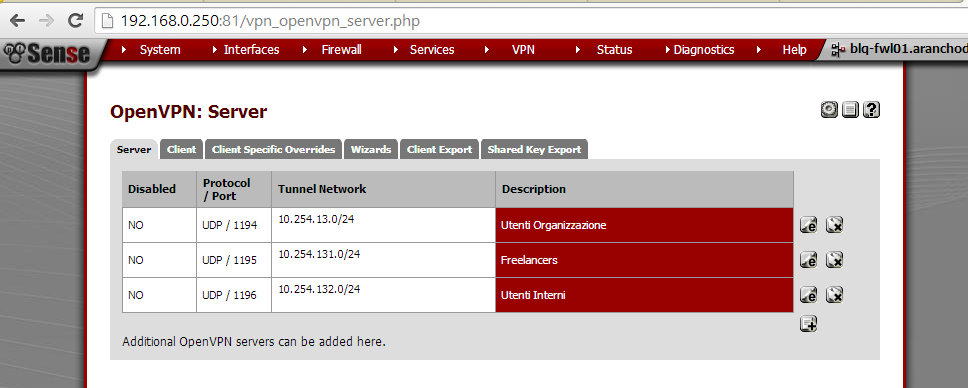
## C - VPN

Instradamento

|  |  |  |  |
| --- | --- | --- | --- |
| **Sede** | Firewall | Versione | VPN IPSEC L2L |
| Bologna | PFSense (principale) | 2.1.3 | SI |
| Bologna | SonicWall 2400 | 5.0.1.3 | NO |
| Rimini | PFSense (principale) |  | SI |
| Mirandola | PFSense (principale) |  | SI |
| Barcellona | PFSense (principale) |  | SI |
| Praga | PFSense (principale) |  | SI |
| Helsinki | PFSense (principale) |  | SI |
| Zurigo | Fortingate B60 |  | SI |
| Bamberg | FritzBox |  | SI |



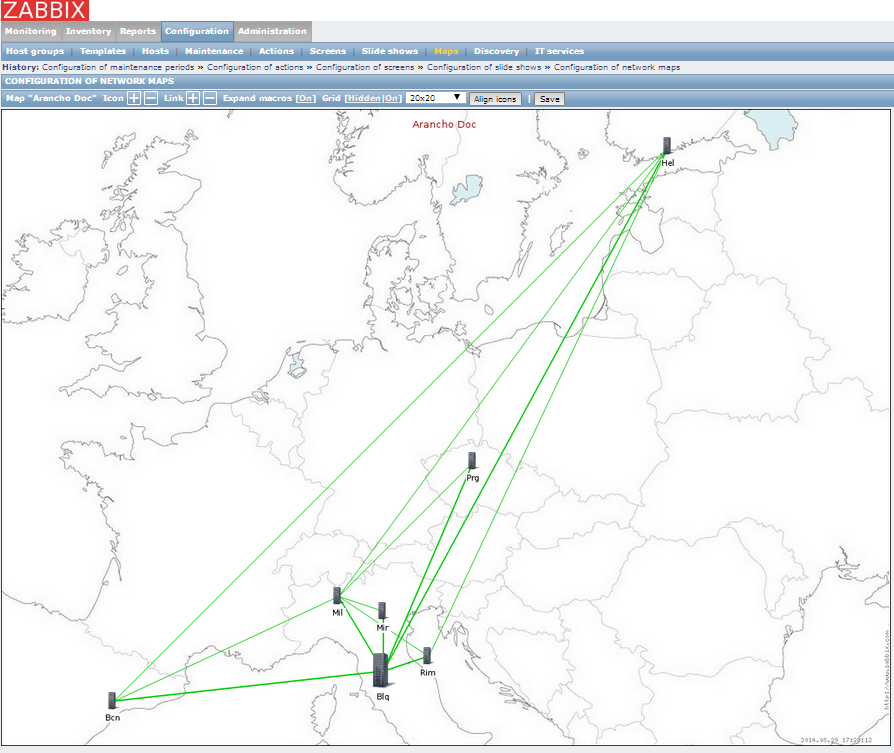
Client VPN

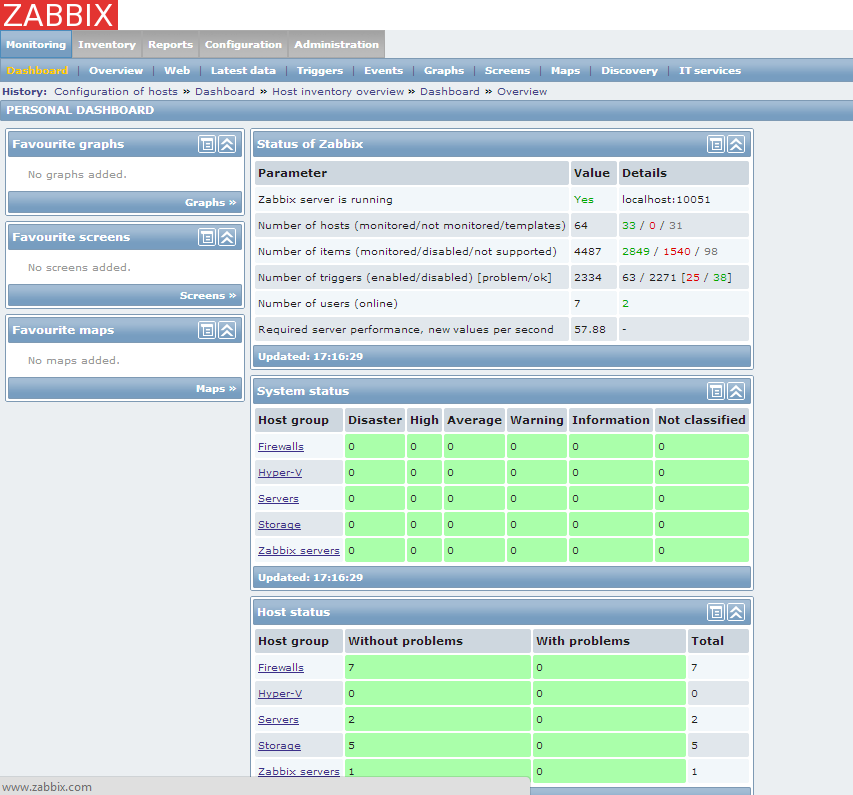


È stato attivato il servizio VPN client sulle sedi che ne hanno fatto richiesta.

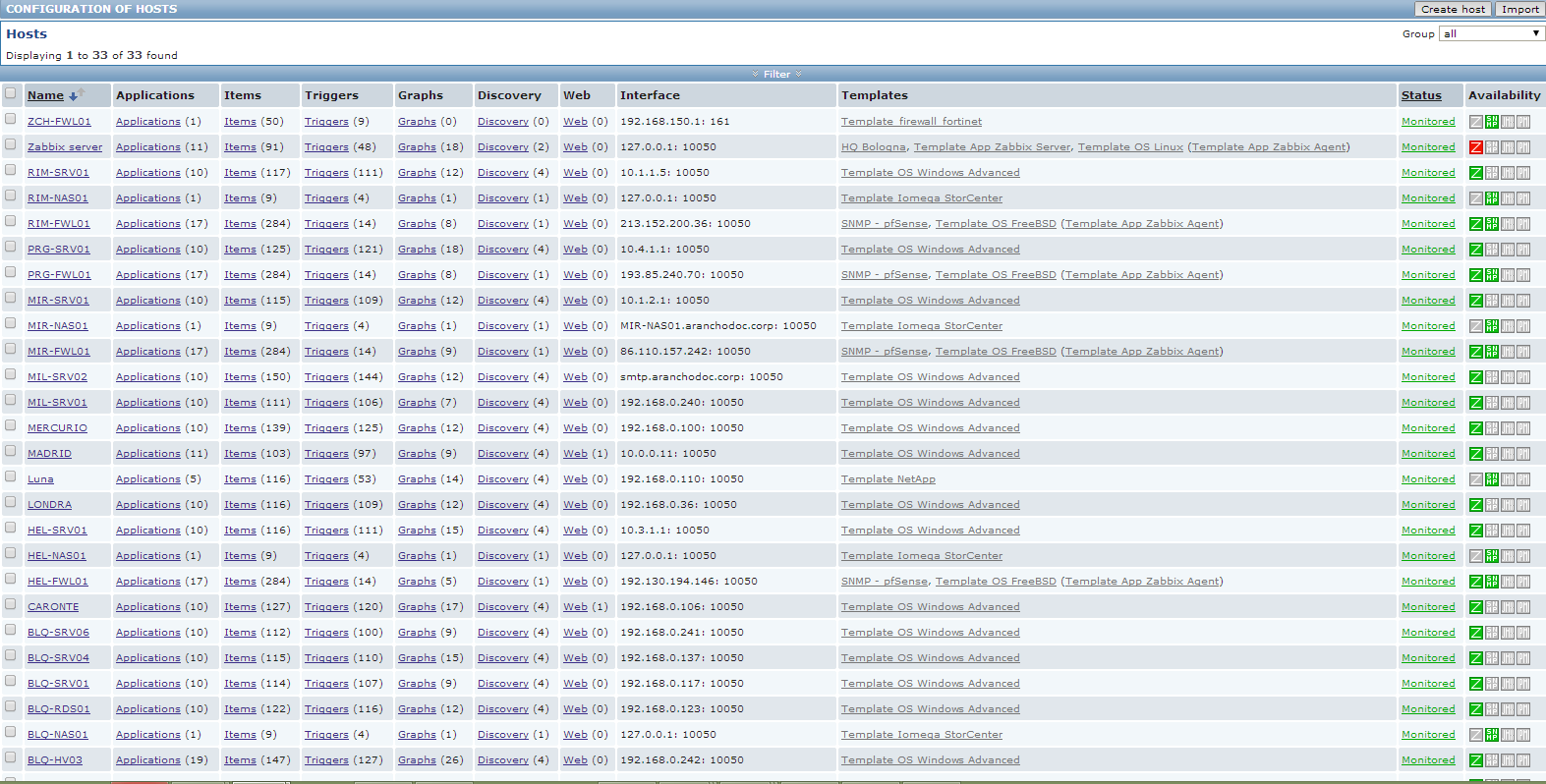
Si: Finlandia, Barcellona, Bologna, Rimini

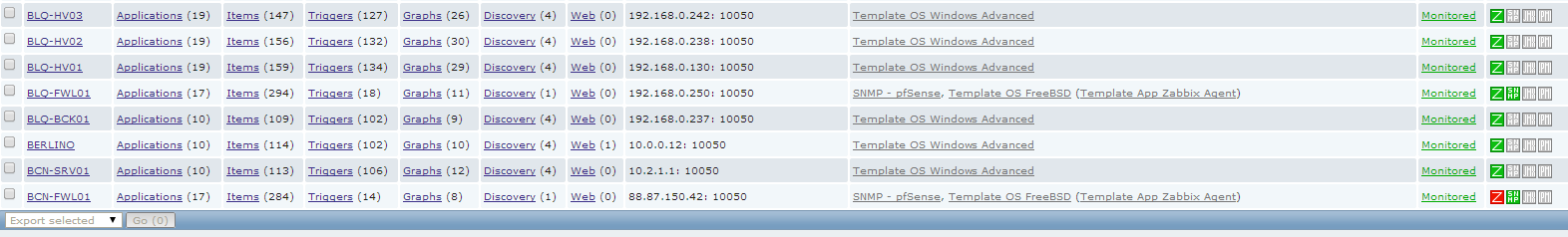
## D – Configurazioni Sistema di Monitoraggio

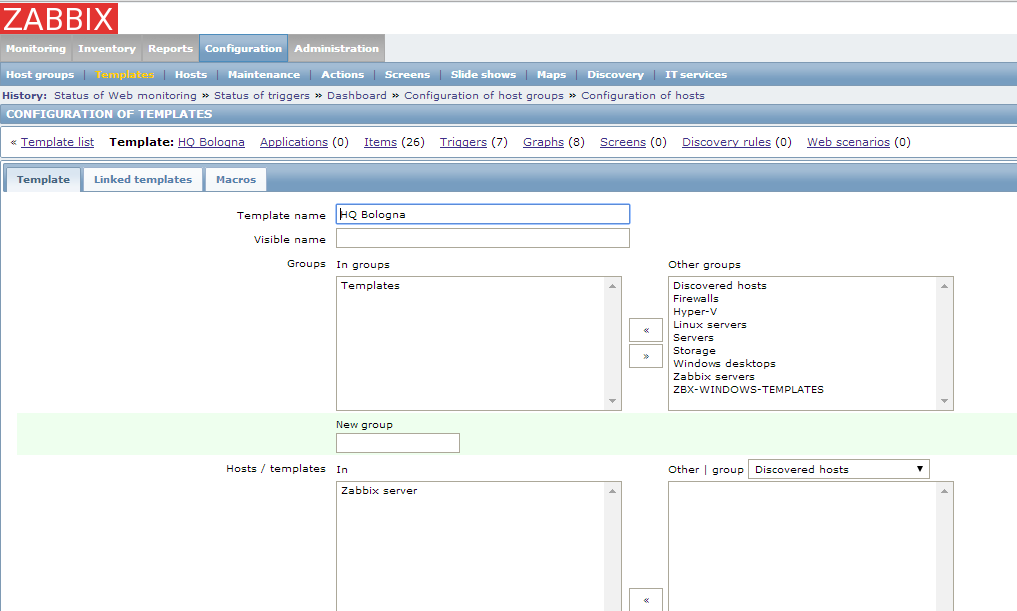


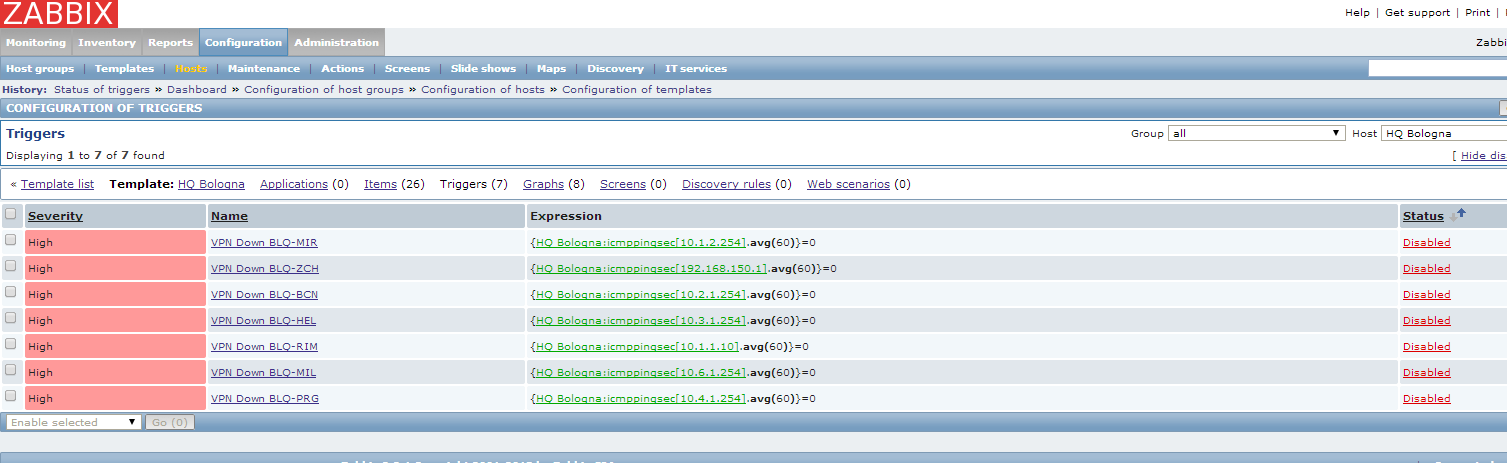


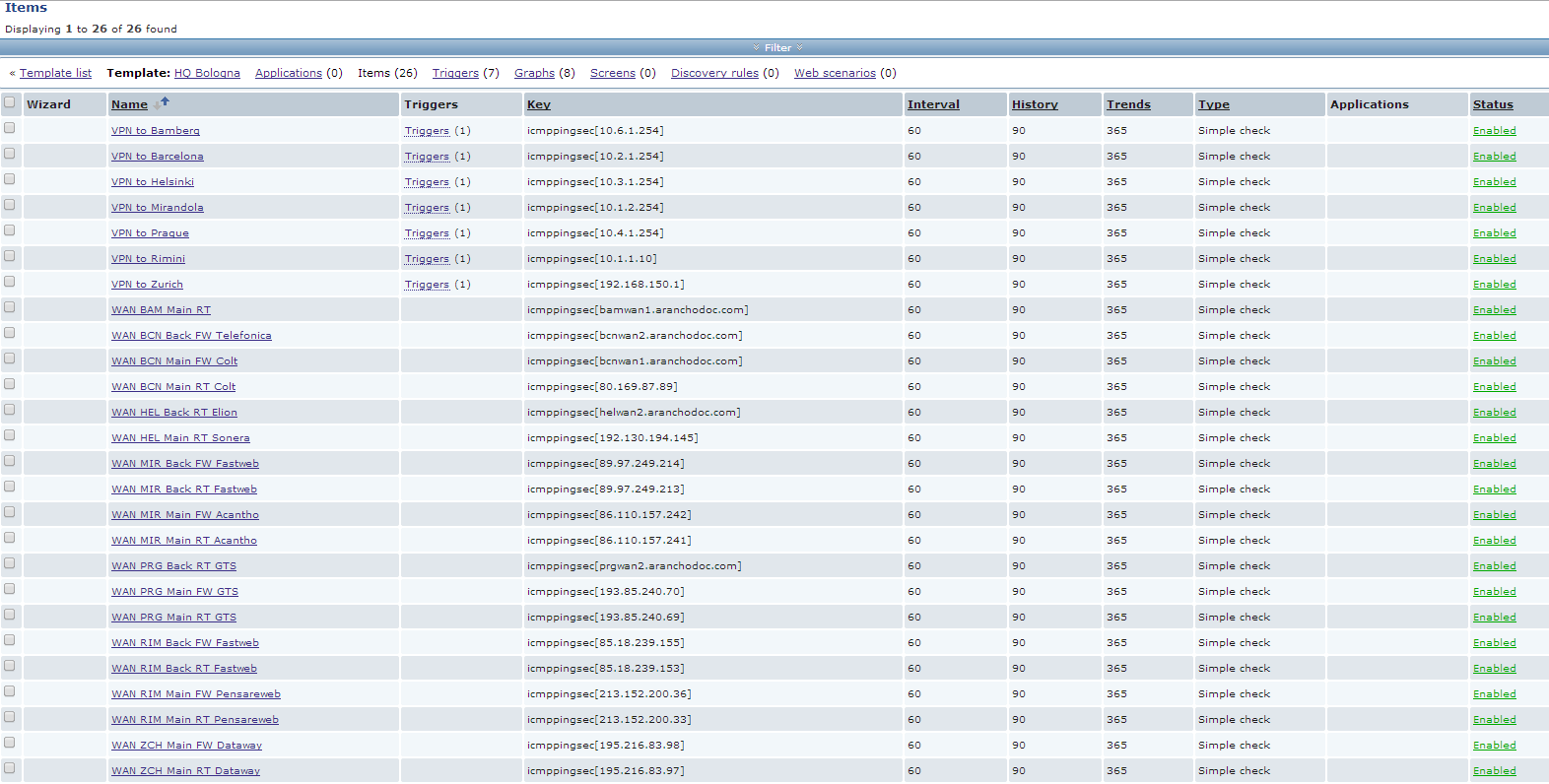


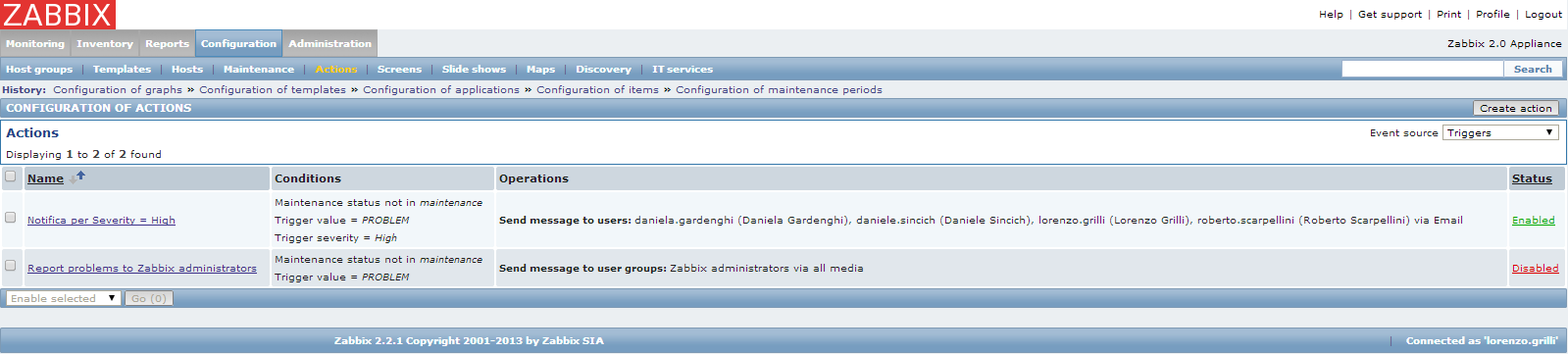


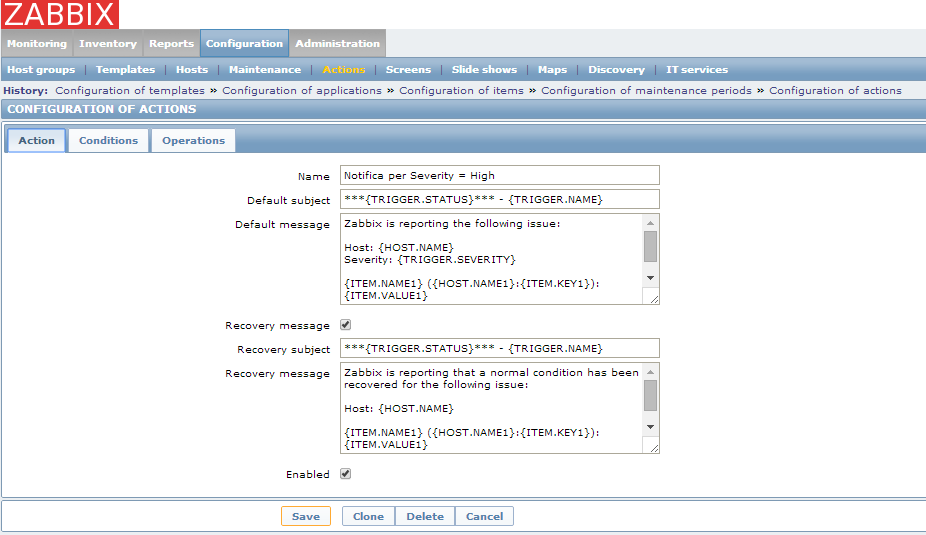


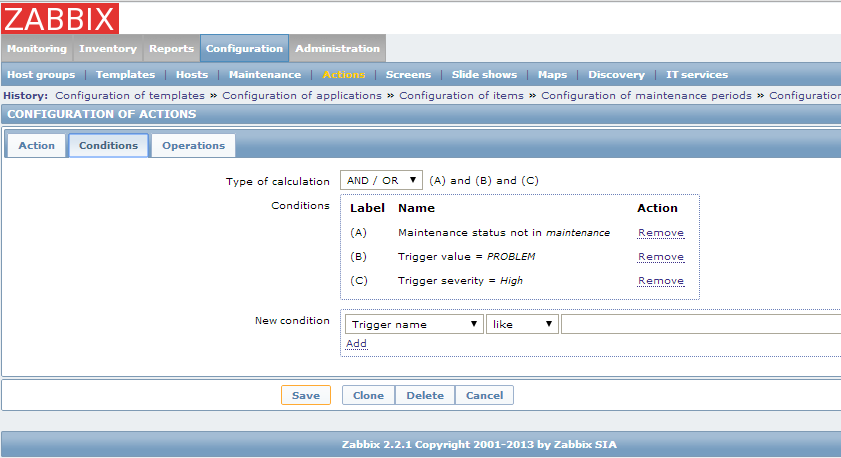






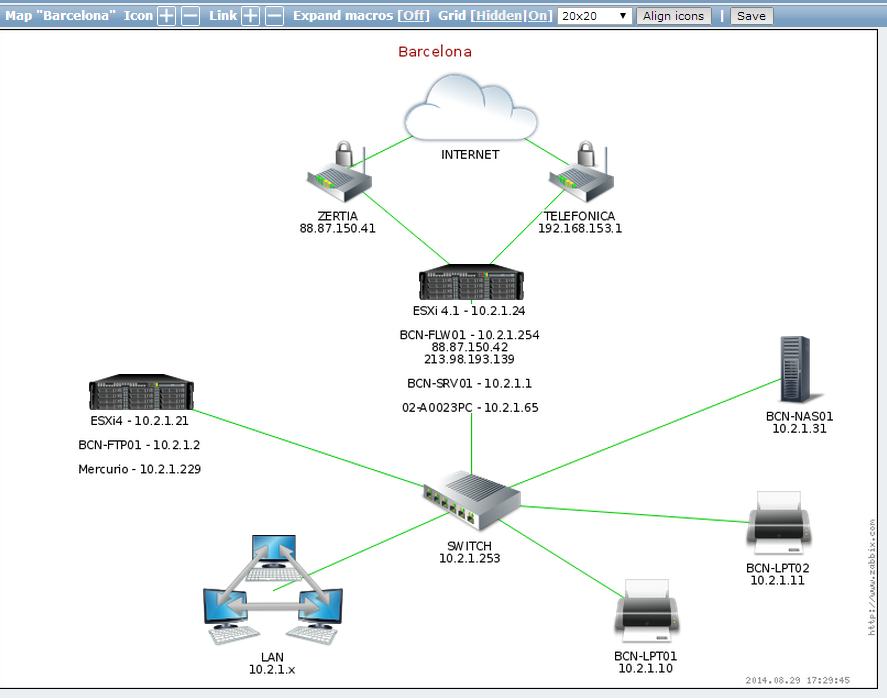




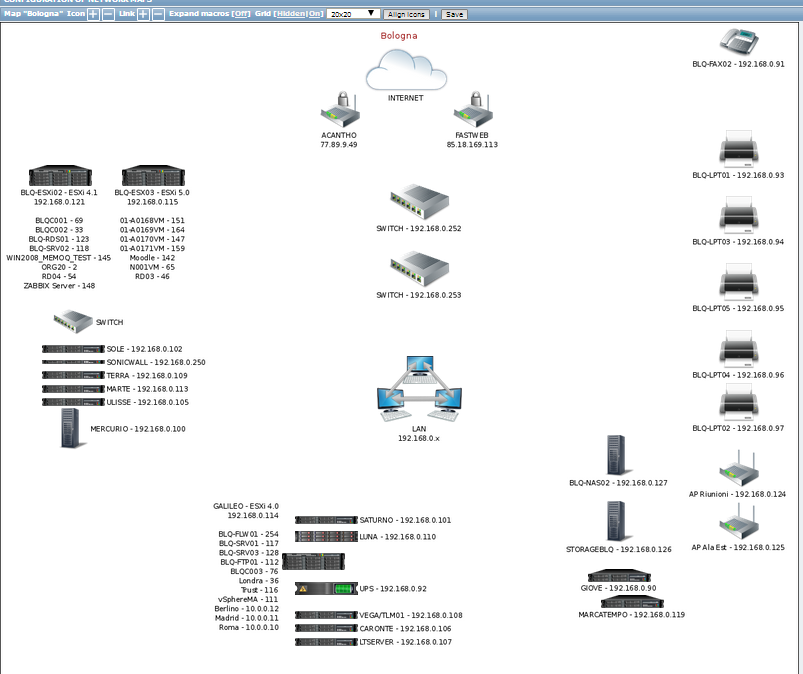




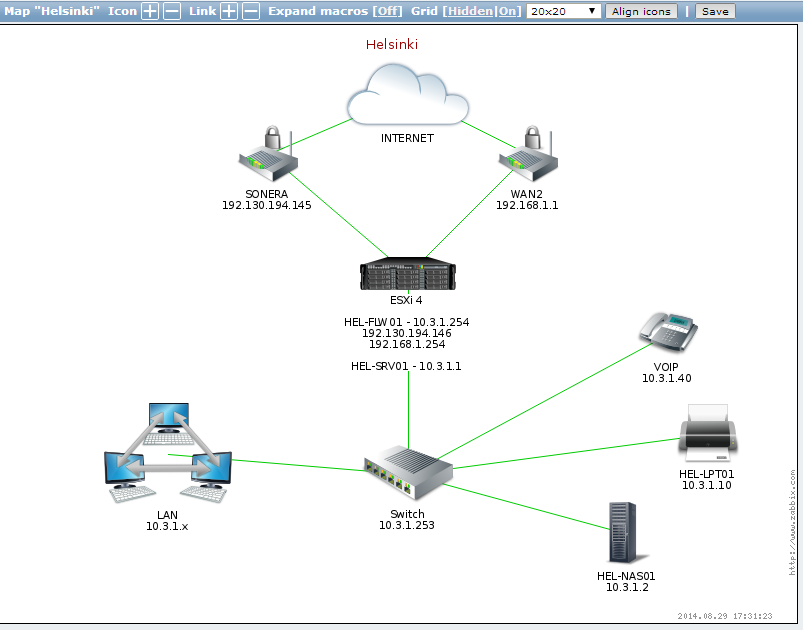
#### Barcellona



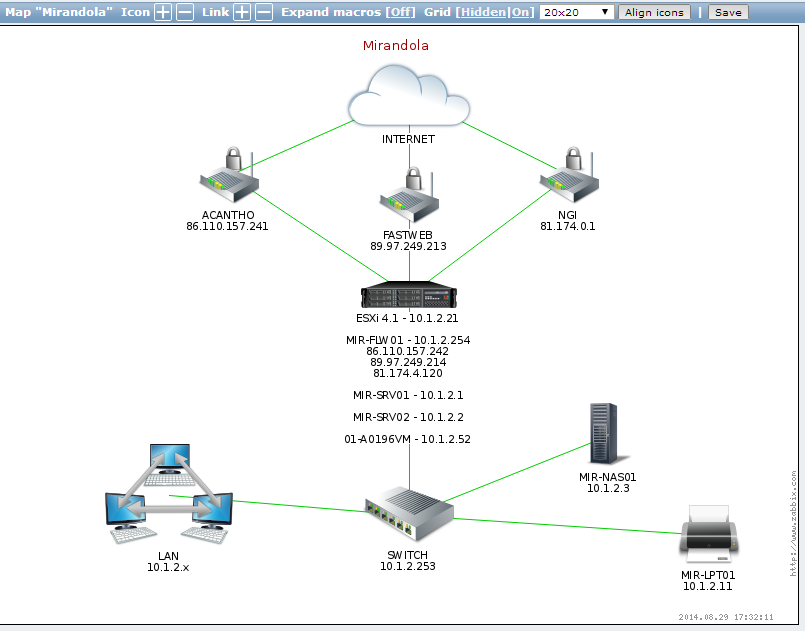
#### Bologna



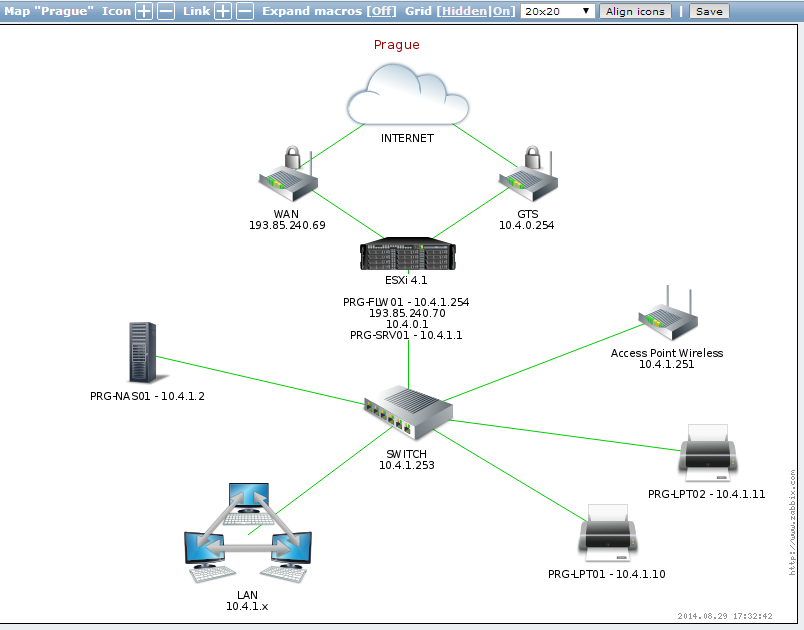
#### Helsinki



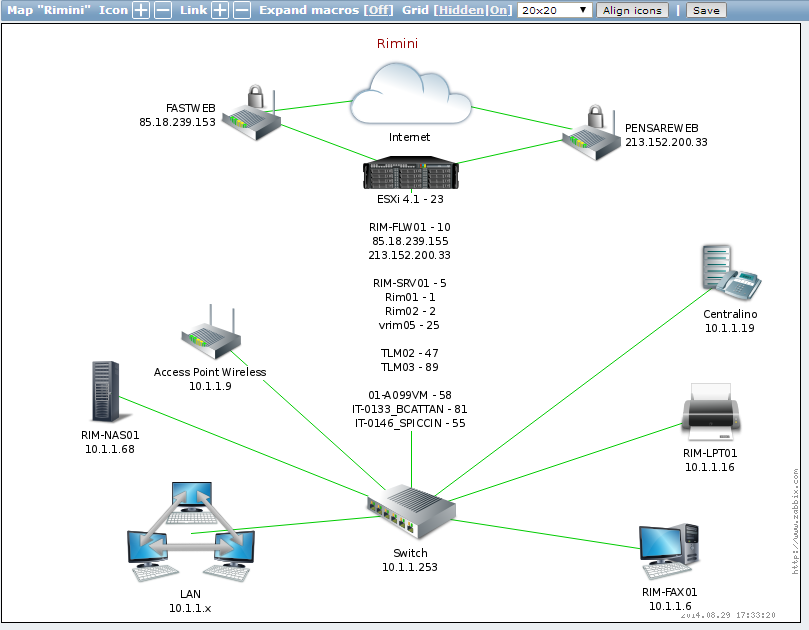
#### Mirandola



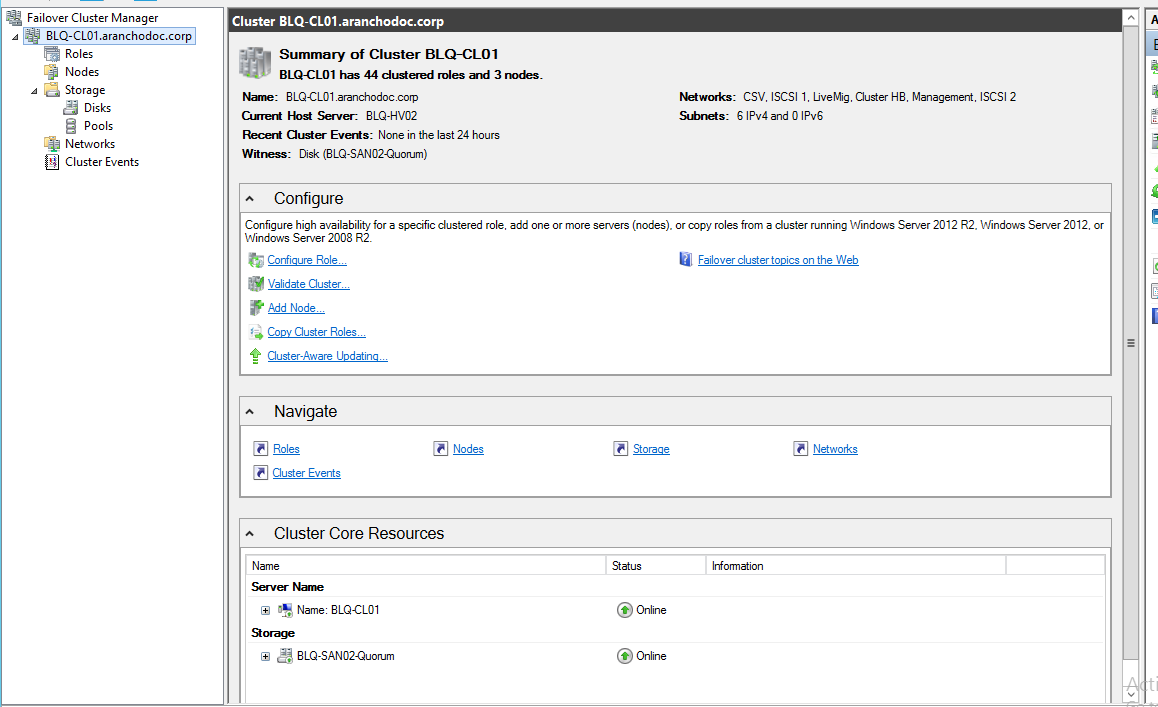
#### Praga



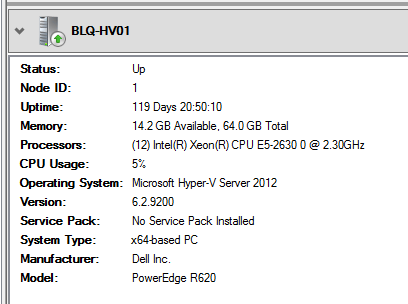
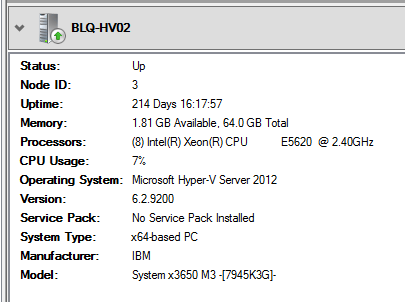
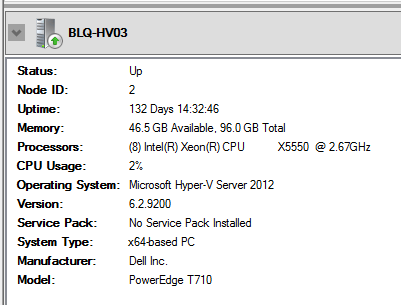
#### Rimini



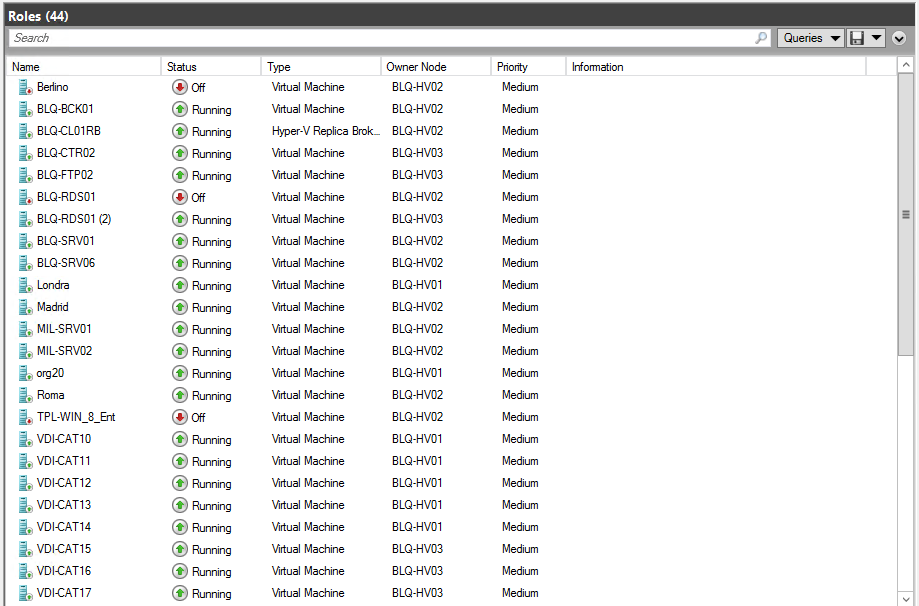
## E – Configurazioni cluster Hyper-V

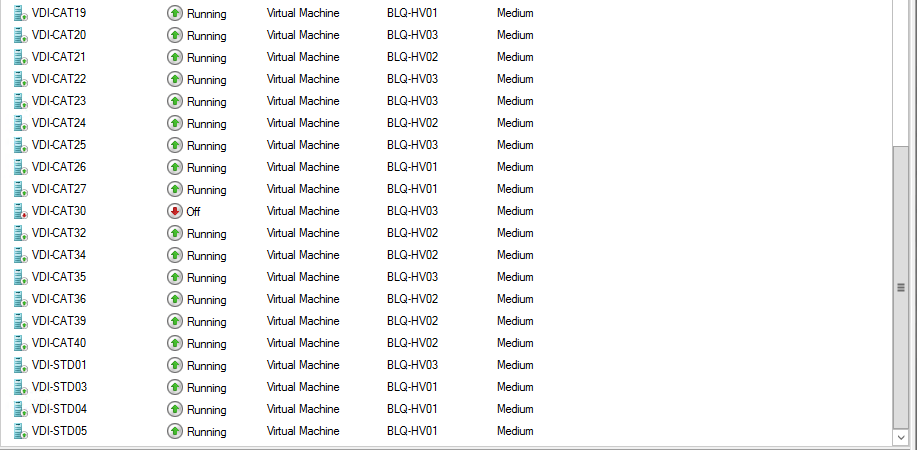


I tre nodi sono:

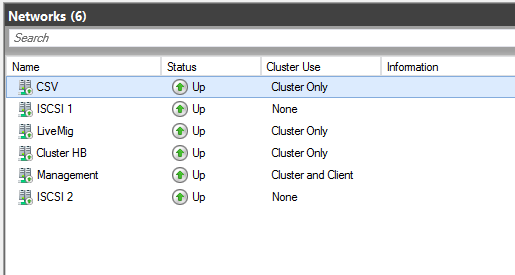
* BLQ-HV01 – 
* BLQ-HV02 - 
* BLQ-HV03 - 

Di seguito le VM rilevate su BLQ-CL01:





Di seguito le reti definite sul cluster:



Testo alternativo generato dal computer:
00254 16/28 

Testo alternativo generato dal computer:
00 0/24 

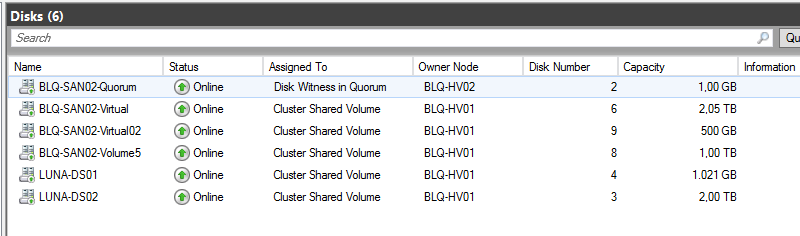
Testo alternativo generato dal computer:
Live* g 
0 0 2540/28 

Testo alternativo generato dal computer:
HB 
0 0 25432.'28 

Testo alternativo generato dal computer:
92 6800/24 

Testo alternativo generato dal computer:
0020/24 

Di seguito le LUN associate al cluster:



Testo alternativo generato dal computer:
BLQ-SAN02-Quorum 
Volu— (I) 
Clustered Disk 071V01umefd432084b-a371-1 
NTFS MB 

Testo alternativo generato dal computer:
BLQ-SAN02-Mrtua1 
Volu— (I) 
aca-SAN02-W,rtuzl M 
CSVFS 255 GB free of 2,05 TB 

Testo alternativo generato dal computer:
BLQ-SAN02-Mrtua102 
Volu— (I) 
SAN02-VIrtua102 (C:iCIusterStorzgeWoIume3) 
CSVFS 104 GB free of GB 

Testo alternativo generato dal computer:
BLQ-SAN02-V01u,ne5 
Volu— (I) 
DS02-VoIume5 (CftCIusterStorzgeWoIume5) 
CSVFS GB 1 024 GB 

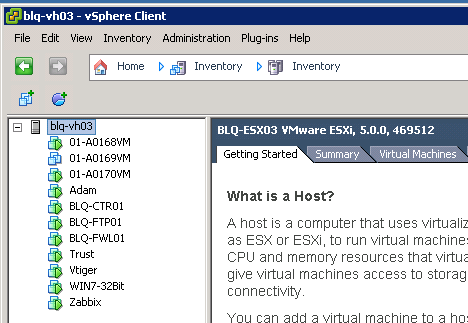
Testo alternativo generato dal computer:
LUNA-DSOI 
Volu— (I) 
LUNA-DSOI (CftCIusterStorzgeWo ume2) 
CSVFS GB free of 1 021 GB 

Testo alternativo generato dal computer:
LUNA-DS02 
Volu— (I) 
LUNA-DS02 (C hCIusterStorageWo ume4) 
CSVFS 1 38 TB TB 

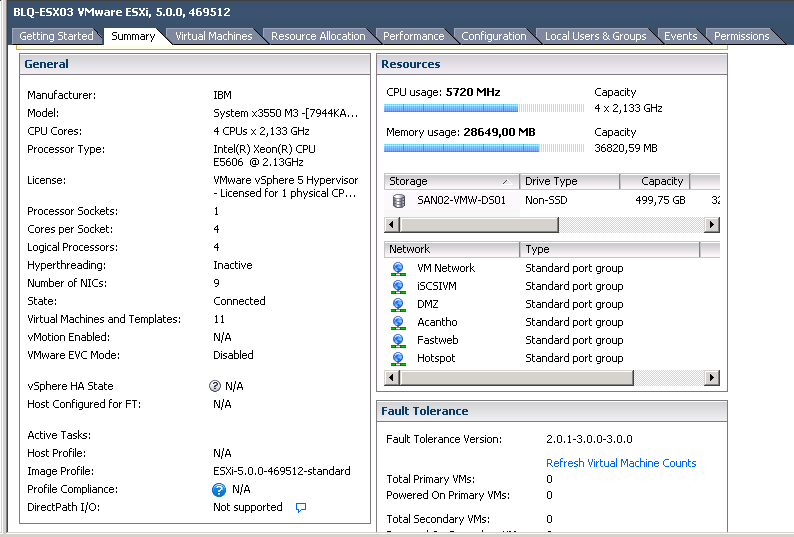
## F – Configurazioni BLQ-VH03

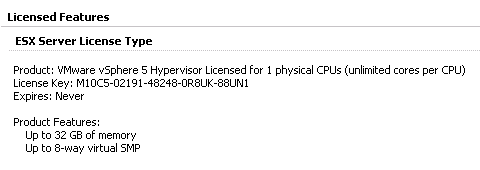
DI seguito la configurazione di dettaglio di BLQ-VH03.

Virtual machines:



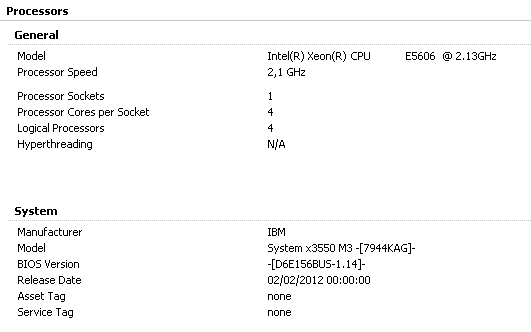
Summary:





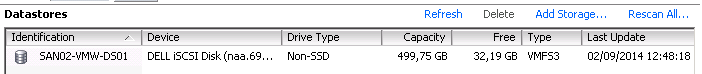
Hardware:

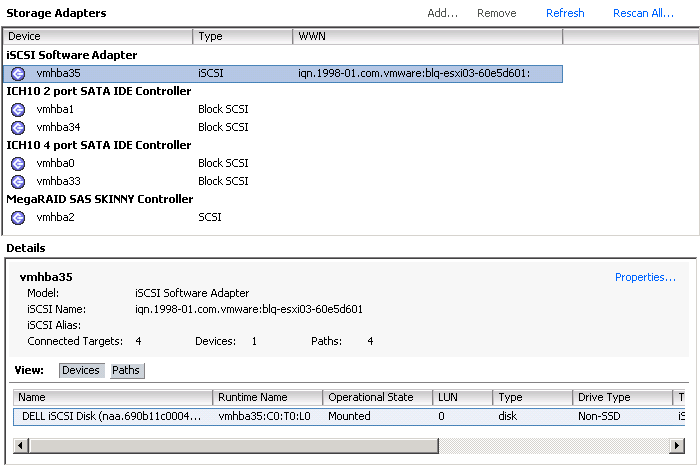




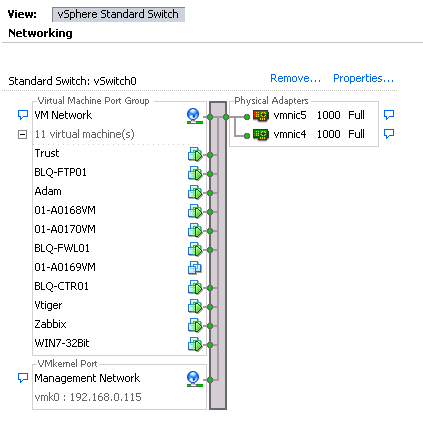


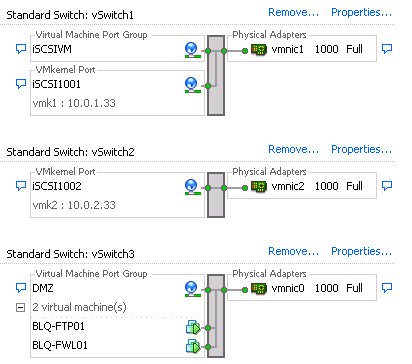
Storage:

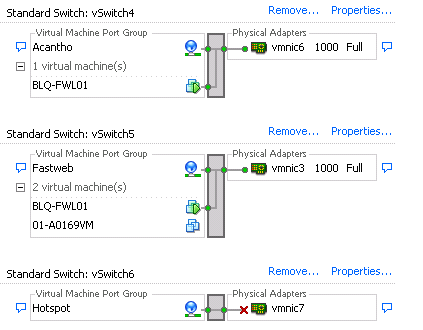


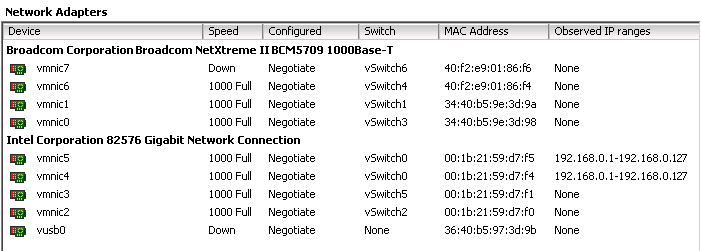


Network:









# Allegati

Si considerano allegati i documenti prodotti durante l’analisi. Non si allegano i documenti raccolti già in possesso del cliente.

|  |  |
| --- | --- |
| **Allegato** | **Descrizione** |
| WindowsVolumeLicensingAssessment-09-18-2014-14h11m27s.xlsx | Raccolta dati sul licensing eseguita tramite Microsoft MAP. |
| VMReport-09-18-2014-12h42m27s.xlsx | Raccolta dati sulle VM eseguita tramite Microsoft MAP. |
| ExchangeServerUsageTracker-09-18-2014-14h11m20s.xlsx | Raccolta dati sulla posta eseguita tramite Microsoft MAP. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Tab. Allegati

# Sigle ed acronimi

|  |  |
| --- | --- |
| Sigla | Descrizione |
| AD | Active Directory |
| API | Application Programming Interface |
| AS | Advanced Server |
| BMG | Banda Minima Garantita |
| COM | Component Object Model |
| DLL | Dynamic Link Library |
| GPO | Group Policy Option |
| HW | Hardware |
| IE | Microsoft Internet Explorer |
| IPS | Intrusion Protection System |
| IT | Information Technology |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| MS | Microsoft |
| MSCS | Microsoft Cluster Server |
| NIC | Network Interface Card |
| OS | Sistema Operativo (Operating System) |
| OU | Organizational Unit |
| RPC | Remote Procedure Call |
| SOHO | Small Office Home Office |
| SMTP | Simple Mail Transfer Protocol |
| SP | Service Pack |
| SSL | Secure Socket Layer |
| SW | Software |
| VPN | Virtual Private Network |

Tab. Sigle e Acronimi