

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

Specifica di Realizzazione del Servizio

DNS della QXN

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

Sommario

0. GENERALITÀ.....	3
0.1 DEFINIZIONE ED ACRONIMI	3
1. SERVIZIO DNS DELLA QXN	4
2. SPECIFICHE DI INTEGRAZIONE PER I DNS SPC DEI Q-ISP ED I DNS DELLA QXN	8

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

0. GENERALITÀ

0.1 Definizione ed Acronimi

Definizione / Acronimo	Descrizione
ACL	Access Control List
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
DNS	Domain Name Service
DNSSEC	Security Extensions for DNS
IXFR	Incremental Zone Transfer
LdS	Livello di Servizio
NOC	Networking Operating Center
NTP	Network Time Protocol
Q-ISP	Qualified ISP
QXN	Qualified eXchange Network
RFC	Request for Comments
SC-QXN	Società Consortile QXN
Servizio	Il termine Servizio coincide con il termine/concetto di sotto-progetto definito nella Procedura CNIPA relativa alla Gestione dei Requisiti.
SLA	Service Level Agreement
SOC	Security Operating Center
SPC	Sistema Pubblico di Connettività
SSH	Secure SHell
TSIG	Transaction SIGnature
TTL	Time To Live

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

1. Servizio DNS della QXN

Il servizio DNS della QXN è realizzato mediante l'utilizzo del software Open Source ISC BIND (Berkeley Internet Name Domain) – ver 9.2.4 distribuita con RedHat. BIND è il server DNS più usato su internet, ed in particolar modo sulle piattaforme Unix dove è lo standard di fatto. Nell'ultima versione ha un'architettura completamente rivista ed è pienamente compatibile con le evoluzioni del protocollo DNS, oltre a incorporare nuove funzionalità ed estensioni per la sicurezza (DNSSEC, TSIG) offre compatibilità con IPv6 e supporto per sistemi multiprocessore.

Per quanto riguarda la configurazione dei sistemi, particolare attenzione viene posta alle tematiche inerenti l'alta affidabilità/disponibilità ed i tempi di risposta, dimensionando opportunamente il numero di serventi, la dimensione della cache dei Name Server e ridondando i meccanismi nativi di replica delle zone.

L'alta affidabilità del servizio riguarda:

1. meccanismi di risoluzione dei nomi,
2. meccanismi di distribuzione delle informazioni tra i diversi serventi della QXN.

Il primo obiettivo ha lo scopo di garantire che vi sia sempre almeno un Name Server in grado di rispondere a ciascuna richiesta dei Q-ISP, il secondo ha lo scopo di garantire che le basi dati dei sistemi DNS della QXN siano sempre allineate in modo che il malfunzionamento di un singolo nodo non infici sulla validità delle informazioni pubblicate.

Per l'alta affidabilità della risoluzione si è deciso di sfruttare i meccanismi di fall-back nativi del protocollo DNS: nei meccanismi di instradamento, infatti, è possibile specificare una lista di Name Server ed è il protocollo di risoluzione stesso a garantire automaticamente l'inoltro della query verso gli altri sistemi, qualora il primo risulti non disponibile.

I DNS dei Q-ISP dedicati alla PA SPC (di seguito indicati come DNS SPC del Q-ISP), pertanto, dovranno:

- avere come “forwarders” gli indirizzi dei DNS QXN, uno dislocato presso la sede QXN del NaMeX (Roma) ed uno nella sede del MIX (Milano);
- avere la possibilità di accedere ai “root server” di Internet in modo da poter fornire alle PA direttamente gestite dai QISP il servizio di risoluzione dei nomi internet anche quando i DNS QXN non sono raggiungibili.

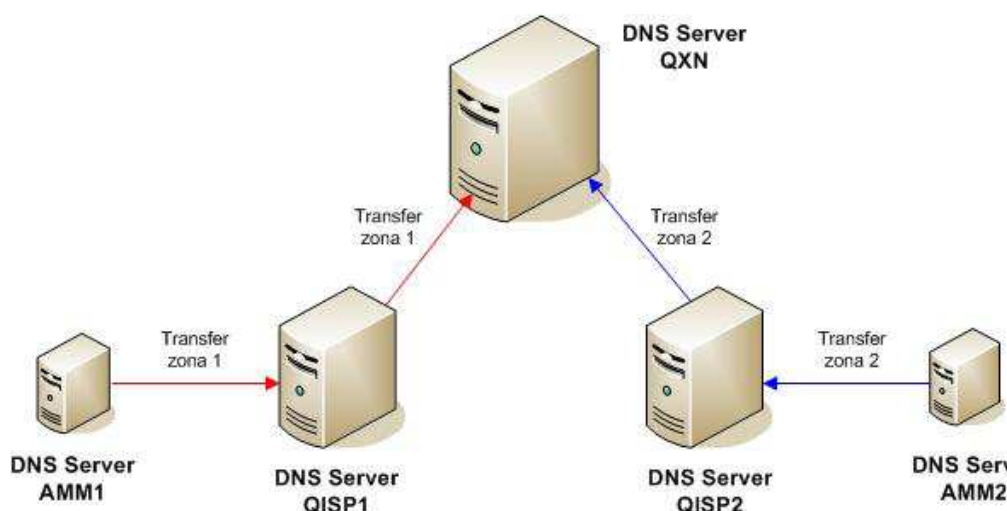
L'alta affidabilità sulla replica delle zone tra i sistemi della QXN è garantita dai meccanismi interni di Zone Transfer e DNS Notify (RFC 1996): tutti i server che compongono entrambi i cluster dovranno essere abilitati ad effettuare Zone Transfer dai DNS SPC del Q-ISP; tali serventi, a loro volta, provvederanno a notificare la modifica a tutti gli altri sistemi tanto sul MIX quanto sul NaMeX.

La soluzione proposta prevede l'installazione presso i nodi della QXN di una batteria di Name Server paritetici, configurati in modo da garantire la replica reciproca delle informazioni.

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

Tali Name Server risponderanno come “DNS Autoritativi¹” per tutte le Zone SPC e saranno configurati come “DNS Slave” rispetto ai DNS SPC dei Q-ISP. Saranno inoltre collegati ai Root Server DNS di internet per la risoluzione e il caching dei nomi esterni allo spazio SPC.

La seguente figura illustra il flusso dei trasferimenti di zona per i domini interni alla rete SPC.



Come illustrato, i DNS SPC dei Q-ISP ricevono le zone delle amministrazioni afferenti; tale informazione viene successivamente replicata sul DNS della QXN che in questo modo diviene il nodo centrale di collezione delle informazioni sullo spazio dei nomi all'interno della rete SPC.

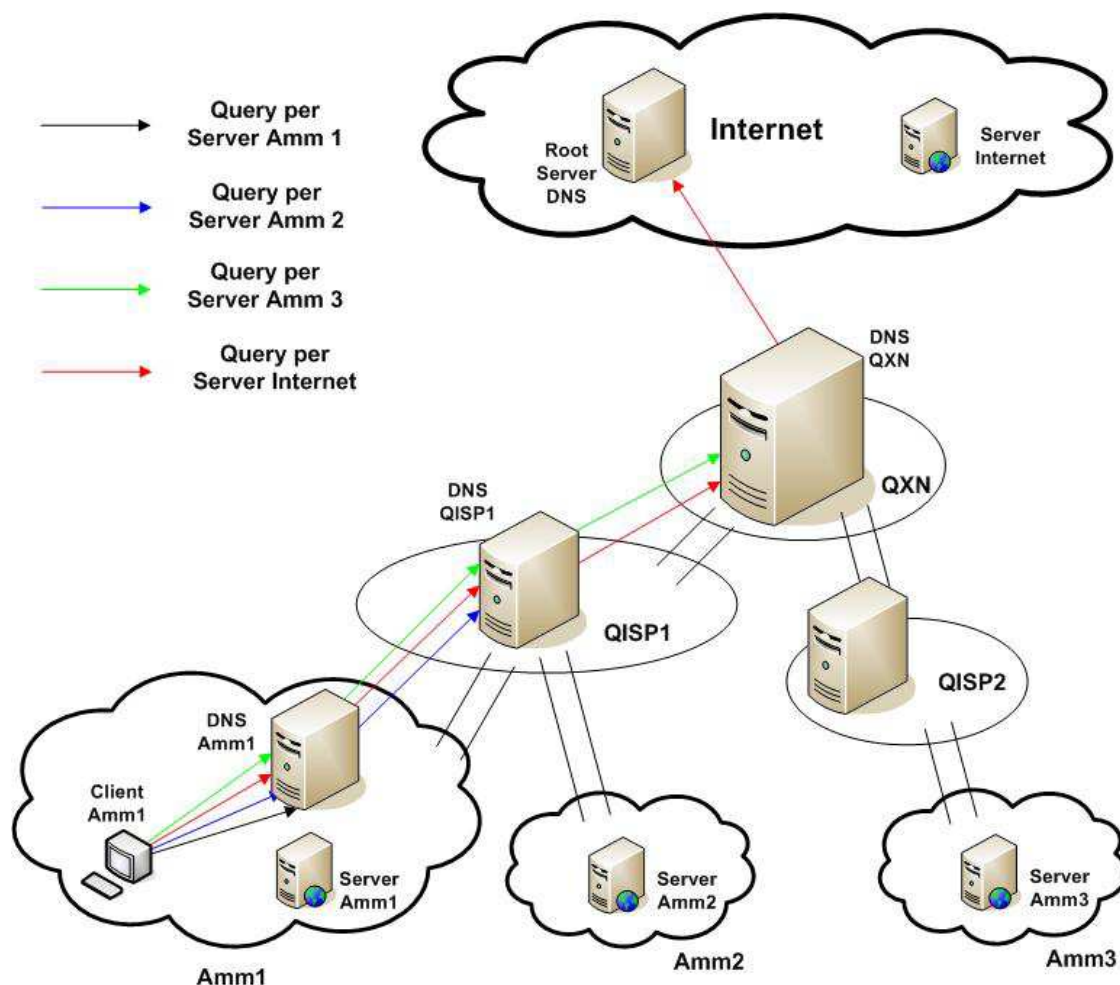
La scelta di effettuare una replica delle zone, in luogo dei meccanismi di forwarding selettivo è giustificata da vantaggi sia in termini di prestazioni che di affidabilità delle informazioni: il poter disporre dell'informazione di zona direttamente sui DNS della QXN, infatti, da un lato, abbassa i tempi di risposta e riduce il traffico perchè non c'è bisogno di inoltrare ulteriormente la richiesta verso altri DNS e, dall'altro, riduce il rischio che il DNS della QXN abbia in cache informazioni non più valide perchè modificate sul Name Server del DNS SPC del Q-ISP, risolvendo inoltre, il problema della gestione dei meccanismi di “forwarding selettivo” che ciascun Q-ISP dovrebbe abilitare per raggiungere dalla rete SPC il DNS SPC degli altri Q-ISP.

La modifica su una zona presente nel DNS SPC di un Q-ISP, infatti, verrà replicata direttamente sul DNS della QXN, in accordo con i parametri di configurazione della zona stessa, oppure immediatamente nel caso di utilizzo del DNS Notify, rendendo la nuova informazione disponibile sul DNS della QXN, senza attendere la scadenza del periodo di cache specificato dal valore del TTL.

¹ Il termine “Autoritativo” indica un server che risponde direttamente alle query, senza quindi interrogare nessun altro server, indipendentemente dal fatto che se sia configurato come Master o Slave rispetto alla zona, garantendo inoltre che su tali informazioni non venga effettuato alcun tipo di caching.

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

Per quanto riguarda la risoluzione dei nomi internet, la generica query proveniente dall'amministrazione viene risolta attraverso il meccanismo di forwarding, illustrato nella seguente figura.



Le richieste dei client vengono tutte inoltrate al server DNS della rete dell'Amministrazione, che risolve direttamente le query per i propri domini, inoltrando, in caso non abbia in cache l'informazione, tutte le altre restanti richieste verso il DNS SPC del Q-ISP fornitore dei servizi di connettività.

Il DNS SPC del Q-ISP fornisce quindi direttamente le risposte per i domini di tutte le Amministrazioni ad esso collegate, inoltrando, in caso non abbia in cache l'informazione, tutte le restanti richieste al DNS della QXN.

Il DNS della QXN, infine, in qualità di collettore dei nomi pubblicati dai DNS SPC dei Q-ISP, risponde direttamente alle query riguardanti lo spazio dei domini nell'ambito della rete SPC, mentre effettua una query ai Root Server internet per tutti gli altri nomi, qualora non abbia in cache l'informazione.

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

Il DNS della QXN risponde esclusivamente alle query provenienti dai DNS SPC dei Q-ISP: ciò viene realizzato mediante opportune regole di filtering applicate sullo strato di sicurezza (firewall) posto a protezione della infrastruttura QXN.

Come maggior garanzia di protezione, ciascun server componente l'infrastruttura avrà impostate delle opportune ACL volte ad impedire la risoluzione di query provenienti da host non esplicitamente autorizzati.

	Qualified eXchange Network
Specifica di Realizzazione del Servizio DNS della QXN	QXN-DNS-SpecificaRealizzazione

2. Specifiche di integrazione per i DNS SPC dei Q-ISP ed i DNS della QXN

I DNS SPC dei Q-ISP collegati ai server DNS della QXN devono essere configurati in modo da annunciare automaticamente a questi ultimi il cambiamento di una zona di propria competenza tramite i meccanismi di DNS Notify (RFC1996). Inoltre il DNS SPC di ciascun Q-ISP deve essere configurato in modo tale da accettare le richieste di AXFR (Full Zone Transfer) e IXFR (Incremental Zone Transfer RFC1995), provenienti dai Name Server della QXN.

Il DNS della QXN è configurato in modo tale da:

- ricevere le DNS Notify da parte dei DNS SPC dei Q-ISP,
- verificare che la notifica sia stata effettuata da un DNS SPC del Q-ISP autorizzato,
- effettuare lo zone transfer delle zone delle Amministrazioni dai server DNS SPC dei Q-ISP , al fine di esporle in ambito SPC.

Sulla base delle definizioni date nel documento di specifica del servizio “QXN-DNS-SpecificaServizio-x.y”, il DNS della QXN dovrà replicare esclusivamente le “zone SPC” presenti sul DNS SPC di ciascun Q-ISP. Tali zone potrebbero coincidere con le “zone pubbliche” qualora l’amministrazione non abbia necessità di distinguere tra “host pubblici” ed “host infranet”.

I meccanismi di Zone Transfer dai Name Server della PA verso i Name Server del DNS SPC del Q-ISP sono di pertinenza di ciascun Q-ISP. La distinzione tra “zone pubbliche” e “zone SPC” della PA, è invece di pertinenza di ciascuna PA e sotto la sua diretta responsabilità.