DnsManager
Versione 3.0

Francesco Gennai

Nota tecnica

Consiglio Nazionale delle Ricerche

Istituto di Scienza e Tecnologie dell'Informazione
"Alessandro Faedo"

Francesco Gennai

Indice

Introduzione

DnsManager è un software per la gestione via web di un name server (Domain Name System), basato sul modello Centralizzato con Delega Amministrativa.
Il sistema risulta particolarmente utile nel CNR dove, in attuazione della riforma dell'Ente, un Istituto può essere costituito da sezioni geograficamente distribuite, come risultato della fusione di più organi di ricerca.
Un Istituto può avere in dotazione un dominio e diversi indirizzi di rete IP, o parti di esse, presso ciascuna delle sue sezioni. La gestione dello spazio dei nomi può avvenire anche assegnando un sottodominio a ciascuna sezione e opzionalmente delegando l'amministrazione della relativa zona.
A questo punto però è importante chiarire come la consuetudine di creare una zona per ogni sottodominio possa essere rivista in base alle nuove possibilità che DnsManager introduce.
E' molto importante non ritenere strettamente associate l'operazione di creazione di un sottodominio con quella di delega della relativa zona. Non sempre vi è la necessità di definire una nuova zona per un nuovo dominio !! (in particolare se questo è visto come sottodominio interno ad una stessa unità organizzativa).
Il mantenimento di un sottodominio all'interno della stessa zona del dominio padre permette una maggiore flessibiltà nella gestione dei nomi.
L'esigenza primaria di creare una zona separata per un determinato dominio (sottodominio) nasce sovente dalla necessità di delegarne il controllo amministrativo. Con l'utilizzo di DnsManager la delega può avvenire ad un livello superiore (delega virtuale) con il risultato che la creazione di una zona per un sottodominio non è più strettamente necessaria.
DnsManager consente, con notevole flessibilità, la scelta della soluzione più adatta ad ogni singolo caso.

Utilizzando DnsManager, l'amministratore può gestire il proprio dominio senza doversi preoccupare della gestione operativa del name server e senza dover necessariamente ricorrere alla definizione di zone per la delega amministrativa di eventuali sottodomini. In questo modo la gestione dell'intero spazio dei nomi di un Istituto risulta più flessibile e gli utenti possono avere tempi di risposta veloci.
L'interfaccia web abilita l'uso ed il controllo del sistema anche a gestori remoti. Per una migliore distribuzione delle competenze sono state previste interfacce indirizzate a differenti categorie di amministratori: personale tecnico esperto, personale non tecnico (senza particolari conoscenze dei fondamenti del DNS). In questo modo informazioni delicate, come la definizione di record NS o record MX vengono trattate solo da un numero limitato di persone.

Il sistema verifica che tutte le informazioni passate dal gestore al server siano congruenti, evitando in tal modo gli errori che normalmente si possono commettere nella gestione di un name server.

Descrizione del sistema

L'amministrazione del servizio avviene attraverso una interfaccia WEB a cui si accede via sessione criptata (https). Il gestore può essere abilitato alla creazione ed alla cancellazione di record di tipo: A, NS, MX, CNAME, PTR. Può inoltre associare a ciascun record informazioni amministrative come la data di scadenza del record, il nome del referente dell'host o la dislocazione dell'apparato registrato.
L'amministrazione si basa su una struttura gerarchica composta da tre livelli di accesso, per ognuno dei quali è possibile definire più utenti di amministrazione:

- **supervisore** per il controllo di tutti i gruppi amministrativi del dominio;
- **amministratori privilegiati** che possono controllare uno o più gruppi con possibilità di accedere a tutti i tipi di record (A, NS …);
- **amministratori non-privilegiati** che controllano uno o più gruppi, limitatamente ai record di tipo A.

Ad ogni utente è associato un file di configurazione che ne descrive le caratteritiche operative, assegna i privilegi ed abilita determinate funzioni di gestione e controllo.
Nella implementazione del sistema particolare attenzione è stata rivolta alle caratteristiche degli organi CNR, tenendo conto degli Istituti con sezioni distribuite sul territorio. Il sistema è stato perciò realizzato per permettere:

- la suddivisione di un dominio in sottogruppi amministrativi, dove un gruppo può essere associato ad un dipartimento, sezione, etc.. ma anche a singoli reparti, laboratori, unità operative interne ad essi;
- la possibilità di assegnare più sottoreti ad uno stesso dominio.
- la possibilità di creare per ogni gruppo, più utenti di amministrazione, ognuno con caratteristiche diverse (abilitazione di funzioni, privilegi, limiti al numero massimo di host registrabili, etc...).
- la possibilità di assegnare ad uno stesso utente il controllo più gruppi amministrativi, anche appartenenti a domini diversi.

Il sistema risulta particolarmente indicato per semplificare la gestione del cambio di nome di un dominio. Per esempio la migrazione degli host dal vecchio dominio dell'Istituto al suo nuovo nome. Tali operazioni possono essere delegate ai gestori di singole porzioni di dominio (dipartimenti, reparti, laboratori, segreterie, etc..) in concorrenza su una stessa LAN e/o dominio.
Ne deriva una notevole semplificazione dell'intera fase di migrazione.

Gestione indirizzi IP

Il sistema prevede sia l'assegnazione automatica sia manuale degli indirizzi che possono essere suddivisi in sub-range di gruppo (uno o più range per Laboratorio, segreteria, etc..) o amministrativi (range dei Router, Server, Host, etc.). L'assegnazione automatica alloca sempre il primo indirizzo libero del sub-

range selezionato. Opzionalmente è possibile richiedere l'allocazione del primo indirizzo libero a partire da un valore interno ad un range, inserendo l'indirizzo di inizio della ricerca seguito dal carattere +. Esempio: 36+.
Il sistema provvede anche alla creazione automatica del relativo record PTR. Le zone delle risoluzioni inverse sono comunque gestibili attraverso la relativa interfaccia web.

Regole di referenza e di conflitto

Ad ogni modifica di un record il sistema, dotato di specifiche regole di referenza e di conflitto, esegue opportuni controlli in modo da rendere minima la possibilità di errore umano. I controlli avvengono tra i valori contenuti in tutte le zone gestite dal sistema.
Per esempio, durante l'aggiunta di un record CNAME (MX o NS) vengono effettuati controlli sulla esistenza del record A referenziato. Durante la rimozione di un record A vengono evidenziati gli eventuali record (CNAME, MX , NS) che lo referenziano.
Questi controlli oltre che guidare l'utente inesperto in un corretto utilizzo del DNS rilevano anche banali errori di digitazione di un nome.

Interazione del sistema con i server SMTP

Il sistema DnsManager implementa una funzione per il controllo degli accessi al servizio di posta elettronica: ad ogni record A è associato un flag che permette l'abilitazione o disabilitazione dell'accesso al server di posta. Si ottiene un miglior controllo della sicurezza permettendo l'uso della posta elettronica solo ai calcolatori espressamente abilitati.
L'integrazione con il sistema INSM permette di rilevare l'emissione di un messaggio con virus e di inviare immediatamente un messaggio (email) di notifica all'amministratore del range di indirizzi a cui appartiene l'indirizzo IP dell'host mittente.
La notifica conterrà l'indirizzo IP del mittente e il tipo del virus.

Funzionalità e loro applicazioni

Il sistema DnsManager è progettato per essere inserito (adottato) in configurazioni del sistema DNS preesistenti senza la necessità di alcuna particolare modifica.
Questo aspetto è fondamentale per inserire DnsManager in una struttura già esistente e con l'aiuto di esso attivare il successivo processo di riorganizzazione del DNS (esempio: cambio del nome di dominio per un determinato gruppo di host, riallocazione di range di indirizzi IP in base alla nuova organizzazione di un organo, etc..).
La particolare flessibilità di DnsManager permette la distribuzione delle attività di modifica (cambio nome dominio, diversa all'allocazione indirizzi IP, etc...) su un ampio arco di tempo. La gestione di un dominio può essere limitata e delegata a

diverse unità organizzative che potranno controllare, in concorrenza tra loro, stessi range di indirizzi IP.

Le singole unità organizzative presenti all'interno di uno stesso dominio (Uffici, Laboratori, Centri, Reparti, etc..) avranno una loro totale indipendenza e potranno controllare le registrazioni dei nomi di host all'interno del range di indirizzi IP loro assegnato.
Come già precedentemente accennato, uno stesso range può essere gestito da diverse unità (cioè diverse unità possono gestire in concorrenza uno stesso range di indirizzi IP), ma ognuna di esse avrà un limite massimo di indirizzi IP assegnabile (presumibilmente in modo tale da evitare che la somma di tutti i limiti massimi, che concorrono su uno stesso range, superi la sua capacità totale).
Questa particolare funzionalità rende semplice l'inserimento del DnsManager e della delega del controllo all'unità organizzativa, in situazioni dove gli indirizzi IP erano assegnati in modo non contiguo (in uno stesso range sono registrati host appartenenti a diverse unità organizzative).
Un esempio: in un organo con 5 reparti ed una classica rete locale, con disponibilità di 254 indirizzi si definiscono 5 amministratori (uno per ciascuna unità organizzativa) e si assegna, ad ognuno di essi, uno stesso range (es.: 15-254) ed un limite massimo al numero totale di indirizzi che ciascun amministratore potrà assegnare:
reparto1 = 50 indirizzi, reparto2 = 20 indirizzi, reparto3 = 60 indirizzi, etc....
Il limite può essere diverso per ciascun amministratore/reparto.

Su una stessa LAN possono essere presenti host appartenenti a domini diversi (per esempio: durante la migrazione di un dominio dovuta ad un cambio di nome dell'organo).
L'amministratore di una unità organizzativa avrà il controllo sui range di indirizzi IP indipendentemente dal dominio in cui un determinato IP è registrato. Questo consentirà di rimuovere un host da un dominio (vecchio dominio) per registrarlo in un altro (nuovo dominio).
Durante questa operazione l'indirizzo IP, anche se reso libero dalla operazione di rimozione dell'host dal vecchio dominio, resterà allocato in modo esclusivo all'amministratore per un tempo prefissato (IP release delay time - stabilito con un parametro di configurazione variabile per ogni singolo amministratore) entro il quale lo stesso amministratore potrà riutilizzarlo per la registrazione dell'host nel nuovo dominio. Passato tale tempo l'indirizzo IP potrà essere utilizzato da qualsiasi altro amministratore purchè lo stesso appartenga ad uno dei suoi range.

L’ambiente operativo

DnsManager funziona in ambiente Unix-like OpenVMS/Bash Shell.
La configurazione, può avvenire attraverso script di configurazione automatica che guidano l’amministratore con una serie di domande, o, per amministratori più esperti, direttamente editando i file di configurazione.
Per la sessione di lavoro è possibile selezionare tra Bash Shell o DCL Shell.

Strutture dati

DnsManager si avvale del file system RMS (Record Management System) di OpenVMS, che permette una efficiente gestione di file ad indici.
Data la relativa semplicità delle relazioni tra i dati da gestire, l’uso di un file ad indice è più che sufficiente ed elimina la necessità di adottare prodotti per la gestione di database che avrebbero, oltretutto, reso i dati non più trattabili con strumenti di base del sistema operativo (è possibile editare un file ad indice con un normale editor di testo come VI).

Ciascun dominio è gestito attraverso un proprio database (Domain Database) che conterrà tutti i record, eccetto il record SOA.
Dal Domain Database viene generato il file di zona in formato testo.
Vi è inoltre un database “generale” (General Database) che contiene i record di tutti i domini sia in versione indicizzabile che preformattati HTML per una loro rapida visualizzazione.
Il General Database è inoltre utilizzato per la gestione ed il controllo delle relazioni inverse tra i record appartenenti anche a domini diversi (esempio: partendo dal nome di un record A permette di determinare tutti record CNAME, NS o MX che lo riferiscono (cioè i record che contengono tale nome nella loro parte “record data”) - Ovviamente questo è possibile solo tra domini gestiti da DnsManager).
Per le relazioni dirette viene utilizzato anche DIG (esempio: verifica dell’esistenza del record A che compare nella parte “record data” di un record MX).
Tutti i database si trovano nella directory /www_service/wwwdnsman/data.
DnsManager mantiene sincronizzati i database di dominio con il database generale, grazie anche a funzioni di recovery, che sono in grado di ripristinare la struttura dati eventualmente danneggiata da una operazione non conclusa correttamente (esempio crash di sistema durante la rimozione di uno o più record).

File di zona

I file di zona gestiti da DnsManager si trovano nella directory identificata tramite il nome INSM_DNSMAN_ZONE_DIR.

Tali file saranno rigenerati completamente ad ogni operazione di “Zone Upload” richiesta tramite interfaccia web. Eventuali modifiche manuali al file di zona saranno quindi sovrascritte dalla generazione della nuova versione di file.
Per l’inclusione “manuale” di record, è possibile editare una coppia di file che saranno automaticamente inclusi nel file di zona, rispettivamente in testa (subito dopo il record SOA) e/o in coda. Questi record non saranno accessibili alle routine del DnsManager per cui si consiglia la massima attenzione nell’utilizzo di questa soluzione.
Il nome del file per l’inclusione in testa (TOP) è dato dal nomedominio con $ al posto dei punti ed estensione zonet, mentre il nome file per l’inclusione in coda (BOTTOM) è dato dal nomedominio con $ al posto dei punti ed estensione zoneb.
La semplice presenza dei file nella directory /www_service/wwwdnsman/zones è sufficiente ad attivare la loro inclusione.
E’ bene comunque ricordare che il BIND non richiede alcun ordinamento dei record internamente ad un file di zona.

File di configurazione DnsManager

Le caratteristiche degli amministratori di un dominio e lo schema di partizionamento per l’allocazione degli indirizzi IP di una LAN vengono definiti attraverso opportuni file di configurazione che si trovano nella directory /www_service/wwwdnsman/config.
Per ogni utente amministratore (privilegiato o non privilegiato) di un dominio occorre creare il rispettivo file di configurazione.
L’accesso ad un determinato utente potrà avvenire con autenticazione HTTP (standard) o con accesso “proxy” da parte di un altro utente precedentemente autenticato via HTTP.
Questo permette di associare l’amministrazione di più domini ad uno stesso utente (Notare che quando un utente “HTTP” ha la facoltà di amministrare più domini, nella parte superiore della pagina web comparirà la url “domain lists” cliccando la quale si potrà accedere alla lista dei domini assegnati).
L’associazione tra un nome utente e il proprio file di configurazione avviene tramite l’inclusione dello stesso nel nome del file di configurazione.
Un altro parametro importante che compare nel nome del file di configurazione è l’identificativo di dominio (domain id) che può avere una lunghezza massima di 3 caratteri ed è scelto liberamente dall’amministratore in fase di prima installazione di un dominio.
Unica condizione è che deve essere univoco all’interno del sistema Integrated Network Systems Manager (DnsManager, MailboxManager).
Uno stesso dominio può avere più amministratori privilegiati e non privilegiati. Per ognuno di essi il rispettivo file di configurazione indicherà gli indirizzi di rete e i subrange entro i quali i record A saranno automaticamente assegnati.
Gli amministartori privilegiati (admin_type = “primary”) avranno comunque la facoltà di scegliere liberamente l’indirizzo IP, anche fuori dai range pre-definiti, gli amministartori non privilegiati (admin_type = “secondary”) avranno la facoltà di

scegliere liberamente la LAN tra quelle loro assegnate e l'indirizzo IP all'interno dei rispettivi range.
Sia per utenti privilegiati che non privilegiati, nel caso non venga immesso alcun valore, il sistema provvederà ad assegnare automaticamente il primo indirizzo libero del range selezionato, o alternativamente il primo indirizzo libero del range a partire da un valore selezionato mediante l'apposizione del carattere +.

Nomi e funzione dei file di configurazione:

DNSMAN_<username>-<domain_id>.CNF
file di configurazione per il primo amministratore privilegiato di un dominio (esclusi domini in .in-addr.arpa)).

DNSMAN_<username>-000.CNF
file di configurazione per i successivi amministratori privilegiati e non privilegiati di un dominio (esclusi domini in .in-addr.arpa)

DNSMAN_<username>-IP0.CNF o DNSMAN_<username>-IP1.CNF
file di configurazione per l'amministratore privilegiato di un dominio in .in-addr.arpa. (Con IP0 l'utente sarà username sarà accessibile anche da amministratori con proxy access = %all (vedi avanti). IP1 disabilita questa possibilità).

IPxxxyyyzzz_000-000.CNF
file per la definizione dello schema di sezionamento della LAN di indirizzo xxx.yyy.zzz e per i relativi netmask, router di default e lista dei name server. Ne può esistere uno solo per ciascuna LAN.

ADMIN_<username>-CONFIG.DAT
Questo file, opzionale, associa all'utente HTTP <username> una lista di utenti e rispettivi domini per il loro accesso via proxy, cioe' senza bisogno dell'autenticazione HTTP e quindi senza conoscere la password dell'utente acceduto.
<username> può essere un utente associato ad un file di configurazione di un dominio (in tal caso comparirà la URL "domains lists" in alto al centro) o un utente appositamente creato per l'accesso proxy di altri utenti (in tal caso, dopo l'autenticazione HTTP, verrà subito presentata la lista cliccabile dei domini gestiti).
Il formato del file è del tipo:
<username> <nomedominio>
o
%all

%all abilita l'accesso a tutti i domini definiti in DnsManager.

Nel file di nome aaa_config_file_example.txt si possono trovare alcune spiegazioni sul signficato dei parametri.
Utili indicazioni si trovano anche nei file contenuti nella directory /www_service/wwwdnsman/doc.

Attivazione di un nuovo dominio

L'attivazione di un nuovo dominio prevede diversi passi che non sono controllabili da interfaccia web data la loro scarsa frequenza ed una certa criticità di alcune delle operazioni necessarie.
Vi sono però due utility che rendono l'attivazione estramente semplice e rapida.
Queste sono rappresentate dai comandi DNSMANAGER_CONFIG e DNSMANAGER_ZONE_LOAD.
Entrambi i comandi effettuano operazioni che potrebbero essere fatte manualmente, editando gli opportuni file.
DNSMANAGER_CONFIG, permette la definizione di un nuovo dominio generando i file di configurazione per l'amministratore privilegiato sia del dominio stesso che dei domini necessari per la risoluzione inversa delle LAN ad esso associate (domini ...x.in-addr.arpa). Le configurazioni per la risoluzione inversa vengono attivate anche nel caso il nostro server non sia master per esse.
DNSMANAGER_CONFIG inoltre inzializza i database necessari al dominio, crea il file di zona contenente il solo record SOA nella directory indetificata dal nome insm_dnsman_zones_dir e genera un file contenente le istruzioni per il completamento della configurazione del dominio.

Una volta configurato, il dominio è pronto per l'utilizzo.
Nel caso si disponga di un "vecchio" file di zona, i database del dominio, potranno essere caricati con il comando DNSMANAGER_ZONE_LOAD.
Tale comando attiva una utility che in input riceve il vecchio file di zona, più altri parametri come il nome del nuovo dominio, il nome utente dell'amministratore privilegiato, il gruppo (scelto tra quelli definiti nel file di configurazione dell'amministratore privilegiato prescelto), etc... ed in output produce, in un area temporanea /www_service/wwwdnsman/work, i nuovi database caricati.
E' consigliabile un controllo mediante editor, SENZA SALVARE e quindi, se tutto sembra ok, la loro copia nella directory di servizio /www_service/wwwdnsman/data
IMPORTANTE:

- DNSMANAGER_ZONE_LOAD disabilita automaticamente l'accesso web a DnsManager.
  Questo potrà essere riattivato, dopo la copia dei nuovi database nella directory di servizio, con il comando: DNSMANAGER_ENABLE
  (Esiste anche il corrispondente comando per la disabilitazione: dnsmanager_disable).
  Durante questa fase è infatti importante che non vengano apportate modifiche ai database correnti, che sarebbero poi sovrascritti da quelli nuovi generati dopo il caricamento.

- I database generati o modificati da DNSMANAGER_ZONE_LOAD si trovano nella directory /www_service/wwwdnsman/work ed hanno l'estensione del nome file uguale a WORK. Questi divengono i database correnti solo se si copiano (o rinominano) nella directory /www_service/wwwdnsman/data.
  Per fare ciò, dopo essersi posizionati in /www_sevice/wwwdnsman/work è' sufficiente il comando
  copy/log (rename/log) *.work [-.data]*.dat
  Se l'accesso a DnsManager venisse riabilitato prima di aver effettuato la copia dei nuovi database in [.data] questi NON possono più essere copiati perchè inconsistenti con eventuali modifiche fatte nel frattempo.
  In tal caso sarà sufficiente ripetere l'operazione di zone_load.
- ZONE_LOAD può essere utilizzato liberamente, anche solo per test.
  Se non vengono copiati i nuovi database in /www_service/wwwdnsman/data l'esecuzione di zone_load NON produce alcun effetto.

Come precedentemente descritto, l'operazione di migrazione di uno o più domini verso il loro nuovo nome può essere amministrata e delegata efficientemente attraverso il controllo via web di DnsManager. Alternativamente è possibile effettuare la migrazione durante la fase di caricamento dei domini nel sistema DnsManager.
Esempio:
supponiamo che i domini alfa.mi.cnr.it (con hosts - record A - definiti sulla LAN 192.49.208) e beta.mi.cnr.it (con hosts – recod A – definiti sulla LAN 192.49.209) debbano migrare nel nuovo dominio alef.cnr.it.
Ecco come procedere in un possibile esempio, in cui si scelga di creare due gruppi, presumibilmente per offrire l'amministrazione separata agli ex amministratori di alfa.mi.cnr.it e beta.mi.cnr.it):

1. mediante DNSMANAGER_CONFIG configurare il dominio alef.cnr.it con due nomi gruppi (alealf e alebet) associati rispettivamente alle LAN 192.49.208 e 192.49.209.
   Notare che sarà necessario scegliere un domain_id (3 caratteri. Scegliamo: ale) che costituiranno il prefisso del nome dei gruppi la cui lunghezza è limitata a 6 caratteri (alealf e alebet).
   Come username scegliamo: alef
   L'amministratore (alef) creato sarà di tipo privilegiato ed avrà il controllo su entrambi i gruppi/LAN. Manualmente creeremo i due amministratori non privilegiati, copiando, per ciascuno di essi, il file dell'utente privilegiato in un nuovo file (con nome definito secondo le regole viste precedentemente). Si modifica quindi il file per rimuovere la LAN e il rispettivo gruppo ed assegnare al parametro admin_type il valore "secondary".
2. editare il vecchio file zona del dominio alfa.mi.cnr.it, per togliere tutta la parte relativa al record SOA.
3. Eseguire DNSMANAGER_ZONE_LOAD rispondendo alle varie domande.

In particolare:
- file di zona in input: quello modificato al punto 2 (alfa.mi.cnr.it)
- nome dominio: alef.cnr.it
- username: alef
- gruppo: alealf

Tutti i record, inclusi i record PTR, saranno caricati nei rispettivi database (zone: alef.cnr.it, 208.49.192.in-addr.arpa, 209.49.192.in-addr.arpa).

4. Verificare i nuovi database nella directory /www_service/wwwdnsman/work e, se ok, copiarli/rinominarli in /www_service/wwwdnsman/data cambiando la loro estensione da .WORK a .DAT.
5. ripetere la sequenza, per il dominio beta.mi.cnr.it, a partire dal punto 2 sino al punto 4 (incluso), facendo attenzione a cambiare le risposte in relazione ai diversi parametri necessari per il dominio beta.mi.cnr.it (dominio: alef.cnr.it, username: alef, nome gruppo: alebet).
   Nota: durante questo secondo caricamento potrebbero essere generati dei "warning" derivanti da conflitto di nomi (esempio: due PC che avevano lo stesso nome nei domini alba.mi.cnr.it e beta.mi.cnr.it). Per i record non caricati a causa di un warning dovremo procedere manualmente attraverso l'interfaccia web.
6. Al termine dell'operazione di caricamento di beta.mi.cnr.it (incluso punto 4) potremo riabilitare l'accesso a DnsManager (DNSMANAGER_ENABLE).
7. A questo punto sarà importante accedere ogni singolo dominio, alef.cnr.it, 209.49.192.in-addr.arpa e 208.49.192.in-addr.arpa per modificare e/o aggiungere i record NS, MX, etc... (Nel caso delle risoluzioni inverse i record NS non saranno sicuramente presenti).
   Ricordo che non esiste la funzione di modifica, che può essere assolta mediante la rimozione e la successiva ridefinizione di un record, tenendo presente che fino a quando non si clicca su Zone Upload ogni modifica è limitata ai database, e non influisce sul file di zona.

Note: ZONE_LOAD non provvede a fare uno ZONE UPDATE.
Il pulsante ZONE UPDATE compare solo dopo una modifica ai database effettuata da interfaccia web.
Per verificare il risultato di una operazione di ZONE UPLOAD (pulsante su pagina web) si possono ispezionare direttamente i file di testo presenti nella directory INSM_DNSMAN_ZONES_DIR.

Rimozione di un dominio

La rimozione di un dominio avviene tramite il comando:
DNSMANAGER_ZONE_UNLOAD.

Descrizione dei file di configurazione

I file di configurazione, con esclusione del tipo ADMIN_<username>-CONFIG.DAT, contengono una lista di parametri definiti secondo la seguente sintassi

nome-parametro = “valore-parametro”

Una riga che a collona 1 ha il carattere ! è considerata riga di commento.
Una riga che a colonna 1 ha il carattere < indica l’inclusione di un altro file. In questo caso il carattere < deve essere immeditamente seguito da una valida “file specification” del file da includere.
Esempio:
<www_service:[wwwdnsman.config]common_example.include

Notare che ciascun parametro deve essere definito su una stessa riga ad eccezione del parametro “grouplist” che può estendersi su più righe.

Alcuni parametri possono essere omessi.
Per una descrizione dei parametri e del loro significato si rimanda all’allegato A: “Release notes”.

Appendice A

Release notes

```
==========
08-10-2003
Nuovo parametro: IP_release_delay
Il parametro (opzionale) stabilisce un ritardo nel rilascio di un indirizzo IP
in seguito alla cancellazione di un record A e del corrispondente record PTR.
L'indirizzo IP non potra' essere utilizzato nell'assegnazione
di un nuovo record in un gruppo diverso da quello a cui apparteneva, per
l'intervallo di tempo specificato nel parametro IP_release_delay.
Il parametro risulta utile quando, in presenza di piu' utenti e gruppi che
concorrono su uno stesso range di indirizzi IP, uno di questi rimuove
un record A per inserirlo con un nuovo nome e stesso indirizzo IP.
Se l'indirizzo IP del record cancellato venisse immediatamente rilasciato,
un altro utente, concorrente sullo stesso range IP, lo potrebbe allocare
per una sua registrazione.
La sintassi del parametro e' la seguente:

IP_release_delay = "d-hh:mm:ss"


==========
02-10-2003
Nuovo parametro:  privileges
Con il nuovo parametro privileges e' possibile limitare le azioni
di un utente, primario o secondario.
Al parametro possono essere assegnate una o piu' keyword, separate da virgola,
il cui valore e significato e' il seguente:

CREATE - abilita le funzioni di creazione record.
DELETE - abilita le funzioni di rimozione record.
READ - abilita le funzioni di visualizzazione dei record.

Esempio di parametro:

privileges = "READ,DELETE"
Che assegna all'utente la possibilità di visualizzare e rimuovere i
record del proprio gruppo, escludendo la possibilità di aggiungere nuovi record
(CREATE).
Nota: l'ordine dei valori e' irrilevante.

==========
17-09-2003.3
File di configurazione.
Nuovo formato del parametro grouplist.
Il parametro grouplist puo' essere spezzato su piu' righe.
Esempio:

grouplist = "istcvs##Creative Virtual Systems"
grouplist = "istdc##Dependable Computing,istha##Domotics"

Ogni riga puo' contenere una o piu' definizioni di gruppo separate da virgola.

==========
17-09-2003.2
Inclusione di file esterni.
Una stringa che a colonna 1, ha il carattere < indica il nome di
un file di parametri che il sistema leggera'.
```

Esempio:

```
domain = "80.48.146.in-addr.arpa."
ipnet = "146.48.80"
<www_service:[wwwdnsman.config]gruppi_isti.inc
grouplist = "istAAA,istBBB,istCCC,istDDD,istEEE,istFFF,istGGG,istHHH,cnuOLD"
```

Nota: il file incluso, non puo' a suo volta includere un altro file.

==========
17-09-2003.1
Per determinare la porzione di un indirizzo IP che rappresenta l'indirizzo di rete,
DnsManager utilizza il parametro subnetmask contenuto nel file di configurazione di tipo:
IPxyz_000-000.CNF;
Dato un indirizzo IP nella forma x.y.z.k, il file di descrizione della rete viene cercato per tentativi a
partire dal nome piu' esteso, composto dai primi tre byte dell'indirizzo IP (IPxyz_000-000.CNF), sino
a quello composto con il solo primo byte dell'indirizzo IP (IPx_000-000.CNF).

Attualmente questo meccanismo funziona solo per la classica separazione tra rete e host
sul confine del byte (255.0.0.0, 255.255.0.0, 255.255.255.0).
Per esempio:
una LAN con netmask di 255.255.248.0 sarà considerata come 255.255.255.0 ai fini della selezione del nome
di file sopra descritta.
Così pure una LAN con netmask 255.255.255.248 sarà approssimata a 255.255.255.0.
La definzione dei range che però è possibile fare con altri parametri di configurazione consentirà
comunque una completa e corretta gestione di LAN definite mediante valori di netmask basati sul CIDR.

Classe della LAN e generazione automatica degli indirizzi.

La generazione automatica degli indirizzi avviene solo
per le LAN il cui netmask è approssimato al valore 255.255.255.0 secondo
il meccanismo precedentemente descritto.

Classe della LAN e controllo dei range.

Il controllo dei range avviene solo per le LAN il cui netmask è approssimato al valore 255.255.255.0 secondo il meccanismo precedentemente descritto.

Nuovo parametro

only_manual

1 = viene disabilitata la visualizzazione della lista degli indirizzi LAN predefiniti
    per l'utente con il parametro ipnetlist. L'indirizzo IP dovra' essere inserito per
    esteso (net+host invece che solo host con net preselezionabile da menù).
0 = opposto di 1

==========
25-08-2003
Possibilita' di predefinire un prefisso per gli hostname inseriti
da un determinato utente di amministrazione (primario o secondario).

```
 Nuovo parametro di configurazione per i file di tipo:
  DNSMAN_<username>-<domain_id>.CNF
 Nome del nuovo parametro
  host_prefix
Puo' contenere uno o piu' prefissi separati da virgola, che saranno presentati
sulla pagina web per la scelta (* obbligatoria *) da parte dell'amministratore.
Esempio:
host_prefix = "pc-,mac-,nb-,wks-,h-,p-,m-"

Questa opzione e' per esempio utile per delegare ad un amministratore
secondario (o primario) la possibilita' di effettuare liberamente
registrazioni nel dns, impedendogli pero' di utilizzare nomi che potrebbero
risultare riservabili per specifici scopi (Esempio: www2, smtp2, dns,
namserver, dhcp, etc...).
L'amministratore e' infatti costretto a scegliere uno dei prefissi
proposti.

==========
27-05-2003
Selezione automatica del primo IP libero piu' flessibile:
- introdotta la possibilita' di specificare l'indirizzo IP
  di partenza per la ricerca del primo indirizzo IP libero all'interno
  del range selezionato.
  Per specificare l'indirizzo di partenza inserire nel campo "Ip node address:"
  il valore seguito da "+".
  La ricerca iniziera' da tale valore e terminera' al primo indirizzo libero
  o al limite massimo specificato nel IP range selezionato.

Esempio: supponendo di selezionare il range predefinito 5-254, per
una determinata LAN. Inserendo come "Ip node address:"  il valore 80+
verra' selezionato il primo IP libero a partire da 80 (incluso),
invece che a partire da 5.

==========
20-05-2003.2
Possibilita' di inserire una descrizione di gruppo.

Nuovo formato del parametro grouplist per inserire la descrizione di
gruppo.
grouplist ="groupname1#maxnodes1#desc-grp1,groupname2#maxnodes2#desc-grp2,...
             ..,groupnamen#maxnodesn#desc-grpn"

La descrizione comparira' nelle tendine a menu' di selezione dei gruppi,
racchiusa tra parentesi.
(Non comparira' nel listing dei record).

Esempio:
grouplist ="istAAA#20#Laboratorio Immagini,istBBB##Laboratorio Reti"
che significa:
definizione di gruppo istAAA con limite massimo di assegnazione
di 20 indirizzi indipendentemente dal/dai range IP in cui essi saranno
assegnati e relativa descrizione: "Laboratorio Immagini"
definizione di gruppo istBBB senza alcun limite massimo al numero
di indirizzi IP assegnabili (notare il doppio ##) e relativa
descrizione: "Laboratorio Reti"

==========
20-05-2003.1
Modificata funzionalita' bind_group_ip

Per default la selezione di un gruppo è indipendente da quella di un range IP.
Le due selezioni sono gestite da due diversi menù a tendina.
Questo parametro consente di modificare il comportamento di default permettendo
```

```
di associare a ciascun range IP un determinato gruppo, riducendo la
selezione gruppo/IP ad un unico menù a tendina.

bind_group_ip = "1"
vengono associati gli n gruppi definiti in grouplist
con le n definizioni di IP range in ipnetlist.
Possibile codice di errore:
 se il numero di gruppi in grouplist e' inferiore al numero di definizioni
 di IP range in ipnetlist comparira', in fondo alla lista, l'errore
 -- ERROR LGN --
 dove:
 LGN = Low Number of Groups

Alternativa al caso precente.

Nel caso si desideri una diversa associazione tra gruppi e IP range, si possono
esplicitamente inserire i nomi gruppi in bind_group_ip.
Esempio:

ipnetlist = "ISTI-80#146.48.80#6-255#Y,ISTI-81#146.48.81#2-254#Y,
                 ISTI-82#146.48.82#2-254#Y,ISTI-83#146.48.83#2-254#Y"
corrisponde alla definzione di 4 IP range (linea spezzata per visualizzazione)

grouplist = "istAAA,istBBB"

corrisponde alla definizione di 2 soli gruppi

con la seguente definizione del parametro bind_group_ip
bind_group_ip = "istAAA,istAAA,istBBB,istAAA"
in pratica si attiva la funzionalita' di bind fra gruppi e IP range,
associando nel rispettivo ordine il primo gruppo (presente in bind_group_ip)
con la prima definzione di IP range in ipnetlist, secondo gruppo con la
seconda definizione di IP range e cosi' via....

Possibile codice di errore:
 se il numero di gruppi in grouplist e' inferiore al numero di definizioni
 di IP range in ipnetlist o un gruppo specificato in bind_group_ip non
 compare nella lista grouplist, nel menu' a tendina comparira' l'errore:
   -- ERROR GNF --
 dove:
 GNF = Group Not Found

==========
22-04-2003.5
Definizione del formato pagine via Cascading Style Sheet (CSS).
Occorre creare la directory www_service:[style] con owner uguale a WWW
Comando:
 create/direc WWW_SERVICE:[STYLE]/owner=WWW

e copiarvi il file: insm.css

==========
22-04-2003.4
Introdotta il nuovo parametro bind_group_ip (file dei parametri).
Questa funziona e' utile quando si hanno piu' raggruppamenti LAN
per uno stesso dominio ed ognuno di essi e' associato ad uno specifico gruppo.
I relativi parametri sono:
ipnetlist che contiene la lista dei raggruppamenti IP
grouplist che contiene la lista dei gruppi

bind_group_ip = "1" il gruppo e' unito alla definizione del range IP
bind_group_ip = "0" o parametro assente: la scelta del gruppo e' indipendente
                    dalla scelta del range IP.
```

```
==========
22-04-2003.2
Funzione Modify Host e parametro modify_group.
Nuova funzione per modifica dei dati anagrafici e del TTL di un
record. La funzione e' attivabile dall'output di "List Records"
selezionando il record da modificare e quindi il pulsante "Modify Host"

 Per attivare anche la modifica del gruppo, definire il parametro (nel
 file dei parametri):
modify_group = "1"

==========
22-04-2003.1
NOTA BENE: cambio nella struttura directory con aggiunta
 directory WWW_SERVICE:[WWWDNSMAN.LOCK]
E' sufficiente dare, dallo user SYSTEM, il seguente comando:

 create/direc WWW_SERVICE:[WWWDNSMAN.LOCK]

==========
15-01-2003
Possibilita' di controllare il numero massimo di nodi (indirizzi IP)
assegnabili in un determinato gruppo da un determinato utente.
Il nuovo formato del parametro grouplist e' il seguente:

grouplist ="groupname1#maxnodes1,groupname2#maxnodes2,...,groupnamen#maxnodesn"

#maxnodes1 e' opzionale per cui il vecchio formato e' ancora valido.
L'assenza di #maxnodesn corrisponde a nessun limite al numero massimo di
nodi registrabili, salvo l'esaurimento dei range IP assegnati.

==========
xx-11-2002
Logging delle attivita'.
Selezione Logs dal menù principale.
Sono visualizzabili i logs relativi agli ultimi 5 mesi, ma sono
comunque mantenuti senza alcun limite di tempo anche quelli antecedenti.

==========
29-07-2002
Modulo di HELP per la visualizzazione e stampa dei parametri
di configurazione di un nodo.
Il modulo è generato in conseguenza all'inserimento di un nuovo record A.
Opzione valida solo per amministratori secondari.
Richiede l'inserzione dei seguenti parametri nel file:
IPxxx.yyy.zzz_XXX-000.CNF

subnetmask = "<netmask>"
router = "<router ip address>"
nameserver = "<name server1 ip addr>,<name server2 ip addr>,...."

Esempio:
subnetmask = "255.255.255.0"
router = "150.145.35.1"
nameserver = "150.145.35.2, 150.145.35.3"

==========
18-03-2002
Aggiunta definizione logico dnsmanager_batch_queue
per coda batch di esecuzione del job di reload del name server.
La definizione va inserita nel file sylogicals.com
in modo che venga effettuata ad ogni reboot del sistema
```

```
Esempio:
define/system dnsmanager_batch_queue "sys$batch"

==========
18-03-2002
Modifica per consentire inserzione di record
MX che puntano al nome stesso.
(esempio: mail.xxx.cnr.it. IN MX 10 mail.xxx.cnr.it. )

==========
11-03-2002
Aggiunta gestione delle zone per dimini appartenenti a in-addr.arpa.
L'attivazione si ottiene creando un normale file di configurazione che
deve avere le seguenti caratteristiche:
DNSMAN_<username>-IP0.CNF
                  ^^^    questi 3 caratteri *DEVONO* essere IP0 o IP1
Il contenuto del file e' come segue (esempio per rete 146.48.65)
> Attenzione: questo file differisce da quelli di dominio
> in quanto il parametro ipnetlist NON e' presente e
> al suo posto e' presente il parametro ipnet.
  ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
domain = "65.48.146.in-addr.arpa"
ipnet = "146.48.65"
grouplist = "ipiat,iat1,iat2"
admin_type = "primary"
update= "yes"
defttl = "86400"
defuserttl = "180"
maxuserttl = "0"
zonec = "francesco.gennai@iat.cnr.it"
pmdf_access_control = "1" ! vale anche per file di definzione gestione IN-ADDR

Deve esistere il file
IP146$48$65_000-000.CNF;
            ^^^ ^^^   questi caratteri non hanno alcun significato
                      per cui si consiglia la sequenza 000-000
                      Imortante _ (underscore) prima della sequenza.

I file contiene i parametri (i valori sono riportati per esempio):

netrange = "SERVERS#5-30,HOSTS#31-60,AAA#61-80,BBB#81-90"
            netrange descrive l'organizzazione dall'intera rete in sottoparti,
secondo
            le proprie esigenze.
subnetmask = "255.255.248.0"
router = "146.48.80.1"
nameserver = "146.48.80.3, 146.48.80.4, 146.48.127.2"


==========
10-03-2002
Attivata gestione "DNS configuration check" tramite il database
CHANGES_DB.DAT.
( Vedi note nel file: WWW_SERVICE:[WWWDNSMAN.DOC]NOTE-CORSO-DNSMANAGER.TXT )

==========
08-03-2002
Aggiunta definizione logico dnsmanager_zones_dir
per directory file di zona letti dal BIND.
La definizione va inserita nel file sylogicals.com
in modo che venga effettuata ad ogni reboot del sistema
Esempio:
```

```
define/system dnsmanager_zones_dir "multinet:"

==========
07-03-2002
Modifica per impedire ad un amministratore secondario di assegnare
piu' indirizzi IP ad uno stesso hostname.
Se l'amministratore e' secondario si ottine l'errore:
The name xxx.yyy.cnr.it. is already assigned. Please choose another name.
Se l'amministratore e' primario viene invece proposta una pagina web
con la lista dei record coinvolti (per esempio: piu' record A
per lo stesso nome) per la conferma da parte dell'amministratore.
Eventualmente possiamo condizionare questo comportamento con un opportuno
parametro di configurazione.
*
Modificata generazione messaggio di succeso dopo aggiunta record A.
Il messaggio e' diverso in base al tipo di amministratore.
Se primario, viene indicata l'aggiunta del record A e del record PTR.
Se secondario vengono riportati su due righe diverse:
Ths assigned IP address is: xxxx
The name is: yyyyy

==========
06-03-2002
Aggiunta selezione per SMTP server access control.
Consente abilitazione/disabilitazione dell'accesso al server SMTP da parte del
nodo con un determinato indirizzo IP.
Il PMDF deve essere opportunamente configurato.
Inoltre c'e' la possibilta' di attivare configurazione PMDF per inibizione
*totale* invio messaggi da quel client oppure flaggare il messaggio
con riga nell'header, come messaggio proveniente da client NON
autenticato/autorizzato.
Disabilitazione:
Il controllo si disabilita medinate parametro:
pmdf_access_control = "0"

==========
19-12-2001

Parametri per il file di configurazione di un utente amministratore di dominio.

domain = "xx.ff.cnr.it"  ! "n.m.t.in-addr.arpa"   dominio gestito
ipnetlist = "net 1#146.48.65#1-255#Y,net 2#146.48.66#30-50#N" ! formati:
                                    - singolo indirizzo 146.48.65#56
                                    - range di indirizzi 146.48.65#30-40
                                    - net 1, net 2... sono commenti di
                                      descrizione
                                    Attenzione: nei commenti di
                                    descrizione possono comparire
                                    solo i caratteri: a..z,A..Z,0..9,:,!
                                    Sono certamente eslusi la virgola e
                                    le parentesi: (), <>, []
                                                #Y significa che la
                                                zona della risol. inversa
                                                è gestita dal nostro server
                                                e quindi dovrà essere
                                                effettuata una opportuna
                                                operazione di UPDATE
                                                quando richiesto.
                                                #N significa che la
                                                zona è assegnata ad
                                                altro server.
grouplist = "iat1,iat2,iat3"
```

```
admin_type = "primary|secondary" ! con primary sono abilitate le funzioni
advanced
                                  presentate sull'interfaccia web
update=yes|no  ! nel caso di config relativa a dominio (es.:
                 risoluzione inversa) gestito
                 dal nostro stesso server, sarà YES e serve a far comparire
                 il pulsante "UPDATE", altrimenti sarà NO (nessun pulsante
                 "UPDATE" sarà visibile)
                 Nel caso di domainIP sembra ridondante rispetto al #Y e #N
                 specificati in IPrange. E' utile comunque per altri casi,
                 dove per esempio un amministratore (secondario) può modificare
                 ma non fare l'update.
defttl = "86400"

defuserttl = "180"  ! Per questi due parametri vedi descrizione in file di
maxuserttl = "0"   ! config per MailboxMaanager
```

Nota:
Il file di zona per la risoluzione inversa sarà creato anche nel caso che la gestione non sia assegnata a DnsManager. Nel caso cioè che la zona per la risoluzione inversa della LAN si su altro name server.
Sicuramente anche in questo caso sarà interessante/importante gestire dei range, presumibilmente assegnati all'organizzazione che utilizza DnsManager.
Il file prodotto potrebbe essere comunque utilizzato dall'organizzazione remota per aggiornare la zona sul proprio server.