DNS Management Requirements

Wes Hardaker and the DCOMA team

July 28, 2008

About DCOMA

Goals

- High Level Requirements Only
  - **What** is needed, **not how** to do it
  - No bias toward one solution space

Work History

- Jul 2007: Formed in Chicago DNSOP meeting
- Dec 2007: Met In Vancouver
- Mar 2008: Met in Philadelphia
- Discussion on the DCOMA mailing list
- May 2008: Agreement on final document

Results

A Requirements Document

- draft-hardaker-dnsop**S**-name-server-management-reqs-03.txt
- "the requirements of a management system for DNS name servers"
- "a shopping list of needed features"

Consensus!

- Results were more agreed upon than not!
- Lots of brain storming; little argument

Notes

- No solution timeline implied
  - requirements don't prohibit a slow solution deployment
  - e.g. monitoring first, then control, then configuration

Presentation Style

Presentation contents

- Each requirement is fully described in the text
- Each requirement is barely described in the presentation

Coloring Conventions

Section	Level	Summary
1.1.2	MUST	be able to do foo
1.1.2	SHOULD	be able to bar (bof)
1.1.2	MAY	want to do baz

Deployment Scenario Support

Deployment Requirements

Section	Level	Summary
2.1.1	MUST	Support large and small zones (e.g. TLDs to 1-10 record zones)
2.1.2	MAY	Support name server discovery
2.1.3	MUST	Support static and highly dynamic zones

Appendix A: Extra Scenarios

- Non standard zones (e.g. local TLDs)
- Redundancy sharing and cooperative agreements

Solution Architecture Requirements

Protocol Requirements

Section	Level	Summary
2.1.4	SHOULD	Use a minimal set of protocols in the solution
2.1.5	MUST	Supply a common data model (regardless of protocol(s) used)
2.1.6	MUST	Minimize impact to the existing service

Server Types

Section	Level	Summary
2.2	SHOULD	Support Master, Slave and Recursive Servers
-	MAY	Out of scope: Stub Resolvers

Management Concept Breakdown

Management Operations Considered

- Control
- Configuration
- Monitoring
- Alarm and Events

Control Requirements

Control Requirements

Section	Level	Summary
3.1	MUST	Support basic service control operations
3.1.1	SHOULD	Support the minimal operations below
3.1.2	SHOULD	Support asynchronous status notifications

Needed Control Operations

- Starting the name server
- Reloading the service configuration
- Reloading zone data
- Restarting the name server
- Stopping the name server

Zone Data Configuration

Zone Data

Section	Level	Summary
3.2.1	SHOULD	Modify Served Zone list (add/modify/delete) DDNS is a perfectly acceptable solution for this But must minimally create an SOA for DDNS to work
3.2.2	SHOULD	Be able to manage a list of DNSSEC Trust Anchors
3.2.2	SHOULD	Be able to manage security expectations (policies)
3.2.4	SHOULD	Be able to manage TSIG keys (add/modify/delete)
3.2.5	SHOULD	Be able to manage DNS protocol authorization (DDNS, recursion, ACL lists, ...)

Monitoring Requirements

Monitoring Requirements

Section	Level	Summary
3.3	MUST	be able to monitor the health of a name server

Example "Nice to Have" Monitoring Tasks

- Number of requests, responses sent
- Performance counters and latency statistics
- Server status ("serving", "starting", "shutting down", ...)
- Access control violations
- List of Zones being served
- Top 10 clients requesting data

Alarm and Events

Alarm and Event Requirements

Section	Level	Summary
3.4	SHOULD	Support delivery of alarm conditions

Example helpful alarms

- Server status change
- Resource exhaustion
- Authorization violation
- A "lonely warning"
  - The server is not receiving any traffic

Security Requirements

Security Requirements

Section	Level	Summary
4.1	MUST	Support mutual authentication
		Doesn't prohibit shared keying (eg, TSIG based)
		Simple implies both sides must verifiable
4.2	MUST	Provide Integrity protection
4.3	MUST	Provide Confidentiality (encryption)
4.4	SHOULD	Provide fine-grained authorization
4.5	MUST	Minimize security risks introduces
		All new technology adds risk; we need to minimize it

Extensibility

Solution needs to be extensible

Section	Level	Summary
5.1	MUST	Be flexible to accommodate future needs
5.1.1	MUST	Allow Vendor Extensions
5.1.2	MUST	Provide extension identification
		Must be able to determine what's an extension
5.1.3	MUST	Protect against name-space collision

Next Steps

Ready to turn over

- Does DNSOP want it?
- Where should follow-on standards work be done?

Questions

- ????