HiRISE and PIRL

Hirise.lpl.arizona.edu

XMDNS System Proposal

1541E University Blvd Tucson, AZ 85721
E-Mail: sys@pirl.lpl.arizona.edu

XMDNS Proposal Introduction

The PIRL/HiRISE System group is submitting this proposal for extending the Lunar and Planetary Laboratory DNS system to include complete support for the DNS protocol. The proposed XMDNS system not only supports the full complement of DNS record types but also adds many other features to build a complete DNS management system. PIRL and HiRISE have an immediate need for many of these currently unsupported DNS features and in some cases have been using temporary workarounds to be able to use these features.

Quick summary of DNS

At the core DNS is a system of mapping IP addresses to human readable names. For example, mapping the name Arizona.edu to the IPv4 address 128.196.250.233 and mapping the IPv6 address of 2001:4860:b002::68 to ipv6.l.google.com. The benefit of this mapping is that users do not need to remember IP addresses.

DNS records are published to the world using an Authoritative DNS server. Each group or organization has a set of DNS servers that are Authoritative that will answer requests for each domain zone that is hosted. When anyone in the world requests a record for example.com the ultimate authority for that record lies with the Authoritative servers that organization publishes to the world.

Current system status

A split type of system that allows for the LDAP DNS system and the XMDNS system to run side by side has existed for over a year. During this time the XMDNS system has been tested quite thoroughly and proven to be an excellent management tool.

HiRISE has been using the XMDNS system while LPL CCS has been using the LDAP DNS system. The limitation of this arrangement, aside from duplication of data and synchronization issues, is that the XMDNS system is not authoritative. LPL

CCS must apply all changes that are to be published globally to the LDAP DNS scheme.

Limitations of the current system

The current LPL DNS scheme is limited in functionality and does not support the complete DNS protocol. The primary limiting factor is the LDAP schema, which is used for the backing store of the records.

The current LDAP based DNS system uses command line scripts which process user input into a LDAP entry. Each DNS server then automatically pulls this information from LDAP using a locally stored username/password, which may be a security issue. The changes are activated via an rndc reload that can be automated or manual. Using an out of band 'Test' server it is possible for the operator to check the changes before reloading the production servers with the latest changes. Verification with the test server is manual and optional.

The LDAP schema does not support any of the following record types:

TXT records that are used for Sender Policy Framework, DomainKeys and Opportunistic Encryption for security. This record type is described in RFC 1035.

SPF records that are used for Sender Policy Framework for fighting SPAM. This record type is described in RFC 4408

AAAA records that are used for publishing IPv6 records. This record type is described in RFC 3596.

Multiple IP addresses per A record. Multiple addresses per A record are commonly used for Round Robin load balancing for many types of services. This record feature is described in RFC 1035

SRV records that are used for Kerberos and VOIP as well as other services. This record type is described in RFC 2782.

DNSKEY records that are used for DNSSEC. This record type is described in RFC 3755.

AFSDB records that are used for setting up and AFS network. This record type is described in RFC 1183.

DNS views (or Split DNS) that are needed for Kerberos to support a multi networked environment.

In addition to the unsupported record types the current DNS system has these other problems:

Indirect bind file creation that requires a separate out of band DNS server to manually test the updated records validity. This takes time and is still subject to human error due to the manual nature and can be bypassed completely.

Validity checks of the Bind configuration files can only be conducted after the updates are committed to the repository and pulled down to a DNS server. This can lead to errors existing in the production LDAP DNS database store that could possibly be pulled down to the DNS servers before the error is detected.

There is no support for version tracking and roll back functionality in case of an error. The user making a change manually date stamps and initials the entry. In case of an error the records must be manually searched and edited to revert to the pre-error change.

The current DNS system offers no access for PIRL or HiRISE staff to make changes or updates to the system. All changes that need to be seen globally must go through LPL CCS. PIRL and HiRISE have a legitimate need to manage and change public records relating to HiRISE and PIRL network space.

XMDNS features

The XMDNS system supports the full complement of DNS records that are mentioned in the previous section. In addition to fully supporting DNS the XMDNS system offers these other features:

XMDNS uses svn for version tracking. This tool allows for saving a complete history of all changes made to the DNS system over time. This very powerful feature allows for reverting back to previous versions in case of an error or observing recent changes to the system.

Along with tracking versions, svn ties the username of the operator making changes to that particular version as well as a description of the changes. This allows other operators to quickly see what changes have been made and who to contact about them if needed. Email notifications of these changes are sent to all operators so that everyone is aware of modifications.

XMDNS uses XML for the data storage format. This allows for using the syntax checking that is built into XML and XSLT to combat any typographical and formatting errors that an operator might make. Typographical errors in DNS changes are common, potentially very destructive and often hard to track down.

The editor for the XMDNS system also adds another layer of error checking for a variety of logical and typographical errors.

The XMDNS system generates the necessary files for Bind before submitting any changes back to the repository for propagation. This allows the operator to review these files for validity before a Bind server receives the changes. Included in the XMDNS system are tools to automate this process.

The Bind DNS servers automatically check for updates to the DNS database and will pull down the updated information on a configurable interval. Using rndc the DNS servers update themselves in a safe manner. Operators do not need to manually ensure than DNS changes have propagated.

By nature the svn repository is replicated to every operator that has checked out a copy. This alone provides backup copies of the repository in case of server failure. In addition to operator copies multiple XMDNS servers can be setup to replicate the data in a master slave relationship.

XMDNS presents an easy way to manage multiple domains and multiple DNS views (Split DNS) of a particular network.

Charts are easy to generate from the XML data to give a visual representation of a network and the hosts that are on that network.

New services and benefits

Here is a sampling of new services or those that will be enhanced with full DNS support available.

IPv6 DNS records will be able to be published. HiRISE is already using IPv6 internally for quite a few services. These services need to be able to be published in DNS to be globally available. The University of Arizona is implementing IPv6 support and currently LPL DNS does not support any IPv6 implementation.

Round robin load balancing allows for using the Barracuda SPAM Firewalls department wide. HiRISE has purchased two Barracuda SPAM Firewalls for mail filtering. These units can be clustered in a redundant manner and support up to 40,000 email messages per hour. Currently these systems cannot be setup in a redundant manner without full DNS support.

Sender Policy Framework is another method for fighting SPAM that relies primarily on DNS and specific record types. SPF will help cut down on false bounce SPAM.

DomainKeys Identified Mail is another method for fighting SPAM that relies on specific DNS record types. DKIM allows for electronic signing of outgoing email. This allows recipients to verify if the email originated from where it claimed. This is typically employed at the mail server level.

The Kerberos protocol can be used for authentication and other security related mechanisms. Mac OS X, Linux and Windows can all make use of Kerberos for secure authentication.

NFSv4 and 4.1 require Kerberos for authentication. NFSv4 has much improved security over NFSv3 that HiRISE is currently forced to use. NFSv4.1 adds Parallel NFS support which can be used to spread out data across multiple NFS servers, among other new features.

DNSSEC is a set of security extensions for use on DNS servers. The recent DNS security hole proves that DNS is a useful target for attackers since it is so very critical to nearly all networked services. Employing DNSSEC is a necessary step to securing a network.

DNS Views (Split DNS) that Kerberos requires in a multi homed network configuration.

Transition outline

Here is an outline for transitioning from the current DNS system to the XMDNS system.

1. One or more XMDNS servers are to be identified and configured.
2. Records must be synchronized between the LDAP DNS system and the XMDNS system ‘master’.
3. Existing and new DNS servers must be modified or setup to use the XMDNS database as the source of their configuration data.
4. Operators must transition to using the new XMDNS server as the DNS management system.

Operational usage

XMDNS uses a menu driven system to add/modify/delete DNS records which helps simplify some of the complexities of DNS including DNS Views and supporting multiple networks and domains.

Legacy style commands are also offered to ease operator transition from the LPL DNS interactions.

For complete information on operational usage please see the User Guide which is available by request or in the existing XMDNS repository.

Remediation

An alternate to upgrading the LDAP DNS system is to leave that system in place under the lpl.arizona.edu domain and control of LPL CCS. HiRISE and PIRL would then obtain a new domain name under Arizona.edu similar to hirise.arizona.edu and pirl.arizona.edu.

These new domain names would be assigned to PIRL and HiRISE Systems. Authoritative DNS servers under HiRISE and PIRL System control would serve the DNS information for these domains. The XMDNS system would be employed to manage these domains and offer the full suite of tools available from DNS.

Definitions

FILL OUT DEFINITIONS, ALPHABATIZE

AFS – A distributed networked file system that is very scalable and secure. Uses Kerberos for authentication.

Authoritative DNS – A DNS server with a complete copy of DNS records for the particular domain it claims to serve.

Barracuda SPAM firewall – An email SPAM and virus filtering solution.

BIND – Berkeley Internet Name Domain a common DNS server for UNIX platforms.

DNS – Domain Name System is a system of mapping IP addresses to human readable names.

DomainKeys (DKIM) – An email authentication system that verifies the DNS domain of an email sender.

IPv4 – Internet Protocol version 4.

IPv6 – Internet Protocol version 6.

Kerberos – A commonly used network authentication protocol.

LDAP – Lightweight Directory Access Protocol.

Opportunistic Encryption – A method allowing for two systems to attempt and setup an encrypted communications channel with no pre-arrangement between the two systems.

RFC1035 - http://tools.ietf.org/html/rfc1035

RFC 1183 - http://tools.ietf.org/html/rfc1183

RFC 1464 – http://tools.ietf.org/html/rfc1464

RFC 2782 - http://tools.ietf.org/html/rfc2782

RFC 3596 - http://tools.ietf.org/html/rfc3596

RFC 3755 - http://tools.ietf.org/html/rfc3755

RFC 4408 - http://tools.ietf.org/html/rfc4408

Round Robin DNS – A method for load balancing across multiple servers for the same or a similar service.

SRV DNS record – A record in DNS used to specify information on available services. RFC 2782 details this record type.

svn (Subversion) – A version control system used to store and maintain current and older copies of data.

TXT DNS record – A record in DNS used to specify human readable text or machine readable data. Specified in RFC 1464

XML – Extensible Markup Language.

XSLT – Extensible Stylesheet Language Transformations.