NETCONF System Management

draft-ietf-netmod-system-mgmt-05
IETF 86, March 2013

Andy Bierman
Martin Bjorklund
March 12, 2013
Agenda

- WGLC Issues
Resolved Issues Since -04

- Boilerplate text for YANG tree diagrams
- RADIUS timeout and attempts leafs should be range 1..max, not 0..max
- iana-timezones I-D expired and needs to be reissued:  
  - draft-ietf-netmod-iana-timezones-00?
- Wikipedia reference for Crypt will be updated
- Change 'ntp-server' identifier to 'server'
- must-stmt for user-authentication-order will be corrected
RADIUS Issues
Jeffrey Lange (2012-11-02)

• Need to identify RADIUS-EAP or not?
  - Add new identity
    identity radius-eap {
      base radius-authentication-type;
    }
  - Add eap-method leaf to radius config
    leaf eap-method {
      when ".../authentication-type = radius-eap";
      mandatory true;
      type ???; (number or name string?)
    }
rounds parameter
Per Hedeland (2013-03-06)

- The "reference implementations" of type 5 and 6 allow for an additional 'rounds' parameter with a value in the range 1000 .. 999999999 (default is 5000), i.e. the "hashed value" can be e.g. "$5$rounds=10000$saltstringsaltst$3xv.VbSHBb41AL9AvLeujZkZRBAwqFMz2.". This is not allowed by the pattern in the typedef - should it be?

- 4) Should there be some text about how a server chooses between the algorithms when hashing a cleartext password (assuming it supports more than one, of course)?
The text could make it clear that there is more to the implementation than the choice of MD5/SHA-256/SHA-512:

OLD:
"The crypt-hash type is used to store passwords using a hash function. This type is implemented in various UNIX systems as the function crypt(3)."

NEW:
"The crypt-hash type is used to store passwords using a hash function. The algorithms for applying the hash function and encoding the result are implemented in various UNIX systems as the function crypt(3)."
location string is useless for automation
Phil Shafer (2013-03-06)

- **country-code**: Two-letter country code
- **postal-code**: Zip code or postal code
- **npa-nxx**: First six digits of phone number (a.c.+exchange)
- **latitude**: Latitude in degree format
- **longitude**: Longitude in degree format
- **altitude**: Feet above (or below) sea level
- **lata**: Long-distance service area
- **vcoord**: Bellcore vertical coordinate
- **hcoord**: Bellcore horizontal coordinate
- **building**: Building name
- **floor**: Floor of the building
- **rack**: Rack number
3.1: Is "name" the DNS name of the device? Can we say that, either here or in the description? "administratively assigned system name" doesn't mean much to the average reader.

3.2: Why have use-ntp? Why not have [system ntp] a presence container?

You list ntp-server, but not peers or boot servers. You are missing authentication keys, source address, version, polling interval constraints (min and max), broadcast server and client info, and multicast client info.

re: enabled: would be good to make a generic means for this, so we don't need to put this knob on every container.

3.3: In JUNOS, we call out the local domain explicitly, distinct from the domain search path. This is similar to the "domain" and "search" fields in BSD's resolv.conf.
3.4: Should RADIUS config be in a distinct module, augmenting this one? Using a feature work, but skey, tacplus, etc need config also. Are we saying that RADIUS is the only modern/needed one?

Passwords without the leading $ are old-school style. Support them?

In the same vein, JUNOS uses $9$ for obfuscating secret data to avoid allowing over-the-shoulder password stealing. It's only obfuscation, but is still useful for secrets that we need in plain text later and cannot use just the hash. Similar with systems that use a single "master password" to encrypt secret data.
Additional Comments (3/3)
Phil Shafer (2013-03-06)

- What is an ssh key's name? Just a user-defined handle? Why not use the complete ssh key as the key?
- Why is ssh key data binary?
- 3.6: Consider making <reboot> a leaf under a single <shutdown> operation, ala the BSD shutdown command.
What is an ssh key's name? Just a user-defined handle? Why not use the complete ssh key as the key?

Why is ssh key data binary?

3.6: Consider making <reboot> a leaf under a single <shutdown> operation, ala the BSD shutdown command.
Under System Identification, should there be some way to identify the system's role or operating mode?

Roles might include if the "system" is a logical-system, stack-member, cluster-member, blade-server, or a blade-server-member.

Operating mode might include if it's configured to run in FIPS-mode or if it's running a variation of code to meet cryptographic export restrictions.

We found a need to have these attributes returned in our proprietary <get-system-information> RPC. Admittedly, some of this could've been learned through the advertisement of a capability, but our "when" expressions needed something to act on. For instance, certain config nodes are disabled or enabled based on the device's role and/or operating-mode.