draft-kwatsen-netconf-zerotouch-00

Zero Touch Provisioning for NETCONF Call Home

Introduction

Zero Touch is a strategy for how to establish a secure network management relationship between a newly delivered network element, configured with just its factory default settings, and the new owner's NMS.

Goals

Security

- MUST <u>implement</u> vs MUST <u>use</u> (RFC 3365)

Flexibility

- Works on SP networks, even if behind a firewall

Ease of Use

- Play-n-play for Installer ("zero" means zero!)

Device Cost

- Mild (COGS + development effort)

Proposal illustrated in following slides

Device State Precondition

```
+--------------------------------+
|           <device>             |
|                                |
|    +----------------------+    |
|    |  <crypto processor>  |    |
|    |                      |    |
|    |  device private key  |    |
|    |  device certificate  |    |
|    +----------------------+    |
|                                |
|  FQDN of vendor's DNS server   |
+--------------------------------+
```

Serial Number

Signed by certificate with chain of trust to Vendor’s well-known CA

Vendor's DNS Server State

```
+-------------------------------------------------+
 |             <vendor's DNS server>               |
 |                                                 |
 |  <sha1-of-device-public-key>.<vendor-zone>      |
 |    - FQDN of NMS to connect to                  |
 |    - flag indicating if SSH or TLS              |
 |    - username NMS will login using              |
 |    - NMS's auth credentials                     |
 |                                                 |
 +-------------------------------------------------+
```

State initialized through a vendor-hosted interface

ZeroTouch Sequence Diagram

```
DEVICE     LOCAL DHCP          LOCAL DNS     VENDOR'S DNS       NMS
  |          SERVER             SERVER      SERVER (DNSSEC)      |
  |             |                  |              |              |
  |------------>|                  |              |              |
  | Lease IP    |                  |              |              |
  |             |                  |              |              |
  |------------------------------->|              |              |
  | Lookup vendor's DNS server     |              |              |
  |             |                  |              |              |
  |---------------------------------------------->|              |
  | Lookup <sha1-of-device-pub-key>.<vendor-zone> |              |
  |             |                  |              |              |
  |------------------------------->|              |              |
  | Lookup NMS IP address          |              |              |
  |             |                  |              |              |
  |------------------------------------------------------------->|
  | Reverse SSH or Reverse TLS     |              |              |
  |             |                  |              |              |
```

NMS State Precondition

```
+----------------------------------------+
|                <NMS>                   |
|                                        |
|  vendor's trusted CA certificate       |
|  serial numbers for expected devices   |
|  username to log into devices with     |
|  auth credentials to log into devices  |
|                                        |
+----------------------------------------+
```

NMS needs CA cert and serial-numbers from Vendor

Supporting Private Networks

- Potential alternatives to source information:
  - Impersonate vendor’s DNS server
  - DHCP (susceptible to a MITM attack?)
  - USB flash drive
  - Near-field wireless

Or just to avoid doing a lookup in the vendor’s DNS server?

Security Considerations

- Long-lived certificates
- Vendor may reveal NMS locations
- Serial Number in certificate

IANA Considerations

- None

Open Issues

- DNSSEC doesn't currently allow client certificates
- Should DNS record provide SSH-specific information?
- Standardize REST API used to set DNS record info?

Not in -00 draft:

- Use something besides DNS? (e.g. HTTPS)

Questions / Concerns ?