CoA Proxying

RADEXT - IETF 9

Alan DeKok

FreeRADIUS

CoA Proxying how ???

- 5176 says “can proxy CoA”, but not how
- The draft suggests using Operator-Realm
    - Name of the visited realm
- Also Operator-NAS-Identifier
    - opaque identifier for the NAS

Limitations

- Only defined for User-Name / realms
  - Other methods of proxying CoA are ???
- How do we prevent realmA from contacting visited network V, and kicking users for realmB offline?

Security

There are no provisions in RADIUS for end-to-end cryptographic authentication of the data being transported. All security is hop-by-hop. The entire system is trusted, and intermediate hops are free to add, change, or delete the data they have access to. However, because systems may break, be misconfigured, or be attacked, we should design the protocol to be as secure as possible under the existing limitations.

What this means

- 5176 “reverse path” checks are necessary, but not sufficient
- The Operator-NAS-Identifier will likely have to be a large opaque token
- So that forged ones are provably caught, or “good” ones are vanishingly rare
  - e.g. 2^30 users distributed though 2^256 random values for the token

Proxies are still trusted

- Any proxy which sees the outgoing token can replay it in a CoA packet
- All we can do is minimize the number of proxies which see the token
- End-to-end encryption of data is outside of the scope of RADIUS

Mandatory attributes

- 5176 says that NASes MUST treat all attributes as mandatory
- Some NASes complain if you send them Proxy-State
  - Filed & accepted errata for this
- But what about other attributes?

Mandatory attributes

- Operator-Name and Operator-NAS-Identifier should probably not be sent to the NAS
- The NAS has no need for (or knowledge of) them
- But what about other, future, attributes?

Suggested text

A CoA proxy MUST NOT send the NAS an attribute in a CoA packet, unless the NAS sent the attribute in an Access-Request or Acccounting-Request packet.

or

All "server" attributes MUST be removed by the final proxy before the packet is sent to the NAS. This includes, but is not limited to, Proxy-State, Operator-Name, NAS-Identifier

Explanation

- When the NAS sends a packet to a local server, that server may add attributes to the packet
- Those attributes are NOT understood by the NAS
- The local server do the inverse process with CoA proxy
- i.e. remove any attributes it had added

Discussion?