Trusted Appliances

Trust between users, cloud administrators, and appliance creators is critical for an effective and dynamic cloud ecosystem.

The StratusLab Marketplace, an appliance registry, promotes trust between these actors and facilitates sharing of virtual appliances.

Endorsers

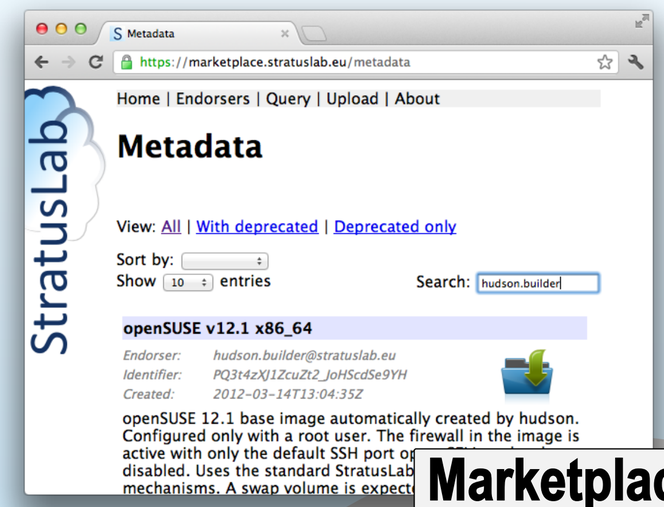
1. Evaluate appliances based on security or other criteria
2. Sign (endorse) appliances that they recommend
3. Deprecate images as they need security updates

End-Users

1. Scientists and engineers browse the Marketplace for useful appliances
2. Easily launch machine instances using the image identifier.

Cloud Administrators

1. Define appliance acceptance policy
2. StratusLab tools enforce policy for each machine instance request.



Marketplace

- Acts as neutral broker for applicance metadata
- Enforces individual timelines for metadata entries
- Accepts only signed, validated entries

Domain Experts

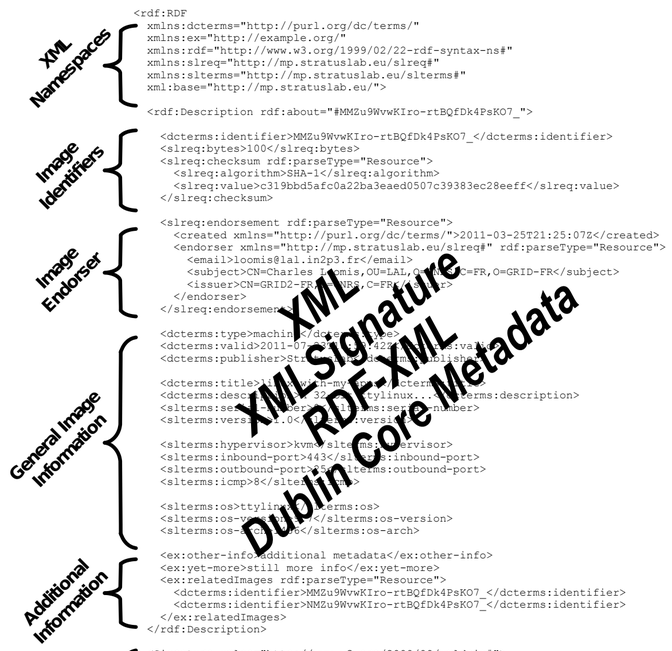
1. Create specialized appliances
2. Upload appliances to cloud or web storage
3. Create and sign applicance metadata
4. Upload metadata to the Marketplace
5. Replace images as they require security updates or enhancements.

Metadata Handling

Client tools provide commands to ***build image metadata***, ***sign*** the metadata entries, ***upload*** the entries to the Marketplace, and to validate them.

Any certificate or key can be used to sign metadata entries. ***Email addresses are verified*** to ensure that image endorsers can be contacted.

The ***policy engine*** uses metadata information and the ***cloud administrator's policy*** to decide whether or not to ***start an image***. Standard policies allow white/black lists of image endorsers and image identifiers. Any policy based on the metadata can be written.




```
<rdf:RDF
  xmlns:dcterms="http://purl.org/dc/terms/"
  xmlns:ex="http://example.org/"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:slreq="http://mp.stratuslab.eu/slreq#"
  xmlns:slterms="http://mp.stratuslab.eu/slterms#"
  xml:base="http://mp.stratuslab.eu/">

  <rdf:Description rdf:about="#MMZu9WvwKIro-rtBQfDk4PsKO7_">

    <dcterms:identifier>MMZu9WvwKIro-rtBQfDk4PsKO7_</dcterms:identifier>
    <slreq:bytes>100</slreq:bytes>
    <slreq:checksum rdf:parseType="Resource">
      <slreq:algorithm>SHA-1</slreq:algorithm>
      <slreq:value>c319bbd5afc0a22ba3eaed0507c39383ec28eeff</slreq:value>
    </slreq:checksum>

    <slreq:endorsement rdf:parseType="Resource">
      <created xmlns="http://purl.org/dc/terms/">2011-03-25T21:25:07Z</created>
      <endorser xmlns="http://mp.stratuslab.eu/slreq#" rdf:parseType="Resource">
        <email>loomis@lal.in2p3.fr</email>
        <subject>CN=Charles ...mis,OU=LAL,O=GRID-FR,C=FR,O=GRID-FR</subject>
        <issuer>CN=GRID2-FR ...,O=GRID-FR,C=FR,O=GRID-FR</issuer>
      </endorser>
    </slreq:endorsement>

    <dcterms:type>machine ...</dcterms:type>
    <dcterms:valid>2011-07-... ...42Z</dcterms:valid>
    <dcterms:publisher>Str... ...Publisher</dcterms:publisher>

    <dcterms:title>... ...-my-...</dcterms:title>
    <dcterms:description>... ...tylinux... ...</dcterms:description>
    <slterms:serial-number>... ...</slterms:serial-number>
    <slterms:version>1.0</slterms:version>

    <slterms:hypervisor>kvm</slterms:hypervisor>
    <slterms:inbound-port>443</slterms:inbound-port>
    <slterms:outbound-port>...</slterms:outbound-port>
    <slterms:icmp>8</slterms:icmp>

    <slterms:os>ttylinux</slterms:os>
    <slterms:os-version>...</slterms:os-version>
    <slterms:os-arch>...e</slterms:os-arch>

    <ex:other-info>additional metadata</ex:other-info>
    <ex:yet-more>still more info</ex:yet-more>
    <ex:relatedImages rdf:parseType="Resource">
      <dcterms:identifier>MMZu9WvwKIro-rtBQfDk4PsKO7_</dcterms:identifier>
      <dcterms:identifier>NMZu9WvwKIro-rtBQfDk4PsKO7_</dcterms:identifier>
    </ex:relatedImages>
  </rdf:Description>

  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/..."/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#..."/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>go6VR...</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>NrTJFF...</SignatureValue>
    <KeyInfo>
      <X509Data>...
        <X509Certificate>...</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>

</rdf:RDF>
```

Security Considerations

A consistent metadata timeline is critical for understanding the evolution of an image and for auditing the metadata if there are problems. The ***Marketplace ensures a valid timeline for each endorser*** by requiring that all entries are dated and accepting only those dated after the last entry.

A hacker in the Marketplace could not forge new entries but could alter the timeline by deleting entries. ***Marketplace servers must be managed following best practices*** and keeping security in mind.

Appliances may contain ***proprietary software*** or other protected material. To avoid Intellectual Property Rights (IPR) issues, the ***Marketplace stores only the metadata***. The appliance is stored elsewhere, where the ***owner may control access*** to the applicance itself.

To ***avoid man-in-the-middle attacks***, the Marketplace is run over HTTPS. This ensures that the server's identity is validated and that messages are not intercepted or altered in transit.

As ***protection against altered or corrupted images***, the SHA-1 checksum and size of the image (stored in the metadata) are verified. to allow validation of the downloaded data. Additional checksums further reduce this risk.

Website: http://stratuslab.eu
Support: support@stratuslab.eu
Contact: contact@stratuslab.eu

Centre National de la Recherche Scientifique *France*
Universidad Complutense de Madrid *Spain*
Greek Research and Technology Network S. A. *Greece*
SixSq Sàrl *Switzerland*
Telefonica Investigacion y Desarrollo S.A. *Spain*
Trinity College Dublin *Ireland*

StratusLab is co-funded by the European Community's Seventh Framework Programme (Capacities) Grant Agreement INFSO-RI-261552.