PSARC Case 2006/683 Issues List

1) jdc-0a Are the provided materials complete? The "readme" file refers to documents (on sunwebcollab) that don't seem to appear with the materials. Are they under review as well?

The materials are complete and have been sent to PSARC_materials@sun.com for posting to ARC site. Here is the list of updated documents sent on 1/25/07 -

1) Service Tags CLI and API Specification - ServiceTag_API_v06.pdf
2) stdiscover man page - in- stdiscover.manpage.pdf
3) stlistener man page - in- stlisten.manpage.pdf
4) st discover protocol specification - stdiscover_prototcol.pdf
5) stlistener protocol specification - stlisten_protocol.pdf
6) SMF Usage specification - st_smf.pdf -
7) Service Tags ARC Functional Specification - with changes for noaccess user. ST_ARC_v2.pdf
8) Service Tags ARC Security Questionnaire - Service_Tags_ARC_Security...pdf
9) SysNet Responses to ARC Issues Reviewed on 1/17/07. - Responses to ARC Issues.pdf

2) jdc-0b Need complete definitions of the new network protocols included in this project. (That it uses the existing well-known HTTP port isn't enough to describe the protocol.)

SysNet has provided a two Protocol Specification both of which have been requested to be posted to to ARC site. See stlisten_protocol.pdf and stdiscover_protocol.pdf.

3) jdc-0c Need to archive committed CLI with case materials.
SysNet has provided an updated Service Tag API and CLI Specification – See ServiceTag_API_v07.pdf.

4) jdc-1 How does this relate to the existing 'prodreg' feature?

See comments in pat ryan's 1/25/06 email Response to Kais and psarc@sun.com entitled “Service Tags Updated Response to ARC Issuesl- 2006/683 - Request for Review on 1/31/07”. See Big picture response.

5) jdc-2 How does it relate to existing SARC cases, each of which appears to have some sort of "software registration" function? Do we need to invite some SARC folks to help review this?

SysNet has reviewed these cases and have determined that these were created by the now-defunct CNS organization. SysNet is reviewing SARC cases and will work to remove obsolete cases.

6) jdc-3 Why a new discovery protocol? Could this perhaps work in concert with something already in progress, like Bonjour?

Yes, I realize that needing to support S8 is a significant constraint. (Have you talked with the folks who maintain SLP?)

(The 1-pager and "ST_ARC_v2" document seem to be at odds about this. Is the proprietary "ST Discovery" useful?)

Service Tags work with both SLP and Bonjour but both of those protocols are use-agnostic in that they are usually implemented with muli-use discovery in mind. If a customer has either (or both) of those environments we can support them. However, the default discovery mechanism uses commonly available UDP Broadcast which most customers would control at their routers. Rather than have them be forced into the complexity (and potential collision) of setting up SLP or Bonjour we chose to include a tiny simple default discovery mechanism.

7) jdc-4 How does this daemon work with existing HTTP daemons?

The network code in Service Tags is separate from existing HTTP daemons and does not actually run in Daemon mode - it runs as an Inetd "run and stop" process. It will not conflict with existing HTTP daemons.

8) jdc-5 I18n answers seem to be inconsistent with the other project goals. Is the CLI intended for use by customers?

No. The Registration Client in ARC Case 699 will provide a UI for customers to interact with Service Tags as part of Product Registration flow.

9) jdc-6 Are there relationships between this project and patch management applications? It seems to me that something that tracks products and versions over the network would be ideal in that space.

Yes. Service Tag information will feed into a hosted repository at Sun (via a customer initiated "gatherer" process) in the Anza Project (see Note 1 above). That "inventory" is intended to be used in the next generation of Sun Connection to "smarten" the management/patching processes (See notes re Coso Project in Note 1 above).

10) jdc-7 Should the wire protocol for service tags be standardized? It seems unlikely to me that Sun will ship all possible useful applications based on them.

SysNet is targeting adding SNMPV1 to the list of supported discovery protocols for Service Tags in a later release. Once this enhancement is completed, Service Tags would be open to most asset management tools.

11) jdc-8 Are there security or privacy issues related to the handling of this data? (Issues reviewed included Secure By Default,

The information intended to be exposed by Service Tags has been vetted by the privacy office as not containing any personal or sensitive data. We also ran this thru the NIST standards for government data processing systems to ensure that nothing outside level 1 "sensitive" data is exposed. Its a VERY minimal data model intended to facilitate registration events only.

SysNet has completed Security Questionnaire.

12) jdc-9 What are the units of currency here? Does it matter? When the ARC reviews future projects, would there be any services that are too trivial to list in this database?

The architectural intent for Service Tags is to represent any Sun product. The practical limitations here are that we are requiring entry into a "product registry of record" for data to be allowed to be received by Sun on the back end. So in theory there would be no limits to what products could expose Service Tags.

13) jdc-10 What does this project do with inetd? (Is this stdiscoverer and stlisten?) What ports are used?

Correct stdiscover and stlisten leverage Inetd to start and stop service. The default port is 4950 SysNet is registering the port. (IANA Ticket Request # 57625)

14) jdc-11 How are the registration details communicated back to Sun?

This communication is covered in Case 2006/699. At a high level, the team will leverage the ARC-approved HTTPS communication and the "agent authentication" model used in SCRK where data is also encrypted using negotiated public key cryptography.

15) What are the security issues associated with that mechanism?

These will be covered fully in Case 2006/699. The intent is to use a customer initiated "gathering" process that is currently still being developed. All data to be sent to Sun will be logged and available for users to review. Users will select the products that they want registered. Also see Service_Tags_ARC Security Questions.txt

16) jdc-12 Where's the security information for the "probe listener" and the "discovery agent"?

SysNet has provided a protocol description and MAN configuration page for the Probe Listener and Discovery components. Additionally, SysNet has completed the Security Questionnaire and requested that this be posted to the ARC site.

17) jdc-13 Is "*/var/sadm.servicetag/*" intentional, or should that be "*/var/sadm/servicetag/*" instead?

Correct. That is a typo.

18) jdc-14 nit: unless the administrator is expected to invoke these things from the command line, they don't belong in /usr/sbin.

Agreed. We completed this. See CR# 6514363 - Move ST inetd daemons out of /usr/sbin to /usr/lib/inet

19) jdc-15 nit: it seems odd that the probe listener is "stdiscoverer" and the discovery agent is "stlistener."

No Response necessary.

20) jdc-16 nit: you might want to talk with the Update release folks before attempting a genesis patch.

Agreed. Understood. No genesis commitments are being made without going thru that very rigorous process.

21) gcs-1 What about this project makes it require a minor release
binding rather than patch or micro?

** - Correct binding is a patch/micro.

22) gcs-2 Shouldn't the service tag DTD live in /usr/share/lib/xml/dtd with the rest of the DTDs shipped with Solaris?

Agreed. SysNet has moved registry to /usr/share/lib/xml/dtd.
See CR# 6514671 Service Tag DTD file location should be changed to /usr/share/lib/xml/dtd

23) gcs-3 Integration with SMF? (Prompted by statement that it uses inetd to start itself.)

See st_smf.pdf for details of integration and manifests.

24) gcs-4 How do customers opt out? (When they do, things like "unregistered products write warning to system log periodically" should be disabled.)

1) The system log writing requirement was dropped by Service Tags. SysNet direction from Jonathon is that Service Tags are to be Default On. Customers may opt out by

2) Removing Inetd/SMF configurations - (**JEFF) (Need to add to documentation)
Stops listener and Agent

3) Never launch Registration Client (no data collected or sent to Sun) or,

4) Do not select a product to be registered with Sun (product data not sent to Sun)

25) gcs-5 New user and group (svctag:svctag) introduced into the system.
Are these really necessary? Could some other existing
administrative entities be used instead?

Agreed. We will use noaccess Yes, see CR#6514707 Service Tag daemons should run under noaccess/noaccess vs. our own created identities

26) gcs-6 Does this project include the modifications required to make existing products incorporate service tags?

This implementation includes only "service tagging" of Solaris.

27) gcs-7 I'm confused about how the service tag registry gets populated.
Are products expected to add entries to it when they're installed? (that is, is information pushed into the registry, rather than pulled into it?)

\The registry is populated by Products pushing their information via calls to sthelper.