

**Subject:** Re: [sacm] Proposed use cases to move forward  
**Date:** Wednesday, August 15, 2012 1:08:32 PM Pacific Daylight Time  
**From:** Gunnar Engelbach (sent by <sacm-bounces@ietf.org>)  
**CC:** sacm@ietf.org

+2

It's worth having a broad document even if parts of it aren't clearly defined to stake out the expected scope of the working group and because considerations of the broader scope might affect decisions on the focus areas.

But I absolutely agree that the best way to make real progress is to focus on a tight subset, and it looks like UC1 and UC3 is the consensus (and there's no dissent on that here).

--gun

On 8/15/2012 3:55 PM, Stephen Hanna wrote:

I love broad scope. Don't get me wrong! But I'm concerned about having a use cases document and an architecture document for this working group that goes way beyond the charter and initial scope for the group.

I'm concerned that this will lead to lots of discussions on the sacm list and lots of effort being spent on topics that are out of scope, diverting us from the tasks at hand and slowing our progress.

I'm concerned that the working group chairs won't be able to cut off discussion of topics by saying they're out of scope for the working group.

I'm concerned that we'll get sidetracked or even derailed by controversies that aren't relevant to the scope of the group.

I'm concerned that by including all of security automation within our use cases and architecture, we may actually prevent the formation of other working groups that could work on those other use cases.

We have plenty of work to keep us busy for years with UC1 and UC3. There's agreement that the technology needed is mature enough for IETF standardization. I suggest that we scope this working group to address only those use cases and that our use cases and architecture be limited to them.

I'm sorely tempted to create an ambitious architecture for security automation that encompasses all of the use cases

that we have described so far and maybe more. I understand that people have a hard time understanding how the NEA and MILE and SACM standards fit together and I would love to address that in an IETF RFC. But I have seen several grand architecture efforts die or come to nothing in IETF. IETF is filled with smart engineers with clever ideas. We're great at solving problems but if we can't agree on the problem to solve or if we choose the wrong problem, we can easily spin an intricate and pointless web.

I think we'll do better if we scope our effort properly.

Maybe a few people can create an individual submission describing a grand architecture and roadmap for security automation and ask people in SACM to review and provide feedback on that document. That would be a good way to get a grand architecture while still ensuring that the SACM effort keeps its focus. In IETF as in so many things, you must keep your focus or you'll never succeed.

Thanks,

Steve

-----Original Message-----

From: [sacm-bounces@ietf.org](mailto:sacm-bounces@ietf.org) [<mailto:sacm-bounces@ietf.org>] On Behalf Of Waltermire, David A.  
Sent: Wednesday, August 15, 2012 1:13 PM  
To: Stephen Hanna; Adam Montville; Luis Nunez; Omar Santos  
Cc: [sacm@ietf.org](mailto:sacm@ietf.org)  
Subject: Re: [sacm] Proposed use cases to move forward

+1 on scoping the charter to UC1 and UC3.

I think we are better served with a use cases document, and eventually an architecture document, that is broader scoped. Both of these documents will help inform the work we will do under the charter as it relates to the larger context.

To this end I would suggest we focus on expanding the use case document primarily in the areas of UC1 and UC3 for now. We can expand the other use cases later.

Sincerely,  
Dave

-----Original Message-----

From: [sacm-bounces@ietf.org](mailto:sacm-bounces@ietf.org) [<mailto:sacm-bounces@ietf.org>] On Behalf Of Stephen Hanna  
Sent: Wednesday, August 15, 2012 11:24 AM  
To: Adam Montville; Luis Nunez; Omar Santos  
Cc: [sacm@ietf.org](mailto:sacm@ietf.org)  
Subject: Re: [sacm] Proposed use cases to move forward

I agree. Let's work on UC1 and UC3. The other use cases are valuable but just doing UC1 and UC3 is plenty of work for this group for the next year or two (maybe five!).

I saw several emails in favor of this a few weeks ago. I thought that it was settled. I'd like to see a revised charter and use case document, scoped down to focus on just UC1 and UC3.

What do others think? Do we have rough consensus on this?  
If so, let's get moving.

Thanks,

Steve

-----Original Message-----

From: Adam Montville [<mailto:amontville@tripwire.com>]

Sent: Wednesday, August 15, 2012 10:30 AM

To: Adam Montville; Stephen Hanna; Luis Nunez; Omar Santos

Cc: [sacm@ietf.org](mailto:sacm@ietf.org)

Subject: Re: [sacm] Proposed use cases to move forward

On 8/6/12 7:27 AM, "Adam Montville" <[amontville@tripwire.com](mailto:amontville@tripwire.com)> wrote:

UC1 and UC3 both require assessment of endpoint state. If not for the NEA ties in UC1, it seems a subset of UC3. So, we should be able to start with the main concern of UC3: Security Configuration Management.

I haven't seen much activity on this thread (there was another thread, "Using the Frame of Reference," discussing some approaches we can use to keep us focused and meaningful).

Are there any objections to tackling UC3 followed by UC1? Does anyone disagree with my assertion that UC3 is a subset of UC1 and that a reasonable starting point is Security Configuration Management?

---

sacm mailing list

[sacm@ietf.org](mailto:sacm@ietf.org)

<https://www.ietf.org/mailman/listinfo/sacm>

---

sacm mailing list

[sacm@ietf.org](mailto:sacm@ietf.org)

<https://www.ietf.org/mailman/listinfo/sacm>

---

sacm mailing list

[sacm@ietf.org](mailto:sacm@ietf.org)

<https://www.ietf.org/mailman/listinfo/sacm>

---

sacm mailing list

[sacm@ietf.org](mailto:sacm@ietf.org)

<https://www.ietf.org/mailman/listinfo/sacm>