2023.12.01 Meeting notes

Date

01 Dec 2023
Time: 15:00 (CET)

Meeting link https://tib-eu.webex.com/meet/georgy.litvinov

Attendees

- Georgy Litvinov
- Brian Lowe
- Mark Vanin
- Dragan Ivanovic
- Miloš Popovi
- Ivan Mrsulja

Agenda

- Meeting notes
- Access control
- Endpoint/procedure isolation
- N3 Template substitutions with array of values
    - Removal of deprecated array implementation from N3Template and SolrQuery operations.
    - Idea: rewrite with JsonContainerArray
    - Draft PR https://github.com/vivo-project/Vitro/pull/426
- Reports
- Meeting schedule

Meeting notes (transcribed automatically)

Georgy Litvinov: First point in our agenda is meeting notes. I'm going to Have a transcribed meeting note. So please I agree with this meeting. audio to be recorded for the transcribed transcription purposes. Yeah Great okay, so This next point in the agenda is access control. Also, there is as you may be seen there is a point about Procedure or endpoints isolation. then we will discuss entry template substitutions then maybe if mark Fine time discuss repo generators and then meeting shadows. Hi, Dragan Hello Dragan this meeting is going to be audio recorded. So for the transcribing transcription purposes, is it? Okay. Yeah. Sure, okay. so let's. Yeah, let's go to the access control. Item Dragan merge today access attribute based access control and in dynamic API Because of lack of that functionality we already had some custom-made access control for the roles. so I think it would be a good idea to align that with the attribute based access control that we have now to be able to specify Requirements for the user or additional requirements in more generic way On level of Procedure or endpoint definition. so even I think have you used dynamic API Role based access Configuration?

Ivan Mrsulja: Yes, I have used it and I've put an admin access on everything that I've worked in on But I didn't touch anything about the attribute based access control that you implemented.

Dragan Ivanovic: yet I have a question here. So when you say that you would like to align this implementation with new havoc So would you like to make it more expressive expressive in the meaning that let's say you can say for this dynamic API endpoint The user with this and these privileges can access and execute that. so the user which has the privilege to edit the?

Georgy Litvinov: Yes, so right now As maybe you have seen there is an option to to make authorization requests. so each authorization request has subject that something that we can take from there From the request from the user. it has a access object so something that is being accessed and I think that's that's the entity that we can configure in our Procedure so we can define what is being accessed. so so far we have Object properties statements and data property statements, so we can reuse something like that or we can invent something new it. it would be easy for the a back and for for the usage of this and we also able to specify for example in the in the request What you rise are being requested or maybe? Yeah, like this type statement type and Yeah, I think we should use it to To be able to check that.

Dragan Ivanovic: so at the moment in dynamic API we can configure based on the role, right? Or anyone with this Right? So it means that at the moment it's important only at the level of roles right which the user belongs. and now you would like to improve that.

Georgy Litvinov: Yeah Yes, I I suppose that now we basically female. if it merged dynamic API today into the main branch then we would have to independent system for check control, so I think it's not the right thing. so The access should be checked only in one place, so we shouldn't have duplicates in that matter. For example if we would like still to be able to specify access control on the level of dynamic API Then we would need to update. We need to update the Attribute based access policies for that or data sets and to load that. so there is there is a need for interaction between this and there is still need to To connect them right. and Yeah, that's That's an interesting task because I suppose we will find new types of access object right. so some some Simple access object could be the procedures I suppose but maybe we would find some something something more and also this would allow us to to to use sparkle queries to check access like we do that on on the stage when some self editor access some page and We need to check if this page that's being accessed is connected to the profile of the users that's gaining this access.

Dragan Ivanovic: Okay, I fully agree. You just said just. I think it's important that we keep Also some simple common cases quite easily to be configured meaning that In a lot of cases it will be the admin can access this endpoint, so it should be also Configurable in some easy way as it's now.

Georgy Litvinov: Yeah Yeah, hi mark, by the way, this meeting is being audio recorded for the transcription purposes. I just let you know. Okay. Yeah Yeah, so if you have an ideas from the Author of the authors of these procedures I suppose even Dragan you Have some experiences and maybe thoughts. How would you like to? What would you like to check? So how would you like to check access? and if we missing something in a back then? Yeah Let's bring it and discuss that and implement that because I think that's would be very good.

Dragan Ivanovic: So what you are already implemented for crowd operations or the person? I Think when you edit a person or add the new person or delete a person it it should be allowed to the Pressure how it's called the editor of that institution. I mean the person is possible for that Department or that faculty or something. is that? So not sure. is it possible that to express and we should find a way how to express it easily To say, okay this procedure can be accessed depending on the URI of the person which you would like to delete and then from that person you should collect Institutions to which it belongs and then from the user you should also collect information for each institution that user is responsible.

Georgy Litvinov: and if those two merge then I mean if those two match to them you can Yes Yes, so before we match today that before Dragan match today a back in Vivo there was as you might know annotation properties to specify access. and this annotation properties could be applied to the object properties to the data properties and to the classes. and the interesting part here is that we have that sets of Classes that are load to some roles, but there They were never checked nor by Vivo accept previous access control implementation nor by advanced role management and At some point my thoughts were to to check it like that. so for example we have a object property statement and the subject of that Sorry subject of that property could be any URI The predicate. predicate could be a def type and the object could be the type of the class That's being created. Does it make sense to you? So basically do we allow this statement? That this class and maybe that represents this? but maybe that's not a good thing because it's we are not adding only one statement We are creating a bunch of statements related to some to some individuals. Yeah, so Should it be another type of the access object because it to me it looks more complicated one.

Dragan Ivanovic: Yeah, it looks also to me complicated especially, you know, if you take into account that in dynamic API we have those Conditional parts and so on. it could even make even more complicated Because you know for some entry templates which should be executed something is that you're not allowed to do that and Then because of that you might be completely restricted to access that endpoint and maybe in your case You walk in that end point that entry template is under some conditional statement And it's not going to be executed

Georgy Litvinov: I see.

Dragan Ivanovic: So maybe then we Remind you that you also implemented that Computation of the inputs for the complete endpoint and there was a lot of complication because of this conditional because of the looks and so on. So I'm not sure is this somehow connected with that Check? additionally, so maybe in That expressing who can access the end point. We should also conditionally define some privileges or something as that. I don't know because you know if this part of the dynamic API This particular part is executed Then it should be granted to the person who is invoking this endpoint. If that part is not invoked Because depending on some input parameters then it's not important as it was.

Georgy Litvinov: No the other conditionals. I think the issue with conditionals that you mentioned is result at this point. So it's it doesn't create any Not obvious things. because but What maybe if I if I understood your idea so maybe the other any cases when we Can't Check the Permission with having all this all this information about input types Before the execution. so maybe in the execution we have some sparkle construct query sparkle select queries and maybe in that case there are some special cases when to check all of that you would have to Compute a lot and basically you able to do that only at the end of the procedure, right? So could that be the case?

Dragan Ivanovic: Yeah And also one scenario might be. So you introduce that one and one operation might be the part of the another.

Georgy Litvinov: right, right?

Dragan Ivanovic: So you can execute the other endpoint. Should we insist that the the creator of the let's say that endpoint a which is including the endpoint be repeat again the Let's say access part Access Because if you can't access the B, then you can't exit the complete a. is that it shouldn't be somehow Just in one line saying that please respect access role from the all included operations? or should we insist that the creator of endpoint a repeat You know the complete Access part and then there could be a problem with maintaining and so on?

Georgy Litvinov: Yes, you think if If we only check the initial requirements for the for the public endpoint It could be complicated to maintain complicated to check. What? What permissions user user should have? right?

Dragan Ivanovic: so If I understood well there is that could be the endpoint b Which or operation which can be included in the operation a right?

Georgy Litvinov: Yeah.

Dragan Ivanovic: And for operation b, there might be some access rules, right who can access that? Should that access rules part from the entry definition be copied in the Operation a and plus extended with some additional access rules? Or should we have the options in in operation a? just to say Respect all let's say sub operations access rules and plus. Yeah, very good question, yeah, but it should be always the case, you know, maybe it's logical that it's always respected.

Georgy Litvinov: So then it should collect all the dependency Requirements. right if you have five or if you can execute five Endpoints, then you need to be able to access all of them, right?

Dragan Ivanovic: I think at this moment, it's important just to discuss about all of those cases and then I think we should that someone say, okay. This is really quite rarely not likely to happen to have so often And in that case the user will have to copy it Manually

Georgy Litvinov: in the definition of this complex operation

Dragan Ivanovic: Even if it will introduce potentially some

Georgy Litvinov: maintaining the issue to change in two places

Dragan Ivanovic: instead of one and so on. But it will be so rarely that we shouldn't Spend a lot of effort on that. So my idea today is just I just mentioned that. Take it into account when you're designing the interface of Let's say Access rules.

Georgy Litvinov: Yes, I think it's very important and very good thoughts and I think that's the whole point of us discussing. so we need to find these These things before we get to implementation. my My idea also was maybe to to reuse Shackle in this matter. So because we have we have Shackle components implemented in dynamic API. Would it be useful if we? for example if we can't check If we can check fully be a Confident that there be able to check access that at the end of the procedure For example if procedure creates some temporary graph and it adds some more information that a temporary graph and at the last stage of execution this procedure writing this temporary data from this temporary graph into for example into full you into a box then before writing that Maybe we should add be we should think of how to define some requirements Shackle requirements, for example, and should that be part of? Authorization cultural on dynamic API site or it or it should be just you know custom things that creator of the procedure or endpoint can add manually and Send for example access denied in case something went wrong.

Dragan Ivanovic: Yeah, and the rule access should be defined at the level of procedure, right? So you don't have the level of the operation or something. is that I'm just thinking for the moment. Is there any sense to define that at the level of operation or step? then then you can reuse that also for other parts and then that you have calculation of Let's say access. Take conditions for the complete procedure based on the operations which are included there. Maybe it might resolve this problem with a conditional step and you know because maybe you can conclude whether that part will be executed and whether it's included in the procedure Requirements, so I want to say maybe we can calculate it on the fly and when you are Accessing that some end point. so maybe you can go through all the operations which are included in.

Georgy Litvinov: Yeah, maybe maybe I'm a little bit, you know, very of us being too To express if I mean on each stage to check every every step, but it's a it's a safety concern. So Yeah, that's a that's a good thing. I think we need to plan and Yeah Create a good architecture from it and implement that. So do we have anything more on that point or we should we go to the next one?

Dragan Ivanovic: Okay, you're just maybe for the conclusion. Are you going to maybe to work further on this and How we're going to proceed further basically here? Are you going to suggest something the next Friday or what is your idea for it? So we started now discussion some discussion.

Georgy Litvinov: Yeah Yeah, that's a good idea. I I would like first to maybe if any of us came up with some practical solutions. if you to add something to the dynamic API side add something to a backside Yeah, so maybe step by step or if you have some ideas then maybe Maybe we can write it down and show and discuss on next meetings. I suppose Because now I yeah my I don't have a full No view to propose to do something. So I have just thoughts that we Yeah discussed. Yes, yes, I suppose I suppose Okay, the next point was endpoint procedure isolation. I I think it's similar to previous Previous topic and we already started discussing that. so I think it's very important for us to be able to isolate already defined procedures and endpoints and to be able to To add some safety for the procedure loading and endpoint loading. otherwise Like we have it right now if we If we Add some bad configuration to our one graph Then all the endpoints can be broken and that's not something we would like to see I suppose. so I think there should be some kind of sandbox where we were able to see some Components already defined and reusable, but once we have Endpoint or procedure ready and we want to even we see that it's Defined component. I think we need a way to Copy that copy that triples related to that required to load this into a separate graph. So But my My thought was that the the biggest concern about that Is that I think that could be complicated on the Jena side. So we have a dev service and Yeah how to do that easily. I'm still not sure how it's done in vitro in vivo Yeah, but can we have the model for let's say draft procedures and then the specific model for Let's say in production procedures and then maybe just to create one endpoint in which you are You are saying this should be moved from the draft to the Let's say in production. Because if I answer you so if we have 10 Procedures and points and if one is failing actually you can't access any of those It dependent on what was broken. so if you add some statement that Made other endpoints broken then. Yes, if you remove for example something or if you added something and it It affects all of them Then yeah. So what do you think about this?

Georgy Litvinov: to have more than one model let's say Yeah, yeah, that's that's what yeah, basically I meant the same. so yeah model or graph it's basically the same.

Dragan Ivanovic: What is the problem from the Jena side? I mean we have a lot of models right or graphs? Yeah, you should to have one more.

Georgy Litvinov: Yes. I'm not sure that we are able to Create and remove graphs from dynamic API easily. I still need to figure out how. I just don't remember how it's done in a dev service jenna or other dev service implementations. Yeah, so we will need to have To connect them. I would say yeah Yeah, and I guess created this as you said Endpoints to manipulate all the products productive And Productive graphs and the sand sandbox graphs. Yeah So I think there is a need for further investigation on that And if you have time, please do so. I'll try to do that, too. I I Don't have much time these days, but we'll see. You'll see how it will be next weeks. Okay, so let's go to the next point. the next point is Entry template substitutions. and even you told me that you wanted to show us something, right?

Ivan Mrsulja: Yes, i've told you that I tried Incorporating your solution into my code, but it didn't quite work. Let me just share my screen real quick Sure. So can you see? Yes Okay So what I did is I tried using it on a first name. Uh, you told me or I remember it that way that you just have to configure the has type to jason container array And then set the default value to the empty array. Is that right?

Georgy Litvinov: I suppose so.

Ivan Mrsulja: Yeah Yeah, and everything else should should then work, right? Uh, well, no I get the error that it cannot Actually interpolate the the first name into the into the expression here Like this. Can you hear me?

Georgy Litvinov: Yes, could you show could you show us the jason request that you're using? So the final request that was sent to the server, do you have it?

Ivan Mrsulja: This was the request.

Georgy Litvinov: Okay Okay, uh I'll try to Test it. and yeah, most likely I know what's what's the case what should be implemented and what I forgot to do. Yeah, but please could you share this example with me so I could test it on my instance?

Ivan Mrsulja: Yeah, I can. I can send you the the located the entry files And I can send you the request if you want.

Georgy Litvinov: Yeah, that would be great.

Ivan Mrsulja: I'll send you after the meeting the request body and we'll send you the necessary Entry files that you need to do.

Georgy Litvinov: Okay. Yeah, sure Thank you. Thank you for testing. Okay, so hi mark, how are you? have you got any uh progress lately?

Mark Vanin: Um report generator sadly sadly You know, there are currently some works that we're having and like ending the job with a paper that we are writing. but I guess maybe like After the next week, then I will. yeah, just uh, I had like one comment, but I saw already that there are There is a pull request regarding the capture usage On the vitro. so I remember maybe two weeks ago when we have discussed The usage of google capture and I just recently saw a very similar library called h capture and They are saying about themselves As analog to google capture but just relying to all the gdpi and everything. and they Have been used and they saw them at lots of organizations in german, but I'm not really sure because You need to Click on some weird images like which image did you see the first time or the second? So it's very it's not like printing the numbers But that's all.

Georgy Litvinov: Okay, thank you, yeah, it's understandable. There are a lot of people I suppose right now are sick in germany and a lot of work to do at the end of the year. Yeah, it's it's also.

Mark Vanin: It's because like the other two has to be developed.

Georgy Litvinov: Sure, okay, and I'll let you know if there will be any updates because I think no no, I guess I have a question. so, uh, I remember.

Mark Vanin: so I tried to Change the type of Of custom rest action from put to post and I do remember that when I sent a request to this it still returned me Four or five arrows saying that method is not allowed. So it's the same as it was before and also Maybe I haven't changed everything but in swagger Interface for this html page swagger ui it still was shown as put request. So I like maybe I haven't done everything. so but maybe you can check it. if you change from A custom resection where it has like this method defined for example import Report generator and then you define import report generator as a post method Something else would it work for you or not?

Georgy Litvinov: Did you try? because you have in this in the in this in vitro in report generators entry you can. You can easily just change the method to the put if or from the put to the post if it's not And try it the same.

Mark Vanin: I I haven't done this. so I have. uh, I have just changed it in the custom restriction. So there is like a If I understood it. so you have. There are some predefined methods such as on get on on put on post and something but then if you want to define Another on post you have to use custom restriction. Yeah, so I have done this.

Georgy Litvinov: I haven't done but you you can you can change the method or or if you If you change the method defined in the entry for custom resection is it uh, does it change?

Mark Vanin: Maybe I can even show it. Yeah, sure Maybe.

Georgy Litvinov: so it doesn't reflect your configuration basically.

Mark Vanin: Yeah. Yeah, so i'm not sure. Maybe I haven't changed everything because like in swagger interface.

Georgy Litvinov: It was still shown as a put method, but maybe custom resection is Not working correctly and you you're using the latest dynamic api 1.14, right?

Mark Vanin: I hope so. Let's Well, that's a good question.

Georgy Litvinov: I hope so but now because I think it's fixed only in the in the latest branch.

Mark Vanin: Yeah Okay Yeah, I think it's not in my case. So I will check this. Yeah, you see I wasn't really sure because like I changed it quite a bit But and then I thought maybe it wasn't all Was needed. So yeah, we'll Look at this one also and tell you Okay Yeah, thank you very much.

Georgy Litvinov: Okay, uh The last item here maybe is maybe we should just meet not every week but every other week because yeah these days I for example, I was quite busy with other tasks and there is not much progress. So what do you think about? what's What's the best for you? Or do you find?

Dragan Ivanovic: The next meeting should be done on 15th of december, right?

Georgy Litvinov: Yeah, yeah I I want to have your opinions about that. So for you, uh, would it be useful to have meetings every week? or it's For your pace, it's completely fine to have it every other week?

Dragan Ivanovic: I think b weekly is okay, huh?

Georgy Litvinov: Mark Ivan milos.

Mark Vanin: Yeah I mean I would say that I don't know. so For me it's like every cases, okay should be fine, but I will also be Yeah, maybe every other week because I'm not that active recently.

Georgy Litvinov: So yeah, even milos. What's your opinions?

Ivan Mrsulja: It's okay for me. Well, I think that last we didn't have that much Things to talk about. so every other week was great options. So I think it would Continue to be every other week okay, so We agreed.

Georgy Litvinov: so, thank you, thank you very much, uh, that's all points for today. Thank you Have a nice weekend. See you.

Mark Vanin: Bye. Bye. Bye.

Georgy Litvinov: Bye. Bye.