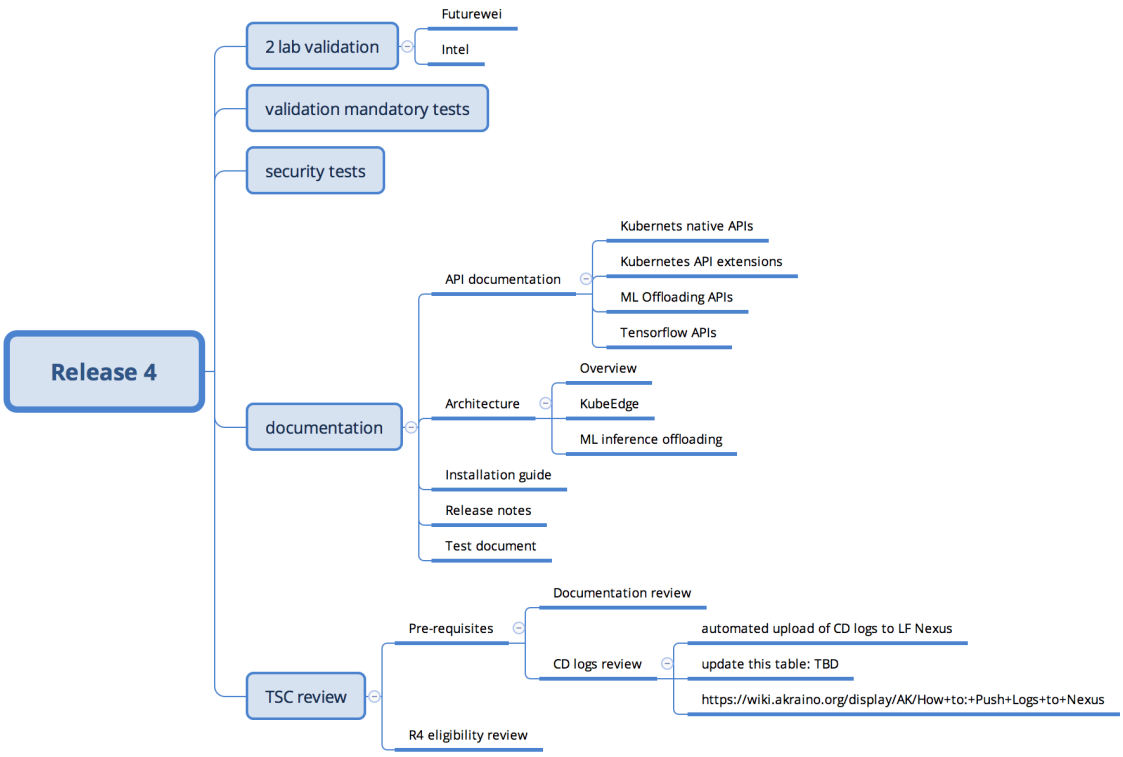
Release 4 planning and tracking

R4 Planning.pdf

Release 4 planning.xmind

KubeEdge Akrain...se 4 review.pdf



Tasks:

		Task	Owner	Status	Date
1	Test	Figure out mandatory Tests and security test list	Hao	Done	

		Lab set up validation	TBD		
		Test in Futurewei Lab	TBD		
		Test in Intel Lab	TBD		
2	Documentation	Architecture (Add Pod Topology)	Yin, Jane		
		Supported Kubernetes native API	Yin, Jane		
		ML Offloading API	Hao/Jiafeng, Jane		
		Installation guide	Hao		
		Release Notes	Yin, Jane		
3	TSC Review	Documentation review			
		Log review			
		R4 eligibility			

Detailed Test Tasks:

Category	Task	Owner	Status	ETA	Comments
CI/CD Logs upload to Nexus	Register an LFID	Hao	Complete		How to: Push Logs to Nexus https://jira.linuxfoundation.org/plugins/servlet/theme/portal/2 https://identity.linuxfoundation.org/ https://jira.linuxfoundation.org/plugins/servlet/theme/portal/2/IT-20459
	Request permission for Nexus log	Yin/Hao	Complete		
	Set up CD pipelines	Yin	In Progress		
	Upload CD logs to Nexus	Hao	In Progress		
Bluval	Provision jumpserver	Yin/Hao	Complete		Bluval User Guide http://gerrit.akraino.org/r/validation
	Test set up and run tests	Hao	In Progress		
	Fix issues for failed tests				
	Report results				
Security Scan	Vuls: test set up and run tests	Hao	In Progress		Steps To Implement Security Scan Requirements Reuse the jumpserver for Bluval tests.
	Lynis: test set up and run tests	Hao	In Progress		
	Kube-Hunter: test set up and run tests	Hao	In Progress		
	Fix issues for failed tests	Hao	In Progress		
	Upload test results to Nexus				

Test Results & Analysis:

Test	Result	Applied Fixes	Comment
Lynis	Pass	27 fixed applied, see Steps To Implement Security Scan Requirements	To maintain the pass result, need to restart the server if it's required
Vuls	8 CVEs with score > 9.0 on Ubuntu 18.04		1. Performed the Vuls tests on two other distros as well: 2. Ubuntu 20.04: 4 CVEs with score > 9.0 3. CentOS 8: 3 CVEs with score > 9.0 4. Manually installed 0.9.4 libssh to fix https://nvd.nist.gov/vuln/detail/CVE-2019-14889, but Vuls still shows the same CVE. 5. The bluval code requires all CVEs to be fixed, no matter what the score is.
Kube-Hunter	1. Remote cluster scan passes 2. Remote node scan passes 3. Inside a Pod shows "fail" but not true.	https://aquasecurity.github.io/kube-hunter/kb/KHV002.html https://aquasecurity.github.io/kube-hunter/kb/KHV050.html Disabled CAP_NET_RAW for default pod security context (a tough one to fix!)	KubeEdge edgecore only listens on localhost, so log is not available from another machine. Tried to let edgecore listen on eth0, but kubectl logs still complains about SSL certificate. Workaround: nginx as a reverse proxy, listens on k8s advertised ip, and pass through the traffic to localhost. Added ssl certificate.

Conformance			1. Sonobuoy can test v1.19, but bluval conformance can only test up to v1.16: akraino/validation:kube-conformance-v1.16 2. KubeEdge architecture does not have kubeconfig available at Edge. Workaround is to provide the kubeconfig manually at Edge?