# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

docs.
Cursor parking lot [¬ ]

**Meeting 89**
Regular standing agenda items only

**Attendees:**
- **...**
- **James Carnegie**

**Meeting 88 - canceled**

**Meeting 87**
- **Review PRs**
- **Schedule Andrey and Mariusz presentations * November 7**
  - **Title: Enhancing Zero Trust for Applications with SPIRE: A Developer-Friendly Approach**
- **Kubecon Workload Identity Day**
- **Y2Q - quantum mandatory date, someday in the future**
-

**Meeting 85**
- **A different and new Tornjak demo**

**Meeting 84**
- **Release update**
  - **V1.11**
- **Kubecon**
- **WIMSE https://datatracker.ietf.org/wg/wimse/about/**
- **New web site :) https://ietf-wg-wimse.github.io/**
- **Open discussion**
- **Presentation by Maia Iyer about Tornjak federation**

**Attendees**
**Maia Iyer**
**Edwin Buck**
**Agustín Martínez Fayó**
**Andrey Brito**
**Marcel Levy**
**Mariusz Sabath**
**Deepak**

**Meeting 83**
- **Release update**
  - **V1.11 coming**
- **Kubecon**
- **WIMSE https://datatracker.ietf.org/wg/wimse/about/**
- **Open discussion**

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: Link
Google Group: Link

---

Zoom Meeting: Link

- **Andrey - Hybrid plugin TOFU – not broken**
  - **Follow up in meetings and on RFC doc**
  - **Possible solution - Hierarchical SPIFFE IDs**
  - **Possible solution - maintain the TOFU data on the agent store**
  -

**Attendees**

- **Daniel Feldman**
- **Andrey Brito**
- **Agustín Martínez Fayó**
- **Edwin Buck**
- **Eduardo**
- **Marcel Levy**
- **Marcos Yacob**
- **Sunil Ravipati**

**(meeting canceled in here)**

**Meeting 82 - August 15, 2024**

- **Kubecon**
- **WIMSE –** https://datatracker.ietf.org/wg/wimse/about/
-

**Meeting 81 – August 1, 2024**

- **Release 1.10.1**
- **Kubecon**
- **Open discussion**
- **Andrey**
  - **Opening an RFC for keeping new server side state for hybrid node attestor**
- **Next time Staklok discussion!**

**Meeting 80, Jul 18 2024**

- **Follow up: Tornjak**
- **Follow up: SEV and Hybrid Attestor**
- **Release status**
- **Kubecon Coming Up**
- **(Ben L.) Status update on DelegateAPI changes to allow delegates to trigger attestation:**
  - https://github.com/spiffe/spire-api-sdk/pull/58
  - https://github.com/spiffe/spire/pull/5272
  - **Looking for feedback /review**
  - **Looking for callouts on what's outstanding/needed to move this forward.**
- **Andres Vega discussion**
  - **Working with Hugo Landau to implement PQS in SPIRE**
  - **Project is in early stages**
  - **Focusing on X.509 initially? (Not sure yet)**
- **Open discussion**

**Meeting 79, Jun 20 2024**

- **Release update**

- **10.1 coming soon**
- **No major changes, just cleanup**

- **CNS meeting**
  - **Free tickets!**
- **Kubecon**
  - **CFP is complete for main Kubecon, but zero day events are still open**
- **Hybrid attestor / SEV update from Andrey Brito & Team**
  - **https://github.com/ufcg-lsd/spire-amd-sev-snp-node-attestor**
  -

**Meeting 78**

- This entire meeting was an update for the Tornjak project with different Tornjak team members. The recording is here: https://zoom.us/rec/share/AuJYuR9OtVE2uuvqS69HuSEtx_4nPTp3SOK1bWr9aTffOhA22eo5kxeaPZUOWdOG.t3lVgPTeVmRGyFsv

**Meeting 77**

- Should we still have this meeting?
  - Different frequency? Different time? Different host?
- Release update
  - 1.9.5 and 1.8.11, next scheduled release is 1.9.6
  - new bundle publisher for GCP, enhanced AWS node attestor
- Follow up from last time
- WIMSE
- O-RAN
- RPMs

## Meeting 76

- SSC Election
- Release Update
- WIMSE
- O-RAN
- Ben Leggett discussion on delegated identity in SPIRE https://github.com/spiffe/spire/issues/5019#issuecomment-2073241698 and https://docs.google.com/document/d/1A1oQHuR6z3bvQtXN17r2EwBr5lazGGPbUPkxoURAAh4/edit
  - Goal for Istio/Solo is to use DelegatedAPI to attest an entire process that they pass in from a central agent, but go through all the SPIRE attestation flow
    - The agent is Rust so it can't easily use Go packages
  - Methods that are possible: pass in a static PID, maybe a PIDFD (a newer feature in Linux for uniquely identifying processes), maybe the cgroup ID
  - After a discussion, we decided that PID is probably sufficient and will have the fewest required changes to SPIRE.
  - This will be essentially a new DelegatedAPI. The old one is much simpler because it just takes selectors, which the client needs to gather (and this really only works for Kubernetes).

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

## Meeting 75

- Release update
- SSC Election
- WIMSE
- Question from Hayden - do we support 3rd party plugins? Pointed at Plugin SDK
- Update on SEV support and hybrid node attestors from Davi

## Meeting 74

- **Kubecon review**
- **Release update**
- **SSC**
- **AMD hybrid node attestor?**
- **WIMSE**
- **O-RAN**
- **Look into DB performance improvements under experimental flags**

## Meeting 73

- **Vsecm demo postponed**
- **SEV demo coming up**
- **Hybrid node attestor**
- **O-RAN**
- **WIMSE**
- **Kubecon coming up**
- **SSC Election**
- **Release**
- **Andrey: Can we have numeric selectors for matching > <  or !=? For example for TCB version**

- - Expected (registration):
- cc:svn:latest
- cc:svn:uptodate
- cc:svn:outdated
- cc:svn:unsupported
-
- - Attestation:
- cc:svn:latest --> listed as "UpToDate" in the Intel Trusted Services API
- cc:svn:uptodate --> listed as "UpToDate" in the Intel Trusted Services API
- cc:svn:outdated --> listed as "OutOfDate" in the Intel Trusted Services API
- cc:svn:unsupported --> unlisted
-

**Meeting 72**

- **Vsecm demo next time**
- **SEV demo in future**
- **Kubecon is coming up!**
- **Release update**
- **Andrey update on SEV RFC**
  - **I want to make sure that I'm running on a real AMD processor with real SEV and real boot volume using vTPM. This only applies in the cloud because they rely on the vTPM to do this part of the attestation. There are other mechanisms on non-cloud.**
  - **Options: Wait for the cloud providers to converge; embed vTPM logic into SEV plugin; or use hybrid node attestor plugin**
  - **Not in RFC document yet**
  - **Question: Are vTPMs similar enough across cloud providers to enable this? Not sure**
    - **Answer: Probably yes?**
- **Helm charts nearing 1.0 release**
- **WIMSE/attested claims**
  - **Process of WG being chartered at IETF**

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

**Meeting 71**

- **Andrey & Eduardo - Hybrid Node Attestor RFC update**
- **Volkan - Update from VMWare - possible need for SPIFFE in telco BU**
- **Evan had requested AMD attestation solely (not hybrid attestor) in previous meeting**
    - **(I wasn't there :))**
- **Let's schedule a time to do AMD node attestor demo**
- **Also let's schedule a time for a secrets manager demo**
- **Let's schedule a time to share the database event presentation Feb 27th**
- **Reviewed PRs for 1.9**
- **Reviewed Helm Chart**
- **Ed Buck – proposal to change log levels dynamically**
- **Ed Buck - Update agent cache for JWT-SVID**

**Meeting 70**

- SPIRE Release Update
- Community Day coming up
    - CFP is open!
- SSC Election is now
- Kubecon is coming up
    - Always need volunteers
- Security audit coming up

**Meeting 69**

- No new release since last meeting
- SSC Election – please nominate yourself or others!
- Kubecon presentations announced

- Andrey Brito - Confidential compute node attestor for AMD SEV
    - GH issue https://github.com/spiffe/spire/issues/4469
    - The SP in SEV can provide an Attestation Report usable for SPIRE Node Attestation
    - There is a potential MITM because the Attestation Report is effectively a bearer token
    - Available in AWS and GCP (GCP seems pretty limited right now)
    - Open questions:
        - How to combine SEV and cloud instance identity node attestors?
        - How to combine SNP and vTPM?
        - How do we verify/extend provider disk encryption
        - Azure seems to have a more mature vTPM approach? (
- Fabian Kammel – Confidential compute
    - Demo of node attestor that uses VCEK and VLEK from SEV for a node attestor
    - Can potentially use any field in the attestation report as a node selector
    - https://github.com/datosh/spire/commit/24ce8b2dc1641d1a090c822d8fd5a3f63779bb10
    -

**Attendees:**

- Daniel Feldman
- Andrey Brito
- Agustín Martinez Fayo
- Davi Pontes
- Daniel
- Eduardo
- Evan Gilman
- Fabian Kammel
- Juan Pablo Cabana
- Marcos Yacob
- Mariusz Sabath
- Maxi Churichi
- Nando
- Torin van den Bulk
- Ryan Turner

**Meeting 68**

- Release Update
- Big pull requests and issues
- Office hours Fridays

- Upcoming election
- Rust note
- Support for Thales Luna HSM

**Meeting 67**

- **Release 1.7.1**
- Office Hours Fridays
- Special Presentation from Marco Antonio Marques (USP)
    - Assertions and Tokens
        - Progress on ShoCo-Biscuits
        - ID mode
            - Bind an OAuth token to a front-end token
        - anonymous mode tokens (with different properties)
        - LSVID format
        - Double mode extensions

**Attendees**

- Daniel Feldman
- Marco Marques
- Ronaldo Medeiros
- Agustîn Martinez Fayô
- Cory Sherman
- Damares Cavalcante
- David Henrique da Costa
- Ekarani
- Evan Gilman
- Federico Quijada
- Guilherme Carvalho
- Lucas Cupertino
- Macelo Ribeiro
- Marcos Yacob

- Maxi Churichi
- Nagarajan Jayabal
- Pedro Mendes
- Pedro Ribeiro
- Raphael Agra
- Charles Meirs
- Yogi Porla

**Meeting 66**

- **Next scheduled SPIRE release: 1.7.1**
-

**Attendees**

**Meeting 65**

- **1.7.0 release!**
- **Office Hours Fridays**
- **Special Presentation from Guilherme**
    - **Figure out how to do platform specific integ testing**
    - **Issue 2168 in SPIRE**

**Attendees**

- **Daniel Feldman**

---

Zoom Meeting: Link

- **Matt Bates**
- **Davi Pontes**
- **Eduardo**
- **Vivek**
- **Juan Pablo Cabana**
- **Unnathi Kumar**
- **Victor Vieira**
- **Spencer**
- **Daniel**
- **Agnish Dutta**
- **Ryan Turner**
- **Federico Quijada**
- **Marcos Yacob**
- **Agustin Martinez Fayo**
- **Edwin Buck**
- **Andrey Brito**

**Meeting 64**

- Release 1.7.0 in progress
- Three big projects:
    - Helm charts
    - Attested claims
    - SPIRE core
- Aegis
- Presentations:
    - Community days
    - Kubecon
    - AWS Containers from the Couch
    - Office hours
- Official blog
- Intern projects

**Meeting 63 – May 25 2023**

- Welcome Volkan
- HPE Interns

---

Zoom Meeting: **Link**

- Release 1.6.4
- Office hours
- Presentations:
    - Community days
    - Kubecon
    - Volkan's Twitch Channel
    - AWS Containers from the Couch
    - Office hours
    - Potential blog posts on blog.spiffe.io / reach out to Umair Khan
-

**Meeting 62**

- SSC Election results
    - First vote was a tie
    - Welcome Volkan Ozcelik
- Kubecon videos https://www.youtube.com/watch?v=ySyJ3TCfH04&list=PLj6h78yzYM2PyrvCoOii4rAopBswfz1p7
- Big features in progress
    - Azure KMS
    - Forced rotation
- Follow up on Tekton issue

**Meeting 60- April 27 2023**

- 2023 H1 SSC Election
- Thanks for joining the SPIFFE and SPIRE April 2023 Virtual Meetup!
- SPIRE release update
- [Brandon] Question about SPIRE Workload API TCP endpoint
    - Context: https://github.com/tektoncd/pipeline/issues/6559
    - Mainly around windows use case but there were some complication around it in terms of authenticating the workloads from the endpoint. Found challenges when you need specific access control.
    - For example, for delegate API, would only be an admin endpoint
    - Based on issue, two potential problems
        - Complaints around hostpath
            - CSI driver needs privilege to do bind socket
            - CSI driver attack surface is fairly small (~100s of LOC) - https://github.com/spiffe/spiffe-csi/blob/main/pkg/driver/driver.go
        - Complaints around priv containers
            - Intended to independently audit k8s workloads, needs to intentionally be separate to de-trust k8s. (e.g. reading into TPMs, crypto modules)
    - When looking at TCP generally have harder problems than is easier

**Meeting 59- March 30 2023**

- ELECTIONS!!!
- Meetup – April 13
- Kubecon
- No new releases

**Meeting 58 – March 16 2023**

- No new releases
- SSC election coming up

- Keylime presentation from Mike Peters
    - Proposal to create SPIRE and Keylime plugins to allow SPIRE node attestation using Keylime as a source of truth
    - SPIRE + Keylime
    - Slides: https://drive.google.com/file/d/1UGcS8BzqIGi3rDjBrMGrS-fyO6J_KRka/view?usp=share_link
    - Link to Michael's presentation form CNCF SecurityCon (ZeroTrust Workload Identity in K8s): https://youtu.be/eyj0UCmJfjo

**SIG-SPIRE notes – MEETING 57, March 2 2023**

- 1.6.1 release
- Helm charts are here!!!
- Kubecon coming up
    - Need booth volunteers
- Forced rotation
- New web site
- OpenZiti
- Indeed – Jeremy
    - Namespace scoped vs cluster scoped resources
    - Slack.spiffe.io
    - https://join.slack.com/t/spiffe/shared_invite/zt-1q18yique-YnzPiIAD~7OQ04qcZJvXsA

**Meeting 56**

- Release update 1.5.5
- Kubecon: prep
- Can we help the maintainers more?
- LFX/Google SoC internship
- Big presentation: Marcos Yacob on forced rotation

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

## Meeting 55 February 2 2023

- **Release Update**
- **Cloud Native Security Con**
    - **Presentations from Mariusz Sabath, Brandon Lum, Andres Vega, Emily Fox, & many others from the SPIFFE/SPIRE community**
    - **Avaialble on Youtube in a few weeks**
    - **Many new projects using SPIFFE/SPIRE as a base**
- **Kubecon Amsterdam April 18**
- **New web site**
- **New "speakers list"**
- **Release Update 1.5.4**
    -
- **Request for a quickstart**

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

**[Meeting 53 and 54 notes to be added later]**

## Meeting 52 Dec 8 2022

- Release update
  - 1.5.0
  - 1.5.2
- Helm chart update
- Need more CFPs for Kubecon EU
  - Also need volunteers for booth, etc
- Galadriel update
  - Connect William and Dennis
- Istio support update
- How can we help the maintainers?
  - Open an issue first (Evan)
  - Smaller, more iterative PRs
- Presentation from Davi Andrade at UCFG –
  - Using AMD SEV attestation reports as a SPIRE attestor
  - Slides: SPIRE AMD SEV Plugin

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

**Meeting 51 Nov 10 2022**

- **Release Update**
- **Helm Chart https://github.com/spiffe/spire/issues/2652**
    - **Ping Manoli Yiannakakis, Eli Nesterov, Mariusz Sabath**
- **Kubecon – Videos**
- **Community Day – Videos**
- **Serverless - KNative – (Mariusz)**
    - **KNative does not support UDS sockets – how can we talk to the agent?**
- **AMD encrypted VM hash (Andrey) – how to reduce length from 512 bytes**
- **Tornjak – make new images public – Mariusz**
- **Kubecon EU 2023 – CFP deadline approaching!**

**Attendees**

- Daniel Feldman
- Evan Gilman
- Agustîn Martínez Fayó
- Alan Gonzalez
- Andrew Harding
- Andrey Brito
- Dennis Gove
- Faisal Memon
- Maia Iyer
- Manoli Yiannakakis
- Maros Yacob
- Mariusz Sabath
- Ryan Turner

- Victor Vieira
-

**Meeting 50 October 13 2022**

- Community Day https://spiffecommunityday-fall2022.splashthat.com/
- KubeCon
- Release Update
- Roadmap Changes
    - Daniel will open a PR to update the roadmap https://github.com/spiffe/spire/blob/b10d5f8073ab4a540353b8efdbe59167c769c4af/ROADMAP.md
    - Big Features
        - Federation Plugin Type (HPE)
    - Smaller Features

**Attendees**

- Marcos Yacob (HPE)
- Maxi Churichi (HPE)
- Mariusz Sabath
- Agustîn Martinez Fayó
- Guilherme Carvalho
- Marcos Yacob
- Mohamed Omar
- Ryan Turner
- Sunil Ravipati

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

**Meeting 49 – Sept 29 2022**

- Community Day https://spiffecommunityday-fall2022.splashthat.com/
- KubeCon
- Release Update
- Special Presentation: Mariusz Sabath, Tornjak

**Attendees**

Daniel Feldman
Mariusz Sabath
Andrew Harding
Evan Gilman
Faisal Memon
Maia Iyer
Marcos Yacob
Ryan Turner
Sunil Ravipati
William Barrera
Dennis Gove
Brandon Lum
Eli Nesterov
Mohammed Abdi

**Meeting 48 – Sept 15 2022**

- Graduation/Kubecon
- Community Day – CFP closes TODAY

---

Zoom Meeting: **Link**

- Release Update
- Special Presentation: Project Galadriel (Maximiliano Churichi, Juliano Fantozzi)
    - RFC Design Document: https://bit.ly/galadriel-rfc-design-doc

**Attendees**

- Marcos Yacob (HPE)
- Andrew Harding (VMware)
- Agustín Martínez Fayó (HPE)
- Eugene Weiss (HPE)
- Max Lambrecht (HPE)
- Max Churichi (HPE)
- Anh Thu Vo
- Tim Pletcher
- Caio Milfont
- Eugene Weiss
- Evan Gilman
- Faisal Memon
- Juliano Fantozzi
- Kennith Mohr
- Marcos Yacob
- Max Lambrecht
- Praneetha Manthravadi
- Sunil Ravipati
- William Barrera
- Yogi Porla

**Meeting 47 – Sept 1 2022**

- GRADUATION!!!
    - Need user quotes
- KubeCon
- Cloud Native Security Day
- SPIRE Community Day
    - CFP closes Sept 15, event Nov 3 in San Francisco/zoom
- Official org member badges?
- Release update

**Attendees**

- Andrew Harding (VMware)
- Anh Thu Vo (Marvell)
- Marcos Yacob (HPE)
- Agustín Martínez Fayó (HPE)
- Maxi Churichi (HPE)

**Meeting 46 – August 18 2022**

- SPIRE release update (1.4.1)
    - Node re-attestation feature
    - LRU cache for storing SVIDs in SPIRE Agent
    - Interface for Credential Composer plugins to allow X509-SVID and JWT-SVID field customization

- Update SPIFFE Community Day
    - Date: Nov 3rd, 2022
    - Hybrid Event (SF + Virtual)
    - CFP Close Date- > Sep 15th

**Meeting 45 – August 4 2022**

- 1.3.2 release
- 1.4 release
    - Kubernetes on windows
    - Key types per workload
    - re-attestation is 1.4.1
- Update on KubeCon
- Update on Production Identity Day
- Tornjak demo and discussion

**Meeting 44 – July 21 2022**

- 1.3.2 release
- 1.4 release – node reattestation
- Tornjak demo - new Entries form (next meeting) Mariusz Sabath (IBM)

**Meeting 43 - July 7 2022**

- **1.3.2 release**
- **Open Source Summit (still not on youtube)**
- **Cloud native security day**
  **https://events.linuxfoundation.org/cloud-native-securitycon-north-america/**
- **OpenSSF Supply Chain Security Kit**
  **https://www.techtarget.com/searchitoperations/news/252518401/Citi-donates-software-supply-chain-security-kit-to-OpenSSF**
- **Future community days / meetups?**
- **Maintainership of spiffe-helper**

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

**Meeting 42 – June 23 2022**

- **1.3.2 release**
- **Open Source Summit**
- **OpenZiti**
    - **Andrew Martinez, NetFoundry**
    - **Openziti.org**
    - **Now has support for SPIFFE workload identities using SPIRE**
    - **Additional talks at KubeCon and Developer Week Cloud in September**

**Meeting 41 – June 9 2022**

- Kubecon – Talks available! https://www.youtube.com/playlist?list=PLj6h78yzYM2MCEgkd8zH0vJWF7jdQ-GRR
- SPIRE 1.3.1 release
- Windows discussion
    - https://github.com/cert-manager/csi-driver-spiffe
    - https://www.youtube.com/watch?v=vKRUq56xDiE
    -
- Discussion with Jake and Charlie from JetStack

**Meeting 40 – May 26 2022**

- **Kubecon**
- **Release update**

- **Cole Kennedy – Witness Demo**

**Attendees:**

- **Cole Kennedy**
- **Andrew Harding**
- **Andrew Martinez**
- **Anh Thu Vo**
- **Faisal Memon**
- **Frederick Kautz**
- **Marcos Yacob**
- **Mikhail Swift**
- **Ryan Turner**
- **William Barrera**

**Meeting 39 – May 12 2022**

- **Kubecon**
- **1.3.0 release**
- **Cilium blog post**
  - **https://isovalent.com/blog/post/2022-05-03-servicemesh-security**
- **Hardware root of trust – Mariusz**

**Here are a few useful links from the talk:**

**slides used during the demo:**
**https://github.com/IBM/trusted-service-identity/blob/main/docs/ppt/Secure%20Supply%20Chain.SPIRE.pptx**
**Keylime attestation:**
**https://github.com/IBM/trusted-service-identity/blob/main/docs/spire-keylime-attestion.md**
**script for deploying x509 via Keylime:**
**https://github.com/IBM/trusted-service-identity/blob/main/utils/deployKeys_keylime.sh**

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: Link
Google Group: Link

---

Zoom Meeting: Link

**deploying agents with x509pop:**
**https://github.com/IBM/trusted-service-identity/blob/main/docs/x509-agent.md**
**creating x509 certs for x509pop NodeAttestor:**
**https://github.com/IBM/trusted-service-identity/blob/main/docs/x509-create.md**
**setting up the Workload Registrar with non-k8s Node Attestor:**
**https://github.com/IBM/trusted-service-identity/blob/main/docs/spire-workload-registrar.md#important-for-non-k8s-node-attestors**

**Meeting 38 – April 28 2022**

- **Not much on the agenda this week**
- **1.3.0 release**
- **Kubecon EU**
- RFC on SIGSTORE
    - https://docs.google.com/document/d/1mHW0T4DHPKm6ns6-i3PWZCNZGXcur-UIRGfvnnXwqlA/edit?usp=sharing
- **SSC Election**

**Attendees**

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

**Meeting 37 – April 14 2022**

- New release! Security fixes
- Open Programmable Infrastructure
- RFC on SIGSTORE
    - https://docs.google.com/document/d/1mHW0T4DHPKm6ns6-i3PWZCNZGXcur-UIRGfvnnXwqlA/edit?usp=sharing
- Istio blog post
- Incubating projects showcase – watch on youtube https://bit.ly/37WST8i
- Kubecon EU
- SSC Elections

**Attendees**
Daniel Feldman
Anh Tu Vo
Evan Gilman
Marcos Yacob
Abraham Jerry Kakooza
Agustin Martinez Fayo
Andrew Moore
Deepak Khetwal
Ryan Turner

**Meeting 36 – March 31 2022**

- **Release update 1.2.2**
- Logging open issue #2865

- **Windows support update**
    - **Planning 1.3**
- **KubeCon Europe talks**
    - Real World SPIFFE Scenarios and Outcomes - Andres Vega & Frederick Kautz,

      SPIFFE Steering Committee

    - Multi-Cloud Workload Identity With SPIFFE - Jake Sanders & Charlie Egan, Jetstack

- SPIRE: Intro & Deep Dive Into Windows Support - Agustín Martínez Fayó & Marcos Yacob, Hewlett Packard Enterprise
- Don't forget to propose talks for KubeCon NA

- SIGSTORE document
- Istio PR for SPIRE support

**Meeting 35 – March 17 2022**

- 1.2.1 release coming soon
- Congratulations to Marcos Yacob as new maintainer!
- Liam - can we do better logging?
  - Evan- needs to be improved, can we have a guideline document?
- SIGSTORE workload attestor demo & discussion

**Attendees**

- Ryan Turner (Uber)

---

Zoom Meeting: Link

- Liam Decker (Indeed)
- Evan Gilman (VMware)
- Andrew Harding (VMware)
- Marcos Yacob (HPE)
- Alan Gonzalez (Plume)
- Mariusz Sabath (IBM)
- Anh Thu Vo (Marvell)
- Faisal Memon (HPE)
- Matteus Silva (UFCG)
- Thiago Jamir e Silva (C.E.S.A.R)
- Agustín Martínez Fayó (HPE)

**Meeting 34 – March 3 2022**

We just had a SPIRE Virtual Meetup on Tuesday with several presentations from the community. So this meeting will be short.

- Release update - 1.2.1
- SPIRE Virtual Meetup recording
- SPIRE+Kubernetes+SIGSTORE update

**Attendees**

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

### Meeting 33

- Tekton Chains with SPIRE for SLSA 3 update and discussion -Parth Patel, Brandon Lum
    - CSI, signing provenance, kubernetes registrar

### Meeting 32 – Feb 3 2022

- Demo session – Mariusz Sabath
    - NodeJS and Python, authenticating to MySQL, using credentials stored in Vault, with access to Vault negotiated through SPIRE, with a Tornjak UI
    - Link to the Sidecar docs: https://github.com/IBM/trusted-service-identity/blob/main/examples/spire-sidecar/

### Meeting 31 - January 20 2022

- 1.2 release
- Kubecon Europe May 4
- **Windows**

### Meeting 30 – January 6 2022

- Next release - 1.2
    - Svidstore
- Windows support?
- Serverless blog post
- Ongoing work on SIGSTORE integration
- Istio update
- Confidential compute update
- Kubecon Europe May 4

### Attendees

- Evan Gilman (VMware)
- Daniel Feldman (HPE)
- Agustin Martinez Fayo (HPE)
- Marcos Yacob (HPE)
- Andrew Harding (VMware)
- Anh Thu Vo (Marvell)
- Zachary Train (Uber)
- Ryan Turner (Uber)
- Mariusz Sabath (IBM)
- …

**Meeting 29 – December 23 2021**

- Due to the holidays, this meeting was very brief and had no agenda items. We're just trying to keep a consistent meeting schedule.

**Attendees:**

- Daniel Feldman
- Agustín Martínez Fayó
- Marcos Yacob

**Meeting 28 -- December 9 2021**

- Zoom link Here
- Release update for v1.1.2
- Discuss SVID Hints
    - Needs a new DB column
    - Probably target 1.2 to do migration and 1.3 to enable the feature
    - Maintainer team is planning to add feature flags, which would make this a faster process
- Azure Key vault SVIDStore/Confidential computing plugin–Matteus, Andrey (UFCG)
    - For SCONE integration, current SVIDStore plugin is tied in tightly with SCONE-specific APIs
    - The UFCG team would like to support other confidential compute platforms than SCONE

- An Azure Key Vault plugin would be a good solution, since most of the confidential compute platforms are integrated with Azure and have access to that API
- How will we ship the bundles (including federated bundles)?

**Attendees**

- Andrew Moore (Uber)
- Matteus Silva (UFCG/Scontain)
- Ryan Turner (Uber)
- Marcos Yacob (HPE)
- Max Churichi (HPE)
- Daniel Feldman (HPE)
- Anh Thu Vo
- Agustín Martínez Fayó
- Alexander Viktorov
- Andrew Harding
- Evan Gilman
- Faisal Memon
- Praneetha Manthravardi
- Ryan Turner
- Zachary Train

**November 25 2021 meeting CANCELED due to US Thanksgiving Day**

### Meeting 27 -- November 11 2021

- Zoom link Here
- Release update for v1.1.1
- Upcoming meetup https://spiffeandspirenov2021virtualme.splashthat.com/
- Election
- Cray helm charts https://github.com/Cray-HPE/cray-spire
- Tornjak quick update

### Attendees

- Mysteries abound

### Meeting 26 - October 28 2021

- Zoom link Here
- Release update
- Elections
- Progress on Kubernetes Operator
- Meetups?
    - Maybe once a quarter
    - Message Umair
    - NSM

### Attendees

- Evan Gilman (VMware)
- Marcos Yacob (HPE)
- Ryan Turner (Uber)
- Glaucimar Aguiar (HPE)
- Agustín Martínez Fayó (HPE)
- Andrew Harding (VMware)

### Meeting 25 - October 14 2021

- Zoom Link: **Here**

### Agenda

- **Production Identity Day Recap**
- **Release update**

### Attendees

-

### Meeting 24 -- September 30 2021

- Zoom Link: **Here**

### Agenda

- Release update - 1.1.0
- Production Identity Day
- Presentation on Kubernetes SIGSTORE plugin RFC -- Glaucimar Aguiar, Thiago Jamir
    - RFC is here, please comment!

### Attendees

- Andrew Moore (Uber)
- Marcos Yacob (HPE)
- Matteus Silva
- Andrew Harding (VMware)
- Glaucimar Aguiar (HPE)
- Ryan Turner (Uber)
- Max Churichi (HPE)
- Rodrigo Lopes (CESAR)
- Alexander Viktorov (Uber)

- Mariano Kunzi (HPE)
- Marcus vinicius Silva (CESAR)
- Willian Alves (CESAR)
- Otávio Silva (CESAR)
- Thiago Jamir (CESAR)

### Meeting 23 -- September 16 2021

- Zoom Link: **Here**

### Agenda

- Release Update
    - 1.1 planned release in October
- Production Identity Day -- Schedule Live
- Federation API Github Project
    - trust-domain-api-contribs channel on slack
    - Needs to be done by Kubecon
- Sigstore workload attestor
- Questions about Azure NodeAttestor + Selectors
    - Github issue

### Attendees

- Daniel Feldman HPE
- Agustín Martínez Fayó (HPE)
- Matteus Silva (UFCG)
- Evan Gilman (VMware)
- Brandon Lum (IBM)
- Madhukesh Wali (HPE)
- Max Churichi (HPE)
- Glaucimar Aguiar (HPE)

- Marcos Yacob (HPE)
- Ryan Turner (Uber)
- Mariano Kunzi (HPE)

### Meeting 22 -- September 2 2021

- Zoom Link: **Here**

### Agenda

- **Release Update**
    - **1.0.2 coming soon**
    - **New release process coming with 1.1**
- **Production Identity Day Update**

### Attendees

- Evan Gilman (VMware)
- Matteus Silva (UFCG)
- Andrey Brito (UFCG)
- Marcos Yacob (HPE)
- Eugene Weiss (HPE)
- Marcos Yedro (HPE)

---

Zoom Meeting: Link

- Andrew Harding (VMware)
- Rahul Jadhav (Accuknox)
- Max Lambrecht (HPE)
- Glaucimar Aguiar (HPE)
- Daniel Feldman (HPE)
- Agustín Martínez Fayó (HPE)
- Max Churichi (HPE)

**Meeting 21 -- August 19 2021**

- Zoom Link: **Here**

**Agenda**

- Release update
- Production Identity Day Update
    - Basic schedule finalized
    - Tell your friends to attend!
- Authenticating Envoy Connections with Federated SPIRE Trust Bundles -- Marcos Yacob HPE
- How to make remote workload registration? -- Benardi UFCG
    - Testing namespacing in SPIRE RBAC's PR

**Attendees**

**Sunil Ravipati - Anthem.ai**

---

Zoom Meeting: **Link**

- Andrew Moore (Uber)
- Evan Gilman (VMware)
- Andrew Harding (VMware)
- Brandon Lum (IBM)
- Matteus Silva (UFCG)
- Benardi Nunes (UFCG)
- Andrey Brito (UFCG)
- Ryan Turner (Uber)
- Brian Martin (Gradient)
- Agustín Martínez Fayó (HPE)
- Max Churichi (HPE)
- Marcos Yedro (HPE)
- Marcos Yacob (HPE)

## Meeting 20 -- August 05 2021

### Logistics

- Zoom Link: **Here**
- Recording: **Here**

### Agenda

- Release Update
- Production Identity Day Update
- Tornjak Demo - Brandon Lum, Mariusz Sabath
- Accuknox demo - Cilium and Spire Integration - Raphael Campos, Rahul Jadhav, Thiago Navarro
    - Slides https://docs.google.com/presentation/d/1A6r9HJ05Movi5ExVQRrJyQ2hu11gubAmdxXOK3Zlb_M/edit?usp=sharing
    - Github https://github.com/accuknox/cilium-spire-tutorials

### Attendees

- Thiago Navarro - Accuknox
- Brandon Lum - IBM

---

Zoom Meeting: **Link**

- Marcos Yacob - HPE
- Rahul Jadhav - Accuknox
- Mariusz Sabath - IBM
- Steve Anderson - HPE
- Max Lambrecht - HPE
- Max Churichi- HPE
- Andrey Brito - UFCG
- Karthik Prabhakar
- Asif Ali
- Maia Iyer
- Raphael Campos
- Mohammed Abdi
- Rahul Jadhav
- Mariano Kunzi
- Max Lambrecht
- Eugene Weiss
- Andres Vega
- Ryan Turner
- Thiago Navarro
- Sunil Ravipati
- Thales Paiva

## Meeting 19 -- July 22 2021

### Logistics

- Zoom Link: **Here**

### Agenda

- Prod Identity Day -- October 11, LA Convention Center
    - CFP open!
    - Hybrid event
    - Also looking for sponsors

---

Zoom Meeting: **Link**

- 1.0.1 release status
- SGX demo -- feedback request - demo
- Heads up - Tornjak Demo next time!

**Attendees**

- Andrew Moore (Uber)
- Matteus Silva (UFCG)
- Andrey Brito (UFCG)
- Evan Gilman (VMware)
- Marcos Yacob (HPE)
- Glaucimar Aguiar (HPE)
- Rahul Jadhav (Accuknox)
- Thiago Navarro (Accuknox)
- Raphael Campos (Accuknox)
- Brandon Lum (IBM)
- Andrew Harding (VMware)
- Marcos Yedro (HPE)
- Max Churichi (HPE)
- Agustín Martínez Fayó (HPE)
- Max Lambrecht (HPE)

## Meeting 18 -- july 8 2021 10:30 PT

### Logistics

- Zoom Link: **Here**

**Agenda**

- Prod Identity Day -- October 11, LA Convention Center
    - CFP open!
    - Hybrid event
    - Also looking for sponsors
- Release Update
- 1.0 Release Celebration!
- Matteus & Andrey -- SGX (Link to slides, Link to Github)

**Attendees**

---

Zoom Meeting: Link

- Daniel Feldman
- Matteus Silva (UFCG)
- Andrew Moore (Uber)
- Andrey Brito (UFCG)
- Evan Gilman (VMware)
- Brian Martin (HPE)
- Marcos Yedro (HPE)
- Marcos Yacob (HPE)
- Ryan Turner (Uber)
- Eugene Weiss (HPE)
- Agustín Martínez Fayó (HPE)

\

## Meeting 17 -- june 24 2021 10:30 PT

### Logistics

- Zoom Link: **Here**

### Attendees

- Daniel Feldman
- Matteus Silva (UFCG)
- Eugene Weiss
- Brandon Lum
- Mariusz Sabath (IBM)
- Marcos Yacob (HPE)
- Marcos Yedro (HPE)
- Benardi Nunes (UFCG)

---

Zoom Meeting: **Link**

- Andrey Brito (UFCG)
- Andrew Moore (Uber)
- Ryan Turner (Uber)
- Agustín Martínez Fayó (HPE)
- Andrew Harding (VMware)

**Agenda**

- Prod Identity Day Update
- SPIFFE June Meetup -- youtube?
- SPIFFE July Meetup
- Release status -- picking a commit soon!
- Datastore perf and KV update (Brian)
- Registration RBAC update (issue, pr1) (Brandon)
- Kubernetes SPIFFE ID templates/formatting (Brandon and Mariusz proposal) (issue, sample code)
- Kafka Spiffe Principal (repo/fork) (Bernardi)
-

## Meeting 16 -- June 10 2021 10:30 PT

### Logistics

- Zoom Link: **Here**

**Attendees**

- Daniel Feldman
- Brian Martin (HPE)
- Ryan Turner (Uber)
- Andrew Moore (Uber)
- Andrey Brito
- Brandon Lum
- Matteus Silva
- Agustín Martínez Fayó (HPE)
- Andrew Harding (VMware)
- Max Lambrecht (HPE)
- Mariusz Sabath (IBM)
- Maximiliano Churichi (HPE)

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

## Agenda

- Production Identity Day -- October 11 2021, Los Angeles Convention Center (Day Before Kubecon US) (Hybrid In-person/Online Event) -- looking for presenters/volunteers!
- SPIFFE Meetup June Recap (Youtube soon)
- Contributor syncups
- Release status
- Datastore perf and KV update
- Registration RBAC update (issue, pr1)
- Kubernetes SPIFFE ID templates/formatting (Brandon and Mariusz proposal)

## Meeting 15 -- May 27 2021 10:30 PT

### Logistics

- Zoom Link: **Here**

## Attendees

- Andres Gomez Coronel
- Andrew Harding
- Brandon Lum
- Brian Martin

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

- Daniel Feldman
- Eugene Weiss
- Evan Gilman
- Faisal Maimon
- Gustavo Coelho
- Marcos Yacob
- Marcos Yedro
- Mariano Kunzi
- Matteus Silva
- Max Churichi
- Max Lambrecht

**Agenda**

- Production Identity Day -- October 11 2021, Los Angeles Convention Center (Day Before Kubecon US) (Hybrid In-person/Online Event) -- looking for presenters/volunteers!
- SPIFFE Meetup June https://spiffe-spire-june21.splashthat.com/
- Contributor syncups
- Release status -- Andrew Harding
- SIG-SPEC update
    - Federation
    - Limited format for spiffe ids
    - Order multiple svids (big project)
- Marcos Yacob
    - Audit logs
    - Filter field in List* APIs
- Brian Martin --
    - Extend CLI node evict command to allow evicting nodes more easily
    - Short term plan, longer term plan

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

## Meeting 14 -- May 13 2021 10:30 PT

### Logistics

- Zoom Link: **Here**

### Attendees

- Evan Gilman (VMware)
- Glaucimar Aguiar (HPE)
- Matteus Silva (UFCG)

### Agenda

- **SSC Election**
- **Kubecon wrapup**
- **Production Identity Day**
- **Upcoming meetup**
- **Contributor syncups**
- **Releases**
    - **0.12.3**
    - **1.0**
- **SIG-SPEC**
- **Federation Management API - Agustín**
    -
    - https://github.com/spiffe/spire/projects/11
- **Automated Schema definition for k8s workload registrar - Brandon/Mariusz**
    - **https://github.com/spiffe/spire/issues/2280**
    - **https://github.com/IBM/trusted-service-identity/pull/95/files**

- **Brian -- Datastore**
- **Brian -- SVID order**
    - **https://github.com/spiffe/spiffe/pull/179**

## Meeting 13 -- April 29 2021 10:30 PT

### Logistics

- Zoom Link: **Here**

### Attendees

- Benardi Nunes (UFCG)
- Evan Gilman (VMware)
- Andrew Moore (Uber)
- Mauricio Vásquez (Kinvolk/AccuKnox)
- Andrew Harding (VMware)
- Brandon Lum (IBM)
- Mariusz Sabath (IBM)
- Ryan Turner (Uber)
- Marcos Yacob (HPE)
- Maximiliano Churichi (HPE)
- Max Lambrecht (HPE)
- Marcos Yedro (HPE)
- Eugene Weiss (HPE)
- Daniel Feldman (HPE)
- Chuck Fuqua (HPE)
- Rahul Jadhav (Accuknox)
- Sachin Singh (GGSIPU)
- Agustín Martínez Fayó (HPE)

### Agenda

- **SSC Election status**

    - https://github.com/spiffe/spiffe/issues/160
- **Next meetup -- 1st week of June**
- **Kubecon**
    - **Boxboat talk**
    - **Office hours**
- **Release status -- 0.12.3 - https://github.com/spiffe/spire/milestone/9?closed=1**
- **Madhu Wali --** improvements to AWS node attestor for multiple accounts with a single SPIRE server ?
- **Mauricio Vásquez** (Kinvolk/AccuKnox) - "Identity issuance delegation" regarding Cilium-SPIFFE integration. (Slack message for more context). Slides here.

**[SHARED] Cilium-SPIFFE Design Document**

### Meeting 12 -- April 15 2021 10:30-11:30 PT

**Logistics**

- Zoom Link: **Here**

**Attendees**

- Andrew Moore (Uber)
- Ryan Turner (Uber)
- Max Lambrecht (HPE)
- Glaucoma Aguiar (HPE)
- Andrey Brito (UFCG)
- Matteus Silva (UFCG)
- Brad Blackard (Uber)
- Brandon Lum (IBM)
- Mariusz Sabath (IBM)
- Brian Martin (HPE)
- Marcos Yedro (HPE)
- Marcos Yacob (HPE)
- Maximiliano Churichi (HPE)

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

- Andrew Harding (VMware)
- Agustín Martínez Fayó (HPE)
- Daniel Feldman (HPE)

**Agenda**

- Spike Curtis -- SIG-SPEC update
    - Federation Doc
    - Valid characters in a SPIFFE ID
    - Next Generation Token
    - Hints in workload API for which SVID to use when there are several choices
- Meetups, conferences upcoming
    - Kubecon
    - CFPs
    - April 21 HPE Dev presentation, later April HPE Workshop, any others?
- SPIFFE Steering Committee Elections
    - Currently in nomination period, 2 seats open, contributors who meet eligibility criteria can nominate & be nominated
- Update on release status (Agustín/maintainers)
    - 0.12.2 released, a few new features & many bug fixes
    - 1.0 is next release planned
    - Quick note on default branch name change
- Marcos Yacob -- Audit Log
- Marcos Yedro -- DevID
- Brian Martin -- Datastore interface refactor
- Mariusz Sabath, Brandon Lum -- Project Tornjak (https://github.com/lumjjb/tornjak/issues/28)
- Daniel Feldman -- helm charts

## Meeting 11 -- April 1 2021 @ 10:30-11:30 PT

### Logistics

- Zoom Link: **Here**

## Agenda

- Shorter meeting due to holidays in several countries
- Advertise Kubecon talks: Andrés Vega https://sched.co/iE8T, Cole Kennedy & Mikhail Swift https://sched.co/iRn2 , 5 min HPE lightning talk
- Meetups!
- Update on release status (maintainers)
- Serverless Update -- Marcos Yacob
- TPM DevID Node Attestor Update -- Marcos Yedro
- Brian Martin - Performance/Scale Update for KV store
- Mariano Kunzi KMS plugin update (Mariano can't attend but he sent a message)
- Brandon Lum -- Tornjak Update (https://www.youtube.com/watch?v=JvukBpf4Qkc)
    - Working to put in SPIFFE org on Github
- Matteus Silva -- SGX
    - Agent running on top of SGX (with SCONE)
    - Problems compiling SPIRE server with gcc-go
    - Encryption of agent files?
- Adam Amridin PR on k8s-workload-registrar
- Add RBAC to rotation of updates? (https://github.com/spiffe/spire/issues/1975)
- Madhu -- how do we align SPIFFE SIG-SPEC and SPIRE? Token 2.0? Other SIG-SPEC improvements? Should we add to the standing agenda?
    - Update from Evan -- currently researching existing technologies for Token 2.0
    - Possible changes to SPIFFE ID spec to limit legal characters to reduce potential security vulnerabilities (some of it is already implemented in SPIRE)
    - SPIRE issues around default SVIDs ("Default SVIDs")

## Attendees

- Daniel Feldman (facilitating)
- Brian Martin (HPE)
- Brandon Lum (IBM)
- Glaucimar Aguiar (HPE)
- Andrey Brito (UFCG)
- Matteus Silva (UFCG)
- Eugene Weiss (HPE)
- Ryan Turner (Uber)

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

## Meeting 10 -- March 18 2021 @ 10:30-11:30 PT

### Logistics

- Zoom Link: **Here**

## Agenda

- Security update
- Upcoming: regularly-scheduled Spire 101 webinars for beginners, first one March 23
- Advertise Kubecon talks: Andrés Vega https://sched.co/iE8T, Cole Kennedy & Mikhail Swift https://sched.co/iRn2 , 5 min HPE lightning talk
- Enabling plugin versioning https://github.com/spiffe/spire/issues/2153 -- Andrew Harding
    - This will require code changes in any existing plugins
    - There will be a doc explaining the process
    - Builtin plugins will be updated in main repo of course (including KMS)
- 0.12 Release update -- Agustín Martinez Fayo
- C-SPIFFE and py-spiffe update -- Glaucimar Aguiar, Rodrigo Carvalho
    - Both are in progress
    - Open source under HPE repo, we might be able to push into the CNCF SPIFFE repo eventually
- Serverless Update -- Marcos Yacob
    - This is getting close
    - Some questions about how it will scale
- TPM DevID Node Attestor Update -- Marcos Yedro
    - Draft PR is waiting for feedback
- KMS plugin status https://github.com/spiffe/spire/pull/2066
    - Main issue outstanding -- will it leave behind extra keys in KMS after scale-down events. Trying to get this plugin into 0.12.3 release very soon
- Performance and scale questions -- Brian Martin
    - We wanted to know roughly how large to test. It sounds like “several hundred thousand” agents is a typical install in large environments.
    - The DB caching in 0.12 should help a lot

    - Work is underway to evaluate options for reducing the cost of API authorization checks without leading to security weaknesses
    - Uber does internal load testing with lightweight mock SPIRE agents, we may be able to copy this for open source to reduce cost of scale testing
- Distribution -- Helm chart, RPM instead of just Docker images
    - No plans

Facilitator Daniel Feldman

### Attendees

- Brian Martin (HPE)
- Max Lambrecht (HPE)
- Marcos Yedro (HPE)
- Glaucimar Aguiar (HPE)
- Eugene Weiss (HPE)
- Ryan Turner (Uber)
- Madhukesh Wali (HPE)
- Agustín Martínez Fayó (HPE)
- Maximiliano Churichi (HPE)
- Andres Gomez Coronel (HPE)
- Rodrigo Lopes de Carvalho (CESAR)
- Matteus Silva (UFCG)
- Ariana Lima (CESAR)
- Andrew Harding (VMware)

---

## Meeting 9 -- March 4 2021 @ 10:30-11:30 PT

### Logistics

- Zoom Link: **Here**

### Agenda

- Advertisement for upcoming meetup March 17
  https://spiffe-spire-meetup-March-2021.splashthat.com
- Also upcoming: regularly-scheduled Spire 101 webinars for beginners
- Quick update for Agustín Martinez Fayo on 1.0 release
    - 0.12 will contain most of the outstanding PRs. We do not have an ETA yet.

    - 1.0 will be about 1 month after 0.12, and will contain any minor fixes that come up post-0.12
- Quick update from Marcos Yedro -- TPM DevID Node Attestor
- Quick update from Brian Martin on performance/scale testing for KV store backend
    - This is a large project that will probably be phased in over 2-3 release cycles post 1.0
- Mariano Kunzi -- AWS KMS plugin
- Tornjak project (SPIRE server UI/management) - Brandon Lum, Mariusz Sabath
    - Tornjak is looking for volunteers, especially volunteers who know React. Get in touch with Brandon

## Action Items

- None, we are all anxiously awaiting the 0.12 release :)
- Invite your friends and coworkers to the SPIRE meetup on March 17!

## Facilitators

Daniel Feldman HPE

## Attendees

- Andrew Moore (Uber)
- Eugene Weiss (HPE)
- Max Lambrecht (HPE)
- Marcos Yacob (HPE)
- Mariusz Sabath (IBM)
- Matteus Silva (UFCG)
- Ryan Turner (Uber)
- Brian Martin (HPE)
- Brandon Lum (IBM)
- Maximiliano Churichi (HPE)
- Marcos Yedro (HPE)
- Glaucimar Aguiar (HPE)

## Meeting 8 -- February 18 2021 @ 10:30-11:30 PT

**Logistics**

- Zoom Link: **Here**

**Agenda**

- Invite everyone to meetups and community day
- Review Action Items from last week
    - Kubernetes Unique Cluster IDs
- Agustin Martinez Fayo - SPIRE 1.0 Release
    - Now doing a 0.12 release first with more community PRs, and later a 1.0 release
    - Question from Brian: Is the API stable and mature? Andrew Harding: Yes. Evan: we won't be guaranteeing API backwards compatibility right away after 1.0 anyway
- Richard Fine - embedded devices & SPIRE
    - Goal: Run SPIRE components on exotic platforms like iOS, nintendo switch dev kits, etc (possibly a stripped down version?)
    - https://golang.org/misc/ios/README
- Brian Martin -- Progress on database refactor
    - https://docs.google.com/document/d/130i5UdJOWcgn7kpogYSEL9ip0p2fmthdfvHQvTa4U_U/edit#
    - Etcd seems to have good performance so far
    - There's an open question about how aggressively we should cache node authorization queries. This can be one of our most expensive queries at scale so we would like to cache it, but we don't want to increase the window during which there could be a race between an agent renewing and an attacker who has compromised agent credentials. Currently in mainline this is not cached at all, but puts a lot of additional load on the DB.
- Marcos Yacob -- Serverless support
    - There are several open PRs for server and agent side changes, with open comments
    - Open questions on what regions to enable serverless SVIDs in
    - Not sure how to do integration tests/CICD
    - Additional challenges on Azure
    - Andrew Harding : Maybe don't use protobufs to communicate to the functions, since they then have to have the protobuf unmarshalling code?
- Matteus Silva -- Support for confidential workloads with SGX

**Action Items for Next Meeting:**

None, all of these projects are still in progress

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

### Facilitators
Daniel Feldman

### Attendees
- Andrew Moore (Uber)
- Ryan Turner (Uber)
- Brandon Lum (IBM)
- Marcos Yacob (HPE)
- Andrey Brito (UFCG)
- Richard Fine (Unity Technologies)
- Max Lambrecht (HPE)
- Maximiliano Churichi (HPE)
- Brad Blackard (UBER)
- Evan Gilman (VMware)
- Matteus Silva (UFCG)
- Luciano Zablocki (HPE)
- Agustín Martínez Fayó (HPE)
- Brian Martin (HPE)

## Meeting 7 --February 4 2021 @ 10:30-11:30am PT

### Logistics
- Zoom Link: **Here**

### Agenda
- Discuss project direction and near-term roadmap
- Review AIs

    - Datastore progress
    - 3-note etcd cluster on AWS c5d.9xlarge with TLS is showing 15-18,000 PUT ops/sec and 64-72,000 GET ops/sec with random 256 byte keys and 1024 byte data.
    - The reference implementation is Attested Node calls (node.go) if you'd like to check it out and/or comment. Nodes and Bundles are all passing current integration tests.
    - https://github.com/bri365/spire/blob/ds-refactor/pkg/server/store/node.go
    - The etcd-specific implementation is only about 130 lines of code
    - https://github.com/bri365/spire/blob/ds-refactor/pkg/server/plugin/store/etcd/etcd.go
- New items
    - k8s unique cluster IDs https://github.com/kubernetes/kubernetes/issues/77487
    - https://groups.google.com/g/kubernetes-sig-multicluster

**Facilitators**

- Andres Vega
- Daniel Feldman

**Attendees**

- Andrew Moore (Uber)
- Ryan Turner (Uber)
- Brian Martin (HPE)
- Brandon Lum (IBM)
- Mariusz Sabath (IBM)
- Dórian Langbeck (HPE)
- Evan Gilman (VMware)
- Andrew Harding (VMware)
- Agustín Martínez Fayó (HPE)

- Eugene Weiss (HPE)
- Marcos Yedro (HPE)
- Luciano Zablocki (HPE)
- Matteus Silva (UFCG)

## Meeting 6 -- January 21 2021 @ 10:30-11:30am PT

**Logistics**

- Zoom Link: **Here**

**Facilitator**

- Daniel Feldman

**Attendees**

- Daniel Feldman

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

- Matteus Silva (UFCG)
- Andrew Moore (Uber)
- Andres Vega
- Brandon Lum (IBM)
- Marcos Yedro (HPE)
- Andrey Brito (UFCG)
- Max Lambrecht (HPE)
- Marcos Yacob (HPE)
- Evan Gilman (VMware)
- Andrew Harding (VMware)
- Luciano Zablocki (HPE)
- Lucas Cavalcante (UFCG)
- Andres Gomez Coronel (HPE)
- Brian Martin (HPE)
- Ryan Turner (Uber)
- Eugene Weiss (HPE)
- Dórian Langbeck (HPE)
- Mariano Kunzi (HPE)
- Agustín Martínez Fayó (HPE)

**Agenda**

- Review AIs -- [Evan] 802.1AR and associated TCG specs, data migration proposal
    - We can probably use the X509 PoP node attestor, but we're not sure yet. Evan and Marcos will keep working on it.
    - Datastore proposal -- still in discussion . We're not spending too much time on the migration aspect specifically yet, K8S registrar may take care of it for many users automatically.
- Update on serverless architecture support (#1843) (Agustín Martínez Fayó - HPE)
    - Waiting for review on the fork, demo video is available
    - Concern about exactly how the selectors should work (SVID store vs others), is it bad to validate the selector strings in the server
    - Create a Github project (issue tracker)
    - Merge this after 1.0
- Support for confidential workloads (#1989) (Matteus Silva / Andrey Brito - UFCG)
    - How do we push new certs/bundles down to the SCONE environment? Just restart it?
- AWS KMS server keymanager plugin (Mariano)
    - Timeouts already added to the core to support this. Might add retries but currently not planning to.
- DS update - etcd perf (Brian)
- SPIRE API manager (Brandon, Mariusz)

**Action Items**

- Review 802.1AR and associated TCG specs [ Evan & Marcos ] X
- Add a Github issue comment to discuss how the SVID store should work [ Evan ] X

- Add a Github issue comment to discuss the confidential workload project [ Evan ] X
- Create a Github issue tracker for the serverless architecture support project [ Agustín and Marcos ] X
- Close issue 1964 -- adding retries to the server keymanager operations, we've decided that will be the responsibility of the plugin [Mariano] X
- Add etcd perf data to datastore proposal [Brian]

## Meeting #5: Nov 12 2020 @ 10:30-11:30am PT

**Logistics**

- Zoom Link: **Here**

**Attendees**

- Agustín Martínez Fayó (HPE)
- Brian Martin (HPE)
- Marcos Yedro (HPE)
- Andrew Harding (VMware)
- Andrew Moore (Uber)
- Marcos Yacob (HPE)
- Evan Gilman (VMware)
- Brandon Lum (IBM)
- Eugene Weiss (HPE)
- Max Lambrecht (HPE)
- Glaucimar Aguiar (HPE)
- Michael Weissbacher (Square)
- Ryan Turner (Uber)
- Luciano Zablocki (HPE)
- Andres Gomez Coronel (HPE)
- Maximiliano Churichi (HPE)
- Matteus Silva (UFCG)

**Agenda**

- Review AIs
- Update on approaches for serverless architecture support (#1843 - Design considerations) (Agustín Martínez Fayó - HPE)
- ...

**Action items**

- [Evan/Andrew] Complete review of .1AR and associated TCG specs
- [Evan] Review data migration proposal from Brian
- ...

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

## Meeting #4: Oct 29 2020 @ 10:30-11:30am PT

**Logistics**

- Zoom Link: **Here**

**Attendees**

- Evan Gilman (VMware)
- Andrew Moore (Uber)
- Ryan Turner (Uber)
- Brian Martin (HPE)
- Eugene Weiss (HPE)
- Andrew Harding (VMware)
- Andres Gomez Coronel (HPE)
- Max Lambrecht (HPE)
- Marcos Yedro (HPE)
- Steve Anderson (HPE)
- Maximiliano Churichi (HPE)
- Alex Viktorov (Uber)
- Agustín Martínez Fayó (HPE)
- Mariano Kunzi (HPE)
- Michael Weissbacher (Square)

**Agenda**

- Review AIs
- TPM node attestor proposal (#1003) (Marcos Yedro - HPE)
- Support pluggable KV and SQL stores (#1945)
- Serverless architecture support (#1843) - Pull vs Push model (Agustín Martínez Fayó - HPE)
  Design considerations

**Action items**

- [Marcos Yedro] Analyze and propose strategies for the feedback received about the TPM node attestor proposal.
  - Consider exposing PCRs values as selectors.
  - Consider using a challenge that ensures we are talking to a real TPM.

## Meeting #3: Oct 15 2020 @ 10:30-11:30am PT

**Logistics**

- Zoom Link: **Here**

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

**Attendees**

- Andres Vega
- Evan Gilman (VMware)
- Brian Martin (HPE) Datastore refactor, negating selectors (1833)
- Ryan Turner (Uber)
- Andrew Moore (Uber)
- Marcos Yacob (HPE)
- Marcos Yedro (HPE)
- Agustín Martínez Fayó (HPE) Serverless architecture support - current status
- Eugene Weiss (HPE)
- Andrew Harding (VMware)
- Eli Nesterov (ByteDance) - (spire server DS caching preliminary data points)
- Mariano Kunzi (HPE)

**Agenda**

- SPIFFE/SPIRE day at Kubecon November 17 - registration through main Kubecon
    - Call For Proposals: https://docs.google.com/forms/d/1oS8KGc5CParYUZ31BAtupauYo8rEoXRd9bREND7tuME/viewform?edit_requested=true
- Security audit by ? starting CW03 and CW04
- Review AIs
-

**Action items**

- [Agustin, Marcos Y] Add API protos and plugin protos to the exchange proposal [link]
    - Worked examples of selectors and entry arrangement would be great too
- [Agustin, Andres] Collect user requirements on the serverless use case to help determine appropriate pro/con tradeoffs
- [Evan] Review and leave notes on certificate transparency RFC
    - Plugin vs core
- [Mariano] Share preliminary research around AWS KMS keymanager
    - Failure Modes link
    - Step-by-step rotation link
- ...

## Meeting #2: Oct 1 2020 @ 10:30-11:30am PT

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

### Logistics

- Zoom Link: **Here**

### Attendees

- ...

### Agenda

- Review AIs
- Certificate transparency update (Eli Nesterov)
- Datastore Plugin Update (Andrew Harding)
- AWS KMS-backed Key Manager proposal (Eugene Weiss)

### Action items

- [Agustin, Marcos Y] Add API protos and plugin protos to the exchange proposal
    - Worked examples of selectors and entry arrangement would be great too
- [Agustin, Andres] Collect user requirements on the serverless use case to help determine appropriate pro/con tradeoffs
- [Evan] Review and leave notes on certificate transparency RFC
- [Mariano] Share preliminary research around AWS KMS keymanager
    - Failure Modes
    - Step-by-step rotation
- ...

### Notes

- Review AIs
    - Proto and registration/selector examples still in the works
    - User feedback on serverless approaches pending, will need a few more weeks
- Certificate transparency update
    - Evan assigned to review the RFC
        - SPIRE won't be handling distribution of the CT public signing key, but if SPIRE is providing a CT feature we should have something (documentation or otherwise) that describes how this public key can/should be distributed to workloads
        - Since the API for obtaining the SCT is standardized, it probably makes sense for this feature to live in SPIRE core rather than as a plugin
    - Eli will provide a demo showing how this can be used, and what the workflows look like
    - Evan to update the RFC with his comments
- SPIRE performance profile
    - Eli has been working on SPIRE load testing
    - Results to be shared with the community in the coming weeks
    - We hope to use this work going forward for detection of performance regressions
        - We'll need to figure out if we can do this upstream in a cost effective way
    - Reusable tooling would be great, even documentation on how to replicate the load testing given your own topology/requirements would be an improvement

        - Eli to share information via GH issue and on a future SIG-SPIRE call
- Datastore update
    - TL;DR there is not a clear direction to move towards at this point in time.
    - Historically, datastore interface has been very difficult to provide any sort of stability around
        - Needs to be extended any time SPIRE changes its object model
        - Also needs to be extended when new features change access patterns
    - Pluggability was removed in 0.11.0
    - There are several requirements for an ideal SPIRE storage solution:
        - Bring-your-own-backend
        - Simple plugin interface (keep the meat in SPIRE core)
        - Flexible query patterns
        - As low maintenance as possible outside of updating models/query patterns (i.e. leverage well-used and understood libraries)
        - Not require expert-level knowledge to maintain
    - Ideally looking for an overlay on top of K/V that provides flexible query semantics, migration support, and supports a pluggable backend but haven't found one yet.
    - Cayley (cayley.io) seemed to fit the bill but the project is more or less inactive. This means that picking it up as a solution would likely require significant investment in the project.
    - There are many overlays on top of K/V for structured data, but they are opinionated in the supported backends (e.g. https://entgo.io/).
    - Embedding a distributed K/V database inside SPIRE (e.g. embedded etcd, badger) would require SPIRE operators to have operation knowledge of distributed storage and consensus..
- AWS KMS KeyManager
    - Mariano and Max working on profiling and proof of concept
    - No issue/proposal has been raised yet - this topic is brought up for discussion with no specific questions
    - This will be the first upstream "non-local" keymanager which raises a few questions that would be good to see addressed with the proposal
        - What happens when the keymanager is ratelimited by the provider?
        - What happens if KMS is unavailable or otherwise returns an error?
        - Does SPIRE core respond to the above cases well, and are the errors and log messages clear? Do we need to change anything in core to better handle these eventualities?
    - Understanding the threats mitigated by using a KMS keymanager will be helpful in assuring that the implementation meets the goals
    - How do we authenticate to KMS?
        - Standard AWS IAM-based authentication methods, using credentials available via environment variable
    - Exact order of KMS operations would be nice to see on a proposal as well
        - E.g. how is key rotation handle, key naming, etc
    - Proposal to be raised on GitHub in the near future
- ...

# [SPIFFE] SIG-SPIRE: Meeting Notes

When: **Every Other Thursday @ 10:30am PT (.ics) [Odd number weeks]**
GitHub Repo: **Link**
Google Group: **Link**

---

Zoom Meeting: **Link**

---

## Meeting #1: Sep 17 2020 @ 10:30-11:30am PT

**Logistics**

- Zoom Link: **Here**

**Attendees**

- Andrew Harding (VMware)
- Daniel Feldman (HPE)
- Marcos Yacob (HPE)
- Ryan Turner (Uber)
- Brian Martin (HPE)
- Eugene Weiss (HPE)
- Evan Gilman (VMware)
- Agustin Martinez Fayó (HPE)
- Andrés Vega (VMware)
- Chen Xi (Uber)

**Agenda**

- Review AIs
- Agentless RFC
- ...

**Action items**

- [Agustin, Marcos Y] Add API protos and plugin protos to the exchange proposal
    - Worked examples of selectors and entry arrangement would be great too
- [Agustin, Andres] Collect user requirements on the serverless use case to help determine appropriate pro/con tradeoffs
- ...

**Notes**

- Questions on the granularity of the SVID-function mapping (can anyone add here)
- Do we want to support OpenFAAS, Serverless.io, etc? Evan has some OpenStack knowledge and said they don't have great node metadata that we could use.
- Evan's first question on the GH issue: can we push SVIDs into cloud-specific storage preemptively rather than pull an SVID as needed during warmup
- Discussion of how to implement the plugin interface itself & naming (credential exchange?)