

CSI Secrets Store

Meeting Notes

Shared Publicly

When: Biweekly on Thursday at 12:00pm-1:00pm EST (9:00am - 10:00am PST)

- [Google calendar invite for Thursday 12pm EST Bi-weekly](#)

Everyone is welcome and encouraged to attend and join this call for participation.

This call falls under the CNCF Code of Conduct and the video will be published.

Slack: [#csi-secrets-store](#) channel on [Kubernetes Slack](#)

Join Zoom Meeting

<https://zoom.us/j/91272289538>

Meeting passcode: 77777

Recordings:

https://www.youtube.com/playlist?list=PL69nYSiGNLP0PCFJrlpV6_nR_j_3Rtnwl

Meeting document link -

<https://docs.google.com/document/d/1q74nboAg0GSPcom3kLWCloWg43Qg3mr306KNL58f2hg>

#####

Template (do not edit): Jan 15, 2025 09:00 GMT-8

Attendees

- Add Name (Org)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator:
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o TBD

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- CSI Driver:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)
- Sync Controller:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)

#####

#####

Aug 21, 2025 09:00 GMT-7

Attendees

- Abhijeet Dargude (Google)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator:
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Abhijeet: In the [1622](#) (Rotation PR), we will remove some of the metrics like total `total_rotation_reconcile`, do we need to announce it for the customers?
 - o Reviews on PR: [150](#) (Support for metrics), [148](#) (structured logging)

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- CSI Driver:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)
- Sync Controller:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)

#####

#####

Jul 24, 2025 09:00 GMT-7

- Cancelled due to leads availability

June 26, 2025

Attendees

- Add Name (Org)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator:
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [mytrea] [Allow file ownership to be set for secrets](#) PR: [1841](#)
 - [Angad Misra] Use RequiresRepublish for secret rotation PR: [1622](#)

Notes

- [858](#): Problem reported, secret files mounted as root:root. ~~No way to make it so others can read the secret.~~ The only way for a non-root container to read the secret is to have wider, world-readable permissions on the secret. When a container is started, FS Group can be used to define a group for the file system. Currently there is no way to change the ownership of the secrets. This is to offer FS Group support by advertising volume mount capability.

- Scenario: Container may have multiple workloads which are running by different users. These different workloads should not necessarily be able to read all of the secrets mounted in the file system. The problem is reported in the issue.
- [1622](#): RequiresRepublish continues to be a hot topic

Action Items

- TBD

#####

April 17, 2025

Attendees

- Add Name (Org)
- Micah Hausler (AWS)
- Anish Ramasekar (Microsoft)
- Ben Petersen (Microsoft)
- Joe Bowbeer (?)

Announcements

- Driver v1.5.0 released!

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish Ramasekar
 - Notes: Ben Petersen
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - Get all k/v pairs
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/529#issuecomment-2518378923>
 - i. This doesn't seem appropriate for the driver, the driver doesn't understand the requirements, its "dumb", individual providers are better fits
 - ii. This issue should be closed here in the driver and possibly reopened in the sync controller as it is relevant to creating secrets in Kube.

- iii. The conversation today, however, is about volume mounting the secrets, not syncing as Kube secrets. This means the request is best for specific providers.
- [micahhausler] RequiresRepublish status:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/1622>
 - o In review
 - o Slated for release in 1.6 in ~May
 - o This change removes the secret sync feature

Notes

- TBD

Action Items

- TBD

#####

Feb 6, 2025

Attendees

- Abhijeet Dargude (Google)
- Anish Ramasekar (Microsoft)
- Suyog Jain (Google)

Announcements

- Driver v1.4.8 released!

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Anish
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Rotation PR: [Use RequiresRepublish in secret rotation. by dargudear-google · Pull Request #1622 · kubernetes-sigs/secrets-store-csi-driver \(github.com\)](#)
 - i. [This likely will introduce https://github.com/kubernetes/kubernetes/issues/121271](#)

Notes

- Review <https://github.com/kubernetes/kubernetes/issues/121271> and start a thread on #sig-storage slack channel.
- GKE plans to run the sync controller in the control plane
 - This was the intention when the project was designed as a controller as well.
 - This requires some changes in the controller
 - Abhijeet and Sujoy will open issue and PRs for the required changes

Action Items

Review issues with leftover time

- CSI Driver:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)
- Sync Controller:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)

#####

Jan 23, 2025

Attendees

- Abhijeet Dargude (Google)
- Anish Ramasekar (Microsoft)
- Ben Petersen (Microsoft)
- Suyog Jain (?)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Ben
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Rotation PR: [Use RequiresRepublish in secret rotation. by dargudear-google · Pull Request #1622 · kubernetes-sigs/secrets-store-csi-driver \(github.com\)](#)

Notes

- Get PR above merged to be part of the 1.5 release
- Patch this week for 1.4 CVEs

Action Items

- Working on adding maintainers! We have quality contributors.
 - o How? Not exactly fixed, but generally a number of PRs merged, reviewed, etc.
See the Kubernetes guide:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/blob/main/docs/MEMBERSHIP.md>
 - o

Review issues with leftover time

- CSI Driver:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)
- Sync Controller:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)

#####

December 26, 2024 - CANCELED (Merry Christmas)

December 12, 2024

Attendees

- Abhijeet Darguder (Google)
- Anish Ramasekar (Microsoft)
- Ben Petersen (Microsoft)

Announcements

- Happy Holidays everyone!

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Ben
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [Use RequiresRepublish in secret rotation. by dargudear-google · Pull Request #1622 · kubernetes-sigs/secrets-store-csi-driver \(github.com\)](#)
 - o [Fix kubeVersion string to validate GKE clusters \(PR\)](#)
 - o Sync Controller: Can we add an option to remove requirement of serviceaccounts/token create permission

Notes

- In Secrets Sync Controller, serviceaccount/token create permission is highly privileged. Discussing necessity, options
 - o SecretSync is treated as a Workload in Sync Controller, as it doesn't know about the workloads.
 - o There may be different instances of Secret Managers.
 - o We want to solve the "God Level Permissions" problem.
 - o SecretSync is bound to namespace.
 - o The Driver does not use its own identity, we want to replicate this concept in Controller as well, as a good security boundary.

- VAPs exist for everything as well, to ensure Controller is only doing what it is supposed to be doing.
- Any users using Sync Controller with GKE plugin today?
 - Customer did flag the above as a concern, thus the discussion today

Action Items

- Anish plans to review [CSI Driver PR1622](#) sometime next week.
- Abhijeet suggests Google contributor possibly assisting with rotation feature.
- Cancel meeting for the Christmas holiday, next meeting in 2025!

Review issues with leftover time

- CSI Driver:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)
- Sync Controller:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)

#####

October 31, 2024

Attendees

- Add Name (Org)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator:
 - Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - TBD

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- CSI Driver:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)
- Sync Controller:
 - [CI testgrids](#)
 - [Issues \(Milestones\)](#)
 - [PRs](#)

Oct 17th, 2024

Attendees

- Ben Petersen (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Abhijeet Dargude (Google)
- Alexander Stocks (Microsoft)
- Anish Ramasekar (Microsoft)
- Marcelo Cyreno (Microsoft)

Announcements

- [CSI Driver Release 1.4.6 cut on 2024. Oct 09](#)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Ben Petersen
 - o Notes: Ben Petersen
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Update the meeting invite with the passcode 😊
 - o [add s390x. ppc64le support \(PR\)](#)

- Topic: Document auto restart of pods on secret rotation (Ewan Chalmers)
 - i. [Document auto restart of pods on secret rotation \(ISS 1647\)](#)
 - ii. [Document auto restart of pods on secret rotation \(PR 1648\)](#)
- [Use RequiresRepublish in secret rotation \(PR\)](#)
- [Fix kubeVersion string to validate GKE clusters \(PR\)](#)
- Topic: Can we add some restrictions to avoid misuse of the service account? (Abhijeet)
- [BUG: Controller never reconciles on update even if secret sync has changed · Issue #83 · kubernetes-sigs/secrets-store-sync-controller \(github.com\)](#)
- Topic: Performance issues on large clusters, throttling with Azure Key Vault (Marcelo)

Notes

- Discussion of topic: restrictions to avoid misuse of service account
 - We have VAP restricting types of secrets, validating audience, etc.
 - User has option to config the types of secrets the controller can create, update
 - Secrets can only be updated if they have a label added by the controller
 - Providers are deployed as sidecars, listening on unix sockets
- Target mid-November for 2nd alpha release? [v0.0.2](#)

Action Items

- Abhijeet will create a few follow-up issues for RequireRepublish regarding items discussed.
- Ben: Add Sync Controller Issues, PRs lists also to the items to the template above.

Review issues with leftover time

- CSI Driver:
 - [CI testgrids](#)
 - [Issues](#)
 - [PRs](#)
- Sync Controller:
 - [CI testgrids](#)
 - [Issues](#)
 - [PRs](#)

Oct 3rd, 2024

Attendees

- Abhijeet dargude (Google)
- Nilekh Chaudhari (Microsoft)

- Anish Ramasekar (Microsoft)
- Ben Petersen (Microsoft)
- Ciprian Hacman (Microsoft)
- Alexander Stocks (Microsoft)

Announcements

- CSI Driver release will be cut next week

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Nilekh Chaudhari
 - o Notes: Ben Petersen
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [Use RequiresRepublish in secret rotation. by dargudear-google · Pull Request #1622 · kubernetes-sigs/secrets-store-csi-driver \(github.com\)](#)
 - i. Use RequiresRepublish in secret rotation (instead of rotation controller)
 - o <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/1483>
 - i. KeyVault 429: TooManyRequests led to infinite loop in reconciler workqueue
 - o <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/1436>
 - i. Race condition between Pods gets deployed and SPC creation/updates
 - o [BUG: Controller never reconciles on update even if secret sync has changed · Issue #83 · kubernetes-sigs/secrets-store-sync-controller \(github.com\)](#)
 - o [helm install fails when deploying VAPs in Kubernetes v1.28.0 · Issue #78 · kubernetes-sigs/secrets-store-sync-controller \(github.com\)](#)
 - o Driver release
 - i. Next week
 - ii. Metrics PR will be deferred until the following month's release, to give time to address comments

Notes

- Discussion about Secret Store CSI Driver, and the spinoff of the Sync Controller
 - o Several use cases at hand, after community feedback it has been decided to split these apart
 - o CSI driver for workloads that expect a secret on the file system, such as a tempfs volume. These workloads may watch for file system changes.
 - o Sync Controller for workloads that expect a native Kubernetes Secret, such as an Ingress Controller
- Caching issues with CSI Driver

- Since it is a DaemonSet and therefore installed per-Node, it is difficult to cache requests to Secret Stores. Therefore the requests are pod specific, many pods results in many requests (even if for the same secret).
- Sync Controller, in contrast, can sync as a Kubernetes Secret, which is cluster scoped, so fewer requests to Secret Stores are necessary.

Action Items

- [Ciprian Hacman]: Schedule a follow-up meeting regarding the KeyVault 429 TooManyRequests issues (next week). Specifically, to continue the Kube Secret vs volume mount discussion and the decoupling of the CSI Driver and Sync Controller.

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Sept 19, 2024 - CANCELED

Sept 05, 2024

Attendees

- Abhijeet dargude (Google)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Nilekh
 - Notes: Anish
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)

- Secrets Store Sync Controller issue triage
- Rotation in csi driver. Created draft [PR](#). Should we remove existing functionality (which used tokenmanager) or make requiresRepublish opt-in feature while keeping default behavior as it is?
-

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Aug 22, 2024

Attendees

- Abhijeet Dargude
- Nilekh Chaudhari

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish Ramasekar
 - Notes: Nilekh
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [driver/pull/1124](#) why it was closed and can we resume work on rotation?
 - Updates on the controller v0.0.1 release
 - Updates on the GCP e2e tests as part of the prow migration

Notes

- RequiresRepublish : It was demoed earlier. We should prioritize for rotation feature.

- <https://github.com/aramase/secrets-store-csi-driver/tree/requires-republish>
- Poll interval - We are not going to remove this even after RequiresRepublish. Driver should decide if we want to perform secret fetch or not. Poll interval would decide if we should actually go ahead and fetch secrets when RequiresRepublish is initiated.
- All PRs to release controller have been merged.
 - Staging image will be published today.
 - Promotion of the image after testing with staging image.
- New issues to be created for v0.0.2 milestone
 - New contributors to help with this
 - Add the issues to the next agenda and plan the milestone
- GCP e2e tests - Trying to figure out if tests can be done on GKE community infra rather than EKS clusters to make it easier. - <https://github.com/kubernetes/test-infra/pull/33340>
- <https://github.com/kubernetes/test-infra/pull/33340>
- v1.4.5 for driver is released with CVE patches.

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

July 25, 2024

Attendees

- Nilekh Chaudhari (Microsoft)
- Abhijeet Dargude (Google)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish Ramasekar
 - Notes: Nilekh
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)

- What is the plan to make sync controller stable (for release)
- Any security concerns in the sync controller ?
- KEP process for sync controller
- Will auto-rotation be available for both the drivers?
- Can we mark auto-rotation as a stable feature? (In secret store csi driver)
- Distroless support: [issues/1391](#) ? do we have any plan or ETA. [Earlier Notes](#)

Notes

- Needs to improve existing Driver Sync feature UX with Sync Controller (along with security)
- VAP and SSA adds additional security for Sync Controller
- For Sync Controller, Alpha release soon and Beta and GA in ~6 months
- After implementation for “Requires Republish” in Driver we will move rotation feature from Alpha
- For Sig project to add features we typically open the issue first, discuss in community call, then take the same to Sig Auth and once approved there we can go ahead and implement.
- Kept SPC same for both Driver and Controller so that it would be easier for users to migrate to Sync Controller

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

May 2, 2024

Attendees

- Nilekh Chaudhari (Microsoft)
- Glen Johnson (CyberArk)
- Alex Stocks (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

- Secrets Store Sync Controller repo is created.

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Nilekh
 - o Notes: Anish
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Conjur CSI Provider demo

Notes

-

Action Items

- TBD

Feb 22, 2024

Attendees

- Anish Ramasekar (Microsoft)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Nilekh
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [mandrea] [Secrets sync controller](#) update and demo

Notes

-

Action Items

- TBD

Feb 8, 2024 - CANCELED

Jan 25, 2024 - CANCELED

Nov 16, 2023 - CANCELED

Nov 01, 2023

Attendees

- Amit Modak (Google)
- Anish Ramasekar (Microsoft)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Nilekh
 - o Notes: Amit
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [amitmodak] <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/1326>
 - i. Vulnerabilities in current version of golang
 - ii. Dockerfile uses 1.20, go.mod uses 1.19
 - iii. The one in go.mod is the minimum supported, need not be updated every time
 - iv. The version in Dockerfile needs to be updated to 1.21
 - v. Recent change (possibly with 1.21) Go toolchain looks at go.mod
 - vi. Upgrade of otel can cause breaking changes
 - vii. We could consider keeping the version in-sync

- viii. Anish can help with otel upgrade, Abhijeet can share the PR
- ix. Fyi, we perform image scan with trivy periodically by building main branch:
<https://testgrid.k8s.io/sig-auth-secrets-store-csi-driver-periodic#secrets-store-csi-driver-image-scan>
- [amitmodak] Impact of sync split on auto-rotation
 - i. Driver will continue to support auto-rotation
 - ii. Kubelet will call the driver via RequiresRepublish, driver can drop root-in-cluster privileges – not tied to the split feature
 - iii. PR open on the driver repo for the sync controller CRD:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/1364>

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Oct 05, 2023

Attendees

- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish Ramasekar
 - Notes: Mandrea

-
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [Abhijeet] Distroless images
 - [Abhijeet] Upgrade go version
 - [Mandrea] SecretSyncClass
 - [Naman] Impact to Secret Sync Feature after Driver split

Notes

- Secret Sync class: we will remove synced secrets section from the secret provider class and move them to the SyncSecret
- Distroless images:
 - Can we use distroless images instead of debian images?
 - We need the mount capability today so we can't use distroless images
 - Poc with a distroless image exists, but the issue is that we need the base image published
 - i. Propose the team who owns the base image to publish it
 - ii. We can change pipelines etc to use new image
 - We publish images for the driver, what blocks us from taking a half step?
 - i. Publish 2 images: distroless and docker image
 - ii. Pull the distroless image and build on that
 - iii. We should pursue the general approach
 - iv. We need to speak with other maintainers
- Go version:
 - Go 1.20 internal scan showed vulnerabilities, should we update to go 1.21?
 - Open issue with CVEs from the scan and we can have a code review
- Impact to Secret Sync Feature after Driver split
 - Existing secret sync feature on the driver will be deprecated and removed
 - The driver will do only the mount: the secret objects from the SPC will be deprecated as well
 - If the sync is required the plan is to deploy the Secret Sync Controller and synchronize the secrets as K8S secrets
 - On the provider side, the documentation on synchronizing secrets as kubernetes secrets needs to be updated
 - The provider needs to document the controller deployment
 - Implementation changes on the provider: there shouldn't be any changes at the provider level

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

#####

September 21, 2023

Attendees

- Nilekh Chaudhari (Microsoft)
- Amit Modak (Google)
- Mo Khan (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

- The community meeting bi-weekly series has been moved by a week and is now on alternate weeks of the sig-auth meeting.
- The community meeting time has changed from 8AM PST to 9AM PST

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Nilekh Chaudhari
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [Secrets Store CSI Driver Sync Secrets](#)
 - o <https://github.com/GoogleCloudPlatform/secrets-store-csi-driver-provider-gcp/issues/242>

Notes

- Sync Secrets:
 - o No offline support for the CSI driver, we will provide a separate sync controller.
 - i. Sync secrets controller will not need to mount secrets first.

- ii. Need consensus from all the providers to add them as a sidecar while installing via helm chart.
- iii. In a disconnected scenario, the user should use k8s secrets synced via the sync controller.
- iv. [mo] Can we just link to the provider helm chart rather than include them in the sync controller helm chart?
 - Need to come up with some guidelines as to how to handle single-provider failure when we pack everything into a single helm chart or reference them.
- Offline support/caching secrets violate node isolation (was discussed in Sig Auth call)
- After split, env var can be used with k8s secrets in Sync controller and maybe with DRA (Dynamic Resource Allocation), we can use it in core Secrets Store CSI project.

Action Items

- TBD

#####

September 14, 2023

Attendees

- Add Name (Org)

Announcements

-

Agenda

- Change meeting date and time
 - Moderator:
 - Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - TBD

Notes

- The current meeting series is the same as sig-auth community calls
 - o Causes a 2 week delay to discuss design in this community call and then sig-auth
 - o Move the bi-weekly meeting series by a week so it's every other week with sig-auth
 - o Also, move the meeting to 9AM PST instead of 8AM PST as folks have conflict

Action Items

- Post on slack about moving the meeting series by a week and changing time to 9AM PST
- Post on slack about “disconnected scenario” not going to be supported in CSI driver and we’re moving forward with the secret split project.

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

#####

August 31, 2023 -

Attendees


- Amit Modak (Google)
- Ashwin (Google)
- Xander Grzywinski (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Mo Khan (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)

- Moderator: Anish Ramasekar
- Notes: Mo Khan
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - Follow up discussion on Secrets Store CSI Driver caching
 - i.  Secrets Store CSI Driver Caching
 - Double opt in (both the admin and provider)
 - Will try to sync with SIG Auth more often to get feedback early
 - Discussed extensions of the caches in terms of
 - Local short second cache (this would be without opt-in from the provider)
 - As a performance improvement for providers on the order of minutes (provider would have to decide how this would be configured)
 - Separate project for secret sync feature
 - i. Have general agreement from SIG Auth to have it as a new sub project
 - ii. Want buy in from providers that they are okay with the slightly different packaging format (Anish will reach out about this)
 - iii. Optional second project that effectively takes the optional sync feature into a separate project
 - iv. Secret sync feature would be deprecated (and eventually removed) after the separate project exists
 - Could be a v2 cutover with v1 maintained for some time
 - v. Amit and Ashwin will reach out to other Google folks to see if they have feedback on this
 - Release v1.3.5

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

July 20, 2023 - CANCELED

Canceled due to no agenda.

July 6, 2023 - CANCELED

Canceled due to no agenda.

June 22, 2023 - CANCELED

Canceled due to no agenda.

June 8, 2023 - CANCELED

Canceled due to no agenda.

May 25, 2023 - CANCELED

Canceled due to no agenda.

May 11, 2023

Attendees

- Anish Ramasekar (Microsoft)
- Anjali (RedHat)
- Martyn Ranyard (MeisterLabs Gmbh)
- Pete Bohman (Akamai)
- Gustavo (Container Solutions)
- Nilekh Chaudhari (Microsoft)
- Lucas Severo (Red Hat)
- Amit Modak (Google)
- Aswin Viswanathan (Google)
- Mo Khan (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Nilekh Chaudhari
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o External Secrets Operator and Secret Store CSI Driver projects and APIs
 - i. <https://github.com/external-secrets/external-secrets/issues/336>
 - ii. <https://kubernetes.slack.com/archives/C013PUP2WRK/p1682354854859329>
 - o 1Password driver demo - Martyn Ranyard
 - o <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/963> Has anything changed since Tommy's feedback last September that would impact the viability of this PR, assuming the feedback was addressed?

Notes

- [Gustavo] Installation of both SSCSI and ESO together can be tricky.
- [Mo] Using both projects might be confusing to the user if either added a feature and expect the same from other
- [Gustavo] Sync secrets could be the main reason for combining forces of the two projects
- Get feedback from users on the integration of SSCSI and ESO
- Docs for adding a provider to SSCSI can be confusing and could be improved.
 - o https://docs.google.com/document/d/1Uxwcc8x0iVhJK_hdWCeqQVrT-sQMCLSmE1tvzp1EA6M/edit#

Action Items

- Start the doc with ideas/use cases/pros/cons for integration between SSCSI and ESO to get community feedback.

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

April 27, 2023

Attendees

- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [nilekh] - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/821>
 - o [Xander] Milestone planning? (determine time in Slack)

Notes

- The metrics issue was last commented on Feb 1st
 - o A user recently commented on the issue to reopen but later mentioned the metrics were working as expected.
 - o We'll add a note in the metrics documentation to indicate driver metrics are generated only when the driver is actually being used for mount/unmount.
- Xander to start a slack thread or doodle for the milestone planning.
- We will be presenting the driver in the ESO community call on 05/10
- ESO will be presenting their project in our community call on 05/11
- Anish will share the sync secret split proposal on slack next week and do a demo of the POC in the next community call on 05/11.

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

#####

April 13, 2023

Attendees

- Xander Grzywinski (Microsoft)
- Anjali Telang (RedHat)
- Rita Zhang (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Xander Grzywinski
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Continue disconnected discussion: [Secrets Store CSI Driver Caching - Google Docs](#)
 - o [Xander] Should we book another planning session for upcoming milestones?
 - o [Anish] Splitting secret sync controller from driver:
 - Secrets Store CSI Driver Sync Secrets

Notes

- Continue disconnected conversation. Starting with POC.
- Rita: Dependency or connection between disconnected and controller separation? No major connection between the two. Proposal is just for the driver running in disconnected scenarios
- Use next meeting for milestone planning (ping Tommy as well, add to Slack)
- Splitting controller originally discussed in 2021. Could reuse existing SecretProviderClass
- ESO is an existing popular option
- Do we want to go forward splitting the controller? Or just recommend ESO?
- Users could just rely on Helm charts to install whichever controller they need

- Nilekh: Should env var injection be part of the scope of splitting the controllers? Could be supported upstream in-tree or from the driver
- Rita: Create specific proposal for splitting the controller? Anish to work on that
- Could still collaborate with ESO, try to meetup with ESO folks at Kubecon EU
- Next steps: resurface issue for splitting the controller, write doc, make a decision
- Start building POC for encryption key indirection
- Mo: Does the driver service account have any auth against the provider? No

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

#####

March 30, 2023

Attendees

- Add Name (Org)
- Tommy Murphy (Google)
- Xander Grzywinski (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Nilekh
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)

- [Xander] Continue disconnected discussion: [Secrets Store CSI Driver Caching - Google Docs](#)
- [Xander] Should we book another planning session for upcoming milestones?
- [Anish] Splitting secret sync controller from driver:
 - ☰ Secrets Store CSI Driver Sync Secrets

Notes

- Caching:
 - When enabled sync feature grants an access to fetch any secret. We need to be mindful of this fact and mitigate.
 - Caching needs to happen for both driver and controller (post split)
 - Caching TTL, at driver or provider? Per secret or SecretsProviderClass?

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

March 16, 2023

Attendees

- Nilekh Chaudhari (Microsoft)
- Xander Grzywinski (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator:
 - Notes:

- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Continue disconnected discussion: [Secrets Store CSI Driver Caching - Google Docs](#)

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

March 02, 2023

Attendees

- Anish Ramasekar (Microsoft)
- Anjali Telang (Redhat)
- Xander Grzywinski (Microsoft)
- Tommy Murphy (Google)
- Mo Khan (Microsoft)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Nilekh
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Discussion on disconnected scenarios -> [Secrets Store CSI Driver Caching - Google Docs](#)

- The driver requires root privileges
<https://secrets-store-csi-driver.sigs.k8s.io/concepts.html#security> has there been any thoughts to restrict access in future?

Notes

- Disconnected Scenario:-
 - There is an increasing ask for the support of disconnected scenarios in Secrets Store CSI Driver
 - The cache would be a fallback cache. The driver should always live pull from Secrets Store
 - Should not have similar behavior to kubelet where the cache does not know which pod has access to which secret.
 - Possibly a driver implementation.
- Drooping root privilege requirements for the driver and the providers has been discussed before but concluded that we can't. We will potentially try to give another round of thought to the same.

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

January 19, 2023 - CANCELED

Canceled due to no agenda.

January 05, 2023

Attendees

- Xander Grzywinski (Microsoft)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [nilekh] - <https://github.com/Azure/secrets-store-csi-driver-provider-azure/issues/885>
 - o [anish] [add nilekhc and salaxander to secrets-store-csi-driver maintainers](#)

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

November 24, 2022 - CANCELED

Canceled due to US holidays.

November 10, 2022 - CANCELED

Canceled due to no agenda.

September 29, 2022

Attendees

- Xander Grzywinski (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Amit Modak (Google)
- Aswin Vishwanathan (Google)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Xander Grzywinski
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o TBD

Notes

- TBD

Action Items

- TBD

September 01, 2022

Attendees

- Xander Grzywinski (Microsoft)
- Tommy Murphy (Google)
- Aswin Viswanathan (Google)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator:
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o TBD

Notes

- Nilekh: patch release next week and work on file ownership planned

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

August 18, 2022

Attendees

- Xander Grzywinski (he/him, Microsoft)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Xander Grzywinski
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

August 4, 2022

Attendees

- Dane Murphy (Comcast)
- Xander Grzywinski (Microsoft)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator:
 - o Notes: Xander
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/963>
 - o <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/858>
 - o

Notes

- Follow up from Slack discussion on PR #963. Updates to `syncOptions`
- “How does the driver consistently parse the JSON returned by the provider?” Responses should conform to the expected structure

Action Items

- Discuss issue #858 at next SIG Auth meeting
- Set next milestone
- Patch version next week

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

July 21, 2022

Attendees

- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)
- Dane Murphy (Comcast)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator:
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Adding Nilekh and Xander as maintainers to the repo:
<https://github.com/kubernetes/org/pull/3532>
 - o Dane's PR:

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

June 23, 2022

Attendees

- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)
- Xander Grzywinski (Microsoft)

Announcements

- V1.2 released

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator:
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Meeting canceled because of no agenda

Notes

- TBD

Action Items

- Xander will post on slack about the v1.3 milestone planning meeting
- We will do a meeting next week to triage features we want to include in v1.3 release

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

June 9, 2022

Attendees

- Dane Murphy (Comcast)
- Xander Grzywinski (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Nilekh Chaudhari
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o SyncOption: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/963>

Notes

- Sync Options
 - o Is there a use case to mount keys separately in different files from json response?
 - o Tommy added few comments in the PR
 - o We will review and also look at what AWS provider is implementing today

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

May 26, 2022

Attendees

- Add Name (Org)
- Daniel Urgell (BlueLabs.eu)
- Phill Gibson (Microsoft)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)
- Idan Trablesi (Microsoft)
- Roy Goldstein (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Amira Solomivici (Microsoft)
- Yuval Harpaz (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [nilekh] - Discuss [Sync all secrets](#) and related [issue](#) in provider
 - o [nilekh] - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/948>
 - o [nilekh] - Proposal for Encryption Provider
(https://docs.google.com/document/d/1AqKz29RXVgHJNurS2ZXrUz_60fr8rnqDP/Cwjx2Skyul/edit?usp=sharing)
Issue - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/906>

Notes

- Discuss sync all secrets and issue in provider
 - o Dane is going to work on another PR to add templating
 - o We need to follow up with Dane on a design doc and PR for implementation
- Ability to set static secrets under secretObjects
 - o This can be a feature request in the provider to set static values

- Provider needs to return the file as part of the grpc response
- Sync secret relies on the files in the mount, so it'll work with any changes in driver

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

May 12, 2022 - No Formal Meeting/Recording

Attendees

- Add Name (Org)
- Tommy Murphy (Google)
- Phill Gibson (Microsoft)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Phill Gibson
 - Notes: Phill Gibson
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - Due to low attendance we'll be discussing the items in the notes for next meeting on 5/26/22

Notes

- [Tommy] - Need to get v1.2 released
- [Nilekh] - Wants to discuss the additional project related to [issue](#)
- [Nilekh] - Discuss sync all secrets [PR](#)

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

April 28, 2022

Attendees

- Add Name (Org)
- Phill Gibson (Microsoft)
- Rey Lejano (SUSE)
- Nilekh Chaudhari (Microsoft)

Announcements

- [Rey] Third-party security audit for Kubernetes will start on May 9 and secrets-store-csi-driver is in scope. Link to RFP:
<https://github.com/kubernetes/sig-security/blob/main/sig-security-external-audit/security-audit-2021-2022/RFP.md>

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Phill Gibson
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [Phill] - Creation of the contribution ladder

Notes

- Security audit happening May 9th through June
- Look into having a contributor ladder locally in the repo and more custom to project activities

Action Items

- Maintainers to be available via Slack channel if needed during security audit

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

April 14, 2022 - No Formal Meeting

Attendees

- Phill Gibson (Microsoft)
- Dane Murphy (Comcast)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o

Notes

- Merged akeyless provider e2e in the driver repo
 - o We have an optional job that can run to validate tests with this provider
 - o Next steps: code audit of the provider - <https://github.com/akeylesslabs/akeyless-csi-provider>

Action Items

- Request all maintainers and contributors to do a code audit of <https://github.com/akeylesslabs/akeyless-csi-provider>. After the code audit issues are resolved, we will add akeyless as a supported provider to the driver.

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

March 31, 2022

Attendees

- Add Name (Org)
- Phill Gibson (Microsoft)
- Dane Murphy (Comcast)
- Tommy Murphy (Google)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o (Dane) SyncOptions w/Demo - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/820>
 - o

Notes

- SyncOption discussion

- create two and or separate the features for the functionality (sync all & json)

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Mar 17, 2022

Attendees

- Add Name (Org)
- Tommy Murphy (Google)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Phill Gibson
 - Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 -

Notes

- <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/899>
 - bug with secret sync edge case, 5min poll time where new pods cannot start
- <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/895>
 - KEP link: <https://github.com/kubernetes/enhancements/pull/1003>
 - terminationGracePeriod - this would make upgrades slow, not guaranteed to work
- Encryption of secrets

- <https://github.com/kubernetes/kubernetes/issues/86186>
-

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Mar 03, 2022

Attendees

- Ori Mankali (Akeyless)
- Nilekh Chaudhari (Microsoft)
- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)

Announcements

- Driver v1.1.0 released:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/releases/tag/v1.1.0>

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Tommy Murphy
 - Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [Ori] Adding a new provider Akeyless:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/878>
 - How to add a new CSI provider. How tests can pass, if we are adding completely new type of CSI provider, that not supported by secrets-store.csi.x-k8s.io/v1
 - [anish] Bugfix for json logging - 1.1.1
 - [anish] Plan for 1.2.0

Notes

- akeyless:
 - <https://www.akeyless.io>
 - <https://docs.akeyless.io>
 - <https://console.akeyless.io>
 - <https://secrets-store-csi-driver.sigs.k8s.io/providers.html>
 - nodePublishRef or prow test-case [GCP identity](#)
 - get tests to pass in PR / create as option in test-infra to trigger the tests on the PR
 - code review of <https://github.com/akeylesslabs/akeyless-csi-provider>

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Feb 17, 2022

Attendees

- Add Name - (Org)
- Phill Gibson (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Shawn Hurley (Red Hat)
- Julie Ng (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)

- Moderator: Phill Gibson
- Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - Phill - Discuss Doodle poll results
 - Tommy - [File ownership](#)

Notes

- Based on doodle results, we will keep the community meeting at the same time as now
 - 8AM PST biweekly on Thursdays
- We need more feedback from the community for file ownerships
- There is a KEP from sig-storage for userGroups and fsGroups

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Feb 3, 2022

Attendees

- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)
- Nilekh Chaudhari (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish Ramasekar
 - Notes: Tommy Murphy

- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Token client merged: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/805>
 - o Removing old helm packages: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/850>
 - o Filesystem permissions: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/722>
 - o Provider Path update:
 - i. <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/823>
 - ii. Providers should switch to listening in /var/run/secrets-store-csi-providers instead of /etc/kubernetes/secrets-store-csi-providers
 - iii. WIP: driver to check both places

Notes

- Token client:
 - o include SA tokens in the requests to the providers
 - o Uses kubelet token cache logic
 - o providers check "token" attribute - if token already exists
 - o requires additional permissions for the driver process
 - i. serviceaccount/token create permission
 - ii. in ~1.2 RequiresRepublish will be enabled on all supported k8s versions, if this works well then we can move "rotation" to GA in ~1.3 and remove permissions/logic
 - o requires "audiences" parameter in the CSIDriver Yaml
- Old helm packages
- Filesystem permissions
 - o this can be solved by providers
 - o if you want per-file permissions extend the provider specific SPC information to support that
 - o future issue may be to override the 'default' permission in the SPC
-

Action Items

- Release 1.1.0
- Review provider implementation documentation
- Doodle poll, find better time

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)

- [PRs](#)

Jan 20th, 2022

Attendees

- Dane Murphy (Comcast)
- Phill Gibson (Microsoft)
- Anish Ramasekar (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Tommy Murphy (Google)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill G
 - o Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [\[nilekh\] - https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/432](#)
 - o

Notes

- Running the provider as non-root user
 - o Should we add a USER directive in the Dockerfile?
 - o [tommy] If we want root privileges, then we probably don't want to add the USER directive and then runAsRoot in the yaml
 - o [nilekhc] we could add some documentation on running as root and potential issues
 - o [tommy] we could use the audit results to see if there any potential issues

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)

- [PRs](#)

Jan 6, 2022

Attendees

- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Tommy Murphy
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Change default directory for providers to ``/var/run``:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/823>

Notes

- #823
 - o reasonable change
 - o driver to support multiple paths for a path to backwards compatible with older versions of provider deploys
 - o create issues in the provider repos to move to new path
 - o update documentation on [writing a provider](#)
 - o minor revision release OK (ex: 1.1.0)
- v1.0.1 release planned for next week with CVE patches
- v1.1.0 release after outstanding PRs for features are merged

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)

- [Issues](#)
- [PRs](#)

December 9, 2021

Attendees

- Phill Gibson - Microsoft
- Dane Murphy - Comcast
- Drew Garrett
- Anish Ramasekar - Microsoft
- Tommy Murphy - Google

Announcements

- [Phill] Suspending community meetings (December 23rd meeting) until January 6th 2022 for holidays.

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [Phill] Discuss CSI Secrets Store functionality/availability on cloud serverless container offerings (Azure ACI, Google Cloud Run, AWS Fargate, etc.)
 - o [Drew] Rotating secrets when pod is not running [Issue #280]

Notes

- Community meeting cancelled on Dec 23rd. We'll resume in the new year.
- [Tommy] Google Cloud Run has an integration with secrets manager
 - o Similar experience to CSI driver but it doesn't use CRD
 - o Knative doesn't support CSI
 - o UX is the secrets are loaded to the filesystem
 - o Knative support: <https://github.com/knative/serving/issues/11069>

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

November 11, 2021

Attendees

- Nilekh Chaudhari (Microsoft)
- Phill Gibson (Microsoft)
- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o File Permissions ([issue](#))
 - i. Think this is possible in the providers, testing on GCP. If successful introduce new field to SPC
 - ii. TODO: readonly mounts are a separate issue
 - o Rotation ([issue](#))
 - i. draft PR
 - ii. One of the next features we'd want to promote to stable
 - o New Timing Poll?

Notes

- File permissions
 - o Tommy validating the file permissions with the GCP plugin
 - o Separate issue to investigate read only mounts

- We'll create an issue to see if we want to perform validation for the user provided file permission
 - i. Validation can be performed at the provider to prevent making external API calls for incorrect file permission configuration
 - ii. Would it be of value to have the validation functions in the driver and use it in the provider as a library?
- Rotation
 - Initial draft PR with the implementation is open
 - This works! However this can produce quite a few calls for generating token for every single pod mount/rotation request
 - Looking into adding a cache for the token requests
 - i. Based on discussion with Tommy, we can use pod UID as cache key
- New Timing
 - We'll send out a doodle poll on slack to gather feedback
 - <https://doodle.com/create>
- Next call is during Thanksgiving, so it'll be cancelled
 - Happy Thanksgiving!!!

Action Items

- Send out poll for community call new meeting time

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

October 28, 2021

Attendees

- Dane Murphy
- Tommy Murphy (Google)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)
- Sertac Ozercan (Microsoft)
- Tom Proctor (HashiCorp)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish Ramasekar
 - o Notes: Tommy Murphy
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Filesystem Permissions
(<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/722> & <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/346>)
 - i. extend CRD with config to apply to all files
 - ii. and/or provider's must extend their YAML for per-file information
 - iii. allow write? Needed to delete secrets
 - to allow write/delete would need to raise with them
 - o 1.0 (and alpha functionality)
 - i. <https://secrets-store-csi-driver.sigs.k8s.io/#alpha-functionality>
 - ii. rotation
 - iii. k8s sync

Notes

- Filesystem Permissions
 - o sig-storage and sig-auth required read-only
 - o azure provider has received feedback on this, OK extending provider YAML
 - o anish: make it provider specific first before introducing a SecretProviderClass yamI/schema change
- Rotation
 - o 1.20 - code needed for backward compatible with RequireRepublish
 - o 1.21 - can use RequiresRepublish directly
 - o Make Pod token as part of driver (instead of how vault/gcp providers do it)
 - o based on K8s version, use requires republish or the rotation controller -> remove rotation controller once 1.20 deprecated
 - o tom: how to configure the frequency of requiresrepublish?
 - i. anish: keep poll interval configuration as flag -> keep track of the requiresrepublish timing per mount and limit how many actually get passed to the provider, later we could make this SPC configurable
- Secret Sync
 - o likely extract out of this project -> standalone controller
 - o todo: create design and present to sig-auth

- benefits: not tied to mount/csi driver (a common user request to not require a mount in order to sync the secret)
 - Keep sync in alpha until its a separate controller and there is a migration path, then plan deprecation from the CSI driver itself
- proto versioning (currently v1alpha1)
 - should this be tied to CRD versioning? will this change?
 - anish: maybe figure out removing of fields first before promoting/versioning to v1+
 -

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Sept 30, 2021

Attendees

- Dane Murphy (Comcast)
- Phill Gibson (Microsoft)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)
- Nilekh Chaudhari (Microsoft)
- Sertac Ozercan (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Phill Gibson
 - Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [nilekh] <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/724>
 - [aramase] Graduating the API from v1alpha1 to v1

- [phillipgibson] Cancellation of Oct 14th meeting due to KubeCon NA

Notes

- <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/724>
 - Follow up with the vault and aws provider
 - Tommy opened PR to add tests for rotation with vault provider
 - For aws provider, review the test suite and update the matrix based on it
- Graduating the API from v1alpha1 to v1
 - Sig-auth recommendation to not rely on alpha apis for stable release
 - Our CRDs haven't changed in a long time
 - We should be good with moving from v1alpha1 to v1 skipping beta
- Cancellation of Oct 14th meeting due to KubeCon NA
 - Next community meeting on Oct 28th

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Sept 16, 2021

Attendees

- Dane Murphy (Comcast)
- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Rita Zhang (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish Ramasekar
 - Notes: Tommy Murphy, Dane Murphy
 - i. <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/704>

- Forcing removal of colon + port for “metrics-addr” flag removes flexibility of configuration for user
- Name of flag should be “port” instead of “metrics-addr” if change is made
- Add comment to PR to let know this is not a change we are following through on
- ii. <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/724>
- iii. 1.0.0 release
 - wait for KEP review
 - Potentially have an RC
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [nilekh] <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/704>
 - o [nilekh] <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/724>
 - o 1.0 release
 - i. <https://github.com/kubernetes/enhancements/pull/2939>
 - ii.

Notes

- TBD

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Sept 2, 2021

Attendees

- Dane Murphy (Comcast)
- Phill Gibson (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Phill Gibson
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [nilekh] Possible implementation for e2e testing of staging images
 - i. <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/688>
 - ii. [notes]
 - Nilekh - Possibly use a github action once image is pushed; once successful we can create release
 - Anish - Pipeline is flexible to run when needed; Will only run against e2e provider
 - Tommy
 - Could build staging images more frequently; May not solve release workflow problem
 - Release process could be use to promote staging image to production
 - Push release to longer duration
 - o [nilekh] <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/724>
 - i. Community to review PR

Notes

- Inline

Action Items

- Community to review PR 724

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Aug 19, 2021

Attendees

- Phill Gibson - Microsoft
- Dane Murphy - Comcast
- Anish Ramasekar - Microsoft
- Nilekh Chaudhari - Microsoft
- Tommy Murphy - Google

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [aramase] Moving helm charts from <https://raw.githubusercontent.com/kubernetes-sigs/secrets-store-csi-driver/master/charts> to <https://kubernetes-sigs.github.io/secrets-store-csi-driver/charts>
 - i. Issue: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/687>
 - o [aramase] Renaming default branch from master to main
 - o [dane] Quick demo for updated syncAll feature
 - i. Issue: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/529>
 - [nilekh] Mock provider logic
 - PR comment - https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/682#discussion_r691671533

Notes

- Moving helm charts to gh-pages
 - o The gh-pages branch has been created with the existing helm packages
 - o The GitHub actions PR has been merged
 - o The helm repo url will be updated in the [install instructions](#)
 - o Update the upgrade documentation
 - i. Check if we can add a banner to call out this change

- After update, post a message on slack and also send out a note on the mailing list for the change.
- Renaming default branch from master to main
 - The PR to prepare for migration in test-infra is merged
 - We'll continue with this after updating the helm charts url
- Demo for syncAll feature
 - The cert and key parsing from single file following the same behavior as today
- Mock provider logic discussion
 - We should trim down the implementation to keep it simple
 - Nilekh is going to update the PR to return a static value from the e2e-provider
 - For rotation tests, the e2e-provider can maintain an in-memory cache with the <pod namespace>/<pod name> as key. If the key is in the cache, return value y for secret. If cache-miss, add to cache and return value x.
 - Tommy: "Less code is always better"
- We're working towards the v1.0 release. If there are any issues that you see as blocker please ping us!

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

Aug 5, 2021

Attendees

- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)
- Dane Murphy (Comcast)
- Rita Zhang (Microsoft)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Anish
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o I have a question (Dane)

Notes

- Released v0.1.0 last week
 - o Adds helm upgrade hooks to handle lifecycle of CRDs.
 - o Installing helm chart v0.1.0 and rollback to previous chart version is not allowed
 - i. Add this to release note
- Issue triage
 - o [Optimize driver build time for multi arch/os images](#)
 - i. Maintain a vendor folder
 - ii. Updates to go.mod will be coupled with updates to the vendor folder
 - o [Pull-secrets-store-csi-driver-e2e-windows flaky](#)
 - i. PR merged in node-driver-registrar to add new mode for liveness check
 - ii. Node-driver-registrar planned in the next 2 weeks
 - iii. We'll update to the latest release when available and upgrade the Kubernetes version to v1.21 for windows tests.
 - iv. Follow Up with sig-windows on adding a test for InfoRequest RPC callback
- Open a issue to discuss deprecation plan for sync controller when the design proposal is available
- Demo from Nilekh on helm upgrade hooks

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

July 22, 2021


Attendees

- Add Name
- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)
- Nilekh Chaudhari (Microsoft)
- Dane Murphy

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Anish
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Plan to have v0.2.0 release before v1.0.0
 - i. Harden the test and build pipelines
 - ii. This would bump v1.0.0 to ~September
 - o v0.1.0 release today
 - i. We're about ~week behind on this
 - o Sync all feature
 - i. [Issue](#)
 - ii. [Proposal](#)
 - o  [Secrets Store CSI Driver Sync Secrets](#)

Notes

- We will have a release v0.2.0
 - o Harden tests
- Release v0.1.0 planned for this week
 - o Goal for this release is for all providers to turn the feature on by default: return files in gRPC response and let driver write the files
- Sync all feature
 - o Sync all data from filesystem if syncAll set to true

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

July 08, 2021

Attendees

- Add Name
- Phill Gibson (Microsoft)
- Micah Hausler (AWS)
- Dane Murphy
- Tommy Murphy (Google)
- Tom Proctor (HashiCorp)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes:
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o

Notes

- Demo from Micah Hausler on using CSI tokens in exchange for AWS identities including pod-specific attributes

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

June 24, 2021

Attendees

- Dane Murphy
- Chris Sun (AWS)
- Rachel Sweeney
- Rita Zhang (Microsoft)
- Tommy Murphy (Google)
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)
- Joe Baro (AWS)
- Tom Proctor (HashiCorp)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Dane
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o (aramase) Demo: Using CSI Driver RequiresRepublish for rotation
 - Proposal: Secrets Store CSI Driver Auto Rotation Using CSI RequiresRepu...
 - o (joebaro) Allow optional JSMEPath specification for K8s secrets in driver (<https://github.com/aws/secrets-store-csi-driver-provider-aws/issues/11>)
 - i. https://drive.google.com/file/d/1sQVVhbuC1V_oZLeF5XfFHkFv0-GiKnpW/view
 - ii.
 - o (dane) Proposal and demo of [secretList](#)

- (tommymurphy) grpc interface status check
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/551>
- (tommymurphy) 15 July, [next release v0.1.0](#)
- (ritazh) helm 3 changes, how do we support crd updates, [PR comment](#)

Notes

- RequireRepublish will update secrets mounted in the pod's filesystem. This change means we can rely on Kubelet for rotation of secrets.
- This feature is available in v1.20+, so we still need to support rotation.
- JSMEPath
 - Should it be applied through the driver or provider?
 - Action item: open issue on github
- SecretList
 - Action item: everyone to comment in the [secretList](#) design doc and continue the discussion there
- July 15 v0.1.0 release
 - Providers should optionally return files to driver
 - Proposed optimization:
https://docs.google.com/document/d/1y1Oc1_-JGxMh-MZ57iqrVnoCln6V-W0vJcj3qmq8EWU/edit#heading=h.wcc6sjt8hen6
- Helm changes
 - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/289#issuecomment-866547334>
 - Pre-upgrade hook for handling upgrading CRDs with helm

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

June 10, 2021

Attendees

- Phill Gibson (Microsoft)
- Dane Murphy
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)

- Nilekh Chaudhari (Microsoft)
- Tom Proctor (HashiCorp)
- Add Name

Announcements

- AWS provider now in the list of supported providers:
<https://secrets-store-csi-driver.sigs.k8s.io/#supported-providers>

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o (Dane) Feature: Get all k/v value pairs from endpoint:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/529>
 - o (aramase) v0.0.23 release today
 - i. [Disables sync secret by default](#) (WARNING!!!)
 - ii. [New rbac role and binding for rotation](#)
 - o (aramase) Syncing as Kubernetes secret without mount:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/298>

Notes

- Feature: Get all k/v value pairs from endpoint
 - o For secretObjects, this is a field defined in the CRD schema and change would be in the driver
 - o Providers will also need to support
 - o Drivers don't have info on the parameters field in the SecretProviderClass. How will the driver be able to get the objectList from the parameters section?
 - o Maybe make SecretProviderClass more aware of the object and file mapping.
 - i. We could start with a proposal
 - ii. This is larger scope and could be done later
 - o Secret objects mapping of wildcards is a feasible usable project
 - i. Post v1.0 release
 - ii. We're prioritizing getting v1.0 with current
 - o **How do we handle when the list changes dynamically?**
 - i. Existing secrets that match regex deleted or new secrets added
 - ii. How to handle errors?
 - iii. Today we have the fixed list of objects to fetch which is static
 - o Action items:

- i. Design proposal
- V0.0.23 release
- Sync as Kubernetes secret
 - o Optionally not mount
 - o Preference to do the volume mount
 - o **Add this topic for discussion in the next sig-auth call**
 - i. Detailed document with pros and cons (Anish)
 - ii. Should this be 2 different projects or functionality within the same project?
 - iii. This could change the pod identity model as we no longer will have access to the pods service account token
 - iv. Share the doc

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

May 27, 2021

Attendees

- Micah Hausler (AWS)
- Phill Gibson (Microsoft)
- Dane Murphy
- Tom Proctor (HashiCorp)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)
- Sertac Ozercan (Microsoft)
- Nilekh Chaudhari (Microsoft)
- Kellin McAvoy
- Chen Xi (Uber)

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)

- Moderator: Phill Gibson
- Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - (lucas/knelasevero kellin/mcavoyk) - Our projects have similar goals and we want to check your thoughts on it <https://github.com/external-secrets/external-secrets>
 - (Oleg) - discuss new feature request [Optionally not fail volume mount for not-found secrets · Issue #567 · kubernetes-sigs/secrets-store-csi-driver \(github.com\)](#)
 - (micahhausler) Demo: prototype AWS credential provider leveraging [#471 \(TokenReview\)](#)

Notes

- External-secrets
 - Golang rewrite of previously owned godaddy project
 - Syncing as Kubernetes secrets without relying on pod mount is a requested feature in CSI driver
 - Is it possible to support SecretProviderClass with external-secrets?
 - External-secrets identity used for accessing secrets from the external secrets store
 - Micah going to demo using pod service account to access external secrets
 - CSI driver and External secrets project maintainers to try out the project and start a doc and possible integration.
- Not fail volume mount request for secrets not found
 - Ask to have an optional parameters to fail when secret not found
 - i. Similar to how Kubernetes secretRef supports optional today
 - Generally supportive of this. It should be an opt-in behavior
 - Rotation reconciler interval will be decider for when the secrets will be re fetched
 - If on SPC level, then implemented on the driver and if for each secret then it would be at the provider
 - Maybe an optional flag in the MountRequest that could be passed to the provider. The provider will send an empty response in the data field for the secret.
 - In agreement to implement this feature in the driver
 - i. Start with a design doc on how to add this feature to the driver
- Review the [release management PR](#) and add your feedback
- Tommy as approver!!! Please add your +1's to [PR](#)
- Micah Demo (YAY!!!)

Action Items

- TBD

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

May 13, 2021

Attendees

- Phill Gibson (Microsoft)
- Tommy Murphy (Google)
- Dane Murphy
- Nilekh Chaudhari (Microsoft)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)
- Sertac Ozercan (Microsoft)
- Rita Zhang (Microsoft)
- Chen Xi (Uber)
- Add Name

Announcements

-

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Anish Ramasekar, Rita Zhang
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o (lucas/knelasevero) - Our projects have similar goals and we want to check your thoughts on it <https://github.com/external-secrets/external-secrets> - (Discussion moved to 5/27/21 for Lucas availability)
 - o (tommymurphy) - aws status
 - i. <https://github.com/aws/secrets-store-csi-driver-provider-aws/issues/7>
 - ii. <https://github.com/aws/secrets-store-csi-driver-provider-aws/issues/12>
 - iii. <https://github.com/aws/secrets-store-csi-driver-provider-aws/issues/13>
 - iv. [integration testing PRs in progress](#)

- (tommymurphy) - atomic writer optimization [follow up](#)
- (tommymurphy) - atomic writer rollout:
 - i. [#520 merged](#) - v0.0.22
 - ii. suggest providers not make it a *default* until v0.0.23, required at v0.0.24
 - iii. Provider tracking issue:
 - <https://github.com/hashicorp/vault-csi-provider/issues/88>
 - <https://github.com/Azure/secrets-store-csi-driver-provider-azure/issues/475>
 -

Notes

- Code audit for aws provider
 - Tommy and Anish have opened issues in the aws provider repo
 - Review [PR](#) for adding aws integration tests
- Atomic writer optimization
 - Issue with the writer is for any update we need all the files to be sent back by the provider.
 - If there are no changes, provider can return empty files
 - If there are changes in just few secrets, providers would still need to return all the files
 - i. Providers can rely on caching/reading from the filesystem to get the current secrets that haven't changed to avoid making API calls.
 - Future work:
 - i. Include secret, path and version for each object
- Atomic writer rollout
 - PR has been merged to vendor in atomic writer
 - This will be included in the next release v0.0.22
 - Suggest providers to add the functionality for returning files to driver behind a feature flag and not make it default
- **Driver writing file feature is introduced in v0.0.21, providers must default to this by v0.0.23, driver required until v0.0.24**
- Release cadence
 - Consider releasing on 2nd Tuesday when windows patches are released
 - Helps mitigate vulnerabilities
- Driver Versioning
 - We are not stable yet. Stable version: v1.0.0
 - Pre-stable, should we cut minor versions allowing us to have patches and release branches?
 - When should we start cutting v0.1.0?

Action Items

- Open an issue with the AWS provider

- Issue in driver to track when the feature is implemented in providers as optional (v0.0.23) and required
- Define release cadence for driver: monthly?
- **Providers add warning in release notes when switching to driver writing file**
- Define semantic versioning for project

Review issues with leftover time

- [CI testgrids](#)
- [Issues](#)
- [PRs](#)

April 29, 2021

Attendees

- Add Name
- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Rita Zhang (Microsoft)
- Dane Murphy
- Sertac Ozercan (Microsoft)
- Tom Proctor (HashiCorp)
- Chris Sun(AWS)
- Nilekh Chaudhari (Microsoft)
- Magno Logan (Trend Micro)
- Joe Baro (AWS)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o (joearo/sunletia) - <https://github.com/aws/secrets-store-csi-driver-provider-aws>
Code audit for csi acceptance

Notes

- Coding audit for aws provider
 - o Integration test using bats or should we move to gingko?

- Related PR: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/245>
- Anish has started a doc for new test framework will share with everyone soon
- Optimization around provider calls and caching same version
- Proposal to let driver write the secrets:
https://docs.google.com/document/d/1y1Oc1_-JGxMh-MZ57igrVnoCln6V-W0vJcj3qmq8EWU/edit
-

April 15, 2021

Attendees

- Phill Gibson (Microsoft)
- Tommy Murphy (Google)
- Tom Proctor (HashiCorp)
- Anish Ramasekar (Microsoft)
- Sertac Ozercan (Microsoft)
- Dane Murphy
- Micah Hausler (AWS)
- Chen Xi (Uber)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Phill Gibson
 - Notes: Phill Gibson, Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [aramase] Making filtered watch default after n+3 releases
 - i. ref: <https://secrets-store-csi-driver.sigs.k8s.io/load-tests.html>
 - [tommymurphy] Removing files on auto-rotation
 - i. When an SPC changes should old files be deleted?
 - ii. Should providers be required to return the entire filesystem every time in the GRPC response even if no secrets have changed?
 - This would make it easier to use logic from atomic_writer.go
 - iii. Does any provider currently perform optimizations to avoid re-fetching secrets?
 - [aramase] Security audit
 - i. Received 2 RFPs. Planning to extend it until there are 4 RFPs.

Notes

- Making filtered watch default
 - o Add a warning in the logs if the node publish secret ref is still not labelled.
 - o Add a warning to the release notes about the upcoming default change.
- Removing files on auto-rotation
 - o Correct behavior would be to clean up files that are no longer referenced in SecretProviderClass as part of rotation.
 - o This is in sync with Kubernetes secrets mounted as volumes.
 - o Providers today don't perform optimizations to avoid re-fetching secrets.
 - o Supporting PATCH in the provider would complicate the driver-provider interface.
 - o Providers returning all the files to be written to the mount seems to be the best approach.
 - o Action:
 - i. Summarize this discussion in the GitHub issue
- E2E testing
 - o PR to add an initial test framework. This includes utilities and other helper functions for the testing.
 - o Today, the tests are defined/re-defined in each provider test suite.
 - o We need to change this behavior to have the driver define the tests and use the provider util to get the required SecretProviderClass for the tests.
 - o Test suite should focus only on the driver capabilities.

April 1, 2021

Attendees

- Phill Gibson (Microsoft)
- Magno Logan (Trend Micro)
- Chen Xi (Uber)
- Tommy Murphy (Google)
- Sertac Ozercan (Microsoft)
- Anish Ramasekar (Microsoft)
- Rita Zhang (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)

- Moderator: Phill Gibson
- Notes: Anish, Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [aramase] Release planned for today
 - i. PRs ready for review as part of release:
 - [chore: update debian base to buster-v1.5.0](#)
 - [chore: bump version to v0.0.21](#)
 - [docs: add load test spec and results](#)
 - [tommymurphy] rotation + deleted files
 - i. How can a provider signal to the driver to delete a file if it no longer exists on rotation?
 - ii. Through diff'ing returned files vs returned ObjectVersion in MountResponse?
 - [tommymurphy] atomic file updates
 - i. <https://github.com/kubernetes/kubernetes/issues/18372>
 - ii. <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/481>
 - [ritazh] discuss comments raised in [Disconnected scenarios design doc](#)

Notes

- [Anish] Release is planned for today
 - The load test doc PR has merged
 - This PR has load test optimizations and new features
- [Tommy] Should the driver handle deleting the files that are no longer required?
 - Today plugin's don't delete the files
 - Driver can determine files to delete based on the MountResponse
 - i. This however can be handled only after all the providers migrate to CSI driver writing to the file system.
 - [Anish] Users could update the SPC after initial deployment and would expect the pods to no longer have access to those old secrets.
 - i. This could be their approach for ephemeral secrets in the mount
 - [Anish] We handle this in synced K8s secret today
 - i. We perform a diff and publish new data in Kubernetes secrets
 - Tommy to open an issue in the driver repo to handle this scenario after all providers migrate to the CSI driver writing the files
- [tommymurphy] atomic file updates
 - This team will work with sig-storage to understand the benefit of atomic writer to see if we need it
- [ritazh] discuss comments raised in disconnected scenario doc
 - Concerns raised around source of truth if mount is optional
 - Need to get more user feedback for the different approaches

March 18, 2021

Attendees

- Phill Gibson (Microsoft)
- Tom Proctor (HashiCorp)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)
- Micah Hausler (AWS)
- Rita Zhang (Microsoft)
- Sertac Ozercan (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [aramase] [Disconnected scenarios design doc](#)
 - o [aramase] v0.0.21 release
 - i. Planned for this week but also want to include [PR](#) in v0.0.21 release so providers can start implementing the changes.
 - ii. Should we merge PR and cut the release next week?
 - o [ritazh] sig-auth is reviewing this project's CI jobs
 - o [micahhausler] - [kubernetes-sigs/secrets-store-csi-driver#453](#) - token request
 - o [aramase] Security RFP extended to 03/26

Notes

- Disconnected scenario:
 - o Make mount optional but sync secret and rotation features are required; need folks to review the design doc
- Next release
 - o Will wait for the PR before cutting v0.0.21
- Issue 453
 - o <https://github.com/kubernetes-sigs/secrets-store-csi-driver/blob/4c81aee69a46f289230f0e1529e3138c965817b2/provider/v1alpha1/service.proto#L54-L56> - how providers can know about results from a previous "Mount()"

- Would be cool to have a fake provider for e2e
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/472>
 - Would be cool to propagate additional volumeContext to the providers:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/475>
- Kubecon talk got accepted. YAY!!!
 - <https://sched.co/iE3L>

March 4, 2021

Attendees

- Add Name
- Magno Logan (Trend Micro)
- Chen Xi (Uber)
- Tommy Murphy (Google)
- Sertac Ozercan (Microsoft)
- Rita Zhang (Microsoft)
- Phill Gibson (Microsoft)
- Anish Ramasekar (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish
 - Notes: Tommy
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [chenxi] Compared to mounting kv values as file, is it possible to have custom yaml/json blob as files? Any plugin system from Provider?
 - [aramase] Optimization based on load testing
<https://docs.google.com/document/d/1ba8gTC-i33Df6uiOB8rW8jBX2B0IK8LszUjYIPzNwIQ/edit?usp=sharing>
 - i. PR: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/458/>

Notes

- TBD

- Providers pass through and write values to files where keys are the filename
- Azure provider has a in-process PR to combine multiple keys into a single file
- In progress - driver writes the files. Provider return all contents of the file
- Is it the provider or driver responsibility to organize the contents into files?
 - o Anish - it's the provider's responsibility
- Custom logic to convert k/v to custom blobs. general plugin or gateway in front of the provider.
- If each plugin implements its own templating, then perhaps it could be common functionality
- Provider is the only source of truth of secrets -> files mapping.
- Complicates mapping of secrets to k8s types for syncing. E.g. cert types. Each provider would have more context in what secret types are supported by this custom blob.
- Create issue in driver repo and start discussion there and corresponding issue in the vault plugin
- Load tests with CSI driver - 250 nodes, scaling # of pods
 - o Review doc + PR
 - o controller-runtime does not have filtered watch, so many API server connections from each node -> vendor cache package from controller-runtime and add filtered watch capability
 - o feature gate of filtered watch for *secrets*.
- Delayed on disconnected doc, stay tuned!
- Security audit: waiting on vendor pitches
-

Feb 18, 2021

Attendees

- Add Name
- Tommy Murphy (Google)
- Tom Proctor (HashiCorp)
- Phill Gibson (Microsoft)
- Sertac Ozercan (Microsoft)
- Rita Zhang (Microsoft)
- Chen Xi (Uber)
- Anish Ramasekar (Microsoft)
- Shoubhik Bose (Red Hat)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o CSI Driver token requests,
 - o <https://github.com/kubernetes/enhancements/blob/master/keps/sig-storage/1855-csi-driver-service-account-token/README.md> (Tom Proctor)
 - i. Follow up: Create an issue and assign to Tom
 - o Disconnected scenarios: Issue created
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/446>
 - i. Will follow up with design doc
 - o [Tommy] Update [Proposal: secret-store-csi-driver file IO consolidation](#)
 - i. Need to figure out if we establish a max size limit of 4mb
 - ii. K8s secret 1mb size limit
 - iii. Currently we have seen 120 secrets in one SPC
 - iv. Maybe consider starting the limit at 1mb for syncing secrets
 - v. Create a flag to toggle support for going beyond the size limit
 - vi. Size limit is also good for supportability and known limitations
 - o [Anish] Security audit: RFP PR merged and Google sheets created for questions
 - i. Has not started, scope is still tbd. Security audit team will contact Anish to get it started
 - ii. Once the audit starts, we will share which version to use for audit
 - o [Anish] v0.0.20 release planned for today
 - o [Phil] Serverless use cases?
 - o [Chen] Curious how this project works end to end. Current use cases are mesos, not k8s, and Hashicorp Vault on Uber infra and Hashicorp Vault on GCP.
 - i. CSI is not specific to k8s, it should work on mesos
 - ii. Sync secret prob won't work since we assume its k8s secrets
 - iii. How to test the csi driver locally? Checkout the e2es
 - o [Shoubhik] reference secrets as part of gitops; all manifests stored in git
 - i. SPC can be stored in git
 - ii. Interested in creating k8s secrets without the mount requirement
 - iii. Issue:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/298>
 - iv. Semi-related project: <https://github.com/external-secrets/external-secrets>

Notes

- TBD

Feb 4, 2021

Attendees

- Phill Gibson (Microsoft)
- Rita Zhang (Microsoft)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)
- Sertac Ozercan (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Anish
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [Rita] Disconnect scenarios (do people have this requirement?)
 - o [Tommy] [Proposal: secret-store-csi-driver file IO consolidation](#)
 - o Security audit will start in few weeks per sig-security

Notes

- Disconnect scenarios:
 - o What is the duration it's offline?
 - o Caching ACL to determine if the pod has access to it
 - o CSI driver today already writes the contents to the mount path and the ACL isn't validate after
 - o If multiple pods using the SecretProviderClass, then we could potentially batch the calls
 - o Change the behavior of the CSI plugin to succeed mounts even with failures

- i. This behavior is different from how Kubernetes secrets works
 - ii. Could be an opt in behavior as this isn't backward compatible
 - iii. Doesn't solve disconnect scenarios but allows pod to startup
- Need to clarify how long the disconnect is
- Syncing as Kubernetes secret could be an option
 - i. The K8s secret will not be cached and can be used by applications to read from in disconnect scenarios
 - ii. The lifecycle of the K8s secret can be controlled by the CSI driver (via TTL)
 - iii. Need to check with sig-auth as this is an anti-pattern
- Next step:
 - i. Create issue for disconnect scenario
 - ii. Ask users for requirements
 - iii. Gauge how many users want this and acceptable behavior
- File I/O consolidation proposal
 - Comments in the proposal

Jan 21, 2021

Attendees

- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)
- Rita Zhang (Microsoft)
- Sertac Ozercan (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Anish
 - Notes: Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [aramase] Driver [v0.0.19](#) released
 - [Tom Proctor] Running providers as non-root users
 - i. Provider needs hostPath, does that require root priv? We could use PSP to restricted priv for restricted access
 - ii. Let driver handle writing of the content instead of the providers
 - Sidecar:

- Cons: need restart of the driver when new providers are introduced
- iii. Tom will open an issue for this and Tommy mentioned he is working on a design proposal for it
- o [aramase] secrets-store-csi-driver has been added to the scope of the RFP for third party audit
 - i. Security audit meeting notes:

https://docs.google.com/document/d/13XC_DpIpfQDv9-PgWBplyWjvYObiF0snR-x2k69ECtl/edit#heading=h.2v1y6eo6pavm
 - ii. ETA ~ 1 month to find a vendor
- o HashiCorp Vault provider needs to be updated in driver's e2e. Tom has a PR.
- o AWS is working on its own provider

Notes

- <Add notes here>

Jan 7, 2021

Attendees

- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Phill Gibson (Microsoft)
- Mael Valais (cert-manager contributor)
- Rita Zhang (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Anish Ramasekar
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Credentials used for driver prow jobs
 - i. Recently we had the gcp test jobs fail because the credentials expired:

<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/418>
 - What can we do to ensure the credentials are valid for a longer time?

- How to rotate prow credentials in a more sustainable manner?
- [Phill] Updating community call Zoom meeting to include a password
 - i. Avoid potential Zoom meeting bombs
 - ii. No default screen sharing (host will promote when needed)
 - iii. Whiteboard feature has been disabled
- [aramase] v0.0.19 last release that'll support backward compatibility with old provider formats
 - i. Should we make grpc default and deprecate invoking provider binary starting v0.0.20 release?
- [Phill] Year goals/plans for the CSI Project
 - i. Any items we want to commit to on the project board for 2021?

Notes

- Credentials used:
 - GCP creds used are governed by Google policy and exported creds have a max lifetime of 90 days.
 - Tommy is exploring options internally.
 - If we have access to base prow identity, we could leverage that for the jobs. Using the same identity will enable faster rotation.
 - Check with Ben Elder on #sig-testing
- Zoom meeting
 - Password included from next meeting.
 - Sharing capability disabled. Request host access to share.
 - The passcode will be added with the zoom meeting url.
- GRPC support:
 - V0.0.20 will deprecate support for old binary provider format.
- Goals for project:
 - Review and make progress on Stable milestones.
 - Check with sig-auth on how to get funding for subproject and security review.
 - V1.0 release after stable milestone is complete
 - Good indicator for stability testing and security reviews.
- Tommy going to work on proposal for driver handling secret writes to filesystem
 - Provider fetches from external secrets store and sends the contents back as part of the GRPC response.
 - Determine impact for a large number of external secrets store objects.

December 17, 2020

Attendees

- Phill Gibson (MSFT)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: TBD
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [Phill Gibson] - Zoom meeting security settings
 - i. We'll be adding a meeting code
 - ii. To share you will need to be granted co-host (Please follow CNCF guidelines)
 - iii. Screen annotations and whiteboard will be disabled
 - o [Phill Gibson] - Next meeting will be January 7th 2021
 - o [aramase] Driver v0.0.18 released
 - o [Tom] gRPC support coming soon, [PR](#)

Notes

- [HashiCorp Vault] Draft PR open for grpc changes

December 3, 2020

Meeting cancelled due to lack of attendance

Attendees

- (add your name/org)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: TBD
 - o Notes: TBD
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o V0.0.18 release planned for next week
 - o Reuse grpc clients PR:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/394>
 - i. Should the provider clients be created on the fly?
 - o Announcement:
 - i. Tommy added as a reviewer

Notes

-

November 12, 2020

Attendees

- (add your name/org)
- Phill Gibson (Microsoft)
- Tom Proctor (HashiCorp)
- Rita Zhang (Microsoft)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Driver [v0.0.17](#) released

- i. CVE disclosed -
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/378>
- ii. TODO:
 - Need to disclose this CVE on slack channel to encourage folks to upgrade to the v0.0.17 release
- Doc for [Secrets Store CSI Driver Membership](#)
 - i. TODO:
 - everyone review this doc before next community call
 - Open PR in the repo for this
- Stable milestone created in driver based on last week community call -
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/milestone/5>
 - i. Need to review
<https://github.com/kubernetes/enhancements/blob/master/keps/NNNN-kep-template/README.md#production-readiness-review-questionnaire> and add to the Stable/GA doc
 - ii. TODO:
 - Open a PR for this
- HashiCorp provider:
 - i. TODO:
 - GRPC changes are WIP
 - PR: 0.0.5 with the breaking changes and 0.0.6 with bug fix should be propagated to the driver e2e
- Netlify doc site [PR](#) needs more review

Notes

-

October 29, 2020

Attendees

- (add your name/org)
- Tommy Murphy (Google)
- Tom Proctor (HashiCorp)
- Anish Ramasekar (Microsoft)
- Rita Zhang (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Anish
 - o Notes: Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o Review Secrets Store CSI Driver GA/Stable proposal -
https://docs.google.com/document/d/1ySjR_Zk93Kk7rel8Zla4Spum-xArx3jRKPsFWTUKNr0/edit?usp=sharing
 - i. Vault has dynamic secrets
 - ii. Partial provider failure results in the mount failure for the pod
 - iii. Create github issues and tag them with stable milestone based on the google docs
 - o Vault grpc update?
 - i. Tom: will work on that next. Suggestion: create issues/milestones in the vault provider repo to signal timeline/roadmap

Notes

-

October 15, 2020

Attendees

- (add your name/org)
- Phill Gibson (Microsoft)
- Tommy Murphy (Google)
- Rita Zhang (microsoft)
- Anish Ramasekar (Microsoft)
- Bryan Leighton (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)

- Moderator: Phill Gibson
- Notes: Rita
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [aramase] Secrets Store CSI Driver GA/Stable proposal -
https://docs.google.com/document/d/1ySjR_Zk93Kk7rel8Zla4Spum-xArx3jRKPsFWTUKNr0/edit?usp=sharing
 - i. Share link on Slack channel, tagging all the provider maintainers. Will review this together in the next community call in 2 weeks.
 - ii. Next step to follow this doc is to create backward compatibility contract doc and release management doc after the project goes to stable
 - [phillipgibson] CSI Azure Provider GitHub page moving to Hugo Docsy theme
 - i. Ref. <https://azure.github.io/aad-pod-identity/docs/>
 - Announcement:
 - i. GCP provider is now integrated!

Notes

•

October 1, 2020

Attendees

- (add your name/org)
- Phill Gibson (Microsoft)
- James Munnely (Apple)
- Tom Proctor (HashiCorp)
- Rita Zhang (Microsoft)
- Anish Ramasekar (Microsoft)
- Tommy Murphy (Google)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Phill Gibson

- Notes: James Munnelly
- Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [aramase] Rotation PR merged. Ready to release v0.0.15?
 - Helm 2 chart update - [Move crds to crds dir for helm3 and install CRDs flag for supporting h...](#) · Issue #289 · kubernetes-sigs/secrets-store-csi-driver
 - Discuss comment on side car for Hashicorp Vault provider
https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/303#discussion_r490361295
 - Supporting reconcile interval per SPC -
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/322>
 - General discussion around SPC & restrictions on volumeAttributes

Notes

- Rotation PR has been reviewed
 - V0.0.15 to be released tomorrow
 - Kubernetes Events are generated when the secrets are rotated to help inform users
 - Depending on the 'target', there are different watch mechanisms for detecting whether rotation is needed (e.g. filesystem vs Kubernetes secret store which supports watches)
- Helm 2 chart update
 - PR looks good, but concerns around how CRDs are deployed/managed
 - CRDs are not upgraded after initial install when they are moved into crds/ directory ([upstream link](#))
 - Will revisit this and share in future call
 - Likely to defer this to v0.0.16 release to avoid too many CRD changes at once
- Sidecar for secret providers
 - Questions around how the sidecar would notify that driver that secrets have been updated on disk in order to sync them back into Kubernetes secrets
 - Currently the driver is responsible for rotating the secrets, which means Vault/the secret store cannot control how often rotations happen (which could lead to wasteful configuration)
 - Anish: the provider *can* actually influence/inform the driver whether to actually update/fetch the secret
- Supporting reconcile interval per SPC
 - Allowing to say "this SPC should rotate every X hours, that SPC should rotate every Y hours"
 - Call for discussion
 - Tommy: helps to reduce the number of requests sent to the secret store

- The rotation reconciler can poll quite often, and the provider can then decide to not to actually service the request until a certain TTL has passed
- The provider is informed of what the current versions of stored secrets are, as pulled from the SecretProviderClassPodStatus object
- If lots of providers are having to replicate this back-off logic, we should try and move this into the driver. Though we can wait and see how this shakes out before taking this action.
- Pending feedback as the project matures
- SPC & restrictions on volumeAttributes
 - Rationale: Pod portability and RBAC: <https://github.com/kubernetes-sigs/secrets-store-csi-driver/issues/42>
 - James: will work on a doc to describe this

September 17, 2020

Attendees

- (add your name/org)
- Phill Gibson (Microsoft)
- Tommy Murphy (Google)
- Tom Proctor (HashiCorp)
- Jason O'Donnell (HashiCorp)
- Rita Zhang (Microsoft)
- Anish Ramasekar (Microsoft)
- Bryan Leighton (Microsoft)
- Rajath Ravikumar (AWS)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Phill Gibson
 - Notes: Phill Gibson
- Standup/Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - [aramase] v0.0.14 release planned for this week
 - i. This release will include gRPC changes
 - ii. Rotation is planned for v0.0.15

- [Tom] Default gRPC service definitions
 - i. Provider should reference the service definitions via:

<https://github.com/kubernetes-sigs/secrets-store-csi-driver/tree/master/provider/v1alpha1>
 - ii.
- [jason] Vault CSI Updates
 - i. <https://gist.github.com/jasonodonnell/a32da16feee5323aa655a2d1daaf1ad3>
 - ii.
- [rita] Default RBAC required for driver:

https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/303#discussion_r486773408
 - i. Should work with node isolation
 - ii. Default should not allow escalation between node workloads
- E2e test framework PR needs more review:

<https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/245>
-

Notes

-

September 3, 2020

Attendees

- (add your name/org)
- Phill Gibson (Microsoft)
- Tommy Murphy (Google)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)
- Micah Hausler (AWS)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - Moderator: Phill Gibson
 - Notes: Phill Gibson

- Standup/Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [aramase] Driver [v0.0.13](#) released
 - o Next milestone - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/milestone/2>
 - o Guidance on adding attribution for code taken/inspired from other projects?
 - i. Is there an official CNCF guidance we can follow?
 - o [aramase] Helm2 and Helm3 chart support - [PR](#)
 - i. Helm3 doesn't upgrade the CRDs as part of helm upgrade
 - o [Rotation reconciler with GRPC](#)
 - o [GRPC support for driver-provider communication](#) merged

Notes

- Check if there is an official process for PR templates for code attribution being identities
- Helm v3 does not support the lifecycle of CRDs
- AWS provider is on the roadmap
- Hashicorp will be looking at adding gRPC support to the Vault provider

August 19, 2020

Meeting canceled due to KubeCon EU

August 6, 2020

Attendees

- (add your name/org)
- Phill Gibson (Microsoft)
- Jay Pipes (AWS)
- Rita Zhang (Microsoft)
- Heba Elayoty (Microsoft)
- Tommy Murphy (Google)
- Colin Man (google)
- Anish Ramasekar (Microsoft)
- Tom Proctor (HashiCorp)
- Oleg Sucharevich (Codefresh)
- Bryan Leighton (Microsoft)

- Rajath Ravikumar (AWS)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson (Microsoft)
 - o Notes: Phill Gibson
- Standup/Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - Rotation reconciler demo based on current design doc - https://docs.google.com/document/d/1RGT0vmeUnN71n_u5fZKsSCa2YQpGw99rfGN9RIFMgHs/edit?usp=sharing
 - How will apps consume the updated content?
 - Events?
 - [tommymurphy] will provide link to K8s issue where K8s has not solved propagating secrets changes to pods
 - POC demo using grpc for driver-provider communication
 - Anish will open a PR for this change
 - It will be flag gated for backward compat until all providers have moved to grpc
 - Need to get a timeline for when all providers will support GRPC
 - controller-gen & separating roles. Makefile generating RBAC roles
 - Single call adds all permissions to a single role, but would like to separate secret permissions into a separate role([PR](#)). split permissions between /pkg and /controller? Other best practices?
 - Provider updates?
 - Google provider is working on integration test
 - AWS has started design, no development yet
 - Review issues backlog
 - Phill Gibson access to create project board for Secrets Store CSI Driver repo
- github.com/kubernetes/kubernetes/pull/93130
 - Big deal for AWS. Want to hear how that is going and how we can help :)
 - KEP <https://github.com/kubernetes/enhancements/pull/1855> was discussed in a previous community call
 - May need to bump this PR if we want it to land in 1.19 (release date: August 25th)
 -

Notes

-

July 23, 2020

Attendees

- (add your name/org)
- Tommy Murphy (Google)
- Colin Man (Google)
- Anish Ramasekar (Microsoft)
- Rita Zhang (Microsoft)
- Tom Proctor (HashiCorp)
- Phill Gibson (Microsoft)
- Jim Kalafut (HashiCorp)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Phill Gibson
- Standup/Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - secrets-store-csi-driver [v0.0.12](#) released
 - Next milestone, Need more contributors! :) - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/milestone/1>
 - Ability to configure provider call context using a flag (--context-timeout)
 - Replacing e2e test suite with ginkgo - [Issue](#) and [PR](#)
 - "get service account token for csi driver" KEP has been merged - <https://github.com/kubernetes/enhancements/pull/1855>
 - Follow-ups from last sync:
 - Secret rotation feature design review - https://docs.google.com/document/d/1RGT0vmeUnN71n_u5fZKsSCa2YQpGw99rfGN9RIFMgHs/edit?usp=sharing
 - Vault provider:
 - Update Vault provider to use latest release
 - Vault provider helm chart
 - Vault provider windows support

- Assignments for next meeting (to be determined by asking for volunteers near the end of this meeting):
 - Moderator: TBD
 - Notes: TBD

Notes

- Make deprecations more obvious for releases and include in release notes
- Do backlog grooming as part of the call
- Create project board
- Create semantic versioning of milestones
- Take a look at PR #245 to see if this enhances the contributor experience
- Review Secret rotation feature design review
- Create table in the readme.md of all the providers, releases, feature matrix, and the features w/ examples for users
- Sync Kubernetes secrets functionality
 - Helm currently does not make this feature optional
 - Having the feature configurable at the driver level
 - Enabled by default for the next 2 releases. Add a clear message to release notes for disabled by default in 2 releases

July 09, 2020

Attendees

- (add your name/org)
- Phill Gibson (Microsoft)
- Tommy Murphy (Google)
- Bryan Leighton (Microsoft)
- Anish Ramasekar (Microsoft)
- Mo Khan (VMware)
- Lachlan Evenson (MSFT)
- Rita Zhang (Microsoft)

Agenda

- Assignments for this meeting: (if not present, then replace)
 - o Moderator: Phill Gibson
 - o Notes: Phill Gibson
- Standup/Discussion items (add items here; include topic, your name, and relevant issues/PRs)
 - o [ritazh] Follow-ups from last sync:
 - i. Discuss what 1.0 requires for providers and the driver:
<https://docs.google.com/document/d/1YZrHMQcizAYoTUY0i9RkOhElf1eBnnwjtTPOr0j1QUY/edit?usp=sharing>
 - ii. K8s secrets sync reconciler feature design review:
<https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/224>
 - iii. Secret rotation feature design review -
https://docs.google.com/document/d/1RGT0vmeUnN71n_u5fZKsSCa2YQpGw99rfGN9RIFMgHs/edit?usp=sharing
 - iv. Update Vault provider to use 0.0.5 release
 - v. Vault provider helm chart
 - vi. Vault provider windows support
 - o [tommymurphy] Point out: <https://github.com/kubernetes/enhancements/pull/1855> "get service account token for csi driver"
 - i. [GCP secrets plugin](#) would like to use this for workload identity and reloading [new values of secrets](#)
 - o [aramase] Discuss supporting custom namespace for SecretProviderClass reference - <https://github.com/kubernetes-sigs/secrets-store-csi-driver/pull/241>
 - i. As part of next release change has been made to only support SecretProviderClass from same namespace as the pod
 - o
- Assignments for next meeting (to be determined by asking for volunteers near the end of this meeting):
 - o Moderator: TBD
 - o Notes: TBD