

Secrets in Kubernetes Across Cloud

"Life is really simple, but we insist on making it complicated."
Confucius

Jhonny Pong (Jhonnatan Gil)

@jthan24



Jhonnatan Gil Chaves

DevOps Engineer @ AppGate

Manage secrets across
cloud on kubernetes

Conf42 DevSecOps 2021

Thursday December 2nd | 5PM GMT



conf42.com

Contents

aws-ssm

azure-keyvault

gcp-secret-manager

hashicorp-vault

Kubernetes

Secrets

external secrets

demo

AWS - Systems Manager Parameter Store

Parameter Store, a capability of AWS Systems Manager, provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, Amazon Machine Image (AMI) IDs, and license codes as parameter values. You can store values as plain text or encrypted data. You can reference Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the unique name that you specified when you created the parameter.

AWS Systems Manager > Parameter Store > Create parameter

Create parameter

Parameter details

Name:

Description — Optional:

Tier
Parameter Store offers standard and advanced parameters.

☒ **Standard**
Limit of 10,000 parameters. Parameter value size up to 4 KB. Parameter policies are not available. No additional charge.

☐ **Advanced**
Can create more than 10,000 parameters. Parameter value size up to 8 KB. Parameter policies are available. Charges apply.

Type

☐ **String**
Any string value.

☐ **StringList**
Separate strings using commas.

☒ **SecureString**
Encrypt sensitive data using KMS keys from your account or another account.

KMS key source

☒ **My current account**
Use the default KMS key for this account or specify a customer-managed key for this account. [Learn more](#)

☐ **Another account**
Use a KMS key from another account. [Learn more](#)

KMS Key ID:

Value

Maximum length: 4096 characters.

My parameters

View details Edit Delete Create parameter

<input type="checkbox"/>	Name	Tier	Type	Last modified
<input type="checkbox"/>	my-secret-aws	Standard	SecureString	Wed, 15 Sep 2021 00:57:22 GMT



Azure - Key Vault Secrets

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed hardware security module(HSM) pools. Vaults support storing software and HSM-backed keys, secrets, and certificates. Managed HSM pools only support HSM-backed keys.

Basics Access policy Networking Tags Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Key vault name *

Region *

Pricing tier *

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover a key vault and secrets for the duration of the retention period. This protection applies to all keys and secrets within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vault period elapsing, you can turn on purge protection. When purge protection is enabled, secrets are deleted by Microsoft.

Soft-delete ☐ Enabled

Days to retain deleted vaults *

Purge protection ☐ ☒ Disable purge protection (allow key vault retention period) ☐ Enable purge protection (enforce a mandatory retention period on vaults and vault objects)

Basics Access policy Networking **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.

Name	Value	Resource
<input type="text"/>	<input type="text"/>	Key vault

Home > Key vaults > kv-test-mode >

Create a secret

Upload options

Name *

Value *

Content type (optional)

Set activation date ☐

Set expiration date ☐

Enabled ☒ Yes ☐ No

Tags



GCP - Secret Manager

Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud.

Google Cloud Platform CamiloTorresJCRutas secret

Seguridad

← Crear secreto

Detalles del Secret

Esta acción creará un Secret con el valor del Secret de la primera versión. [Más información](#)

Nombre

my-secret-gcp

El nombre debe poder identificarse y ser único en este proyecto.

Valor secreto

Ingresar tu valor secreto o importarlo directamente desde un archivo.

Subir archivo EXPLORAR

Tamaño máximo: 64 KiB

Valor secreto

my-secret

Política de replicación

Según la configuración predeterminada, Google administra automáticamente la ubicación en la que se almacena este Secret. Si necesitas administrarlo de forma manual, marca la siguiente casilla para personalizar las ubicaciones. Se puede acceder a nivel mundial a todos los Secrets sin importar cómo están replicados y almacenados. La política de replicación no se puede cambiar después de que se crea un Secret. [Más información](#)

☐ Administrar ubicaciones de forma manual para este Secret

Encriptación

Este secreto está encriptado de forma predeterminada con una clave administrada por Google. Si quieres administrar tu encriptación, puedes usar una clave administrada por el cliente en su lugar. [Más información](#)

☐ Usar una clave de encriptación administrada por el cliente (CMK)

Rotación

Si configuras un periodo de rotación, se enviarán notificaciones de rotación a los temas de Pub/Sub. Secret Manager no rotará de forma automática el valor del Secret. [Más información](#)

☐ Establecer periodo de rotación

Notificaciones

Selecciona los temas de Pub/Sub que recibirán notificaciones de eventos cuando se modifique el secreto o una de sus versiones. Estos eventos pueden ser eventos iniciados por el usuario o programados. [Más información](#)

CREAR SECRETO CANCELAR

← Detalles del secreto EDITAR SECRETO BORRAR

Secret: "my-secret-gcp"

projects/417425098745/secrets/my-secret-gcp

DESCRIPCIÓN GENERAL VERSIONES PERMISOS REGISTROS

Versiones + VERSIÓN NUEVA HABILITAR INHABILITAR DESTRUIR

<input type="checkbox"/>	Versión	Estado	Encriptación	Fecha de creación ↓	Acciones
<input type="checkbox"/>	1	✓ Habilitada	Administrada por Google	15/9/21 01:49	⋮

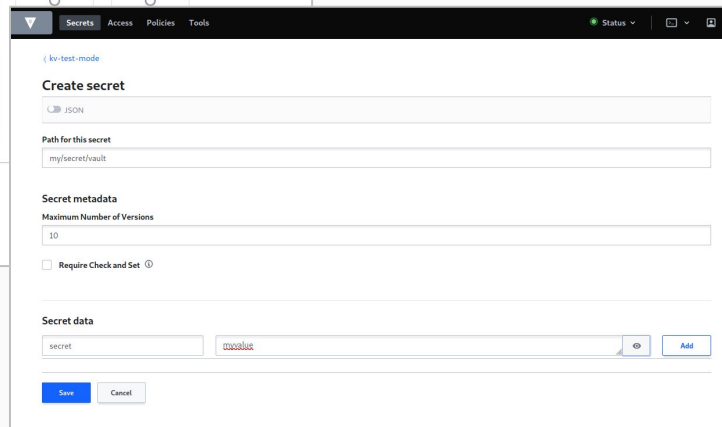
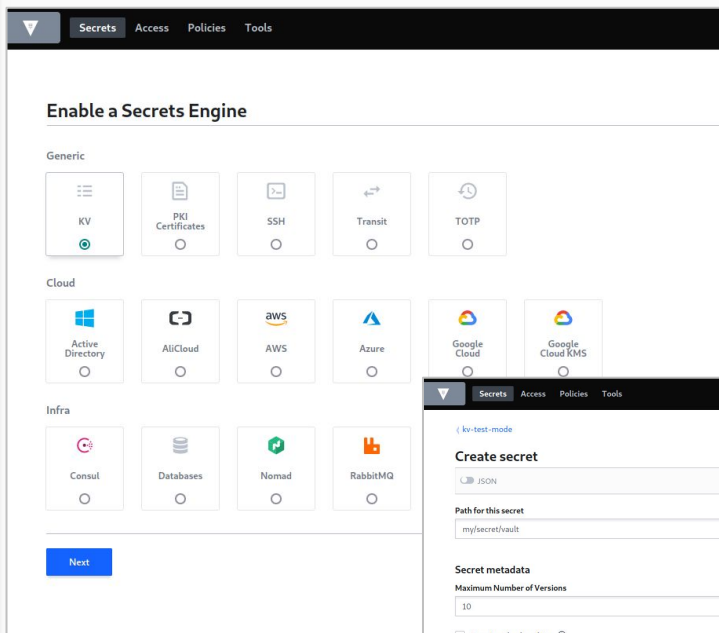
No se seleccionaron versiones



Hashicorp - Vault

Vault is a tool for securely accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. Vault provides a unified interface to any secret, while providing tight access control and recording a detailed audit log.

Secure Secret Storage: Arbitrary key/value secrets can be stored in Vault. Vault encrypts these secrets prior to writing them to persistent storage, so gaining access to the raw storage isn't enough to access your secrets. Vault can write to disk, Consul, and more.



Kubernetes

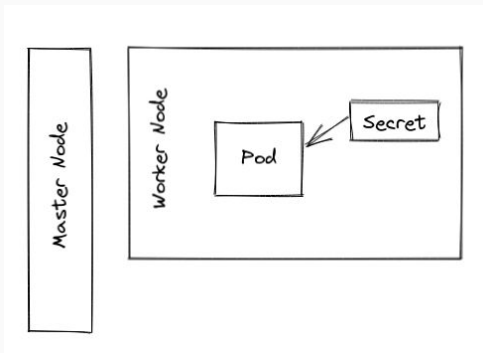
What is kubernetes

Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available.



Secrets

A Secret is an object that contains a small amount of sensitive data such as a password, a token, or a key. Such information might otherwise be put in a Pod specification or in a container image. Using a Secret means that you don't need to include confidential data in your application code.



External Secrets

External Secrets Operator is a Kubernetes operator that integrates external secret management systems like AWS Secrets Manager, HashiCorp Vault, Google Secrets Manager, Azure Key Vault and many more. The operator reads information from external APIs and automatically injects the values into a Kubernetes Secret.



What, ¿operator?

Operators are software extensions to Kubernetes that make use of custom resources to manage applications and their components. Operators follow Kubernetes principles, notably the control loop.

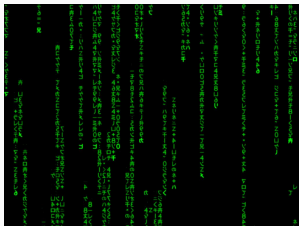


External Secrets - Architecture

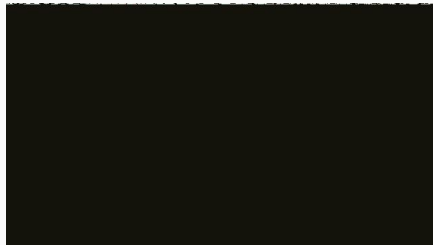
First, define secret in your cloud or on premise (Bare Metal) provider.



Second, write your YAML config file to obtain secret.



Third, use the secret in your Cluster.



Demo Time



Back to slide 7

First create a secret in vault.

[illegible]

Second deploy external secrets with helm in Kubernetes cluster.

```

1 #!/usr/bin/perl
2 #
3 # Name: SecurityTools
4 #
5 # Name: vuln-backend
6 #
7 # Author:
8 #
9 # server: http://192.168.10.130:13307
10 # path: /vuln-backend/
11 # url: http://192.168.10.130:13307/vuln-backend/
12 #
13 # vuln-backend()
14 #
15 # name: vuln-backend
16 # url: http://192.168.10.130:13307/vuln-backend/
17 #
18 #
19 #
20 #
21 #
22 #
23 #
24 #
25 #
26 #
27 #
28 #
29 #
30 #
31 #
32 #
33 #
34 #
35 #
36 #
37 #
38 #
39 #
40 #
41 #
42 #
43 #
44 #
45 #
46 #
47 #
48 #
49 #
50 #
51 #
52 #
53 #
54 #
55 #
56 #
57 #
58 #
59 #
60 #
61 #
62 #
63 #
64 #
65 #
66 #
67 #
68 #
69 #
70 #
71 #
72 #
73 #
74 #
75 #
76 #
77 #
78 #
79 #
80 #
81 #
82 #
83 #
84 #
85 #
86 #
87 #
88 #
89 #
90 #
91 #
92 #
93 #
94 #
95 #
96 #
97 #
98 #
99 #
100 #
101 #
102 #
103 #
104 #
105 #
106 #
107 #
108 #
109 #
110 #
111 #
112 #
113 #
114 #
115 #
116 #
117 #
118 #
119 #
120 #
121 #
122 #
123 #
124 #
125 #
126 #
127 #
128 #
129 #
130 #
131 #
132 #
133 #
134 #
135 #
136 #
137 #
138 #
139 #
140 #
141 #
142 #
143 #
144 #
145 #
146 #
147 #
148 #
149 #
150 #
151 #
152 #
153 #
154 #
155 #
156 #
157 #
158 #
159 #
160 #
161 #
162 #
163 #
164 #
165 #
166 #
167 #
168 #
169 #
170 #
171 #
172 #
173 #
174 #
175 #
176 #
177 #
178 #
179 #
180 #
181 #
182 #
183 #
184 #
185 #
186 #
187 #
188 #
189 #
190 #
191 #
192 #
193 #
194 #
195 #
196 #
197 #
198 #
199 #
200 #
201 #
202 #
203 #
204 #
205 #
206 #
207 #
208 #
209 #
210 #
211 #
212 #
213 #
214 #
215 #
216 #
217 #
218 #
219 #
220 #
221 #
222 #
223 #
224 #
225 #
226 #
227 #
228 #
229 #
230 #
231 #
232 #
233 #
234 #
235 #
236 #
237 #
238 #
239 #
240 #
241 #
242 #
243 #
244 #
245 #
246 #
247 #
248 #
249 #
250 #
251 #
252 #
253 #
254 #
255 #
256 #
257 #
258 #
259 #
260 #
261 #
262 #
263 #
264 #
265 #
266 #
267 #
268 #
269 #
270 #
271 #
272 #
273 #
274 #
275 #
276 #
277 #
278 #
279 #
280 #
281 #
282 #
283 #
284 #
285 #
286 #
287 #
288 #
289 #
290 #
291 #
292 #
293 #
294 #
295 #
296 #
297 #
298 #
299 #
300 #
301 #
302 #
303 #
304 #
305 #
306 #
307 #
308 #
309 #
310 #
311 #
312 #
313 #
314 #
315 #
316 #
317 #
318 #
319 #
320 #
321 #
322 #
323 #
324 #
325 #
326 #
327 #
328 #
329 #
330 #
331 #
332 #
333 #
334 #
335 #
336 #
337 #
338 #
339 #
340 #
341 #
342 #
343 #
344 #
345 #
346 #
347 #
348 #
349 #
350 #
351 #
352 #
353 #
354 #
355 #
356 #
357 #
358 #
359 #
360 #
361 #
362 #
363 #
364 #
365 #
366 #
367 #
368 #
369 #
370 #
371 #
372 #
373 #
374 #
375 #
376 #
377 #
378 #
379 #
380 #
381 #
382 #
383 #
384 #
385 #
386 #
387 #
388 #
389 #
390 #
391 #
392 #
393 #
394 #
395 #
396 #
397 #
398 #
399 #
400 #
401 #
402 #
403 #
404 #
405 #
406 #
407 #
408 #
409 #
410 #
411 #
412 #
413 #
414 #
415 #
416 #
417 #
418 #
419 #
420 #
421 #
422 #
423 #
424 #
425 #
426 #
427 #
428 #
429 #
430 #
431 #
432 #
433 #
434 #
435 #
436 #
437 #
438 #
439 #
440 #
441 #
442 #
443 #
444 #
445 #
446 #
447 #
448 #
449 #
450 #
451 #
452 #
453 #
454 #
455 #
456 #
457 #
458 #
459 #
460 #
461 #
462 #
463 #
464 #
465 #
466 #
467 #
468 #
469 #
470 #
471 #
472 #
473 #
474 #
475 #
476 #
477 #
478 #
479 #
480 #
481 #
482 #
483 #
484 #
485 #
486 #
487 #
488 #
489 #
490 #
491 #
492 #
493 #
494 #
495 #
496 #
497 #
498 #
499 #
500 #
501 #
502 #
503 #
504 #
505 #
506 #
507 #
508 #
509 #
510 #
511 #
512 #
513 #
514 #
515 #
516 #
517 #
518 #
519 #
520 #
521 #
522 #
523 #
524 #
525 #
526 #
527 #
528 #
529 #
530 #
531 #
532 #
533 #
534 #
535 #
536 #
537 #
538 #
539 #
540 #
541 #
542 #
543 #
544 #
545 #
546 #
547 #
548 #
549 #
550 #
551 #
552 #
553 #
554 #
555 #
556 #
557 #
558 #
559 #
560 #
561 #
562 #
563 #
564 #
565 #
566 #
567 #
568 #
569 #
570 #
571 #
572 #
573 #
574 #
575 #
576 #
577 #
578 #
579 #
580 #
581 #
582 #
583 #
584 #
585 #
586 #
587 #
588 #
589 #
590 #
591 #
592 #
593 #
594 #
595 #
596 #
597 #
598 #
599 #
600 #
601 #
602 #
603 #
604 #
605 #
606 #
607 #
608 #
609 #
610 #
611 #
612 #
613 #
614 #
615 #
616 #
617 #
618 #
619 #
620 #
621 #
622 #
623 #
624 #
625 #
626 #
627 #
628 #
629 #
630 #
631 #
632 #
633 #
634 #
635 #
636 #
637 #
638 #
639 #
640 #
641 #
642 #
643 #
644 #
645 #
646 #
647 #
648 #
649 #
650 #
651 #
652 #
653 #
654 #
655 #
656 #
657 #
658 #
659 #
660 #
661 #
662 #
663 #
664 #
665 #
666 #
667 #
668 #
669 #
670 #
671 #
672 #
673 #
674 #
675 #
676 #
677 #
678 #
679 #
680 #
681 #
682 #
683 #
684 #
685 #
686 #
687 #
688 #
689 #
690 #
691 #
692 #
693 #
694 #
695 #
696 #
697 #
698 #
699 #
700 #
701 #
702 #
703 #
704 #
705 #
706 #
707 #
708 #
709 #
710 #
711 #
712 #
713 #
714 #
715 #
716 #
717 #
718 #
719 #
720 #
721 #
722 #
723 #
724 #
725 #
726 #
727 #
728 #
729 #
730 #
731 #
732 #
733 #
734 #
735 #
736 #
737 #
738 #
739 #
740 #
741 #
742 #
743 #
744 #
745 #
746 #
747 #
748 #
749 #
750 #
751 #
752 #
753 #
754 #
755 #
756 #
757 #
758 #
759 #
760 #
761 #
762 #
763 #
764 #
765 #
766 #
767 #
768 #
769 #
770 #
771 #
772 #
773 #
774 #
775 #
776 #
777 #
778 #
779 #
780 #
781 #
782 #
783 #
784 #
785 #
786 #
787 #
788 #
789 #
790 #
791 #
792 #
793 #
794 #
795 #
796 #
797 #
798 #
799 #
800 #
801 #
802 #
803 #
804 #
805 #
806 #
807 #
808 #
809 #
810 #
811 #
812 #
813 #
814 #
815 #
816 #
8
```

Third using external secrets operator for configure vault.

[illegible]

Fourth sync secret from vault to secret in kubernetes.

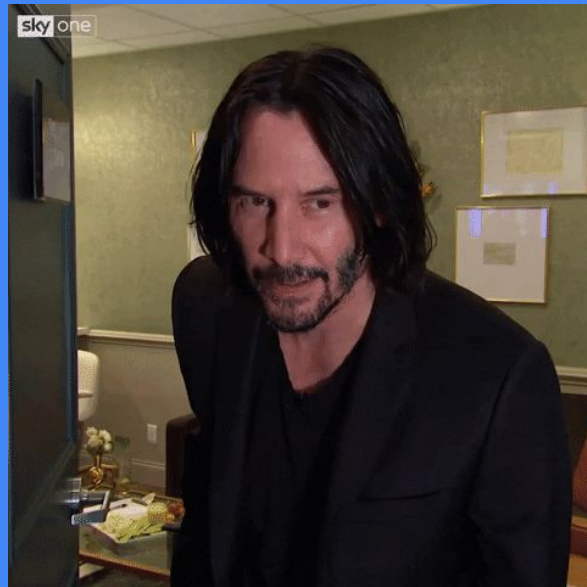
Questions ¿?



Thank you!!

Thank you for your time!!

I hope you learn something
new!!



@jthan24

