bypamic secrets: * Dynamic secrets allow you to generate and one automation revoked after a certain duration * not all the secret engine supports dynamic * Common supported engines: AWS, Database, Google Cloud, Azua * Dymnic secret does not provide any stronger apprographic tey generation Jease Minagement: * with every dynamic servet and service type authorbication to ton, valent creates a base; moradosa Containing informations such as a time duration, renewability and more * Once the lease is expired, voult can automatically rounds the data, as of the conscience of the secret can no longer be cartain that it is valid Lease options bescription Poneio This command renews the leave on a secret, entronding the time that it can be used before it is revoked by vault when a lease is revoked it inalidates BOVOLO that socset comediality and prevents any fuller renewals

Vaut lease renew -increment=3600 my-loane-in
(would request that the TTL of the Locate
be adjusted to 1 hour (3600 soconds)
vault lease revole my-lease-id
Vault bosse revole my-bosse-id Characte a spourfic loanes
The state of the s
Vault-revote base - profix aus/
(Perope all Aws access roys)
Transit secrets Engine:
* The hansit socrets engine handles comprense
Aunctions on data-in-hamit
* All phintext data must be base by-encoded
- * The reason for this requiement is that weelt
does not requie mat the placetext is text" It could be
a binary file such as a PDF on image
* we can sotate energy has veys at regular intervals
to ensure that not all date is encrypted with just 1
enouption toy
Transit socrets engine - key version:
*The Transit orgine supports the versioning of roys
* trey versions that are cortion that a keys
specified min decryption version get archived and
yest of the key voisions belong to the working set
* This leads to both performance benefits as
well as security benefits
* By disallowing decryption of old version of recys
found ciphotext to obsolete (but sensive) data
can not be decorpted, but in an emergency, the

min decryption version can be moved back to allow
Les legitimate de cryption.
Vault policies:
* Vault policies are used to govern the access of
weeks and voles (authorization)
* When you first initialize vault, the root and
defaut policy gots created by default
* policies are donéed by default so an empty
policy grants no permission in the system
path "Sys/mounts" C
capabilities = ["read"]
<u> </u>
Defauet policy:
* The defencet policy is a built-in vacely policy
that count be removed
* By default, it is attached to all totens, but on be
explicitly excluded at at token one ation kine by
Jupposting authoritication methods
* The policy contains basic functionality such as the
ability for the token to looker data about itself and
to use its cutbyhole data
* However vaut is not perspective about its contents,
It can be modified to suit your noods.
POOT policy:
- The root policy is a besit is valet policy that
- Can not be mortified too removed.
* A root user can do anything within the variety
As such as it's highly recommended that you revote

any root tokens before running valet in production. & When a want sorver is first initialized, there always exists one goot user that civer is used to do the initial configuration and solup of voult. * After configured the initial root toron should be revoked and more strictly controlled were and auguntication should be used. Total Accessor! This accessor is a value that acts as a reference to a token and can only be used to perform limited actions: * Lookep a token's properties (not including the actual to ren (P) * Lookup a token's capabilities on a path * perpu a token * Povoke the tokon policy Assoliation! * During the total execution hime, the policy is associated with the token. KAT the later stage, if you altack a new policy to the user (08) role, it will not affect the existing pokens-* For such cases, a new token must be excepted * A policy which is updated and is already attacked to the token the rules will be reflected accordingly as pout of the token's permission

Token Capabilities!
* The token capabilities command Petches the capabilities
of a total As a given path.
* Total Accessor can also be used to chack the
capabilities et a specific bobon
vant jores appabilities sources soo
O/p: road
Duthophication Methodo:
+ Three are multiple authorization methods
available in Valent.
* After saccess ful authorbication, a token is general
which can be used for authors interaction with vacet
* komombou that the gither auth method is a user
oriented method and is easiest to use for double pais
machine
+ For servous, Applole method is the recommended
Choice
- vault auth erable -pam=my-loga userpass
Dirabling Auth Method:
* A specific authorbication method can be
disabled with the following command:
Vanut auth disable (meshod-name)
* when an auth method is disabled, all usees
- authorbitated wa that methods are automatically
logged out.

Shoage Backenol:
* vacut has multiple storage backends, each for
different use-cases.
* showing backends represents the location for the
duable storage of vault's information
k temetoba that not all the storage book ands
supports high-availabilly.
storage "dy namodb" 2
ha enabled = "bocce"
region = "as-west-?"
table = "voult-data"
y
Disabling secret Engine:
the secrets disable command disables a
secret engine at a given PATH
A Once a secrets engine is disabled all secrets
generalist via secrets engine are immediately revoked
vault socrets disable aus
Login based on Usupass Auth Method:
while logging is via userpass auth method
It is impostant to not define the password discitly
within the cu command.
Vault login - meshod = useipass useiname = der
use
the state of the s

Unseal Vault
* when a voult souver is started, it starts in
sealed state
* Unsealing is the process of constructing the most
try necessary to road the decryption try to decrypt so
data, allowing access to the voielt.
* unsealing is the process of reconstructing this
maske key
Vault Agent:
The Vault agent does not pewist anything
to storage Everything lives in memory.
There are two primary functionalities related
Vault Agent.
- Automatically authorizate to vacel-
manye the token renewal process
anching >+Allows client-side caching of respons
- Containing howly created tokens.
* of configured with use auto auth tota
- Chest will not be required to provide a
valet token to the regless made to the
Agont.
Pesponse Wrapping Toten!
* When response weapping is requested, voult
- creates a temperary single-use token curapping token;
and cisalt no the response like the the toloten's
certbyhole with a short TIL

* If the wapping toten is compromised and attacker anusaps the secret, the application will not be able to unusap again and this can sound an alarm and you can revoke things accordingly Shami Secret sharing for Unrealing Vault + The strage backend is considered to be consustage and vault lises an eneryption key which is lised to Protect all the data. That key is protected by a mastes by * Vacelt uses a technique knows as shaming secret sharing algorithm to split the master key who 5 shores, any of 3 which are required to reconstruct the master trey. * The best practise states that the key shares that are entered to get the master key should be done from a different workstation by different lesces having an individual key

	_
Seal Stanza!	
* The sear Stansa configures the seal type	
to use for additional data protection, such as using	
HSM on closed this solutions to encrypt and decrypt	
He muster buy.	
* This skanza is optional and in the case of the	
master key, vacelt will use the shamu algorithm to	
cryptographically split the moster key it this is not	
configured.	
seal [NAME] C	
3	
Vault Replication:	
* For performance replication, secondary cluster	
will service roads locally.	
+ Some date is also stored locally and not repla	Co
to the primary cluster	
* In DP, all the data is replacated but the second	10
abute another scant to stack a return to	
chole application the copy chole co)
Replicated combot, compisent across vault cluster:	
- secret configuration Chrisecrets, hant toy.	0
-AUMENTICATION METHOCUS	
service been service to the and located	
and teases service rotens and leaves	
Valid for Valid for Chister A&C	
Cluster B	

Ephilies and Dhases:
* Each quent is ustourally termed as an entity
An entity can have muliple aliases.
* The policy defined at entity large are associated
with the aliases
[entity]
name: bob-smith
entity_id:63125661-8523-9838-
powy: base
motocolata:
organization: Acme Inc
Advases:
policy: lest policy: team 20
poury. eggs
Lantite Comme
Hentity Groups:
* A group can contain multiple entities as its
members.
* policies sot on the group is granted to all
Group momber of the group
namo: enginoous
group_id: 81 bolc 90-284a-768c-5fa7693bc
policy: toam-eng
motaclata:
team: Engineery
region: North America
Group Gorsly Membel
Cohily
hame: bobsmith
antity_121 63125667-8523-9038-5001
POWY 1 BOND

metadara:
organization: Acme Inc
toam: QA
Atiases:
[Dame: bob frame: bsmith
policy: test policy: tomem-ga
Vasut output:
we can have vault output it the following
mode: Table, JSON, JAML
The default is the Table
Table View > Vant Secrets list - format tal
JSON View > vacut secrets list - format for
multiple Encryption key:
* For Transit Engine, it is considered ones a
best practice to rescularly rotate the encryption key.
* This limits the number of data enemypted via a
Single key
k All the data should not be energypted with the
single encryption by
* The above increases the risk.
Poading output from EV path:
you want to be abled to read a specific
secret at secret/domosecret, which capability needs to
be used;

There are two primary capabilitis!
+ LIST
* PEAD
* List allows who values at the given path.
I Poad allows reading the data at the given path.
Audit Devices:
* Audit devices are the components is voselle
that toop a detailed tog of all regions and response
to vault.
+ when a vacult server is first mitalized, no
audiking is enabled.
* Audit devices must be embled by a root user
using voult audit enable.
Vallet Browson CLI:
* Allows renning of busic CLI commands like wrote,
read, delete and list.
* you will be not be able to perfrom various
appearions like creating new acesterixation
methods and others
vaeilt token looteips
Well total lookup & GIBH & 5mm DNO6 & B3W TB LOOK
It will show creation til, orphan and til.

Orphan Tokans
* Coppen totens are not children
of their passons; there fore orphan totans do not
expire whom their parent does.
* They are the root of their oven for
* Orphan loters Still expire when their ocen more
THE is roached
Total Copprared Tokery
(parent token)
(pater) recess)
create a John with Explicit TTL:
+ TTL = Initial TTC to associate the with the total
* Explicit Max TTL: Moximum lifetime for the total
* Houd limits and cannot be exceeded
* The system more TTL, which is 32 days but
can be changed in the variet's configuration his
Vaccet totan create [+1=100 explicit-max-H]=
Namouring a Totan:
Vauelt Joten veneus Commend can be used to
extend the validity of the renovable tokens.
Vaccet token renew increment = 30m
S. YCHX FMgNq. T7606iER
3.761.19

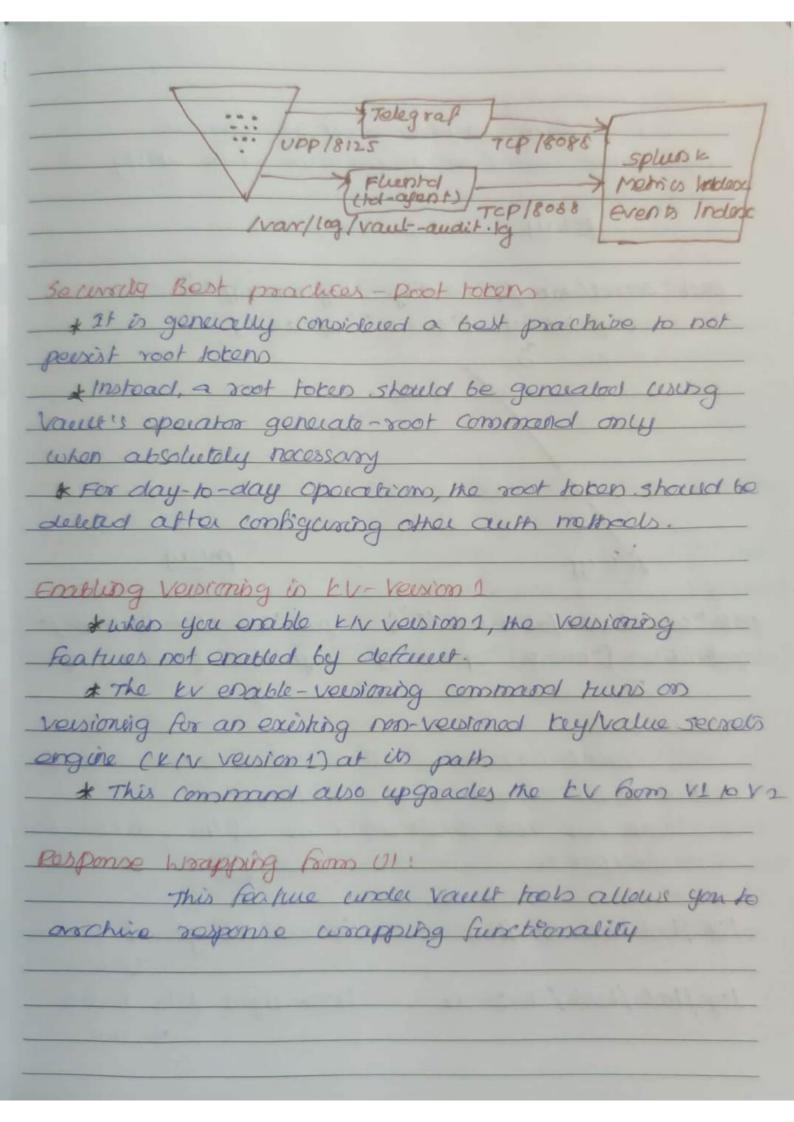
	-
Pasic Environment Variables:	
VACLT BOOR	
Address of the vowelt source expressed as a CIEC	
and post, for example, https://127.0.0.1: 8200/	
http://p7.0.0.1:8200 can also be replaced with	
hltp://8200	
export VAULT_ADDR = 'bHp://: 8200'	
Socrets Engine!	
* Multiple secrets engine of the Same type con	2
be enabled at a given time.	
+ We can distinguish Hom uniquely by 30paia	Ou
them by the path	
KIN secret engine mounted on secret	
en socret engine maintal on / ky	
Supported Backenal - Hashiler Support	
* Following Back Ends are officially supported to	1
Hashicorp	
the will receive technical support for these	
backombs.	_
In-Memory	
Filesystem	
Consul	_
Natt	
	_
	_
	_

Vault Epholpride Features
Vault entrappise includes a number of
partues that vony be useful in specific workflows.
It is impostant for us to under stand the unique
Fratues that are part of variet Enterprise
Dixaster Recovery
Namespaces
Monitoring
Multi-Factor Authorbication
Auto-unseal with HSM
Vaut Name Spaces:
*Namespaces are isolated environments
that Auctionally exists as "valles within a vaule"
* They have separate logis paths and support
creating and managing data isolated to their
minespaces.
Each pamespaces hours can have Us own:
policies
Auth methods
secrets Engines
Tokens
Identity entities and groups
NS2 NS2
Vaut withi vaut

James Popication: + who never you have sophication enabled all of the secondary clusters existing data will be deshoyed. This is inverocable. * Valett does not support as automatic failure/promotion of a DR secondary cliester + Vault Repuration is enterprise only feature. * De replicated cluster will replicate all dorsa from the primary clusters, including totens. * A performance replicated churter, however will not replicate the totons from the primary Auto-Completion Features * voult Auto-complete fectus allows automatic completion for flags, sul commands and arguments. * Be sue to restruct your shell after installing auto completion! Installation Command: Vaut -autocomplote-install Vault CLI commends Exable Secrets engine - vault secrets enreble EV-V2 - vault kv put secret/myse cro Store data admie = presevord list key names a secret - vacut ku list socret/my-apt polete version of socret - vanut ku delete socret/my-att Delete all vousions & vault ku metadaka delete meta-dara secret/my-app

Auto Unseal:	
6	Auto asseal delegates the responsibility
of socuring the	consear bey some uses to a trustool
	are some of the supported services:
0	ANS KMS
	Transit Secret Engine
	Azue beg vareet
	HSM
	acp cloud long
* For private	connectivity, upc emporits can be used
Identify output	t of Francis Engine!
	encryption/encrypt/demo
The same	plaintext = \$16cese 64 200 Samp
0/p:	dala
Vault: V3: H	- KVy PMMSk+ 29 Oa a4HO Oat V2 Tombol 2
* Va inclicates to	rewins of keys exists
	to reysing is clemo
* Transit seur	et engine is oncentred at leneryphon pad
PICI Secrets GO	
	ets engüe generales olynamic x.509
certificates.	
	1 Secrets Engines:
	n act as a intermediate CA
	(or eliminating confiscate revocations.
<u> </u>	ine to got a constitute by eliminating to
	ponerate a private bey and cse

TOTP Secrets Engine:
* TOTP stands for Time-based one-hime passes
* These are temporary passcodes and they typically
exper after 30,60,120 con 240 seconds.
* The TOTP secrets engine can act as both a general
(like Google Authorshicutors) and a provider (like the
acagle com sign-in service)
Vault road totp/code/zeal
0/p:
Coole: 357893
Vaut plugaris:
* All vacut outh and secret back and are
considered physics.
* This simple consept allows both besit is and
external playing to be beaution like legers.
(Vacut aux methods) (custom
core (secret backends) Plugio
Secret backeras
E
Vault
Tolerrotay in Vaut:
Telemotry related motions are available at
Isys/motrics endpoint
Important metrics & logs to be analysed:
* Mothics
* vaut audit logs



part temphing:	
Do the tempolati	ung allows variable
replacement based on a	formation of the entity.
- Egraces cases	The state of the state of
policy	A. A. S.
pung	
path " secret/data/ssidenti	ily. ophily. mame gy/* "
capabiblies = ["ore	
3	
	AL BURE BURE BURE BURE
4	Dalicu
policy	The state of the s
path "socret/data falice-wer/*	"E path secret/data/blob-use/+
apabilities = ["create", "cepdate	
7	3
Vault tools:	
	certain set of took that will
allow us to achieve a	
Thora are also arai	lable in the sys/tools endpoint
- End pon's	Description
Chapero	Caropia o
1545 [tools] random /164	aerocate 164 tytes of rounds
	Value
1sys/tools/hash/shaz-512	Hash input data bresed
	on SHA2

an be poot totens	11-1	
	yes	No
an creat Child	yes	No
totens		Send The
can ponewastle		No
an se periodic		No
an have explicit Mox 9		Notalway
The second section of the second	2 Aprilland Billiand	wer a fixed TTL
las Accessors	yes	No
las cubbyhole		No
Povorad with parent	-	and house
cifnot coppens		Stops Worker
Dynamic servots lease	CATLE SAME CAS	Silver Mary
Assignment	Self	parent Cit not
		orphour
can be used Across		161 181 181
porformano Poplication	No	yes Cif orpha
Chester	The get the treet	A CONTRACTOR OF THE PARTY OF TH
creation scales with	THE CHARLES	condition bear
performing standing	No	Yes
Node Count		Acres and
Cost	Heavy weight,	Lightweish
	mutiple storage	no storage a
	writes per toten	for token
	creation	creation

Miscellaneous pointers-1:
k roof and defauet are the him default policies
in valet
+ when a lease is revoted, it invalidates that second
immediately and provents any fulter voncessel
* To remove all socrets at a specific path:
vall lease revote -prefix <patt></patt>
and the second s
* usupass auth method cannot read busernames
and passwords from an externe source.
Misællaneous pointees-2
* The 1sys/leader emporit is assed to char the
high availability structus and current leader of
voult.
* vault operator isit command initializes a
racelt server
* Value configurations file can be wed to configure
various settings like Cluster name, stronge backens
soal soldings and so on. Other things like tremespaces,
auth mothods are directly configured within the
vault ioself.
* The Identity secrets engine is mounted by default
* storage for words are not brustool for some
* storage fackends are not trusted by variet

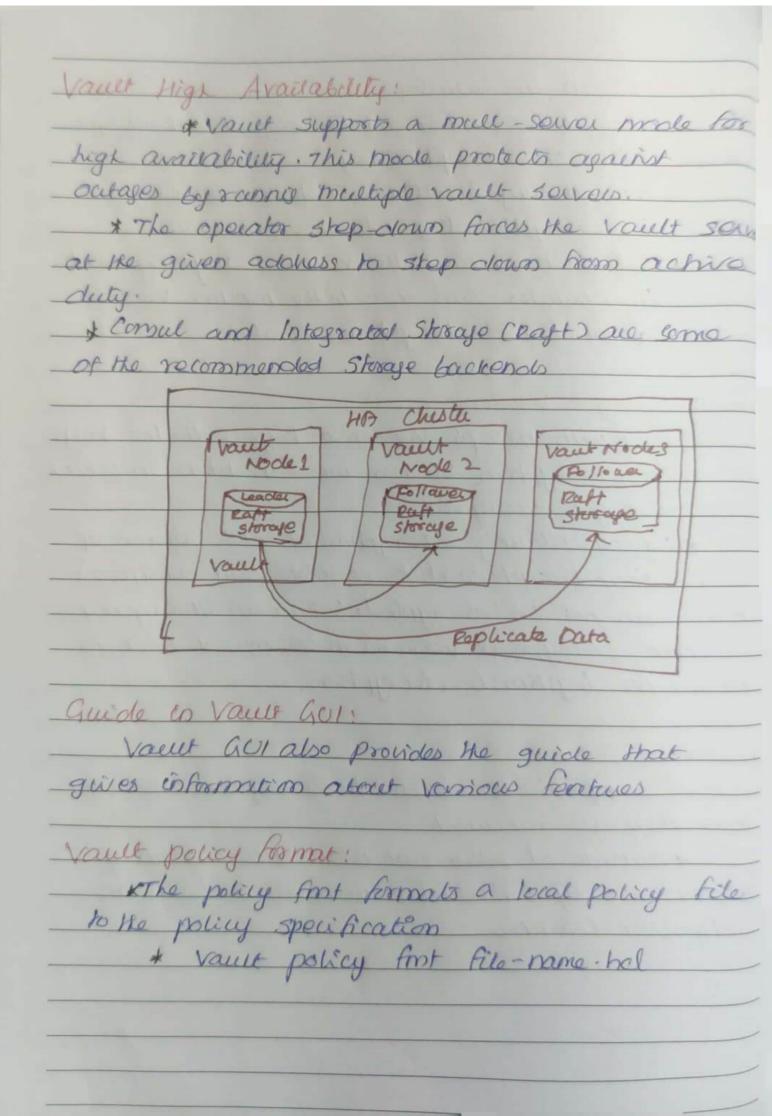
Miscellaneous printous: 4 * Transit secret Engine does not store any chila * if you receive the following error, trante sure to Sor the VAULT, ADDR Vormable to HTTP Vault Stalts Olp: http: server gove HTTP response to HTTPs: Cl. *After authentication the CLI and Gul automatically assume the token for subsequent requests. * Api on the other hand will require to capy the token and use it his all subsequent requests. Miscellaneous pointers:	Important post Numbers: 8200: Vacult Apri and UI 8201: Chustre to Chuster Communication I Red totens in the Vacult are not associated with the TIL'S and Herefore they not at not expire. Non-root totens are associated with TTL'S * Defauet Max Truef toten is 32 days but it can be medicial from the configuration file. Miscollaneous Pointers: 4 * Trainit secret Engine closs not store any chita- * if you receive the following error, thate sure to ' sor the Vacet, appe variable to HTTP Vacult Stalts Olp: http: server gave HTTP response to HTTPs cli * After authentication the cultural Gul automatically assume the toten for subsequent requests. Api on the other hand will require to capy the toten		
Important post Numbers: 8200: Vacult Apr and UI 8201: Chuster to Chuster Communications I feed totens in the vacult cue not associated with the TILLS and Herefore they not about expire. Non-most totens are associated with TTL's * Defauet Man Truef toten is 30 days but it can be modified from the Configuration file. Miscellaneous Pointein: 4 * Transit secret Engine closs not stope any chitated in the Vacult States Old the Vacult Appel vorsable to HTTP Vacult States Old: http: server gove HTTP response to HTTPs cl * Appl on the other hand will requests. * Appl on the other hand will require to capy the toten and we it for all subsequent requests. Miscellaneous pointers: * Warrell secret engines supposts ramious closes	Important post Numbers: 8200: Vacut Apr and Ul 8201: Chuster to Chuster Communication A feet totens in the vacuat are not associated with the This and therefore they not as not expire. Non-root totens are associated with Thes * Defauet Mare Truef toten is 32 days but it can be modified from the Configuration fite. Miscellerneous pointers: 4 * Transit secret Engine does not store any chita: * if you receive the following expos, thate sure to ' set the Vacet apper variable to HTTP Vacut Statis "Ip: http: server gave HTTP response to HTTPs cli * Apri on the other hand will require to capy the toten and we it for all subsequent requests. * Apri on the other hand will require to capy the toten and we it for all subsequent requests. Miscellaneous pointers: * Vacut server engines supposts various cloud providers like thus, pare, plebata cloud a act.	miscellaneous porifous: 3	
8200: Vault Apr and Ul 8201: Chuster to Chuster Communication I feed totens in the vault are not associated with the TILL'S and Herefore they not as not expire. Non-most totens are associated with TILL'S * Default Max TILL of John is 32 days but it can be modified from the Configuration file. Miscollameans printers: 4 * Transit secret Engine does not stose any data * if you receive the following expose, toute sure to Set the VAULT, ADDR Variable to HTTP Vault Statis "Ip: http: Server gave HTTP response to HTTPs cl *After authoriscation the CLI and Gul automatically assume the token for subsequent requests. * API on the other hand will require to capy the token and we it for all subsequent requests. Miscollaneous positors: * Noticellaneous positors:	Exot totens in the value are not associated with the TILS and therefore they not at not explic. Non-root totens are associated with TIL'S * Defauet Man TIL of toten is 30 days but it can be modified from the configuration file. Miscallaneous printers: 4 * Transit secret Engine does not store any data. * if you receive the following error, trate sure to: Set the VAULT APPL Yomable to HTTP Value Stalis "Ip: http: server gove HTTP response to HTTPs cli * Appl on the other for subsequent requests. * Appl on the other hand will require to capy the toten and use it for all subsequent requests. * Appl on the other hand will require to capy the toten and use it for all subsequent requests. * Appl and other hand will require to capy the toten ond use it for all subsequent requests. * Appl and other hand will requests. * Appl and other hand will request requests. * Appl and other hand will request requests. * Appl and other hand will request requests.		
* Recot botens in the valuet are not associated with the TILS and therefore they not at not expire. Non-root tokens are associated with TIL's * Default Man TIL of token is 30 days but it can be modified from the configuration file. Miscallamancus printers: 4 * Transit secret Engine does not store any data * if you receive the following errors, toute some to Sot the VAULT, ADDR Varriable to HTTP Valuet Statis "Ip: http: Server gove HTTP response to HTTPS CL * Apt on the other for subsequent requests. * Apt on the other hand will require to capy the token and we it for all subsequent requests. Miscallaneous positions: Miscallaneous positions:	**Root botens in the variet are not associated with the TILL'S and Horefore they hot at not expire. Non-root lokens are associated with TILL'S * Defauet Man TILL of John is 30 days but it can be modified from the Configuration file. Miscollameaus printen: 4 * Transit secret Engine does not store any data. * if you receive the following error, thate sure to ' Set the VAULT, ADDR Yomable to HTTP Variet Stalts "To: http: server gove HTTP response to HTTPs cli * Apt on the other for subsequent requests. * Apt on the other hand will require to capy the toten and we it for all subsequent requests. Miscollaneous positors! * Nacula secret angulas supposts various cloud providers like thus, pake, Blibaba Cloud & GCP. * Cubbyhole is a default secret engine track in		
* Peot totens in the vault are not associated with the THIS and therefore they not at not expire. Non-root totens are associated with TTU'S * Default Max THE of toten is 30 days but it can be modified from the configuration file. Miscollaneous pointers: 4 * Transit secret Engine closs not store any chila * if you receive the following errors, trate sure to: Sor the VAULT, ADDR Vorniable to HTTP Vault Stalts Olp: http: server gowe HTTP response to HTTPs cl * April on the other for subsequent requests. * April on the other hand will require to capy the toten and we it for all subsequent requests. Miscollaneous pointers: Miscollaneous pointers: * Warrell secret engines supposts various claus * Name to secret engines supposts various claus	* Peot lotens in the value are not associated with the TILLS and therefore they not about expire. Non-root lotens are associated with TILLS * Default Max TILL of John is 30 days but it can be modified from the Configuration file. Miscollameaux pointers: 4 * Transit secret Engine does not store any data. * if you receive the following errors, make sure to ' Set the VAULT, APPR Variable to HTTP Value stalls "Ip: http: server gove HTTP response to HTTPs cle * Appl on the other for subsequent requests. * Appl on the other hand will require to capy the toten and we it for all subsequent requests. * Appl on the other hand will require to capy the toten and we it for all subsequent requests. * Appl on the other hand will request to capy the toten and we it for all subsequent requests. * Appl on the other hand will request to capy the toten and we it for all subsequent requests. * Appl on the other hand will request to capy the toten and we it for all subsequent requests. * Appl on the other hand will request to capy the toten and we it for all subsequent requests. * Appl on the other hand subsequent requests.		
Miscellaneous poilers Appl on the other for subsequent requests. * Appl on the other for subsequent requests. * Appl on the other for subsequent requests. * Appl on the other for all subsequent requests. * Appl on the other panel subsequent requests.	TILLS and Holefore they not at not expire. Non-root tokens are associated with TTL's * Default Man TILL folken is 30 days but it can be medicial from the configuration file. Miscellameaus pointers: 4 * Transit secret Engine does not store any data. * if you receive the following ensor, make sure to ' Sor the VAULT ADDRE Verriable to HTTP Value Shalts Plp: http: Server gowe HTTP response to HTTPs cle * Apt authentication the CLI and Gold automatically assume the token for subsequent requests. * Apt on the other hand will request to capy the token and we it for all subsequent requests. Miscellaneous pointers: * Valuet secret engines supports various closes providers (ito thus, note, plebata cloud & Golf. * Cubbyhole is a default secret engine trace in		
* Defauet Max Truef Joken is 30 days but it can be modified from the configuration file. Miscellerneous pointers: 4 * Transit secret Engine does not store any data * if you receive the following error, thate sure to set the VAULT, ADDR Vornable to HTTP Valuet Stalis "Ip: http: server gove HTTP response to HTTPs: cl * After auther fication the CLI and Gul automatically assume the token for subsequent requests. * Apl on the other hand will require to capy the token and we it for all subsequent requests. Miscellaneous pointers: * Wallet servet engines supposts various closes	Mon-root lokens are associated with TTU's * Default Max TTU of John is 30 days but it can be medicial from the configuration file. Miscollameous pointers: 4 * Transit secret Engine does not store any data. * if you receive the following exxos, make sure to ' Sor the VAULT, APPLE Variable to HTTP Variet States Olp: http: server gowe HTTP response to HTTPs clu * After authentication the CLI and Give automatically assume the taken for subsequent requests. * API on the other hand will require to capy the toten and we it for all subsequent requests. Miscollaneous pointers: * Name server engines supposts various cloud providers like thus, thus, Alebata Cloud & acp. * Cubby hole is a default seaset engine trace in		
* Defauet Max Truof John is 30 days but it can be modified from the configuration file. Miscellaneous position: 4 * Transit secret Engine does not store any data * if you receive the following error, make sure to ' Sor the VAULT. ADDR Vomable to HTTP Vault Stalis Olp: http: server gove HTTP response to HTTPs: cl * After authentication the CLI and Give automatically assume the token for subsequent requests. * API on the other hand will require to capy the token and we it for all subsequent requests. Miscellaneous positors: * Available source engines supposts vomous closes	* Defauet Max Truof John is 30 days but it can be modified from the configuration file. Miscollectreacus printers: 4 * Transit secret Engine does not store any chita: * if you receive the following error, make sure to: Set the VAULT. ADDR VONSable to HTTP Vacult Stalis Olp: http: server gove HTTP response to HTTPs clu * After authentication the CLI and Gul automatically assume the token for subsequent requests. * Apl on the other hand will respuise to capy the token and we it for all subsequent requests. Miscollaneous positors: * Nacult secret engines supports various closes providers like Aus, passe, Alchaba Cloud & ACR. * Cubbyhole is a default seaset englie true in		
Miscellaneous printous: 4 * Transit secret Engine does not store any chila * if you receive the following error, trante sure to Sor the VAULT, ADDR Vormable to HTTP Vault Stalts Olp: http: server gove HTTP response to HTTPs: Cl. *After authentication the CLI and Gul automatically assume the token for subsequent requests. * Api on the other hand will require to capy the token and use it his all subsequent requests. Miscellaneous pointers:	Misrollerneaux paintous: 4 * Transit secret Engine cloes not store any chila. * if you receive the following error, trate sue to ' sor the VAULT. ADDR VORNAble to HTTP Vault Stalis "Ip: http: server gave HTTP response to HTTPs cli * After authentication the CLI and Gul automatically assume the token for subsequent requests. * Apl on the other hand will require to copy the token and up it for all subsequent requests. Misrollaneous pointers: * Availt secret engines supposts various cloud providers like Alus, Ashe, Alebata Cloud & ACR. * Cubbyhole is a default secret engine true in		an
Miscellaneous painten: 4 * Transit secret Engine does not store any chila * if you receive the following error, trate sure to! Set the VAUCT, ADDR Vorniable to HTTP Valuet Stalts Olp: http: server gove HTTP response to HTTPs cl *After authentication the CLI and Gold automatically assume the token for subsequent requests. * Apl on the other hand will require to capy the token and we it for all subsequent requests. Miscellaneous pointers! *Nacet severt engines supposts various closes	Miscellaneous printers: 4 * Transit search Engine does not store any data. * if you receive the following error, make suce to: Sor the VAULT, ADDR Vornable to HTTP Vault Stalis Plp: http: server gowe HTTP response to HTTPs cla * After authentication the CLI and Gall automatically assume the token for subsequent requests. * Api on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous positors: * Avail secret engines supposts various cloud Providers like thus, the plant to cloud & GCP. * Cubby hole is a default secret engine that in		
* Trainsit secret Engine does not store any data is if you receive the following error, trate sue to set the VAULT. ADDR Vorniable to HTTP vault states "Ip: http: server gove HTTP response to HTTPs cl. *After authentication the CLI and Gul automatically assume the token for subsequent requests. * Apl on the other hand will require to capy the token and we it for all subsequent requests. Mis reliances positors: * Warrell secret engines supposts versions closes	* Transit secret Enguire does not store any data. * if you recoive the following error, make suce to ' Set the VAULT. ADDR Vornable to HTTP Vault Stalis Olp: http: server gove HTTP response to HTTPs cla * After authentication the CLI and Gul automatically assume the token for subsequent requests. * API on the other hand will require to capy the token and we it for all subsequent requests. Miscollaneous pointers! * Valuet secret engines supports various claus Providers like thus, the Alchaba Cloud & GCP. * Cubby hole is a default secret engine tract in		
* Trainsit secret Engine does not store any data is if you receive the following error, trate sue to set the VAULT. ADDR Vorniable to HTTP vault states "Ip: http: server gowe HTTP response to HTTPs cl. *After authentication the CLI and Gul automatically assume the token for subsequent requests. * Apl on the other hand will require to capy the token and we it for all subsequent requests. Miscellaneous pointers! * Warrell secret engines supposts removes closes	* Transit secret Engine does not store any data. * if you recoive the following error, trake suce to ' Set the VAULT APPLE Vornable to HTTP Vault Stalis Olp: http: server gove HTTP response to HTTPs cla * After authorisation the CLI and Gul automatically assume the token for subsequent requests. * ApI on the other hand will require to capy the token and we it for all subsequent requests. Miscollaneous pointers: * Nacult severt engines supposts various claus Providers like thus, the Alchaba Cloud & GCP. * Cubby hole is a default secret englise tract in	Miscellernoous pointers: 4	
Sor the VAULT. ADDR Vorniable to HTTP Vault Statis Olp: http: servor gove HTTP response to HTTPs: Cl *After authentication the CLI and Gal automatically assume the token for subsequent requests. *Apl on the other hand will require to capy the token and we it for all subsequent requests. Miscellaneous positors! *Vault- secret engines supports various clous	Set the VAULT. APPR Vorniable to HTTP Vault Statis Olp: http: server gove HTTP response to HTTPs cli *After authentication the CLI and Gul automatically assume the token for subsequent requests. *Apl on the other hand will require to capy the token and we it for all subsequent requests. Miscellaneous pointers: *Novellaneous pointers: *No		
Sor the VAULT APPR Vornable to HTTP Vault Statis Olp: http: server gove HTTP response to HTTPs cl. *After authentication the CLI and Gul automatically assume the token for subsequent requests. * API on the other hand will require to capy the token and we it for all subsequent requests. Miscellaneous positors: *Valuet secret engines supposts various clous	Sor the VAULT ADDR VONSable to HTTP Valuet States Olp: http: server gowe HTTP response to HTTPs cli *After authentication the CLI and Golf automatically assume the token for subsequent requests. * API on the other hand will require to capy the token and we it for all subsequent requests. Miscollaneous positors! *Valuet source angines supposts various cloud Providers like thus, note, Alchaba Cloud & GCP. * Cubbyhole is a default secret englise true is		
Pault Statis Olp: http: server gove HTTP response to HTTPs cl. *After authoriscation the CLI and Golf automatically assume the token for subsequent requests. * ApI on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous positors! *Nacellaneous positors!	Mis relianeous pointers! *Note the source of the control of the total and we to first all subsequent requests. *Note that hard will require to capy the total and we it for all subsequent requests. *Note that all subsequent requests remove closes of the source of		
After authentication the CLI and Gul automatically assume the token for subsequent requests. Apl on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous pointers: * Navel- source engines supposts various clous	ABITE Server gove HTTP response to HTTPS Che ABITED Authoritication the CLI and Gill automatically assume the token for subsequent requests. API on the other hand will require to capy the token and we it for all subsequent requests. Miscollaneous pointers: *Nacell server anguines supports various cloud Providers like thus, Ashe, Alebaba Cloud & GCP. *Cubbyhole is a default secret engine that is		
ABFTER authoriscation the CLI and Golf automatically assume the token for subsequent requests. A API on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous positors! * Nacell secret engines supposts various cloud	After authoriscation the chi and Gul automatically assume the token for subsequent requests. * Api on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous pointers! * Availate source engines supposts remous cloud providers like thus, now, Alchaba Cloud & GCP. * Cubbyhole is a default secret engine that in		cle
Assume the token for subsequent requests. API on the other hand will require to capy the token and use it for all subsequent requests. Miscollaneous positors! *Valut socret engines supposts various clous	Assume the token for subsequent requests. API on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous positors: *Valuet source engines supports various cloud providers like thus, there, Alebaba cloud & GCP. **Cubbyhole is a defect seasot englise three is		
Assume the token for subsequent requests. API on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous positors! *Valut severt engines supports various clous	Assume the token for subsequent requests. * API on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous positors! * *Varent secret engines supports various cloud providers like thus, Azue, Alébaba Cloud & GCP. * Cubbyhole is a defent secret englise tract is	*After authoriscation the chiand Gal automatica	elly
API on the other hand will require to capy the token and use it for all subsequent requests. Miscellaneous positors! *Vacent source engines supports various clous	API on the other hand will require to capy the toten and we it for all subsequent requests. Miscellaneous positors! *Valuet sourcet engines supposts various cloud providers like thus, have, Alebaba Cloud & GCP. **Cubbyhole is a defeut- secret engine tract is	assume no token for subsequent requests.	
mis relianeous ponitors: *Valut source engines supports various clous	mis relianeous ponitors! *Varent source engines supports various cloud providers lite Aus, Ashe, Alchaba Cloud & GCP. **Cubbyhole is a defent seasot engine that is		en
Miscellaneous ponitors! *Valent sourcet origines supplies various clous	Mis collareous poritois! *Valent sourcet origines supports various cloud Provider like Ams, Azme, Alebaha Cloud & GCP. **Cubbyhole is a defent seaset englie mut is		
*Valut source engines supports various clous	Provides like Aus, Azue, Alebaha Cloud & GCP. * Cubbyhole is a default secret englise that is		131
*Valut source organes supports various clous	Provides like Aus, Azue, Alibaba Cloud & GCP. * Cubbyhole is a default secret englise that is	miscellareous poritois!	
	provides like Aus, Azue, Alebaha Cloud & GCP. * Cubbyhole is a default secret englise trace in		2010
DAVICKUM CITY FILMS FILMS FILMS	* cubby hole is a defeut secret englise that is		
			ò

Miscellaneous ponteis: 6 * while generating dynamic secrets, voult returns the leave i'd which can in hun to used with commands such as Vault leave remen, revore and others. * Vault logis command is used for author to catio * After onthalizing, vault provides the root token to the user, this is the only way to by login to Vacet to configure additional auth mothods * + and * are the two characters that are used for denoting wildrand paths in policies * The vault coopiquation file supports either JON COO) HCL Miscellaneous porites - 7: * When data is decrypted via transit engine the output is in base by formet. * To Fetch the original plaintext data, you will have to decode the data with base 64 - de rode * Vault 01 roods to be enabled from the configuration tile and not the CLI * In order to renew a toten, a cuer can issue a valent total varous command to extend the TTO

Miscollaneous poritous: 8 * when variet is sealed, the only two options available are viewing the varely status and unrealing the vault. All offer actions performed after the vaule is unrealed and the use is authoriticated *If vault (1) is able to access a specific path C/secrets/apps/sneds) but the user is not able to view it via QUI then the issue is related to musing LIST pointision so that the less can browse the path that leads to a Spocific key-value path. * if the secret has been minually removed, it you by to do a vault lease revoke, it will result in an error stating "credential could not be found". In such a case, you need to use the -force flag. Miscellaneous poriteus: 9 * storage back and and HTTP API are outside of the society barrier hance can't be protected. *WAL skinds for Write-Aload-Logging. The changes are first recorded at the log, which must be written to stable storage before the changes are written to the datastoro.

Dealing with Layer Data Sizes- Transit Engine
*when the data size is laye (say 10 GB), we
do not want to send it over the notwork to variet
and got the eneryphod data back. It will increase
He latency and slow things down.
* Instead, you can generate a data key and
encrypt it locally and use the same data key to
doesypt it locally when needed.
Vault policy Rules - Transit Engine
Be aware of the important policy rules and
capabilitis related to havit engine
path "transit/encrypt/demo-tey"?
capabilités = ["cipolate"]
y '
path "bransit/deexypt/demo-vey"?
capabilities = ["update"]
y
path "banxo/koys" [
capabilités = ["list"]
<i>y</i>
path " boarset / reys / demo- bey " ?
apabelitées = ["read"]
2,

pey Potation in Vanue.
* It is not recommend to energet all of your
data with one onexyption by.
* Transit engine allows Coustomes to poeforo
the oncryption key rotation
* vacet maintains the versioned regard and
the operators can decido the minimu vaesion
allowed for docryption operations.
mis Decrypt Versim:
* with mulaple vousion of keys, with the help
of min_decryption_ version, we can plan on which
data lan got decrypted.
* By disallowing decryption of old vewion of
reys, found ciphoetaxf to obsolete (but sonsitive)
data can not be docrypted, but in an omergency,
the min decryption vewsion can be moved back to
allow for legitimate decryption.
periodic Totons:
* periodic totens have expire provided
Host they are renewed.
poutside of token root token, it is currently
Ho only way for a token in valet to have an
custimitées lifetimo.
the desire of the same district



miscellaneaus paitoes:
* Kuboenolas Autonbication is required for
kaboenotes based workload.
* Note that for kuboinoles Authoriscation, passing
Just token is not required for all the API requests
* /sys/seal endpoint is used to seal the valent.
If requies to loten with root policy on sudo
capability on the path
* For Eco Eared workloads, you can make use of
AWS Authorbication Method.
* Note that it is not mandatory to use the Aws outh
method. You can aways use office mothods like
Applolo-