Exam Objective 9

Use Gossip Encryption

Use Gossip Encryption

Objective 9a: Understanding the Consul security/threat model

Objective 9b: Configure gossip encryption for the existing data center

Objective 9c: Manage the lifecycle of encryption keys

[✓ 1]	2	3	4	5

Difficulty Level

Security Model

REVIEW

1. Gossip Protocol Encryption
2. Built-In ACL System
3. Consul Agent Communication
4. mTLS for Authenticity + Encryption
5. Certificate Authority

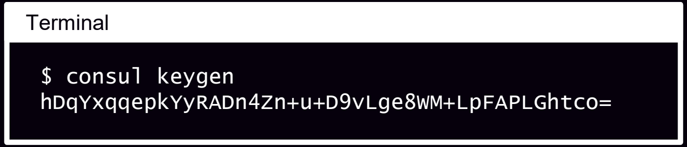
Gossip Encryption

Gossip Protocol Encryption

- Gossip protocol uses a symmetric key
- Essentially a 'shared secret' method for both servers and clients in a cluster
- The same key must be used across all agents in the cluster
- Agents in any federated datacenters must ALSO use the same key

Encryption Key

- 32-byte, Base64 encoded key used for encryption
- You can use the built-in tool `consul keygen` to generate a new key
- Can use `consul keyring` to list and manage keys in Consul

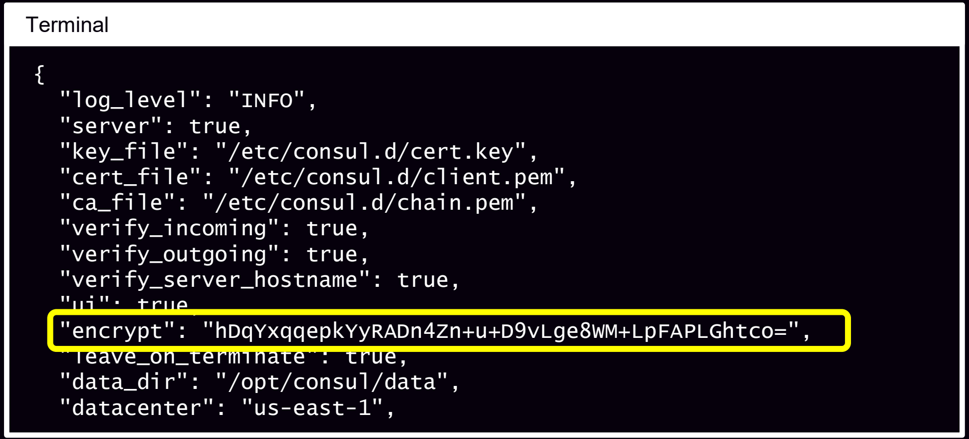


```
$ consul keygen
hDqYxqqepkYyRADn4Zn+u+D9vLge8WM+LpFAPLGhtco=
```

Gossip Encryption

Configuration

- By default, gossip encryption is not enabled, so messages are sent in clear-text
- Gossip key is added to the agent configuration using the encrypt parameter
- Can also specify the key using the –encrypt flag if launching from the CLI
- Encryption key needs to be added to servers <u>and</u> clients



```
{
  "log_level": "INFO",
  "server": true,
  "key_file": "/etc/consul.d/cert.key",
  "cert_file": "/etc/consul.d/client.pem",
  "ca_file": "/etc/consul.d/chain.pem",
  "verify_incoming": true,
  "verify_outgoing": true,
  "verify_server_hostname": true,
  "ui": true,
  "encrypt": "hDqYxqqepkYyRADn4Zn+u+D9vLge8WM+LpFAPLGhtco=",
  "leave_on_terminate": true,
  "data_dir": "/opt/consul/data",
  "datacenter": "us-east-1",
```

https://github.com/btkrausen/hashicorp/blob/master/consul/config.hcl

Modifying an Existing Cluster

Configure Existing Cluster with Gossip Encryption

- You can modify a cluster to enable gossip encryption without incurring Consul downtime
- Does require rolling restarts of Consul agent (`consul reload` will not work here)
- Requires the addition of two parameters
  - encrypt_verify_incoming – used to disable the encryption enforcement for incoming gossip
  - encrypt_verify_outgoing – used to disable the encryption enforcement for outgoing gossip

Workflow to Modify an Existing Cluster

1. Generate a new gossip encryption key

   ```
   $ consul keygen
   ```

2. Add new key and parameters in the Agent config file with a value of 'false'

   ```
   encrypt: hDqYxqqepkYyRADn4Zn+u+D9vLge8WM+LpFAPLGhtco=,
   encrypt_verify_incoming = false,
   encrypt_verify_outgoing = false,
   ```

3. Perform rolling update of all agents

   ```
   $ systemctl restart consul
   ```

4. Set encrypt_verify_outgoing as 'true' on all agents

   ```
   encrypt_verify_outgoing = true,
   ```

5. Perform a rolling update of all agents

   ```
   $ systemctl restart consul
   ```

6. Set encrypt_verify_incoming as 'true' on all agents

   ```
   encrypt_verify_incoming = true,
   ```

7. Perform a rolling update of all agents

   ```
   $ systemctl restart consul
   ```

Much Easier If You
Use A Configuration
Management Tool

Manage Encryption Keys

After initial deployment, use `consul keyring` to manage encryption keys

- List existing keys
- Distribute new keys
- Retire old keys
- Change the key used for encryption

You still use `consul keygen` to create keys

- Consul keyring doesn't generate new keys

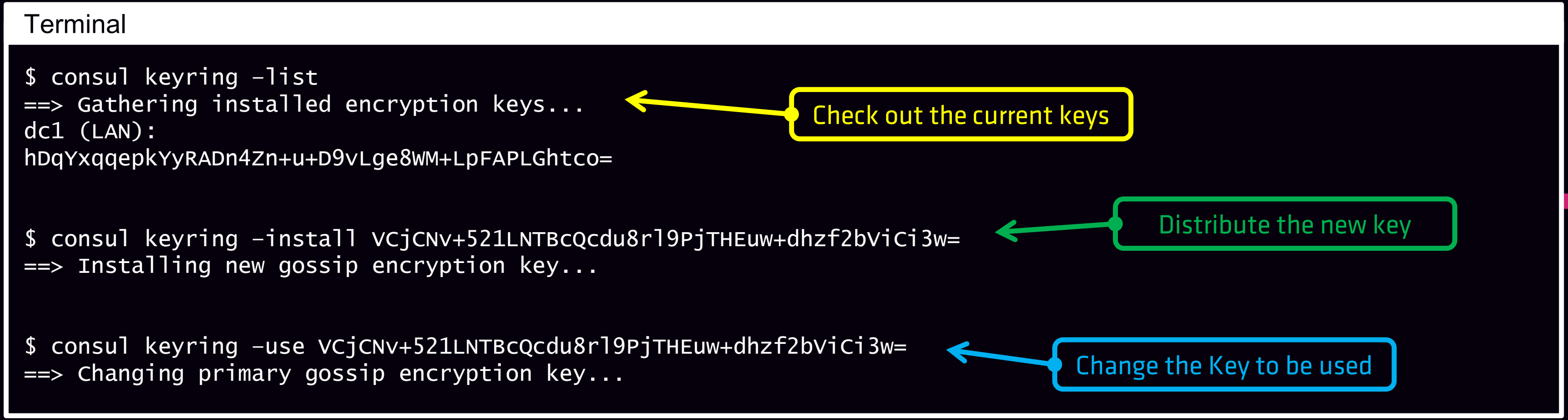
There can be multiple keys at any given time, but it's not recommended

- Becomes more expensive with multiple keys, since Consul would require multiple attempts to decrypt the key. Recommended to have multiple keys only during rotation operations

Manage Encryption Keys

Use `consul keyring` command:

- `-list` – review the installed keys
- `-install` – install a new encryption key
- `-use` – change the primary encryption key used to encrypt messages
- `-remove` – remove the key from the cluster



Terminal

```
$ consul keyring -list
==> Gathering installed encryption keys...
dc1 (LAN):
hDqYxqqepkYyRADn4Zn+u+D9vLge8WM+LpFAPLGhtco=


$ consul keyring -install VCjCNv+521LNTBcQcdu8rl9PjTHEuw+dhzf2bViCi3w=
==> Installing new gossip encryption key...


$ consul keyring -use VCjCNv+521LNTBcQcdu8rl9PjTHEuw+dhzf2bViCi3w=
==> Changing primary gossip encryption key...
```

Check out the current keys

Distribute the new key

Change the Key to be used

Manage Encryption Keys

Workflow to Rotate Encryption Key

1. Generate new key - `consul keygen`
2. Install (distribute) the new key - `consul keyring -install <key>`
3. Change the primary encryption key to the new key - `consul keyring -use <key>`
4. Remove the old key - `consul keyring -remove <key>`

This process allows you to rotation the gossip encryption keys without any downtime to Consul or clients

This workflow can be done manually, or you can automate this process, so the encryption key is regularly rotated based on your internal policies

Use Gossip Encryption

Objective 9a: Understanding the Consul security/threat model

Objective 9b: Configure gossip encryption for the existing data center

Objective 9c: Manage the lifecycle of encryption keys

1	2	3	4	5

Difficulty Level

END OF SECTION