‹ Previous

Unit 6 of 6 ⌄

✓ 100 XP ▶

Summary

4 minutes

Once you have a key vault, you can start using it to store keys and secrets. Your applications no longer need to persist this confidential data, but can request them from the vault as needed. A key vault allows you to update keys and secrets without affecting the behavior of your application, which opens up a breadth of possibilities for your key, secret, and certificate management.

In this module, you've learned about several security benefits of AKV:

- You can create a segmentation of security roles – no one person has the keys to the kingdom.
- The service is monitored and access is logged – this gives you the capability to track user activity to prevent, detect, and minimize a security incident.
- You can avoid human mistakes – other than the creation of the vault, the services can be automated.
- AKV cloud service are available, accessible, and distributed to ensure high reliability for your services.

Further reading

Continue learning about Azure Key Vault in the Microsoft Learn module Manage secrets in your server apps with Azure Key Vault.

Read Azure Key Vault documentation on topics we covered in this module.

- What is Azure Key Vault?
- Azure Key Vault pricing
- Certificate operations
- Implementing bring your own key (BYOK) for Azure Key Vault

Module complete:

Unlock achievement