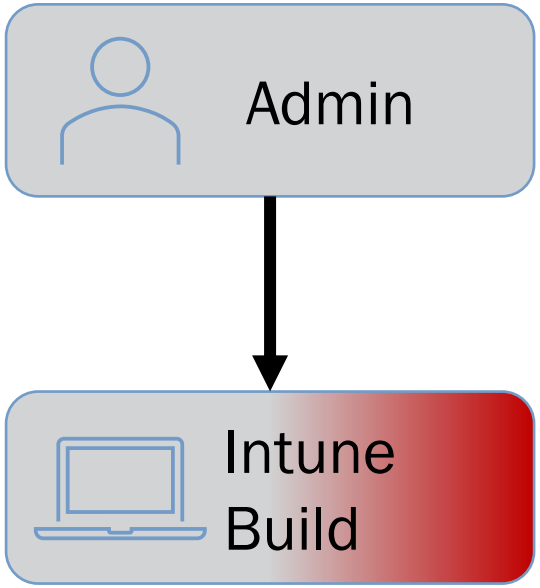
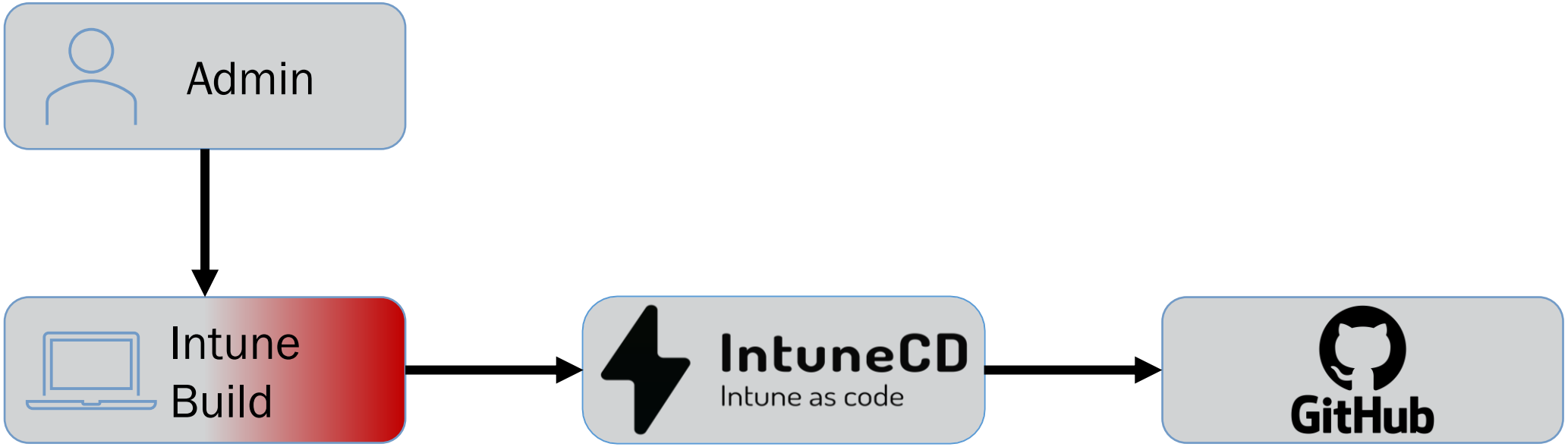
Applying Continuous Delivery to Intune

Applying Continuous Delivery to Intune

What is happening?

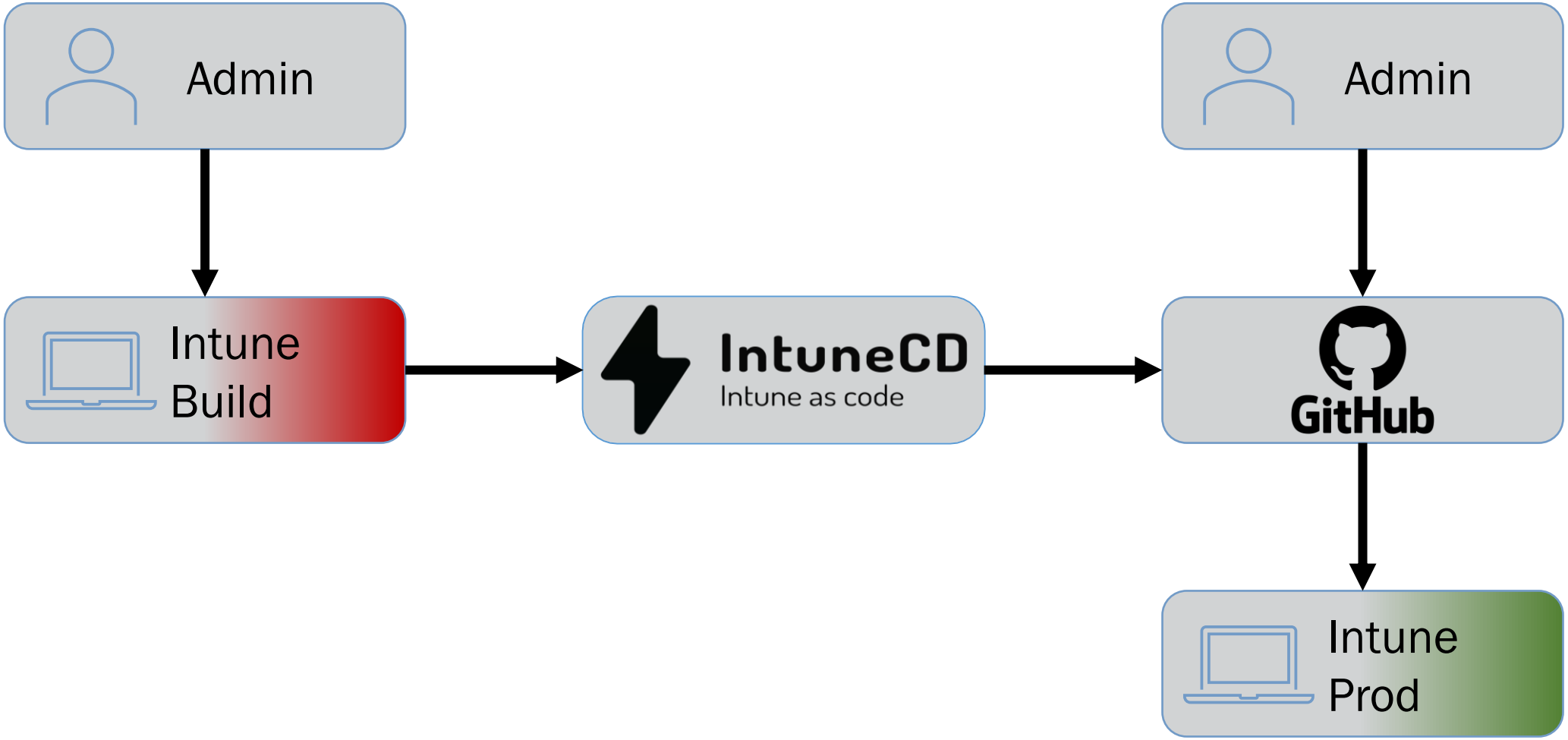


What is happening?

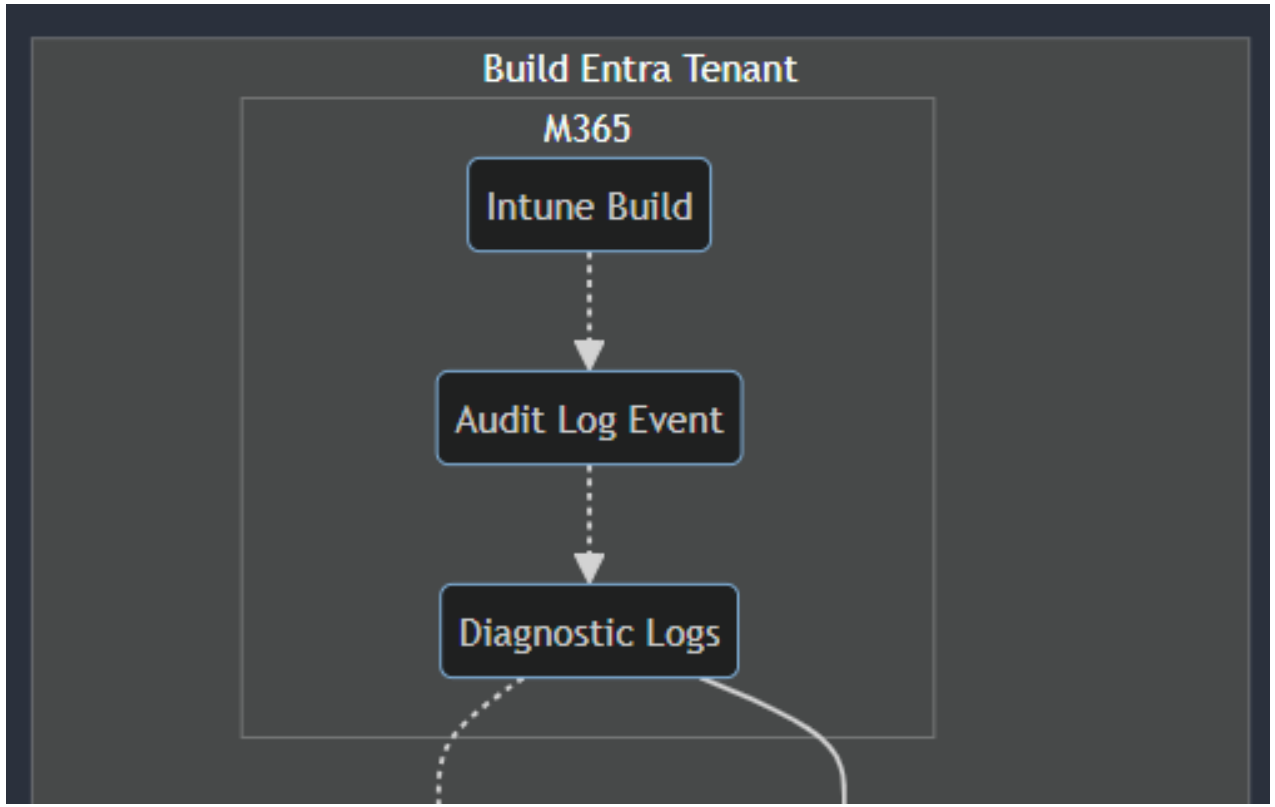


- Backups
- Documentation
- Change Management

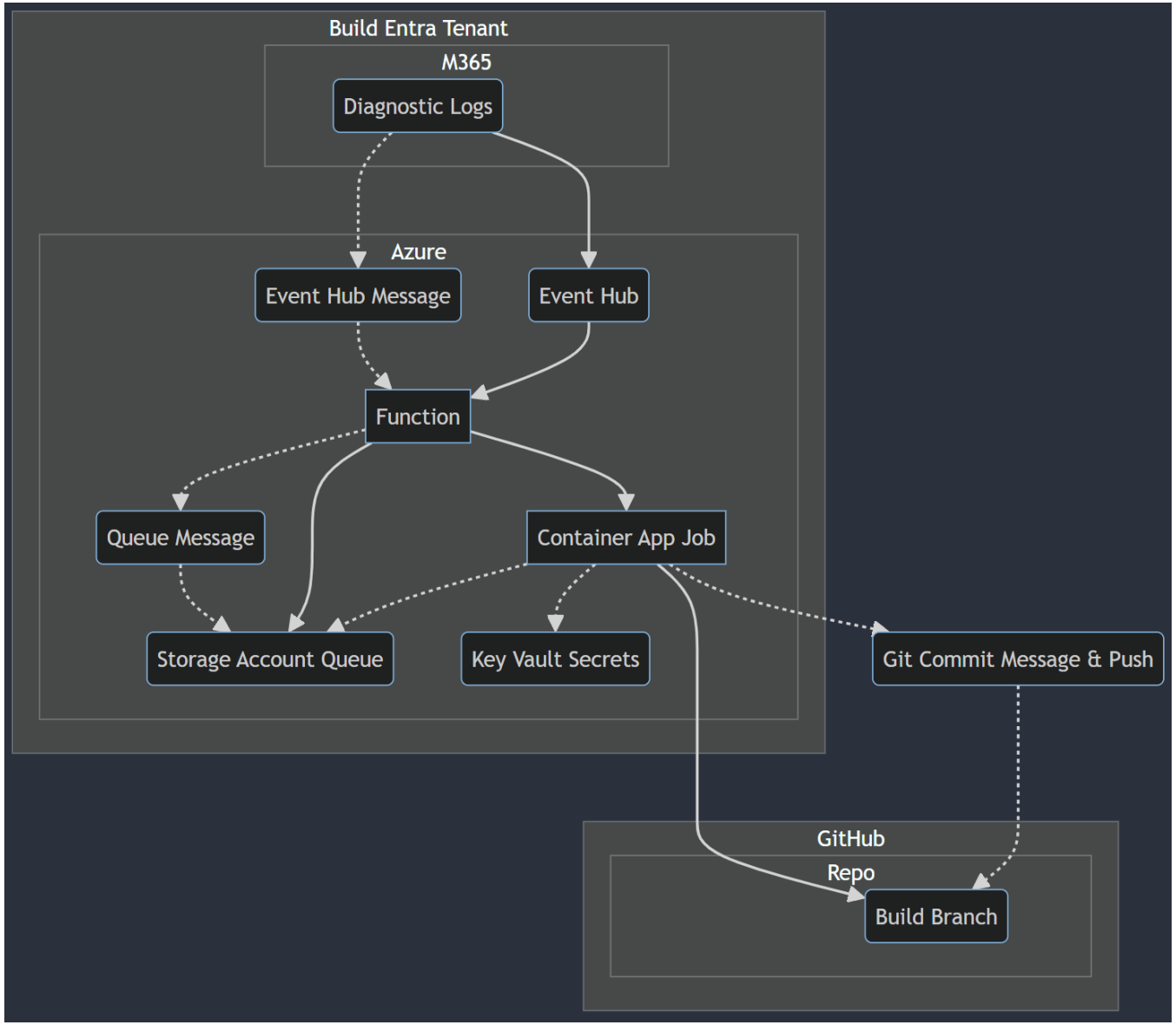
What is happening?



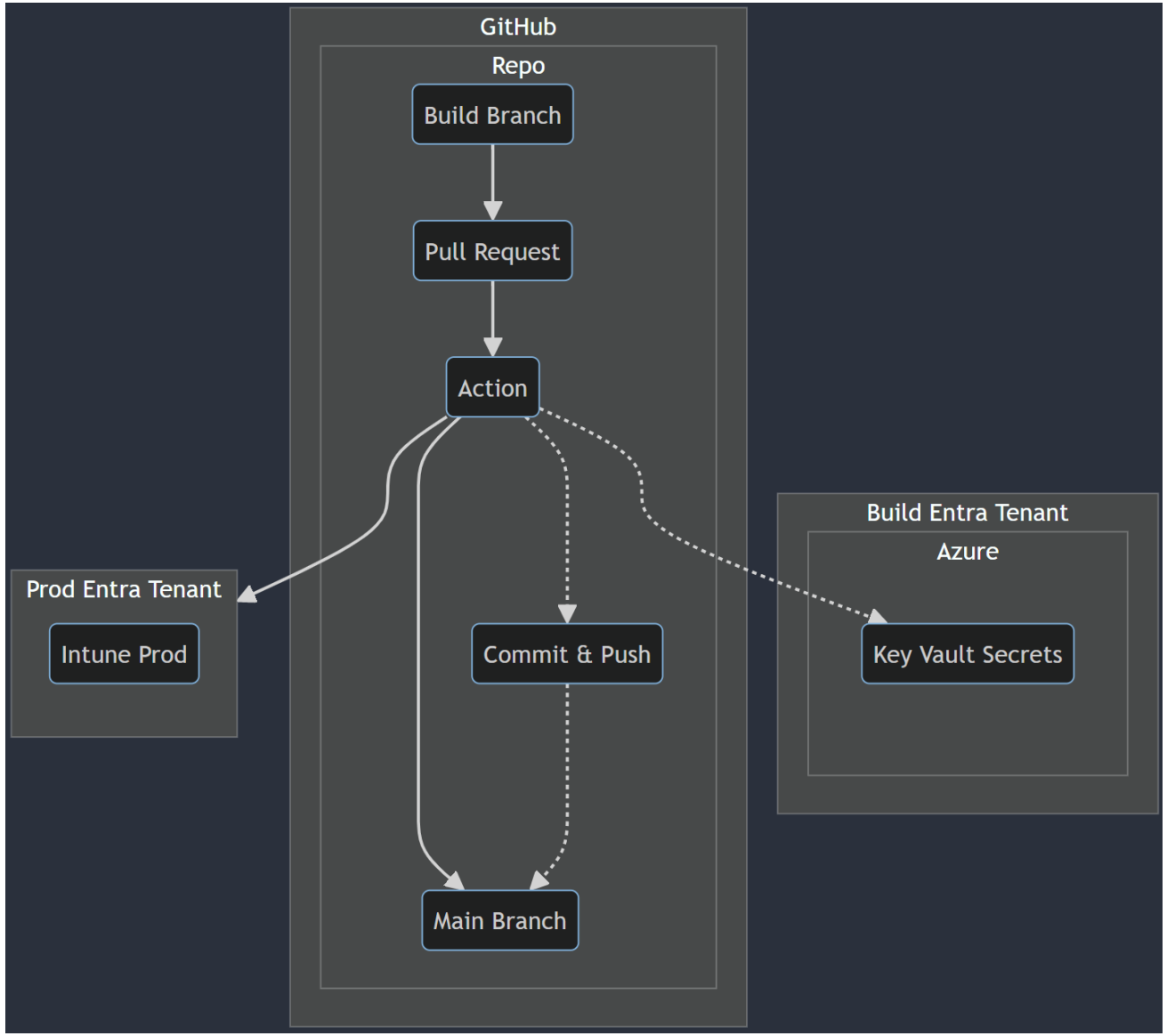
What is happening?



What is happening?



What is happening?



Does not compute…

Azure Function

- **Build** Entra System Assigned Managed Identity
  - Event Hub for reading message
  - Storage Account Queue for pushing commit messages
  - Container App Job for starting the run

GitHub Action IntuneCD

- ***Build** Entra User Assigned Managed Identity
  - Key Vault Secret for Prod App Registration
- **Prod** Entra App Registration
  - Graph API

Azure Virtual Machine

- **Build** Entra System Assigned Managed Identity
  - Creating the Docker image & Testing access

Azure Container App Job

- ***Build** Entra System Assigned Managed Identity
  - Storage Account Queue for processing commit messages
  - Key Vault Secret for GitHub SSH Private Key
  - Key Vault Secret for Build App Registration
- **Build** Entra App Registration
  - Graph API

What is next?

Use **System Managed Identities**
- Azure VMs or Azure Arc clients for interactive

Rule out permissions quickly
- Directory.AccessAsUser.All

Use tenant boundaries
- Be less restrictive in test/build environments
- Minimize interactive to prod/tier0 environments

Use the Audit Log as your friend
- Automatic change summaries
- Trigger automatic backups

https://merill.net/
- https://graphpermissions.merill.net/

If you are completely lost, use **Browser Dev Tools**
- XHR > Copy as…

The beta version
- A lot of Intune features (e.g., Win32 Apps)

Links

Use M365 DSC for even more functionality	https://github.com/microsoft/Microsoft365DSC
IntuneCD was the core library used	https://github.com/almenscorner/IntuneCD
Begin importing baselines or sharing your own	https://github.com/SkipToTheEndpoint/OpenIntuneBaseline
Review Microsoft's PAW guidance	https://github.com/Azure/securedworkstation
Another example of leveraging Graph for Intune	https://github.com/Micke-K/IntuneManagement
Automate your app packaging processes	https://github.com/aaronparker/packagefactory

Who is Michael Soule?

Michael Soule
National Director
Sentinel Technologies
misoule@sentinel.com

SENTINEL®

FORTIS By Sentinel
Advancing Your Protection

- Migration & Modernization
- Identity & Security
- Hybrid Cloud
- Licensing & Cost Optimization

What is next?

Use **System Managed Identities**
- Azure VMs or Azure Arc clients for interactive

Rule out permissions quickly
- Directory.AccessAsUser.All

Use tenant boundaries
- Be less restrictive in test/build environments
- Minimize interactive to prod/tier0 environments

Use the Audit Log as your friend
- Automatic change summaries
- Trigger automatic backups

https://merill.net/
- https://graphpermissions.merill.net/

If you are completely lost, use **Browser Dev Tools**
- XHR > Copy as…

The beta version
- A lot of Intune features (e.g., Win32 Apps)