TWO FACTOR AUTHENTICATION FOR ZABBIX
(THROUGH THE POWER OF OPEN SOURCE)

- EVGENY YURCHENKO
  Co-Founder, BGmot Inc., Canada
Two factor authentication (2FA)

Why 2FA for Zabbix?

- increased security
- complying with corporate policies
- if Zabbix UI exposed to Internet it’s a must
Two factor authentication (2FA)

- How does it work?

Two 2FA methods implemented:
- using Google Authenticated application (simple)
- using DUO 2FA provider (sophisticated)

Regardless of method the workflow is the same:

- a user is authenticated using configured Zabbix logic (internal, LDAP etc)
- if previous step succeeds then the user is required to confirm his identity using registered device
Enable 2FA in Zabbix UI. This is a global setting, i.e., affecting all the users.
2FA – Google Authenticator

- When a user logs in for the first time
2FA – Google Authenticator

- User scans QR code and his device gets “enrolled”
From now on this user will have to enter only the one-time code generated by Google Authenticator application.
Another method of performing 2FA is using third party service – DUO

Benefits:

- DUO is widely used in many companies -> natural integration/adoption
- Users management/audit at DUO web site
- DUO application on your device provides much more flexibility in providing security confirmation: push-acknowledgement, voice call, SMS
- Up to 10 users for free
Two factor authentication (2FA)

- See demos and detailed instructions at:
  - https://bgmot.com/zabbix_twofa_gglauth
  - https://bgmot.com/zabbix_twofa_duo

Source code (available for 5.0 and 5.2 at this moment):
https://github.com/BGmot/zabbix

The code DOES NOT affect default Zabbix server bahaviour!