Bolavá místa Microsoft Intune a jak je řešit

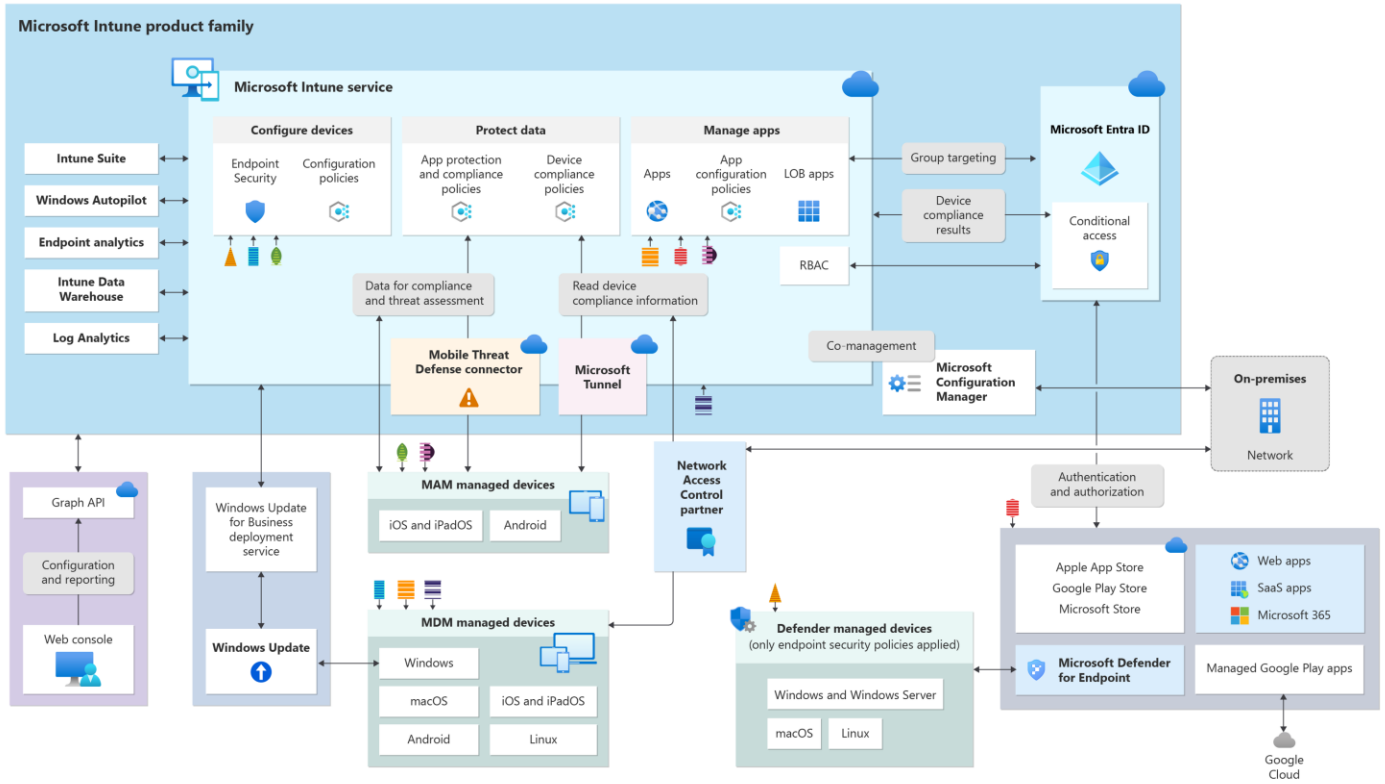
WUG Admin Day 2026

Jan Grundmann
Senior Consultant | grundmann@kpcs.cz

KPCS

Co je to Intune

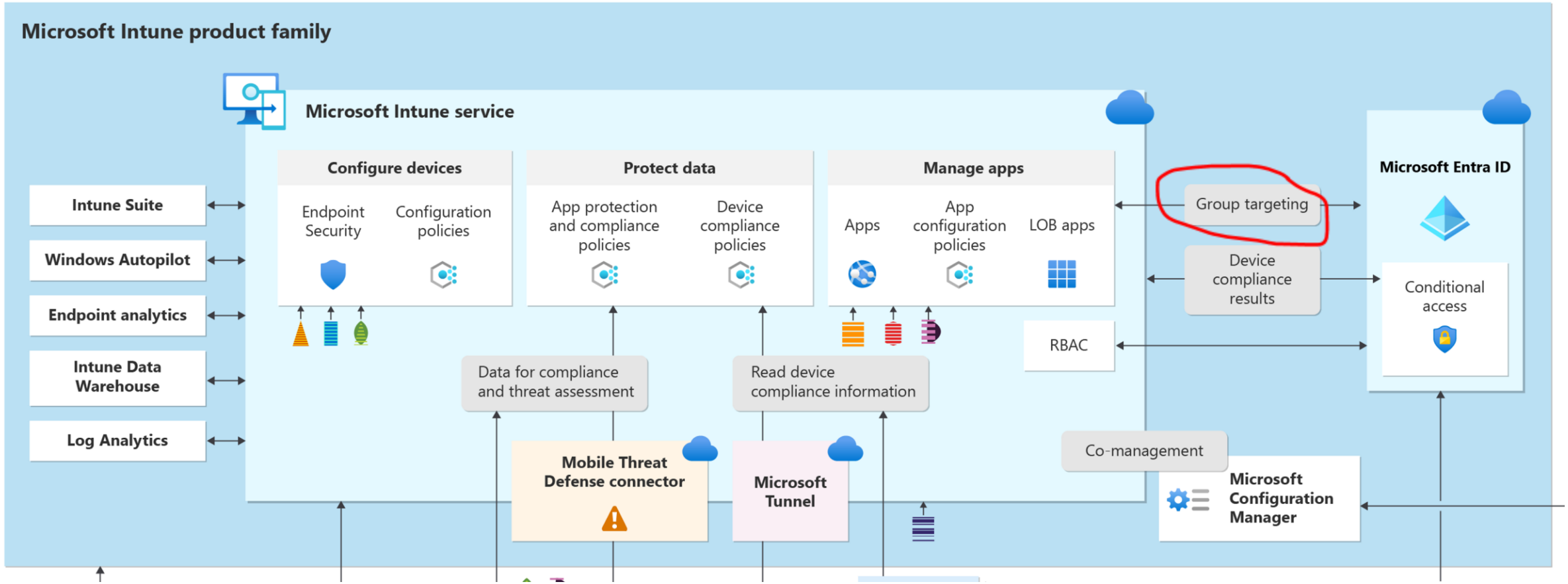
- Internet & cloud
- Nástupce ConfigMgr/SCCM/SMS



Rychlost

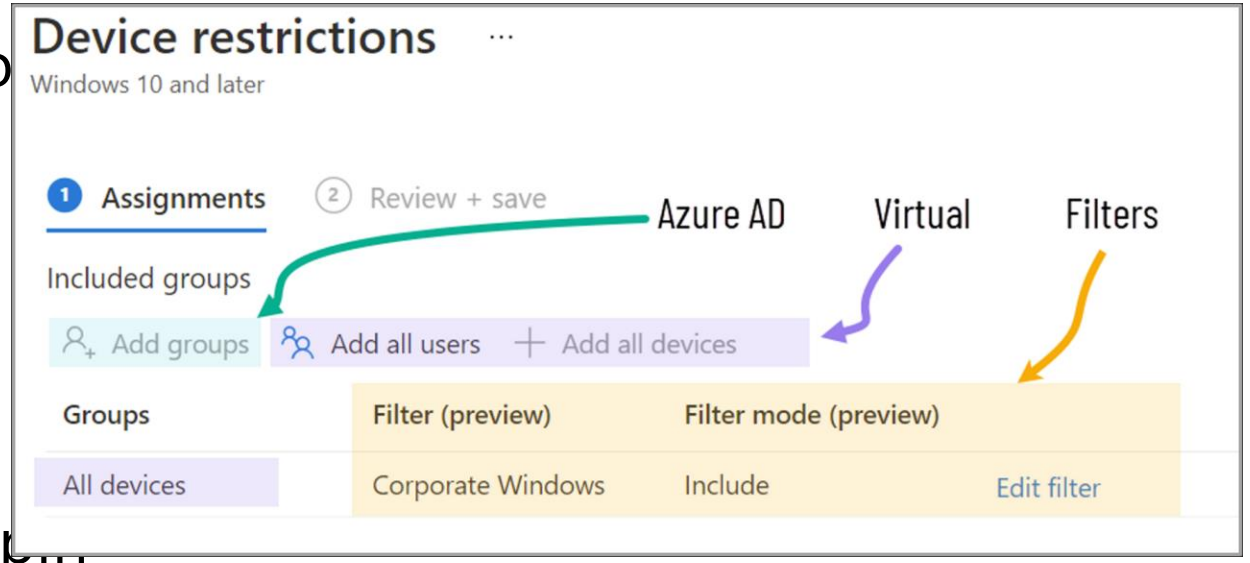
- Propagace policy
  - Vyhodnotí se cílení - group + filter a převede se na device
    - *Not applicable*
  - Pro daný device se aktualizuje celková policy
    - *Conflict*
  - Pošle se notifikace (možná)
  - Zařízení se jde synchronizovat. (task 1x za 8 hodin, user logon, user action)
    - *Pending*
  - Aplikace policy
    - *Success/Error*

Rychlost - Vyhodnocení cílení

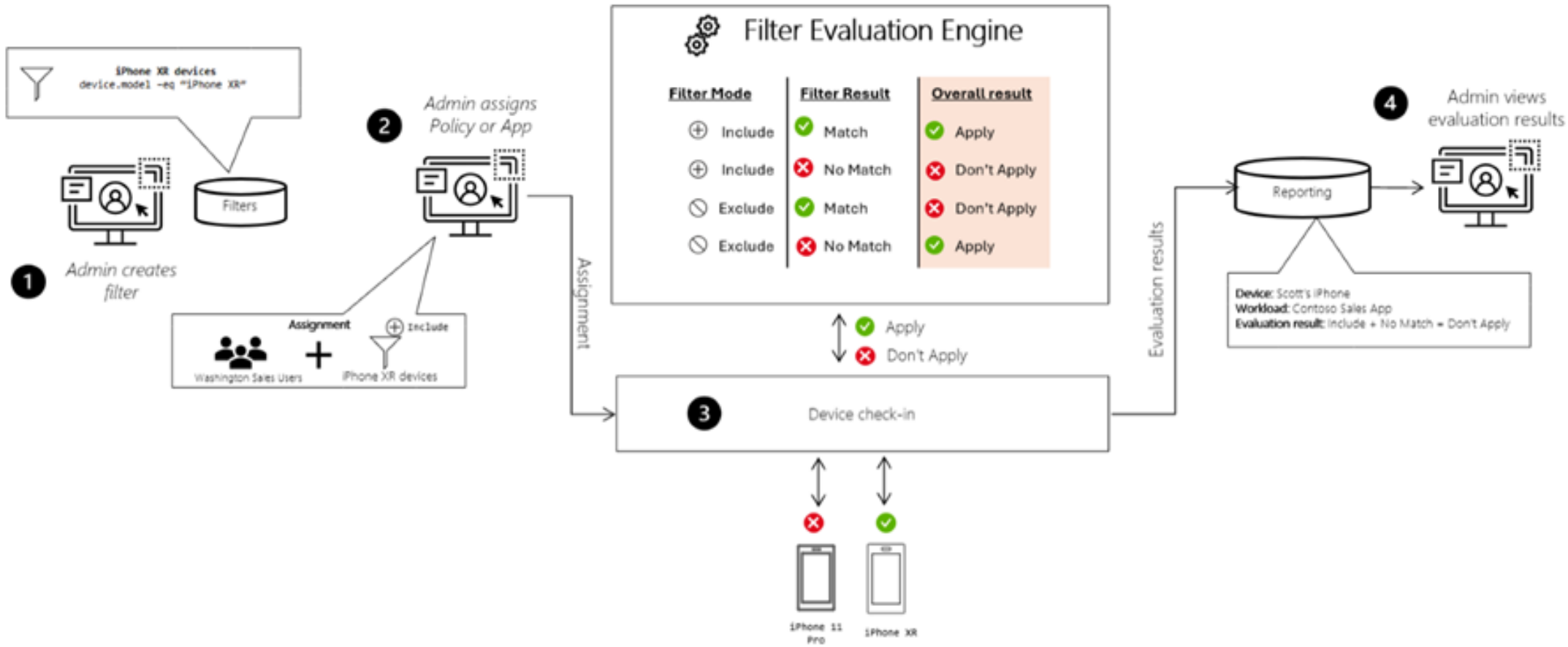


Rychlost - Vyhodnocení cílení

- Intune načítá Entra ID skupiny
- zpomalení
  - vyhodnocení Entra ID dynamic gro
  - sync do Intune
    - úvodní Full sync
    - následné Delta sync
- řešení
  - Minimalizovat použití Entra ID skup
    - All devices/All users „virtuální skupiny"
    - Opakovat použití Entra ID skupin napříč Intune
    - Využít filtry namísto dynamic (device) group



Rychlost – Vyhodnocení cílení - Filtry



Rychlost – Vyhodnocení cílení - Filtry

- MDM vs MAM
- Logika množin a priorita vyhodnocení
- Max 200 per tenant
- Ne pro všechny workloady
  - PowerShell & shell scripts, Update policies for iOS/iPadOS, Feature updates for Windows, Custom compliance policies for Windows, Linux
- Neumí device extension attributes

Rychlost – aktualizace celkové policy

Rychlost – notifikace zařízení

- Intune nemá spojení na zařízení => vždy směr od klienta ke službě
- Platform notification services – prostředník pro realtime akce
  - Apple - top
  - Google – OK
  - Microsoft – au
    - CIS benchmark disable W(P)NS
    - Cloud PC optimized image
- Zdroj
  - Change based – new assignment, policy update, group membership change, app store
  - Admin based – Device actions – sync, wipe, ..
- Kdy neproběhne?
  - limity Intune -> PNS
  - Time-out notifikace pro daný device

Rychlost – synchronizace zařízení

- Trigger
  - Notifikace
  - Action based
    - Admin action – Intune console -> notifikace
    - User logon – mám konektivitu k Intune? (proxy, VPN, DNS)
    - User action – Company portal /Settings app sync
    - Client change – e.g.: firewall update – compliance eval+report
  - Task based (1x8hod) => zpoždění
    - \Microsoft\Windows\EnterpriseMgmt\GUID\Schedule #x created by enrollment client
- Limity
  - Per device
  - Per org

Rychlost – aplikace policy

- Zařízení porovnává verze celkové policy, stahuje deltu, aplikuje a posílá výsledek
  - Synchronní session s mnoha výměnami
  - Největší zátěž na client facing infra
- legacy MDM vs DDM
  - legacy MDM - učitelka zkouší u tabule (synchronní)
  - DDM - učitelka rozdá písemku (asynchronní)

Rychlost – aplikace policy

- Legacy MDM

Client	Intune
1. What's up	
	2. [GET] Délka PIN
3. PIN=6	
	4. [SET] Nastav PIN=8
5. OK	
	6. [GET] Máš PIN=8
7. ANO PIN=8	
	8. OK. Konec

- DDM

Client	Intune
1. What's up, tohle je můj stav	
	2. [SET] tohle je delta novinek a pošli mi reporty
3. Tady je stav+reporty	
	4. OK. Konec

- Single document
- Periodická re-aplikace (i offline)
- WinDC

Konfigurace - profily

- Nepřehledné
  - Templates, Settings catalog, Admx, Custom oma-uri, Endpoint security, Skript, …?
- Neumí řešit konflikty
- Neumí "preferences" (registry)
  - Feature x Bug => Skripty/Remediace
    - Remediace a licence (Business Premium)
- Windows update
  - Feature update policy issue
    - Problém s přepočtem user-device
    - Problém s exclusion vyhodnocením
  - Driver service
    - Instalace nepodléhá řízení času jako standardní updaty - instalace a restarty pro uživatele náhodně

Konfigurace - aplikace

- LOB (msi) vs Win32
  - konflikt v Autopilotu. Dělat vždy jen win32.
  - built-in Office pro Windows stejný problém jako LOB
- Velikost app objektu
  - pomalý upload - dojde k session timeout dříve než se nahraje. Využít AVD/W365 stroj.
  - překračuje limit – LOB 8GB, win32 30GB
- Windows app install sekvence
  - retry/re-evaluace neúspěšných appek
    - 3x po 5min podle exit code, pak až s GRS za 24h, přestože app install běží každou hodinu.
    - řešení je promazat GRS registry a restartovat IME službu

Konfigurace - housekeeping

- Naming convention
- Policy design – single policy vs 1 setting 1 policy
- Change mgmt
  - Verzování
- Release mgmt
  - Fázování nasazení
- Multiple tenants

- Opustit Intune 1st party GUI
  - Manuální – např. https://github.com/Micke-K/IntuneManagement

Monitoring & reporting

- MDM protokol
- Špatný design backendu
- Koupit (1st vs 3rd party) vs postavit vlastní

- Optimistický výhled
  - Properties catalog
  - Device query
  - DDM
  - Backend improvements
  - Intune Suite v E3/E5

Velká prostředí - governance

- Centralizace vs delegace
  - Sdílené prostředky
    - Aplikační katalog
    - Config profiles
    - Compliance policies
    - Connectors – AD, CA
    - …
- Multiadmin approval
  - Scripts & Apps only

Velká prostředí - RBAC

- Intune console RBAC
  - Koncept role & nasazení – “Members”, “Scope Group”, “Scope Tag”. Scope tag assignment
  - Dokumentace – nezačínat od 0, ale od existující role
  - Granularita – Device config obsahuje i Device platform restrictions
- RBAC vs rychlost
  - Scoping vyžaduje Device group (dynamic ☹). Latence syncu => neviditelné zařízení
    - Enrollment time grouping (APv2, Android fully managed, WPCOD, dedicated)
- Device group for Personal devices (iOS, Android)
- Entra RBAC – BitLocker, LAPS, device lifecycle
- Assignment – Entra PIM (for groups), Access package

Závěr

- Rychlost
  - Cloud => FUP
  - Services & microservices => synchronizace (Entra ID -> Intune)
    - Minimalizace použití Entra ID skupin. Maximalizace filtrů.
  - Zprůchodnění notifikací
- Konfigurace
  - Settings catalog, Endpoint Security templates
  - Win32 apps
- API je kamarád
  - …když už ten boj s ním svedl někdo jiný

Q&A