Devices management, then and now

The journey to a modern device management solution

Thank you Sponsors

Microsoft

DEVICIE

About me

Role

Solution Architect at AC3

From

France

Blog

https://blog.hametbenoit.info

Certifications

Microsoft MVP Enterprise Mobility and M365 Apps & Services

Various certifications

Hobbies

Lego and watches collector

Contact

https://blog.hametbenoit.info
https://twitter.com/benoit_hamet
https://www.linkedin.com/in/benoithamet/

Agenda

What is ‘modern’ device management?

Definition of a modern device management solution

Device management, then and now

Little history of device management

Migration options

Journey to move to a modern device management solution

Migration journey

Plan your journey to modern device management

Experience

Dos and Don'ts

What is modern device management

What is ‘modern’ device management?

- Referring to essentially translates to ‘cloud-based’
- ‘modern (device) management’ is Microsoft’s recommended overall strategy for managing Windows 10 users and devices utilising the power of cloud technologies
- Cloud platforms will work in conjunction with other Microsoft programs such as Autopilot and Intune to automate a lot of the device management process
- Less time is spent managing both the devices and the tools used to govern them
- Under the hood, devices will move from being managed via Configuration Manager, Active Directory and Group Policy to being cloud-managed through Intune and joined to Azure Active Directory

Challenges of traditional MDM

- Reliance on a corporate network
- Complex infrastructure
- Higher infrastructure costs
- Problematic content delivery
- OS deployment

Benefits of modern MDM

- No on-premises requirements
- Content delivery and management delivered securely over Internet
- User centric OS deployment
- Reduce costs and administrative overhead
- Allows secure BYOD
- Modern device management helps in digital transformation
  - Accelerate
  - Improve
  - Streamline

Components of ‘modern’ device management

- Windows 10 or later
- Deployment and provisioning to deliver devices to end-users ready to use
  - Windows Imaging
  - Configuration Manager
  - Autopilot
  - Intune
- Identity and authentication
  - Azure AD / Hybrid joined devices
  - Conditional Access
- Configuration and updates management
  - MDM policies
  - Windows Update for Business
  - Telemetry
- …

Device management: then and now

A brief history of device management

1994

- SMS 1.0
  - MS-DOS
  - For Workgroups
  - NT 3.5

1999

- SMS 2.0
  - Y2K remediation
  - Active Directory

2003

- SMS 2003
  - Advanced Client (MP)

2007

- SCCM 2007

2012

- SCCM 2012

2011

- Windows Intune
- service portal on top of the Microsoft Malware protection engine

A brief history of device management

2015

- SCCM CB

2019

- MECM CB
  - Co-management

2013

- Unified endpoint management
- Single place to manage PC and smartphone
- Use of AAD

2014

- Intune
- Mobile application support
- Email profile

2015

- Support for MacOS

2019

- MEM
- Co-management

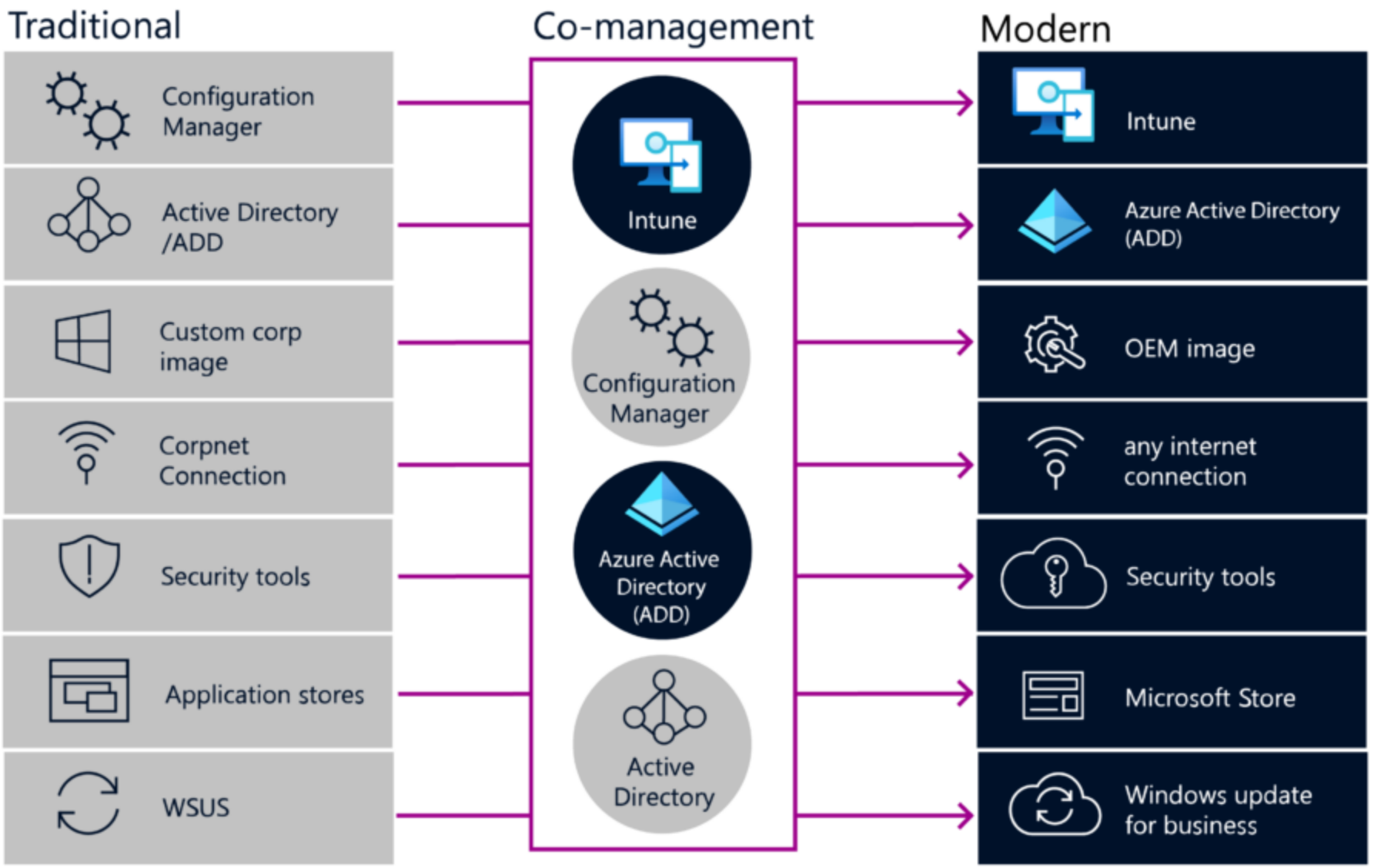
202x

- Tenant attach
- Support for Linux
- Support for Google Chrome

Migration options

Migration Options

- From scratch
  - If you have no management solution, third party solution or don’t use SCCM
- Co-management
  - If you have SCCM
    - SCCM cloud attach
    - SCCM cloud management gateway
  - Gradually migrate management workloads
- M365 Basic Mobility & Security
  - If you don’t have Intune but use the M365 Basic Mobility and Security feature (M365 MDM)
  - Migration evaluation – evaluate and create configuration profiles
- For all create device configuration, compliance profiles and applications


Traditional
Co-management
Modern
Configuration Manager
Active Directory /ADD
Custom corp image
Corpnet Connection
Security tools
Application stores
WSUS
Intune
Configuration Manager
Azure Active Directory (ADD)
Active Directory
Intune
Azure Active Directory (ADD)
OEM image
any internet connection
Security tools
Microsoft Store
Windows update for business

Migration Journey

Migration Journey

wpninjas.au

Start

01 Assess source environment

02 Migration strategy

03 Target preparation

04 Pilot

05 Migration

06 Decommission

Finish

On-Premises management

Co-management

Cloud native management

Preparation steps

- Identity and access management
  - Identity management (cloud vs AD)
  - Conditional Access
- Review existing configuration policies
  - Group Policies
  - SCCM policies
- Devices
  - Supported OS (Windows 1x, macOS, iOS, Android, Linux*, Chrome OS**)
  - What do you need

* https://learn.microsoft.com/en-us/mem/intune/user-help/enroll-device-linux/
** https://learn.microsoft.com/en-us/mem/intune/enrollment/chrome-enterprise-connector-configure/

Preparation steps

- Applications
  - Utilisation
  - Version
  - Source (MSI, exe, script…)
- Windows Update
- Intune tenant
  - Licenses
  - Configuration Profiles
- Current management solution(s)

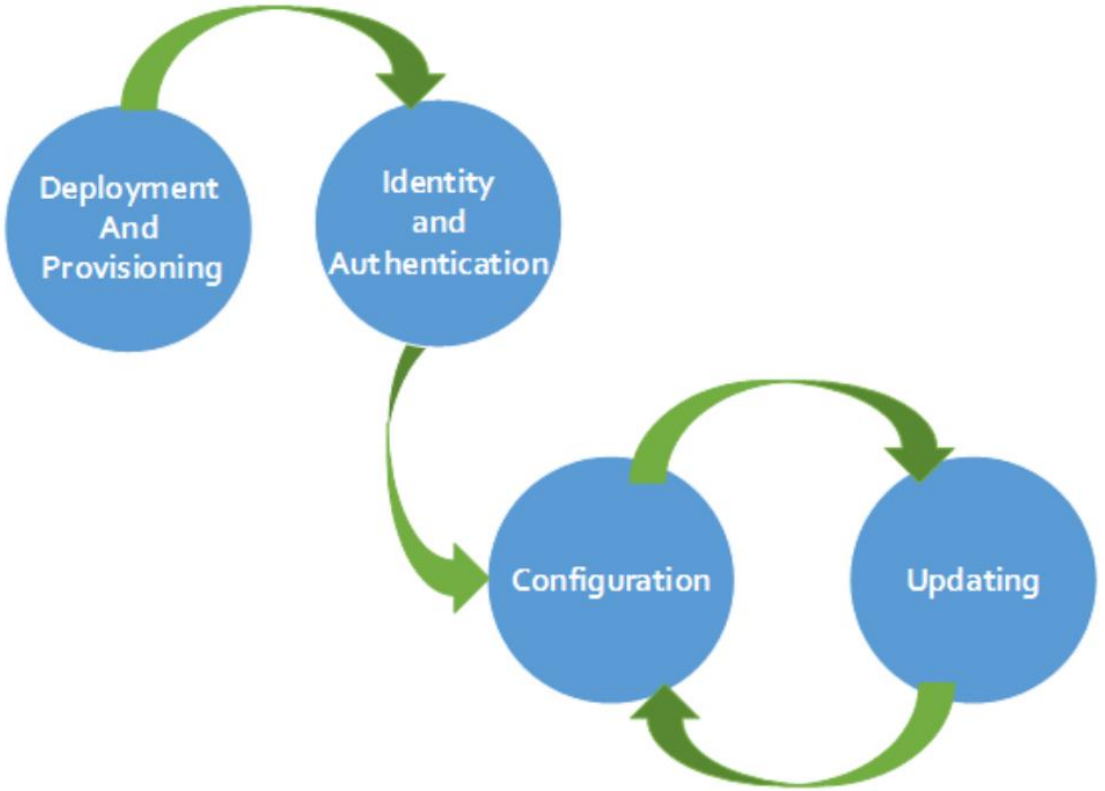
Experience

Experience

- Brand your tenant (see Add company branding to your organization's sign-in page (preview) for new options)
- It is not just a device management migration
- Don’t replicate your legacy
- Don’t over complicate
  - Limit number of profiles
  - Use appropriate profiles (configuration, endpoint security…)
  - Limit use of custom profile (CSP)
- Disconnect from Active Directory
  - Cloud based device (AAD Joined)
- Automatic provisioning
  - Autopilot
  - Apple ADE
  - Google Zero Touch
  - Samsung KME
  - Android Enterprise enrollment

Experience

- Use modern capabilities
  - Conditional Access
  - Azure AD Joined Device Local Administrator, with PIM
  - Administrative Units
  - Dynamic groups
  - App Configuration portal (https://config.office.com/)
- Enforce minimum OS version
- Modern applications (SaaS)
- Application Protection policies
- It is an ongoing process



Thank You

Workplace Ninjas Australia