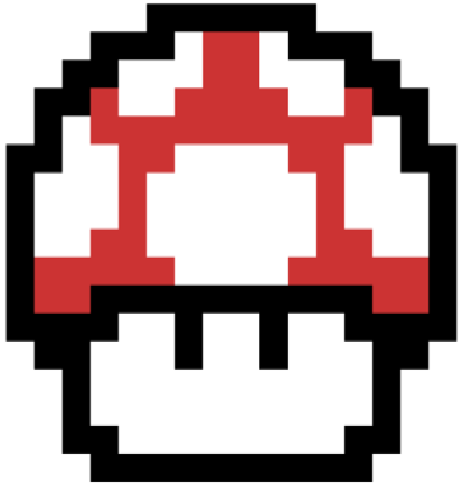
MC2MC

How to grow to a Modern Workplace in 16 steps with Microsoft 365



Jasper Bernaers

Modern Workplace Lead @ Synergics

@Jasper_be

https://www.jasperbernaers.com

https://www.linkedin.com/in/jasperbernaers/

Tim Hermie

Senior Modern Workplace Architect @ Synergics
Microsoft MVP Enterprise Mobility

@_Cloud_boy

https://www.cloud-boy.be

https://www.linkedin.com/in/timhermie/

Agenda

- Azure AD Connect
- Exchange Hybrid
- OneDrive/ESR
- Teams/Sharepoint
- MEM
- Voice
- Autopilot
- Increase security
- Software deployment
- GPO to CSP
- Windows Updates
- Azure
- Legacy AD migration
- Collaboration platforms
- Rethink on-premises
- Automate

Why are we bringing this pitch?

- IT-Strategy
- Long-term decisions will reflect in Microsoft 365
- We are not expert in every aspect
- We should know something about everything :-)
- Microsoft 365 is connected in the collaboration stack
- We are working for mid-size companies (SMB), they don't have a specific profile for everything

1. Azure AD Connect

Azure AD Connect

- Install Azure AD Connect (best practice not on your DC).
- Sync your users and groups to Azure AD.
- Sync password hashes to Azure AD.
- Use Azure AD as primary authentication method.
- Enable password writeback (Self-Service).

Why?

- Microsoft Azure AD is beyond the current ‘legacy’ integration and is a next-gen identity platform. Make it simple. If you don’t need third-party solutions (which always limits new capabilities) don’t go for it.
- Use native Azure AD. Also it’s a big opportunity to leave things behind and smoothly shift to ADDS or Azure AD.
- Built-in integration with a lot of SaaS apps.

2. Exchange Hybrid

Exchange Hybrid

- Change the UPN’s if required, same as e-mail preferred. Easier for users.
- Run the hybrid Exchange wizard and connect your exchange with EXO.
- Pre-sync all mailboxes to a state of 95. Throttled, change the maximum in your virtual webservices.
- Move to Office 365 in 1 a cut-over scenario.
- Cut-over migration is best-practice under 2000-5000 seats you can do more, over a weekend.

After the migration

- After the migration of hybrid Exchange the next steps is shifting the mail relay to O365.
- Make it simple, don't create a super complex mailflow is has no real value.
- Don’t over-think, don’t create complex hybrid mail flows. You could keep hybrid-Exchange for the first phase with management to AD and Exchange Online.
- You could stop the Azure AD Connect and go cloud only, but..

3. OneDrive + ESR

OneDrive

- Document data is one of the post important things running in any workplace.
- Personal data is crucial for considering for migration.
- OneDrive migration will help support the shift to M365 when you help to create a better collaboration space for the people.

OneDrive

- Use OneDrive Known Folder move so you can automatically discover your Desktop, documents and pictures and place them on OneDrive (automatically). People love this feature. It's easy to implement and has additional value without changing the core.
- Migrate your home drives, to OneDrive with the SharePoint migration tool or different tools when you need more control. Document shift is important to get away from the current system(s).

ESR – Enterprise State Roaming

- Use ESR to sync favorites and Windows settings to the cloud.
- This together with OneDrive KFM makes sure a user always gets the "same" device back after refreshing devices.

4. Teams/SharePoint Online

Teams/SharePoint Online

- Assess your current environment and understand the needs.
- Migration of team data could result in Microsoft Teams Libraries.
- Migration of organization data should result in SharePoint Online.
- Still personal data (only touched by 1 person) can land in OneDrive.
- There are great tools on the market to do the assessments. Phased approach is necessary. Standards & building blocks will help with speed of implementation.

5. MEM

MEM

- Implement Microsoft Endpoint Manager (Intune) for your Windows 10 devices.
- Onboard all current devices with Hybrid Join and rollout new devices full Cloud (Azure AD Joined).
- Implement MAM for mobile (Android/iOS) at least. Manage all your company owned devices.

6. Voice

Voice

- Don’t go for less. Use Microsoft Teams. :-)
- And if you will choose other platforms think about what Microsoft is preaching: trust – compliance – Inclusion - Security, segmentation..
- More important: Think about the speed of implementation comparted to the easiness of one platform
- Also think about adoption, everything is changing faster. It's our 'responsibility' to govern these solutions so different creates complexitiy.

7. Windows Autopilot

Windows Autopilot

- Enroll new device with Windows Autopilot (staging Principe)
- Onboard current domain joined devices with a Group Policy.
- Onboard current hybrid joined devices with an Autopilot profile.

8. Increase Security

Increase Security

- Multi-Factor Authentication or Azure Security Defaults.
- Conditional Access.
- Connect your devices to Azure AD with Microsoft Endpoint Manager. Hybrid Join – Full Cloud. Just connect it.
- Enroll devices into MDATP if you have the license :-) we have seen..
- Risky User Sign-in policies. Define some security policies. Just basic alerting.

Increase Security

- Self-Service Password Reset (SSPR) – enable password writeback in Azure AD Connect.
- Create control on lifecycle management of identities. Expiration, onboarding, offboarding etc..
- Automatic password reset or disablement of account when breached.
- Shift to primary Azure AD, later ☺

9. Software deployment

Software deployment

- Microsoft 365 Apps can be quickly deployed by Microsoft Endpoint Manager.
- Windows Updates is easy with MEM.
- Built an Update strategy (1 x year / 2 x year?)

Software deployment

- Microsoft Edge will deliver great value when it comes to browser support, can support old ‘sessions’ as well. Azure AD integrated, great new stuff, super modern. Configure Edge with MEM.
- Use third-party mechanisms as PatchMyPC or Chocolatey for ‘simple’ deployable software.
- Use own written scripts and create packages when necessary.
- Wrap everything as IntuneWin (++ advantages).

10. GPO to CSP

GPO to CSP

- Microsoft is currently working on Policy Analytics which will help the migration of GPO’s to MDM policies with control. But keep in mind, a lot of policy are used for legacy.
- We don’t believe in migration of GPO’s. We believe in a basis workplace ‘greenfield’ were you build standards for everyone. Not for groups. And if you do. For 10 groups. and 90% same architecture and flavors.
- So: Don’t migrate non used GPO’s.
- Rethink GPO’s -> MDM.

GPO to CSP

- Start with Security Baselines.
- ADMX backed baselines (ADMX ingestion) will help for smooth and faster configuration. Whenever it’s not possible use the OMA-URI’s.
- Most important try to be prepared for 80% to shift the authority from GPO’s to MDM. And leave the GPO’s in your on-premise DC’s behind.

11. Windows Updates

Windows Updates

- Create a Windows 10 update ring with peer-to-peer caching to not kill the internet break out. VPN etc.. (Delivery Optimization!!!)
- Create segmented of pre-test groups to validate the update version in production. (Minimum of 2/3 Update Rings!)
- Use the standard Security Baselines to implement the W10 MDM Baseline and MDATP configuration. Baselines are great but complex. Test it with a POC!

12. Azure

Azure

- Think about Wim: **Rehost, Refactor, Rearchitect, Rebuild, Replace!**
- Assess and write down all infrastructure and start with rearchitecting were possible.
- When you’re hosting well known vendor applications try to get in touch and ask if they are planning for SaaS, Azure, others.

Azure

- Create an Azure Migrate project and add the Server Assessment solution to the project.
- Set up the Azure Migrate appliance and start discovery of your server. To set up discovery, the server names or IP addresses are required. Each appliance supports discovery of 250 servers. You can set up more than one appliance if required.
- Once you have successfully set up discovery, create assessments and review the assessment reports.

Azure

- Use the application dependency analysis features to create and refine server groups to phase your migration.
- Migrate machines as physical servers to Azure.
- Don’t forget: Rehost, Refactor, Rearchitect, Rebuild, Replace.
- Say goodbye to old legacy applications that are not secured in a modern world.

13. Legacy AD Migration

Legacy AD Migration

- Shift applications that use AD Groups or AD Authentication to authenticate applications towards Azure AD worst case ADDS.
- Try to isolate all applications, monitor the active usage of AD and try to find and understand what you can transform easily.
- Sometimes there is an application which is old for billing or accountants, mostly used by some people. Don’t integrate, isolate and shift with dedicated accounts to Azure IaaS. But write it in the long-term plan and push these vendor for integration of choose other platforms.

14. Collaboration platforms

Collaboration platforms

- Build your new Microsoft Teams Sites for collaboration.
- Create a SharePoint Hub for all SharePoint sites – create a frame and design of the requirement and visual for your full organization.
- Build out department and long-term SharePoint collaboration spaces.
- Migrate the old ’20’ years old applications to SharePoint list, with PowerApps and integrate with power Platform.

15. Rethink on-premises

Rehost, Refactor, Rearchitect, Rebuild, Replace

Rethink on-premises

- Rethink the new needs of on-premises. All collaborations spaces are shifted to Office 365. Your devices are managed with MEM. Documents are shifted to OneDrive, Teams and SharePoint. Authentication and integration with Azure AD is shifted. Printers with Universal Print of different cloud print solutions as Printix. Core applications are moved to IaaS and are waiting to become SaaS overtime.
- **What else is there?**

16. Automate

Build security mechanisms that can be automated

Automate

- SecOps and your incident responds can be done with MDATP/MCAS/Sentinel.
- Build on the next level Modern Workplace with Unified Sensitivity Labeling – which automatic labels classified documents. Use the unified data classification platform.
- Get grip on actionable risks on devices, users with MDATP in combination with Cloud App Security to identity and isolate risks. Sometimes automatic remediation.

Automate

- Start with MAM (Mobile Application Management) to isolate corporate applications from personal applications on BYOD Devices.
- Evaluate regularly which users have access to data, devices and physical network.
- Work on Secure Score and Azure Secure Score.
- Automate alerts with Logic Apps.
- Leverage the power of Sentinel.

Q&A