Azure Virtual Desktop without a golden image

Markus Lintuala

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_ SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

AppManagEvent.com
2022
October 7
Netherlands

dinext.

About Markus

Focus

Public cloud architectures and solutions with a focus on security

From

Finland

My Blog

Bloggerz.cloud

Certifications

Hobbies

- IT
- Aviation
- Cooking

Contact

LinkedIn: lintuala

Twitter: @MarkusLintuala

E-mail: markus@lintuala.fi

Agenda

Key takeaways:

- **Another way to manage AVD infrastructure**
- **Suits for some organizations, but not a silver bullet**

Imaging approaches

Different methods for imaging

Idea of standardized AVD management

Why we even thought this is a good idea

Pros and cons

Why to use and why not to use

Drain mode and other challenges

Challenges that can be faced

Future

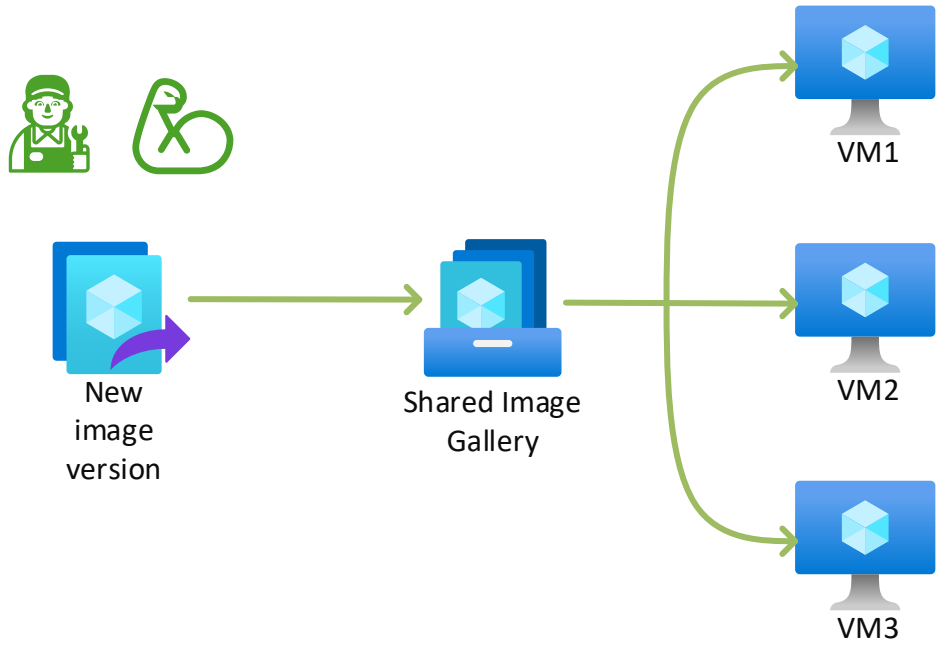
What next?

Imaging approaches

Standard manual *thick image*

Standard manual thick image

- New applications and application versions are installed manually to golden image
- Golden image is prepared for cloning
- New version of image is updated to Shared Image Gallery
- New VMs are deployed from updated image

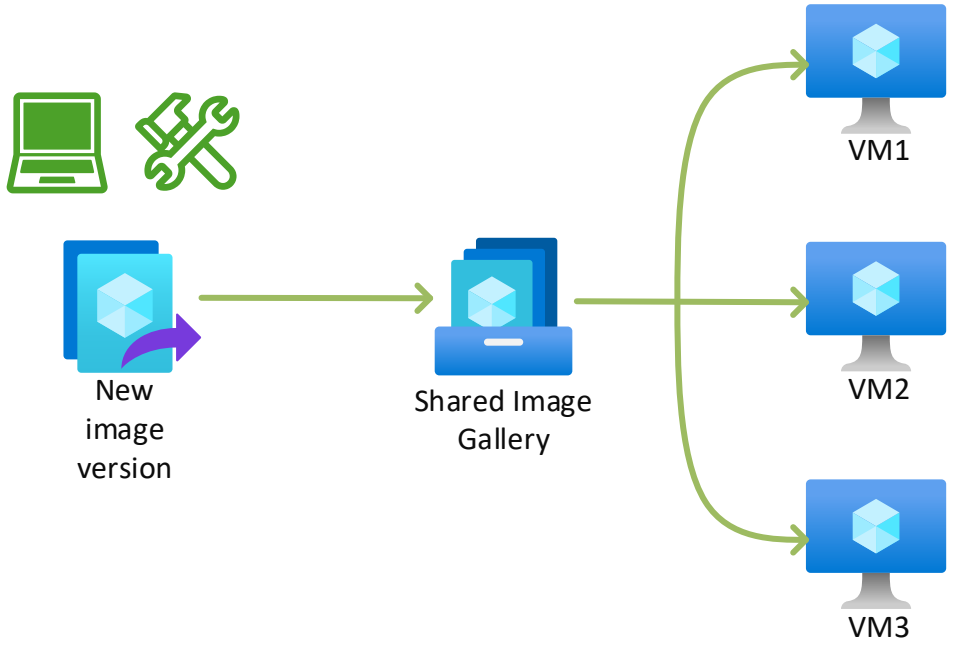


Imaging approaches

Standard automated *thick image*

Standard automated thick image

- New applications and versions are installed automatically to golden image
- Golden image is prepared for cloning
- New version of image is uploaded to Shared Image Gallery
- New VMs are deployed from updated image

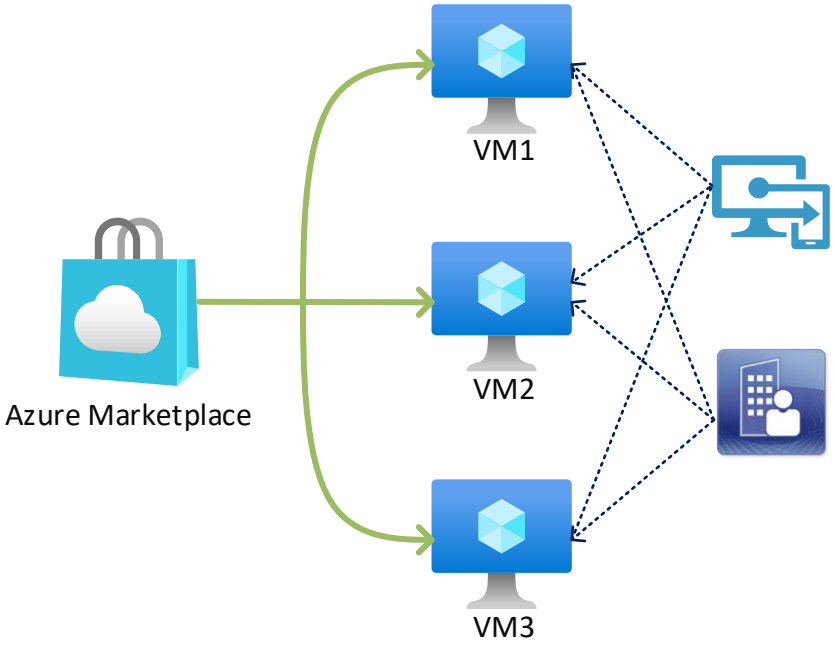


Imaging approaches

Without a *golden image*

Without a golden image

- Install new VM with Vanilla image from Azure Marketplace
- Deploy required applications and versions to new VMs with Microsoft Endpoint Manager or with Configuration Manger
- Use Azure functions to *release* ready VM for users



Phases in without a golden image

VM deployment

Post-deployment

Release

Monitoring

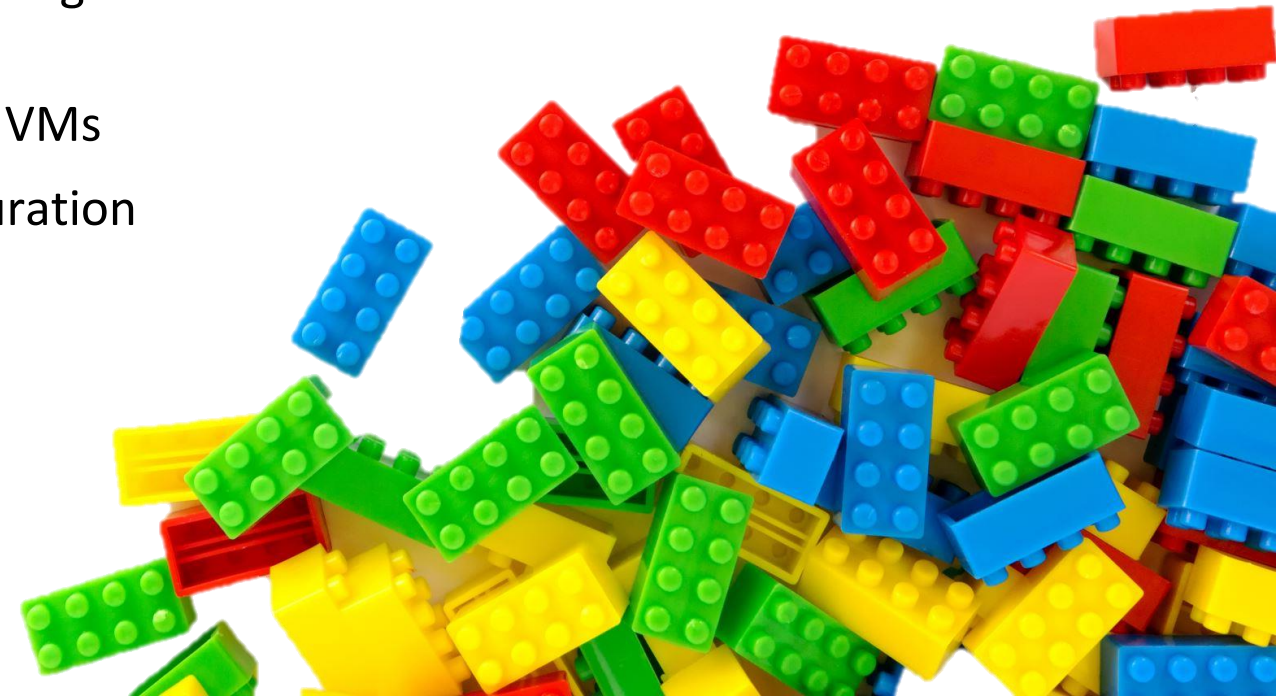
Example is written for Configuration Manager

VM Deployment phase

- Deploy VM normally with Infrastructure-as-Code
- Join to Azure Virtual Desktop host pool
- Join to domain
- Turn drain mode on
- Update group policies and release new VM to GPO’s and MECM

Post-deployment phase

- All post-deployment tasks are described in Configuration Manager's task sequence
- Group policies installs Configuration Manager Client to new VM with PROVISIONTS property
- Group policies are setting up all normal policy settings to client as always
- Configuration Manager installs all applications to VMs
- Settings configurations can be made with Configuration Manager or Group Policy



Release phase

- Last step of the task sequence is release phase
- After all applications are installed successfully (Do **NOT** add **Continue on error** steps!!)
- Remove drain mode from session hosts
- Release new session hosts for end users

Monitor phase

- Monitor devices normally as any other AVD Session host in Azure
- Manage all devices with Microsoft Endpoint Manager: OS Management, configuration updates, security updates etc.
- Manage all application lifecycles with Microsoft Endpoint Manager: Installations, updates, uninstallations
- When it is time to retire the VM, retire it with normal processes

Idea of standardized AVD management

“Could I integrate my current workstation management processes to AVD?”

”Everyone can do everything”

End device specialist

- End device specialists understands end user much more than cloud specialists
- End device specialists could manage their part without changing any their processes – Only physical laptop is changed to virtual machine
- End device specialists are focused much more to configuration management than cloud automations and enhancements
- There are enough work to do already for end device specialists

Cloud specialist

- Cloudification is in their soul
- Cruel fact that cloud specialists does not care so much end users than end device specialists
- Cloud specialists are working with cloud automations, not with end device management or troubleshooting
- Cloud specialists manages automations and VM creation itself

Idea of standardized AVD management

1. Could you take pros from both and create something cool?
2. What cons you get if you change the way of people working?
3. What cons you get if you change the way of how it technically is planned to work?

Pros and cons

Pros

Can be managed as a regular workstation

Same group policy objects

Same applications

Same patch management

All workstation admins knows how Windows client works

No codebase requirements

Cons

Takes time to complete after a deployment

Problems

- Drain mode not available in ARM schema
- If Group Policies are messing up the whole domain?
- Configuration manager’s provisioning task sequence takes time depending of the application list that it should install

Drain mode handling

- Prevent user for getting a device that is not provisioned to the end
- Azure function that takes host pool name, host pool resource group name, and session host name in JSON-body

Example input body


```
{
    “hostName“ : “AVDPER1-1372.company.tld”,
    “hostpoolName” : “hp-per1”,
    “hostpoolRgName” : “rg-weu-avdmanagement”
}
```

Drain mode handling

- Prevent user for getting a device that is not provisioned to the end
- Azure function that takes host pool name, host pool resource group name, and session host name in JSON-body
- Connections allowed only from AVD session hosts
- Drain mode is turned off by session host in the last step of the provisioning task sequence if all applications installed successfully
- Hide azure function’s key in task sequence variable as a secret value (Do not display this value)

How to manage image creation in scale?

Integrate it to your end user’s self-service portal

Depending your scaling requirements, you can pre-provision devices to host pools and only add users to assignment groups

Pooled host pools works similar way or if using scaling plans, just create the thick image just be aware that scaling plans handles the drain mode under the hood

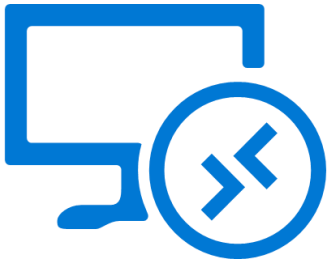
How to support it?

- Everything over operating system is supported by end device management specialists
- No separate teams for physical and virtual operating system management in end device management
- Everything else is supported by cloud specialists
- Service desk can handle same way support for end user

Future

Waiting a support for a drain mode switch in ARM schema

More automations to support different use cases



More integrations to end user portals

Continuous development when service goes forward

Wednesday, September 14

10:30 CEST

Sentinel log ingest with Azure Monitor Agent deep dive
Markus Lintuala

16:30 CEST

Passwordless - Phishing proof identities?!
Markus Lintuala

Thank You