

Sandbox AD-Azure-Office Subscription

Last updated by | Paul Kelleher | 17 Jun 2020 at 08:02 GMT



Template Sandbox AD

Contents

- [Executive Summary](#)
 - [Ownership and Contacts](#)
- [Logical Separation](#)
- [High Level Components](#)
 - [Azure Subscription and Assets](#)
 - [Azure Active Directory](#)
 - [Office 365 Licence and management](#)
- [Implementation](#)
 - [Asset and Cost Protection](#)
 - [User Management and Roles](#)
 - [Audit](#)
 - [pknw1 Implementation Stages and Templates](#)
- [Impact Assessment](#)
 - [Positive Risk Impact](#)
 - [Negative Risk Impact](#)
- [Data Control & Flows](#)

Executive Summary

Development and integration to existing services has always been required in the bank but done in ways that caused high or medium risks to existing implementations. The new environment layout proposed as 2 sandbox environments are as below

Billing	Directory	Azure	Office
pknw1 Billing	VCAPv3.onmicrosoft.com 	Azure pknw1 Core AAD Sandbox	VCAPv3 integrated
pknw1 Billing	pknw1EUP.onmicrosoft.com 	Azure Core EUP Sandbox	pknw1EUP Integrated

The subscriptions should be looked on as a lower level than the existingf MSDN subscriptions due to

- ☒ No Exchanged user data
- ☒ No Exchanged application data

- ✓ No Shared Resources
- ✓ No private networking integration

Ownership and Contacts

Instance Set	Contact	Secondary Contact
Core AAD Test	Paul Kelleher	Russell Tebay
Core EUP Sandbox	Jagdeep Bamrah	James Johnson

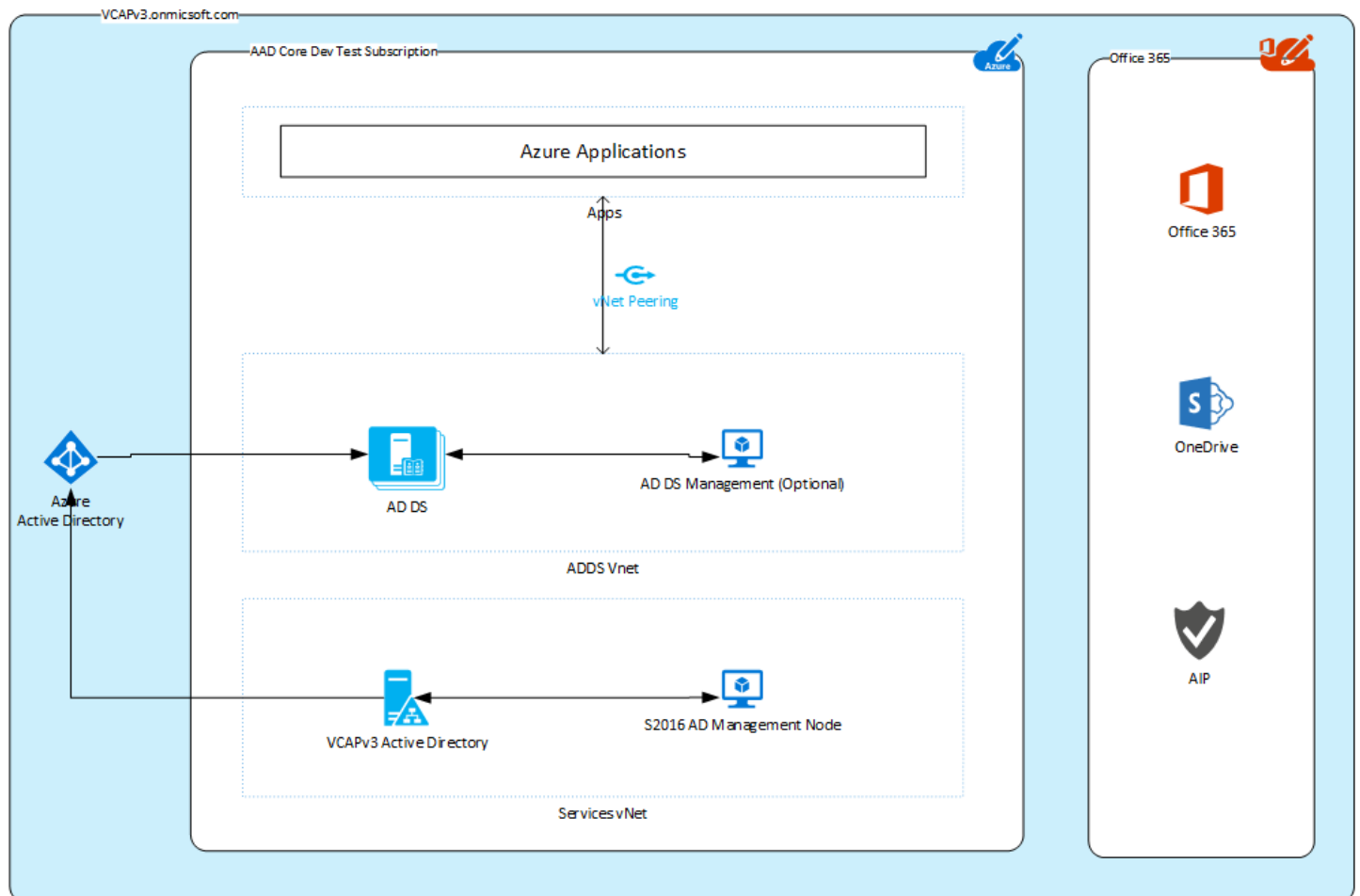
Logical Separation

 Azure AD Subscriptions and Directories.png

High Level Components

VBL CutOff Environment

HLD and Design for complete segregation for RAD in EUP/Infra



Azure Subscription and Assets

for each instances set there will be

Azure Active Directory

- ☐ [vcapv3.onmicrosoft.com](#) or
- ☐ [pknw1eup.onmicrosoft.com](#) which is associated to
- ☒ Azure AD Subscription containing the AAD instance
- ☒ AD "Clone" structure (separate data)
- ☒ AD Management Servers

and also associated to Office 365 Subscription

Office 365 Licence and management

Implementation

Asset and Cost Protection

- ☒ In order to prevent mis-use of assets, access should be limited to named IP ranges (for users home access and for Wireless Network Access from office)
- ☐ There should be no access from standard network and desktops
- ☒ Asset reporting should be enabled and reviewed periodically

User Management and Roles

- ☒ Roles will be transient in nature and changed per project or test process
- ☒ Roles will be created by the Instance Set Owner
- ☒ Responsibility for the Instances set will lie with the Instance Set Owner

Audit

- ☒ Audit will be enabled and provenance provided by Azure Logging

pknw1 Implementation Stages and Templates

- ☒ No Naming conventions or pknw1 associations should be on this subscription

Impact Assessment

Positive Risk Impact

- ☒ Services can be built and tested without affecting the business in any way
- ☒ Best practice and design can be tried and fail with zero business impact

Negative Risk Impact

- ☐ failure to audit users could allow assets to be used for non sanctioned use

Data Control & Flows